Libro de Actas

Actas del VII Congreso Iberoamericano de Seguridad Informática
CIBSI 2013
Panamá, República de Panamá, 29 al 31 de Octubre del 2013

Compiladores

Giovana Garrido
Jorge Ramió Aguirre
Gaspar Modelo Howard
Arturo Ribagorda Garnacho

ISBN: 978-9962-676-43-0

Facultad de Ingeniería de Sistemas Computacionales
Universidad Tecnológica de Panamá
Panamá, República de Panamá

Avales Académicos

Patrocinadores

Comité del Programa

Modelo Howard Gaspar (Chair)	Universidad Tecnológica de Panamá, Panamá
Arturo Ribagorda Garnacho (Chair)	Universidad Carlos III de Madrid, España
Jorge Ramió Aguirre	Universidad Politécnica de Madrid, España
Giovana Garrido	Universidad Tecnológica de Panamá, Panamá
Santiago Acurio	Pontificia Universidad Católica del Ecuador, Ecuador
Nicolás Antezana Abarca	Sociedad Peruana de Computación, Perú
Javier Areitio Bertolín	Universidad de Deusto, España
Waltea Baluja	Ciudad Universitaria Juan Antonio Echeverría, Cuba
Gustavo Betarte	Universidad de la República, Uruguay
Carlos Blanco	Universidad Cantabria, España
Jorge Blasco Alis	Universidad Carlos III de Madrid, España
Joan Borrell Viader	Universidad Autónoma de Barcelona, España
Pino Caballero Gil	Universidad de La Laguna, España
José Jeimy Cano	Universidad Pontificia Bolivariana, Colombia
Mauro Adriano Cansian	Universidade Estadual Paulista, Brasil
Eduardo Carozo	Universidad de Montevideo, Uruguay
Enrique Daltabuit Godas	Universidad Nacional Autónoma de México, México
José María De Fuentes	Universidad Carlos III de Madrid, España
Ángel Martín Del Rey	Universidad de Salamanca, España
Josep Domingo Ferrer	Universidad Rovera i Virgili, España
Josep Lluis Ferrer Gomilla	Universidad de las Islas Baleares, España
Angélica Flórez Abril	Universidad Pontificia Bolivariana, Colombia
Amparo Fúster	Consejo Superior de Investigaciones Científicas, España
David García	Universidad de Castilla-La Mancha, España
Luis Javier García	Universidad Complutense de Madrid, España

Comité Organizador

Nicolás Samaniego	Universidad Tecnológica de Panamá, Panamá
Jorge Ramió Aguirre	Universidad Politécnica de Madrid, España
Giovana Garrido	Universidad Tecnológica de Panamá, Panamá
Crispina Ramos	Universidad Tecnológica de Panamá, Panamá
Amarilis Alvarado	Universidad Tecnológica de Panamá, Panamá
Isabel Leguías	Universidad Tecnológica de Panamá, Panamá

INDICE

PONENCIAS CIBSI

PONENCIAS TIBETS

PRESENTACIÓN

El VII Congreso Iberoamericano de Seguridad Informática CIBSI 2013, tuvo lugar del 29 al 31 de Octubre de 2013 en la ciudad de Panamá, siendo organizado por la Facultad de Ingeniería de Sistemas Computacionales de la Universidad de Tecnológica de Panamá y la Universidad Politécnica de Madrid, España, a través de la Red Temática de Criptografía y Seguridad de la Información Criptored.

Las jornadas se desarrollaron en el Auditorio de la Universidad Tecnológica de Panamá y en el Salón de Conferencias del Edificio de Postgrado.

El evento está pensado desde la perspectiva de compartir experiencias a nivel de investigación en tecnologías de la seguridad informática, imprescindible actualmente para el desarrollo del conocimiento humano y del estado de bienestar de la sociedad. De esta manera, el propósito de CIBSI es promover y desarrollar el área de la seguridad de la Información, creando para ello un espacio tecnológico que facilite el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación, el desarrollo y la innovación tecnológica.

Así mismo, se llevó a cabo el II Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS. Desarrollado como un espacio propio dentro del congreso CIBSI, su objetivo es la presentación de experiencias en la enseñanza y formación en seguridad de la información, innovación educativa en dichas áreas, nuevas propuestas docentes y análisis de proyectos de colaboración académica y de programas de postgrados, de forma que fomente el planteamiento de posibilidades reales de colaboraciones docentes entre países.

A partir de los objetivos antes mencionados, la participación giró en torno a los siguientes ejes temáticos: Fundamentos de la seguridad de la información; Sistemas de gestión de seguridad de la información; Riesgos, recuperación y continuidad del negocio; Normativas y legislación en seguridad; Algoritmos y protocolos criptográficos; Vulnerabilidades y criptoanálisis; Técnicas de control de acceso e identificación; Técnicas de intrusión y análisis forense; Infraestructuras de clave pública; Seguridad en redes; Hacking; Ciberdelitos.

En estas actas se recogen 20 trabajos enviados para el congreso CIBSI y 8 para el taller TIBETS, seleccionados por un Comité de Programa compuesto por 43 especialistas de una docena de países Iberoamericanos. No se incluyen, sin embargo, la conferencia magistral inaugural de CIBSI 2013 "Capacidades Esenciales para una Ciberdefensa Nacional" del Dr. Jorge López Hernández-Ardieta, la charla invitada "Confiabilidad de Cumplimiento de Tiempos de Recuperación en Continuidad de Negocios" del Dr. Julio Escobar, y la conferencia magistral inaugural de TIBETS 2013 "Presentación del Proyecto MESI: Mapa de Enseñanza de la Seguridad de la Información" del Dr. Jorge Ramió Aguirre.

Giovana Garrido, Jorge Ramió Aguirre, Gaspar Modelo Howard,

Arturo Ribagorda Garnacho

HC+: Desarrollo de un marco metodológico para la mejora de la calidad y la seguridad en los procesos de los Sistemas de Información en ambientes sanitarios

L. E. Sánchez, I. Caballero, A. Santos-Olmo, E. Fernandez-Medina, M. Piattini

Abstract— **In some sectors, where common business processes are run, quality and security of data play a paramount role. In order to better estimate if levels of quality and security of data are properly achieved, some process-focused methodological artifacts are required. Given the very nature of each sector, such artifacts should be conveniently adapted and parameterized to the specific problems. We are especially interested in Health Management, one critical sector in which there exist a lot of complexities. For instance, in Spain, hospitals located at the same region, they do use different data structure to manage users' patient within different software applications for similar processes. To the best of our knowledge, there do not still exist such kind of artifacts that hospital managers could use to identify which processes are malfunctioning due to inadequate levels of quality and/or security in the data they use. In this paper, we present a framework that allow Health organizations to identify sources of malfunctioning of their more critical process in order to provide feasible plans to fix common errors. The framework named HC+ consists of an information model and a PDCA-based methodology.**

Keywords— **Health Management Information System, Quality health information, Security health information, Software Engineering, Security, Quality, HIS, Personal Health Record (PHR), electronic healthcare records (EHR)**

I. INTRODUCCIÓN

Desde la aparición de los sistemas de información en los entornos sanitarios, tanto su seguridad como la calidad de los datos se ha considerado como un problema crítico al gestionar datos que contienen información muy sensible [1], que debe tener las adecuadas medidas de protección. Diversos estudios demuestran la importancia de la calidad y seguridad de los datos sanitarios [2-5]. Además, la información sanitaria tiene que ser fácilmente accesible, máxime cuando actualmente los ciudadanos se mueven en pocas horas entre diferentes ciudades e incluso países pudiendo requerir asistencia clínica en un mismo año en diversos sistemas sanitarios.

Sin embargo, la tendencia actual es que cada región cree su propio Sistema de Información Sanitaria (HIS), desarrollado por tanto para grupos de población relativamente pequeños, e incluso utilizando diferentes estándares de información sanitaria y tecnologías. Esto provoca importantes problemas de interoperabilidad entre diferentes HIS, que a su vez redundan en grandes problemas relativos a la gestión de la seguridad y calidad de los datos que estos sistemas gestionan. De esta forma, en el caso de la sanidad española, regiones separadas por pocos minutos cuentan con sistemas de información sanitarios completamente diferentes, y en muchos casos son incapaces de compartir los historiales clínicos de los pacientes, lo que genera una serie de problemas con graves consecuencias como duplicidades en pruebas, retrasos en diagnósticos, etc. En este sentido, existen estudios muy completos que demuestran que esta implantación de HIS independientes ha creado muchos problemas a la hora de compartir información, a lo que se suma el problema de que cada HIS se encuentre en una fase de evolución diferente [6]. Dentro de estos estudios destaca el de Mäenpää [7], asegurando que uno de los grandes problemas para unificar los procesos de los HIS era la diferencia en la cultura de la organización y la visión del sector.

De hecho, diversos estudios han detectado la problemática sobre que la interoperabilidad semántica entre diferentes sistemas de información sanitaria es uno de los principales retos para mejorar la calidad de datos de los servicios clínicos y la seguridad de los pacientes [8, 9], y que es un reto que se debe afrontar, ya que la falta de calidad y seguridad en los datos de los pacientes no sólo supone elevadas pérdidas económicas, sino que además puede costar vidas humanas. La propia Comisión Europea [10] dictaminaba recientemente la importancia que tiene el poder compartir información entre diferentes entidades sanitarias para poder aportar mejoras en la calidad y la seguridad de la atención a los pacientes, así como para poder realizar mejoras en la salud pública.

Dada la importancia del problema, en los últimos años muchas investigaciones han intentado aportar soluciones basadas en estándares específicos que satisfacían los requerimientos de un escenario determinado, pero que tenían el problema de no poder adaptarse a otros escenarios, lo que solucionaba el problema sólo de forma parcial. Para poder realizar este intercambio de información entre HIS se han desarrollado estándares internacionales como HL7-4 [11], openEHR [12, 13], la ISO13606 [14-18], la ISO22220 [19], la ISO14265 [20], la ISO727953 [20] y otras muchas. La mayor parte de estas normas son de reciente creación, lo que demuestra que la problemática de los HIS (Health Information Systems) y los EHR (Electronic Health Records) en el sector sanitario están de plena actualidad, y se sigue trabajando activamente para encontrar una solución.

Sin embargo, la heterogeneidad de los diferentes sistemas

L. E. Sánchez, PROMETEO, Escuela Politécnica del Ejército extensión Latacunga (ESPEL), Latacunga (Cotopaxi), Ecuador, luisenrique@sanchezcrespo.org

I. Caballero, Grupo de Investigación Alarcos, Universidad de Castilla-la Mancha, Ciudad Real, España, Ismael.Caballero@uclm.es

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

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

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

sanitarios hacen que muchas veces estos estándares no se apliquen de forma adecuada, y en el caso de que lo hagan aparece un nuevo problema: ¿Cómo podemos medir la calidad y la seguridad con la que estos datos han pasado a formar parte del nuevo HIS? Actualmente no existe ningún mecanismo sencillo para dar respuesta a esta pregunta; más bien se trata de ir analizando cada uno de los diferentes aspectos y procesos que forman parte del HIS y, después de un trabajo muy laborioso que puede durar años, determinar la calidad y seguridad que tienen los datos que conforman dichos procesos. Esto hace que la labor necesaria para mantener la calidad y la seguridad de los datos en un sector como el sanitario sea muy compleja.

De esta forma, si no podemos medir ni controlar la calidad y seguridad de los datos sanitarios, el nivel de riesgo asumido es demasiado elevado como para no intentar encontrar una solución a este problema.

Por lo tanto, y una vez identificado un problema que la comunidad científica considera crítico y que sigue sin resolverse, creemos necesario afrontar la creación de una metodología y una herramienta que la soporte, y que permita que los hospitales puedan tener un mecanismo para identificar y medir el nivel de calidad y seguridad de sus datos, y en caso de que los resultados obtenidos no sean los esperados, poder determinar qué procesos del sistema de información están fallando. Además, la metodología que estamos desarrollando busca cumplir con otros tres objetivos: i) Que sea una metodología basada en estándares que puedan aplicarse en todos los hospitales, con independencia de la implementación de su HIS; ii) Que sea una metodología fácil de aplicar y con un coste bajo que permita la detección temprana de los problemas; iii) Que englobe tanto los datos y procesos clínicos (orientados a dar soporte y analizar la historia clínica de los pacientes) como de gestión (orientados a garantizar la calidad de la asistencia y el correcto flujo de la información) del HIS.

En resumen, podemos concluir que nuestra propuesta consiste en el desarrollo de una metodología que permita mejorar los procesos relacionados con los entornos sanitarios, en especial en hospitales, mediante un mejor control de la seguridad y la calidad de los datos contenidos en los sistemas de información de dichos hospitales.

En la segunda parte del artículo analizaremos algunos de los principales estándares relacionados con el entorno sanitario que nos pueden ayudar a desarrollar nuestra metodología. La tercera parte del artículo presenta los diferentes elementos que componen la metodología planteada. Finalmente la cuarta parte presenta las principales conclusiones extraídas y el trabajo futuro.

II. TRABAJO RELACIONADO

Actualmente se están desarrollando a nivel internacional un conjunto de investigaciones y estándares que intentan solucionar aspectos tan complicados como el tratamiento adecuado de la información relacionada con ambientes sanitarios. El problema principal de estos estándares e investigaciones es que están afrontando la problemática centrándose en aspectos específicos de la problemática y no abordan la misma desde un punto de vista global, ni tienen en cuenta aspectos que para nosotros son críticos como la capacidad de poder medir la calidad y la seguridad de los datos involucrados en los procesos sanitarios.

El objetivo de esta sección es identificar aquellos trabajos, investigaciones y estándares que nos permitan obtener un modelo metodológico basado en normas internacionales, que actualmente se están utilizando en los ambientes sanitarios. El objetivo perseguido con este estudio es proporcionar directrices sobre la forma de afrontar ciertos problemas conocidos y de identificar aquellos que son desconocidos. Aunque el conjunto de normas que hemos identificado en este trabajo contiene algunas normas que tratan específicamente cuestiones de calidad y seguridad de datos, estas dimensiones, en muchas ocasiones, no están directamente relacionadas con los conceptos de mejora de procesos en ambientes sanitarios.

Los problemas de calidad y seguridad asociados a los datos de salud pueden tener un importante efecto negativo en la calidad de los resultados a la hora de su utilización para determinar mejoras en los procesos, detección enfermedades, etc [21]. El conocimiento de los expertos sobre la recopilación de datos, procesamiento y análisis se debe tener en cuenta cuando se utilizan y analizan datos de salud. El proceso de la asistencia sanitaria, y el consiguiente registro de los datos en los registros electrónicos de salud, debe entenderse adecuadamente con el fin de analizar correctamente los datos y evitar interpretaciones erróneas. Algunas de las normas de TIC existentes podrían ayudar a proporcionar directrices, con el fin de garantizar de alguna manera que los niveles de seguridad y calidad son adecuados y apropiados para los datos. Sin embargo, este trabajo todavía no se ha llevado a cabo. Dado el gran número de normas existentes o en desarrollado, hemos decidimos analizarlas y agruparlas en conjuntos de acuerdo a su naturaleza.

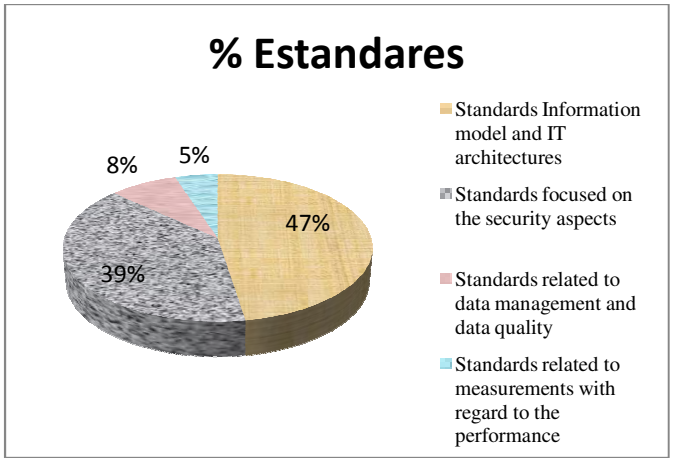

Figura 1. Conjunto de estándares considerados en el desarrollo de HC+

En una primera aproximación, hemos identificado los siguientes conjuntos (véase la figura 1):

- En un primer grupo se incluyen los estándares que se utilizan para generar el modelo de información y la arquitectura del framework que apoyará a los sistemas

de información sanitaria, ya que proporcionan los conceptos más relevantes relacionados con los ambientes sanitarios. Estos representan el 47% de las normas a tener en cuenta.

- Las normas que se incluirán en un segundo grupo son aquellos que se centran en los aspectos de seguridad de los datos y de los sistemas de información. Estas representan el 39% de las normas a tener en cuenta.
- En un tercer grupo se incluyen cuestiones relacionadas con la gestión y la calidad de los datos. Esto representa el 8% de las normas a tener en cuenta.
- Por último, el objetivo de la cuarta serie de normas será abordar cómo definir las mediciones con respecto al rendimiento de los Sistemas de Información. Esto representa el 5% de las normas a tener en cuenta.

A continuación analizaremos de forma más detallada cada uno de los grupos mencionados y las normas en que nos basaremos para desarrollar la metodología.

El primer grupo, se puede dividir en dos partes: por un lado el intentar definir un lenguaje común para todos los datos y aspectos relacionados con los ambientes sanitarios. En este grupo podemos destacar:

- HL7 CDA R2 [22, 23]: Su objetivo es crear un lenguaje común para el intercambio de datos relacionados con enfermedades, efectos secundarios de medicamentos, etc. Relacionada con esta norma, podemos destacar también la ISO/HL7 10781:2009 [24] que describe el contenido y la forma de funcionamiento de HL7 y que actualmente está siendo revisada y será sustituida por la norma ISO/LH7 CD10781 [25]. Finalmente y dentro de la familia de estándar HL7 están desarrollándose normativas especificas como la ISO 13449 [26].
- ICD-9-CM [27]: Es el sistema oficial de asignación de códigos a los diagnósticos y los procedimientos asociados con la utilización de los hospitales en los Estados Unidos.
- ISO 13606 [15, 17]: Especifica la comunicación de una parte o la totalidad de la historia clínica electrónica (EHR) de un paciente entre las diferentes partes del HIS. La ISO 13606-3:2009 se ocupa de definir la lista de términos que podrá utilizar la ISO 13606-1:2008.
- ISO 1828 [28]: Es un estándar que está actualmente en desarrollo y que pretende establecer las categorías y el sistema de codificación para la clasificación de los procedimientos quirúrgicos.
- ISO 11073-10101:2004 [29]: Proporciona la sintaxis y la semántica de los términos que deben manejarse en los puntos de atención al paciente y la comunicación de los dispositivos médicos.
- ISO 11073-10201:2004 [30]: Se ocupa de la definición y estructuración de la información que se intercambia en los entornos sanitarios.
- ISO 11073-10404:2010 [31]: Define la normativa que regirá la comunicación entre dispositivos de telesalud y otros dispositivos móviles, para garantizar la interoperabilidad entre dispositivos. Se centra en los dispositivos de control de oxigeno.
- ISO 11073-10407:2010 [32]: Define la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos de control de presión.
- ISO 11073-10408:2010 [33]: Define la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos de control de temperatura.
- ISO 11073-10415:2010 [34]: Define la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos de control peso.
- ISO 11073-10417:2010 [35]: Define la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos de control de azucar.
- ISO 11073-10420:2012 [36]: Se encuentra en desarrollo, y definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos que controlaran diferentes aspectos del cuerpo humano.
- ISO 11073-10421:2012 [37]: Se encuentra en desarrollo, y definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos que controlaran diferentes aspectos de los dispositivos para respiración artificial.
- ISO 11073-10471:2010 [38]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos de Independant living activity hub.
- ISO 11073-10472:2012 [39]: Se encuentra en desarrollo, y definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los dispositivos de monitores de medicación.
- ISO 11073-20101:2004 [40]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en dispositivos estándar.
- ISO 11073-20601:2010 [41]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los protocolos de optimización.
- ISO 11073-30200:2004 [42]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los cables de conexión.
- ISO 11073-30300:2004 [43] : Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en las redes inalámbricas.
- ISO 11073-30400:2012 [44]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en la red Ethernet.
- ISO 11073-90101:2008 [45]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los point-of-care test.
- ISO 11073-91064:2009 [46]: Definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en los Computer-assisted electrocardiography.
- ISO 11073-92001:2012 [47, 48]: Se encuentra en

desarrollo, y definirá la normativa que rige el intercambio de información entre dispositivos, pero centrada en las reglas de codificación.

- Existe otro grupo de estándares, algunos de los cuales están actualmente en desarrollo y que se ocuparan de la identificación de productos médicos: ISO 11238 [49], ISO 11239 [50], ISO 11240 [51], ISO 11615 [52], ISO 11616 [53]
- Otra norma que será útil para definición de la Ontología y que se encuentra actualmente en desarrollo es la ISO 12300 [54] que se ocupara de establecer un mapa entre la terminología, definiendo las relaciones existentes.
- Existen otras normas que se revisarán ya que pueden aportar conceptos a la Ontología: ISO 12309 [55], ISO 13119 [56], ISO 13120 [57], [58], ISO 13940 [59],

La segunda parte del primer grupo busca entender los Sistemas de Información Hospitalarios a partir de la identificación de los procesos involucrados y la creación de las arquitecturas necesarias. Dentro de este grupo podemos destacar:

- ISO 13606 [16, 18]: La ISO 13606-2:2008 especifica la arquitectura de la información necesaria para las comunicaciones entre los sistemas y servicios que necesitan o proporcionar datos de EHM. Y la ISO 13606-5:2010 define un conjunto de interface para interconectar el resto de normativas y la metodología.
- ISO 12967 [60-62]: Es un estándar que define la arquitectura para el desarrollo y la integración de nuevos sistemas, en especial en la integración de los datos.

Un segundo grupo busca cubrir aspectos tan importantes como la seguridad del sistema de información y de los propios datos. Dentro de este grupo podemos destacar:

- ISO 13606 [14]: La ISO 13606-4:2008 define la metodología que seguirá para la concesión de los privilegios que permitirán acceder a los EHM.
- ISO/TS 14265 [20]: Define un conjunto de categorías de alto nivel de los propósitos para los cuales se puede obtener información personal en entornos sanitarios. Se centra en aspectos de clasificación de información y está orientada a mantener la Confidencialidad de los datos que es uno de los principales criterios de riesgo de la seguridad.
- ISO/IEC27799 [63]: Es parte de la familia de estándares ISO/IEC 27000 [64]. Pero está centrando en controles específicos de ambientes sanitarios, y se puede complementar con la ISO/IEC 27002 [65].
- ISO/CD TS 21298 [66]: Se ocupa de definir todos los roles de las personas involucradas dentro del sector sanitario.
- ISO/TS 21091:2005 [67]: Contiene el directorio de servicios para la seguridad, comunicación e identificación de profesionales y pacientes.
- ISO 11633 [68, 69]: Estándar para la gestión de seguridad de la información centrada en el mantenimiento remoto de los dispositivos médicos y sistemas de información médica.
- ISO 14441 [70]: Estándar en desarrollo orientado a definir los requisitos de seguridad y privacidad para las pruebas de conformidad de los sistemas de EHR.
- ISO 17791 [71]: Es una guía en desarrollo que describirá las normas para la Habilitación de Seguridad en el software de Sanidad.
- ISO 21547 [72] e ISO 21548 [73]: Define los requisitos de seguridad para los EHR.
- HIPAA [74]: Es una norma de obligado cumplimiento en el sector sanitario de EEUU y está orientada a mantener el criterio de riesgo de Privacidad de datos sanitarios.
- ISO 22857 [75, 76]: Define las directrices sobre la protección de datos para facilitar los flujos internacionales de datos personales de relacionados con la salud.
- ISO 25238 [77]: Guía de clasificación de riesgos asociados con el software en ambientes sanitarios.
- IEC 80001 [78-81]: Define como realizar la aplicación y gestión de los riesgos asociados a los sistemas de información sanitarios.
- ISO 22600 [82-84]: Guía para la gestión de privilegios y control de accesos en ambientes sanitarios.
- ASTM E1762-95 [85, 86]: Guía estándar para la autenticación electrónica de la información médica.
- ASTM E1986-98 [87]: Guía para la gestión de los privilegios de acceso a la información sanitaria.
- ASTM E1869-04 [88]: Guía estándar para la confidencialidad, privacidad, acceso, y los Principios de Seguridad de Datos de Información de Salud incluyendo los registros electrónicos de salud.
- ASTM E1988-98 [89]: Guía estándar para la formación de las personas que tienen acceso a la información de la Salud.
- ASTM E2147-01 [90]: Estándar para la realización de las auditorias y logs de control en Sistemas de Información de Salud.
- ISO/TS 17090 [91-93]: Es el estándar que define la infraestructura de PKY que debe tener los hospitales para mantener segura la información.

Un tercer grupo se encarga de cubrir aspectos relacionados con la calidad de los datos, con el objetivo de minimizar el número de errores en el tratamiento y gestión de los mismos. Dentro de este grupo podemos destacar:

- ISO/TS 22220 [19]: Indica los elementos de datos y estructuras adecuadas para la identificación precisa de las personas y los datos de salud relacionados con ellas, proporcionando directrices para mejorar la identificación positiva de las personas en entornos sanitarios.
- ISO 13131 [94]: Es un estándar en desarrollo que se ocupara de definir los criterios de calidad para los

servicios y sistemas de telemedicina.

- HL7 13972 [95, 96]: Es un estándar en desarrollo que se ocupara de mantener la calidad de los procesos sanitarios.
- ISO 16279 [97]: Es un estándar en desarrollo que se ocupara de generar información de alertas para registros sanitarios.
- AHRQ (Agency for Healthcare Research and Quality): La Agencia para la Investigación y Calidad (AHRQ) ha desarrollado un conjunto de herramientas para la mejora de la calidad y la toma de decisiones en ambientes sanitarios.

Finalmente el cuarto grupo se encarga de establecer mecanismos de medición de todos los aspectos relacionados con los datos. Entre estos podemos destacar:

- ISO 27809 [98]: Medidas para garantizar la seguridad de los pacientes en el software sanitario.
- IQIP (International Quality Indicator Project): El objetivo del proyecto es ayudar a las organizaciones sanitarias a identificar los indicios que permitan la mejora de la atención sanitaria a los pacientes, ofreciendo un detallado conjunto de indicadores que puede aplicarse en sanidad.
- Metodología propuesta por Freitas et al [31]
- Marco de referencia de IQMF [32]

Estas normas se utilizan para proporcionar soluciones a los problemas técnicos y de gestión más importantes. Para hacer frente a estos problemas, es necesario tener en cuenta que en los ambientes sanitarios existen muchas fuentes de datos diferentes, tanto administrativos como de salud. Por eso es necesario extraer los datos de estas fuentes de datos que son necesarios para el cálculo de los indicadores de medida, incluidos los datos administrativos (por ejemplo, los datos de facturación), los datos de los historiales médicos electrónicos, los datos derivados de los pacientes (cuestionarios), informes y observaciones directas, etc. Cuanto más alto sea el nivel de calidad de los datos, más reales y fiables serán los resultados obtenidos de estos indicadores. Sin embargo, existen problemas en la calidad de datos [99-102] que hacen que muchas veces no puedan ser utilizados. Estos datos contienen información de las altas, se utilizan para facturar y pagar los servicios hospitalarios, tienen un formato estándar (Ej: HL7), y se puede utilizar para muchos otros fines, como la investigación o la presentación de informes públicos [103]. Los datos administrativos son un recurso importante para la adecuada gestión de los hospitales. Por lo general contienen datos demográficos (edad, sexo), "datos administrativos" (duración de la estancia, tipo de ingreso, pagador, etc) y o el uso del estándar ICD-9-CM para la codificación de datos clínicos (diagnóstico, los procedimientos, las causas externas) [104].

Como hemos visto del análisis realizado, se están creando actualmente muchas nuevas normas que pretenden acometer parte de la problemática, pero no existe ninguna metodología global que permita medir la calidad y seguridad de los datos sanitarios de forma global, por lo que es necesario acometer el proyecto que hemos planteado.

III. HC+: Marco Metodológico

El objetivo de nuestra investigación es desarrollar un marco que permita mejorar el rendimiento de los procesos relacionados con los sistemas de información sanitario por medio de la mejora de la calidad y la seguridad de los datos.

Actualmente, las organizaciones sanitarias no controlan adecuadamente sus procesos de negocio debido principalmente a la gran cantidad de procesos que se ejecutan de forma simultánea. Además, las dependencias de datos entre diferentes procesos hacen aún más difíciles de seguir algunos de los problemas de sensibilización.

Para hacer más fácil la evaluación y la mejora de los procesos de negocio en las organizaciones de salud, hemos planteado la necesidad de crear un marco integral que aborde los problemas especificados anteriormente. Estamos especialmente interesados en los problemas relacionados con la calidad y la seguridad de datos, ya que se ha demostrado que son el origen de la mayoría de los problemas.

A continuación introduciremos las diferentes partes que conforman el marco metodológico que proponemos (ver Figura 2).

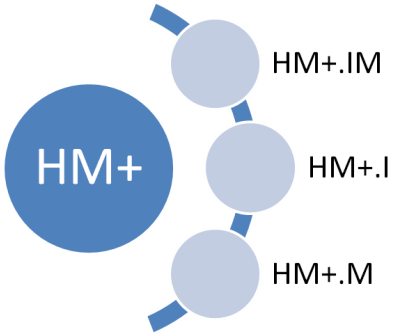

Figura 2. Fases de la metodología.

A. *El modelo de información HM+.IM*

La primera parte de framework que proponemos para mejorar la calidad y seguridad de los procesos en ambientes sanitarios contendrá un modelo de información que recogerá todos los conceptos relacionados con la metodología que se pretende desarrollar.

Este modelo de información será desarrollado para reunir conceptos a partir de los siguientes dominios: salud, seguridad, calidad de los datos y métricas (ver Figura 3):

Figura 3. Dimensiones de la Ontología sobre la que se construirá la metodología.

- *Conceptos relacionados con el campo de la sanidad (HC):* Para generar un modelo de información que cubra el espectro más amplio posible, vamos a comenzar por la realización de una revisión sistemática exhaustiva de la literatura científica relacionada con estándares para sistemas de información en ambientes sanitarios (Ej: HL7, ICD-9-CM, ...).
- *Conceptos relacionados con el campo de la seguridad (S):* Con el fin de ser capaces de describir los conceptos de seguridad, es necesario añadir y adaptar adecuadamente los conceptos proporcionados por los estándares de seguridad para entornos de salud [105]. Estos marcos de conocimiento se componen principalmente de ciertos estándares internacionales relacionados con la gestión de la seguridad, tales como los descritos anteriormente en la sección dos (Ej: ISO 27000, ISO 27799, ...).
- *Conceptos relacionados con el campo de la calidad de datos (DQ):* Como ocurrió con la seguridad, los conceptos de datos y la calidad de la información serán redefinidos para su uso en el entorno de la Salud. También nos ocuparemos de los conceptos que se están introduciendo en los nuevos estándares de calidad de datos que actualmente están en desarrollo. Los sistemas para la medición de la calidad de los datos presentados en [106] podrían ser muy útiles en la realización de esta tarea.
- *Conceptos de indicadores de desempeño (PI):* Los indicadores de rendimiento, también llamados indicadores de calidad e indicadores de gestión, son por lo general las medidas cuantitativas para una característica particular de una institución y se puede utilizar para detectar, comparar y evaluar la calidad de un servicio [107]. Los indicadores pueden ser utilizados para describir las piezas de la organización (por ejemplo, recursos materiales, recursos humanos, estructura organizativa), la capacidad de los procesos (por ejemplo, la proporción de pacientes tratados de acuerdo a las guías clínicas) o el resultado de la atención de la salud (por ejemplo, la mortalidad, morbilidad, calidad de vida) [108]. Por lo tanto el establecimiento de un conjunto básico de indicadores, puede dar una respuesta a la demanda de transparencia y eficiencia en la gestión sanitaria. Este conjunto de conceptos se completará con otros relacionados, con el fin de describir los indicadores de rendimiento para la calidad y seguridad, como los generados en el proyecto IQIP (International Quality Indicator Project) [109].

El conjunto resultante de analizar estos dominios sobre un campo como es la sanidad, dará lugar a una Ontología común que podamos aplicar sobre la metodología que estamos desarrollando para mejorar los procesos en ambientes sanitarios.

B. El modelo de información HM+.I

La segunda etapa para el desarrollo de nuestro framework se centrará en el estudio y desarrollo de un conjunto de indicadores, reglas de negocio y métricas vinculadas a los procesos de negocio de los hospitales. Los indicadores de desempeño deben ser identificados mediante entrevistas (con los interesados y profesionales de la salud) y mediante la revisión de la literatura [110]. A continuación, deben clasificarse y seleccionarse de acuerdo a la disponibilidad de los datos y la facilidad de aplicación, entre otros criterios (validez, fiabilidad, sensibilidad, especificidad, simplicidad y aplicabilidad). El objetivo de esta fase es facilitar que pueda determinarse de forma semiautomática la calidad de los datos y qué procesos están fallando a la hora de gestionar estos datos.

El objetivo último perseguido en esta fase es ser capaces de localizar y desarrollar indicadores que nos permitan identificar valores dentro de los procesos sanitarios en los que podamos optimizar la calidad y seguridad de los datos, además de poder delimitar los rangos de valores que podrían ser aceptables para cada indicador en situaciones similares. Esto permitiría a las diferentes organizaciones de salud establecer comparaciones en la calidad de los procesos que cada una tienen implementados. Es importante tener en cuenta que los límites de los valores aceptables se fijan en términos de riesgo asumido que un determinado tipo de organización puede ser capaz de pagar ante una incidencia por el incumplimiento de calidad en los datos. Sería deseable obtener mecanismos que permitan medir los indicadores de forma automática, o semi-automáticamente.

Con respecto a los límites de la gama de valores válidos, deberían estar representados por medio de las reglas de negocio. La representación de estas reglas de negocio se define en la Metodología.

C. HC+.M: Metodología

La tercera parte del framework que estamos desarrollando contiene la metodología que se aplicará para la mejora de la calidad y la seguridad de los datos sanitarios, y por tanto de los procesos que lo contienen.

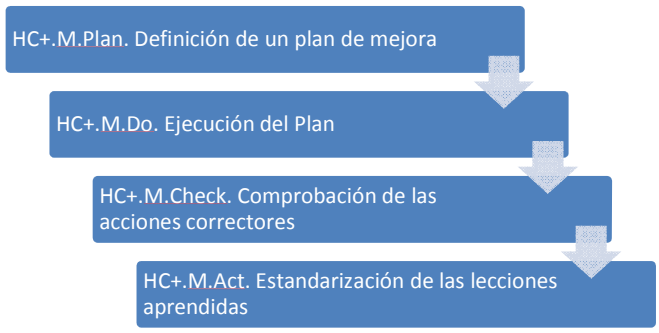

Figura 4. Fases de la metodología siguiendo el ciclo de Demming.

Para el desarrollo de esta metodología se está aplicando el ciclo de PDCA de Demming [111] basado en la mejora

continua y estará formado por cinco procesos, los cuatro que conforman el ciclo PDCA (ver Figura 4) y un proceso inicial de configuración del sistema. A continuación se describen brevemente cada uno de estos procesos:

- *HC+.0. Definición de un entorno de mejora:* Antes de iniciar el ciclo PDCA de Demming para el desarrollo de la metodología, definiremos el entorno sobre el que realizar el proceso de mejora. Este entorno deberá incluir el alcance del proceso de mejora, que partes estarán involucradas, los equipos de trabajo, etc.
- *HC+.M.Plan. Definición de un plan de mejora:* En este proceso definiremos el plan de mejora, identificando los procesos mejorables dentro del alcance definido en el proceso anterior. Una vez identificados los procesos mejorables, seleccionaremos los indicadores que mejor se adecuen para analizar el problema y desarrollaremos un plan de optimización.
- *HC+.M.Do. Ejecución del Plan:* En este proceso se realizará la ejecución del plan previsto en la fase anterior, con el objetivo de determinar si los cambios realizados en el proceso han proporcionado las mejoras previstas en el mismo.
- *HC+.M.Check. Comprobación de las acciones correctoras:* En este proceso, analizaremos si los resultados obtenidos después de la ejecución del plan han sido los esperados, y en caso contrario analizaremos las causas y emitiremos un informe de mejora.
- HC+.M.Act. *Estandarización de las lecciones aprendidas*: Finalmente, y a partir de los resultados obtenidos en los procesos anteriores, se aplican las mejoras en los procesos.

A continuación se describe con mayor detalle cada una de las etapas de la metodología:

1) HC+.M.0: Definición de un entorno de mejora:

Antes de iniciar el ciclo de PDCA de Demming, debemos definir el entorno sobre el que queremos acometer la mejora del proceso y obtener el compromiso de la alta dirección, ya que es de suma importancia para el impulso de los esfuerzos del plan. Sólo cuando se cuenta con el apoyo de la dirección se pueden abordar proyectos de mejora [112].

Este proceso estará formado por un conjunto de actividades (ver Figura 5), que pasamos a definir brevemente:

- *0.1. Creación de un equipo específico de trabajo (SDQ):* Se definirá un equipo de trabajo acorde al alcance definido en el proyecto. En el ambiente sanitario este punto es muy importante, ya que se ve involucrado un alto número de especialistas de diferentes sectores que deben aportar un conocimiento crítico para entender el proceso.
- *0.2. Creación del mapa de procesos de la organización:* Si aún no existe (por ejemplo, la organización no ha obtenido una certificación de calidad como la ISO 9001), entonces será necesario definir un mapa de los procesos más críticos, o al menos los que son susceptibles de mejora. Como parte de esta descripción hay que identificar no sólo las entradas y salidas de productos, sino también una descripción clara de las responsabilidades que tendrán los roles involucrados, además de los datos que van a utilizar para llevar a cabo sus tareas.
- *0.3. Formación de expertos en seguridad:* Los expertos en seguridad formarán al resto del equipo en los principales conceptos que se quieren llegar a implantar en el sistema para obtener la mejora prevista. De esta forma, todo el equipo será capaz de entender el objetivo perseguido. Esta formación implica cuestiones tanto de gestión como de carácter técnico. Por ejemplo, cómo diseñar e implementar los cambios realizados en el HMIS (*Health Management Information Systems*) para que las estrategias de seguridad puedan ser operativas.
- *0.4. Formación de expertos en calidad de datos:* Los expertos en calidad de datos formarán al resto del equipo en los principales conceptos de calidad que se pretenden implantar en la mejora del proceso.
- *0.5. Definición de políticas de seguridad:* Una vez que todo el equipo conoce los principios de seguridad que se quieren implantar se definirán las políticas de seguridad para el proceso a mejorar.
- *0.6. Definición de políticas de calidad de datos:* Una vez que todo el equipo conoce los principios de calidad de datos que se quieren implantar se definirán las políticas de calidad para el proceso a mejorar.

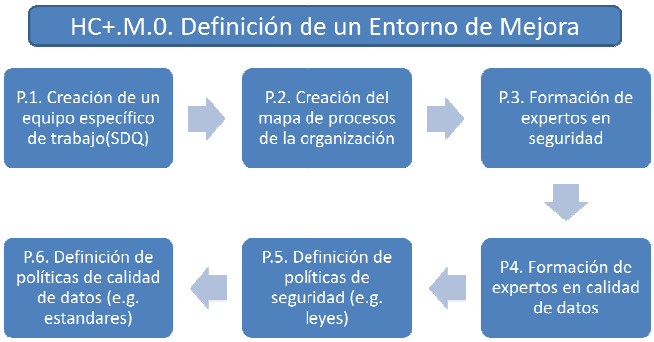

Figura 5. HC+M.O. Definición de un entorno de mejora.

2) HC+.M.Plan: Definición de un plan de mejora:

La primera fase del ciclo de mejora de la metodología, consistirá en definir un plan de mejora para el entorno definido en el proceso inicial, para lo que realizaremos una serie de actividades (ver Figura 6), que pasamos a describir brevemente:

- P.1. Identificación del Proceso "defectuoso" y sus dependencias: La primera de las actividades de este proceso consistirá en identificar el proceso principal del alcance definido que queremos mejorar y sus dependencias con otros procesos.
- P.2. Identificación de las necesidades de información: Identificamos qué fuentes de información necesitamos

consultar para analizar en detalle el proceso a mejorar. Es esta actividad necesitamos conocer el proceso en profundidad para poder entender qué está fallando en el mismo, y cómo podemos mejorarlo.

- P.3. Evaluación actual. Identificación de las medidas (indicadores) que permiten describir el problema: Todo problema debe poder ser cuantificado y debemos tener unas medidas que nos permitan identificar si estamos resolviendo el problema o no. Por ello, es necesario seleccionar del conjunto de indicadores definidos en la segunda parte del framework cuáles nos permiten medir el problema y la evolución del mismo.
- P.4. Definición de los valores deseados/requeridos: Una vez que hemos definido el proceso principal y los indicadores que utilizaremos, debemos establecer los umbrales que queremos obtener y que nos permitirán considerar que el proceso está funcionando en la forma correcta.
- P.5. Análisis de las fuentes del problema en el proceso: Analizamos los resultados que ofrecen los indicadores sobre el proceso en vivo, con el objetivo de determinar las dependencias de las variables con los diferentes indicadores de calidad y seguridad de datos definidos.
- P.6. Definición de un plan viable para optimizar el proceso: Establecemos el plan que aplicaremos durante todo el ciclo, que incluirá todos los indicadores definidos para realizar el seguimiento en la mejora del proceso.

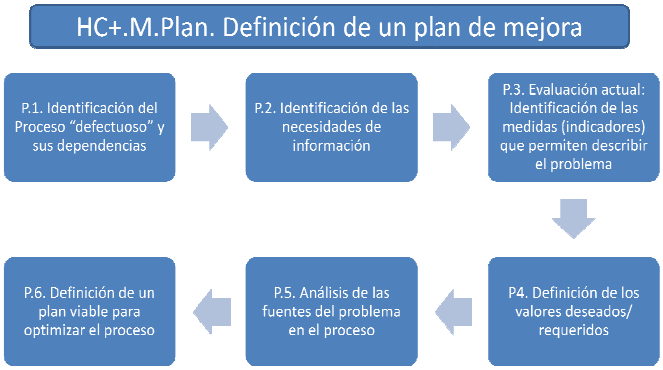

Figura 6. HC+M.Plan. Definición de un plan de mejora.

3) HC+.M.Do: Ejecución del Plan:

Una vez establecido el plan entraremos en la fase de ejecución del mismo, que estará formada por un conjunto de actividades (ver Figura 7) que pasamos a describir brevemente:

- D.1. Preparación del Entorno de ejecución del plan: Preparamos el entorno que engloba los procesos que pueden verse afectados por el plan. En muchos casos es necesario introducir trazas que nos permitan realizar el seguimiento de los procesos, para verificar su funcionamiento con respecto al plan establecido.
- D.2. Provisión de los recursos necesarios: Establecemos los recursos que necesitaremos durante la ejecución del plan, ya que éste puede suponer sobrecargas en el sistema, así como la dedicación de parte del personal involucrado en el proyecto para la toma de datos.
- D.3. Ejecución del plan: Ejecutamos el plan establecido y almacenamos toda la información relevante del mismo. Durante el proceso de ejecución se mantendrá una supervisión con el objetivo de identificar si las trazas activadas para la monitorización detallada del mismo han podido ocasionar algún cambio que afecte al correcto funcionamiento del plan que se estableció inicialmente.
- D.4. Análisis de la ejecución del plan: Finalmente, a partir de todos los datos recogidos durante la ejecución del plan, analizamos si hemos alcanzado los objetivos previstos.

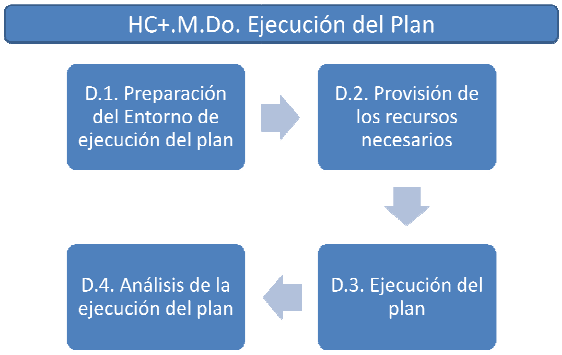

Figura 7. HC+M.Do. Ejecución del Plan.

4) HC+.M.Check: Comprobación de las acciones correctoras:

A partir de los resultados de la ejecución del plan y en el caso en que los resultados obtenidos difieran de los resultados ideales, analizaremos las causas y propondremos medidas para solucionar el problema, para lo que realizaremos una serie de actividades (ver Figura 8) que pasamos a describir brevemente:

- C.1. Evaluación de la situación tras la ejecución del plan: Analizamos en qué situación han quedado los objetivos propuestos después de la ejecución del plan. En algunos casos podemos estar cerca de conseguir los objetivos propuestos, mientras que en otros casos el proceso puede haber fallado y deberemos analizar el problema.
- C.2. Análisis de las causas de la no implementación: En caso de que no se hayan conseguido los objetivos, analizamos las causas por las que no los hemos conseguido. Para ello, investigaremos en detalle todos los resultados obtenidos.
- C.3. Creación de un informe de mejora: A partir de la investigación realizada creamos un informe en el que proponemos mejoras en el proceso que nos permitan alcanzar el objetivo deseado.

- C.4. Comunicación de los resultados: Una vez que el informe ha sido cerrado y consensuado por todo el equipo involucrado, se comunican los resultados del mismo y las acciones que se tomaran.

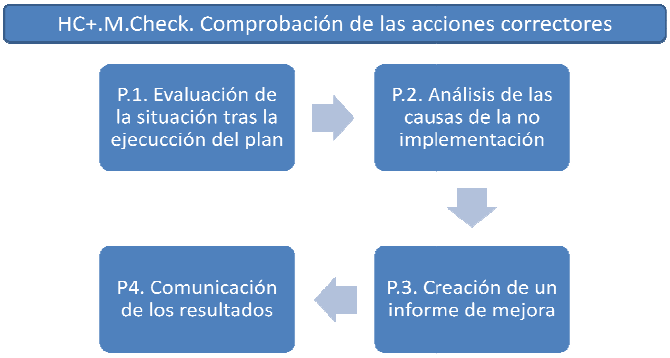

Figura 8. HC+M.Check. Comprobación de las acciones correctoras

5) HC+.M.Act: Estandarización de las lecciones aprendidas

A partir del informe de mejora obtenido en el proceso anterior iniciamos la última fase del cliclo, que consistirá en revisar el proceso y aplicar los cambios, y que estará formada por una serie de actividades (ver Figura 9) que pasamos a describir brevemente:

- *A.1. Revisión de las políticas de seguridad:* Revisamos la política de seguridad vigente actualmente sobre los datos de los procesos involucrados en el alcance, para ver qué cambios se tienen que realizar en base al plan de mejora desarrollado.
- *A.2. Revisión de políticas de calidad de datos:* Igual que en la actividad anterior, vemos qué cambios tenemos que realizar en la política de calidad de datos para adecuarla al plan de mejora.

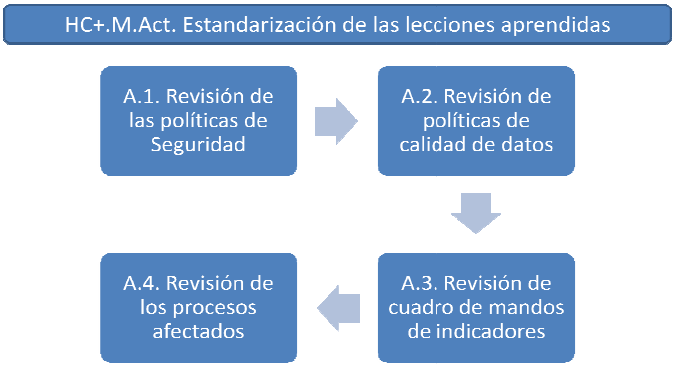

Figura 9. HC+M.Act. Estandarización de las lecciones aprendidas

- *A.3. Revisión de cuadros de mandos de indicadores:* Actualizamos, si fuera necesario, el conjunto de indicadores que hemos seleccionado. El algún caso, los cambios propuestos por el plan de mejora pueden hacer necesario incluir nuevos indicadores para medir nuevas variables.
- *A.4. Revisión de los procesos afectados:* Finalmente, revisamos los procesos afectados por todo el ciclo e iniciamos una nueva fase del ciclo desde la etapa HC+.M.Do.

IV. Conclusiones y trabajos futuros

En el presente artículo, hemos analizado algunos de los principales problemas que actualmente afectan al sector sanitario a nivel mundial, en concreto los relacionados con aspectos de calidad en los datos. Además, estos problemas están aumentando su frecuencia de aparición, debido al fenómeno de la globalización. Este nuevo paradigma global ha generado un nuevo reto como es la interoperabilidad semántica de los registros electrónicos de salud (EHR), es decir, el intercambio de los expedientes clínicos de pacientes entre diferentes sistemas de información sanitarios (HIS) y la necesidad de poder medir y controlar la calidad y seguridad de los datos que conforman los HIS.

Hemos presentando las bases de la metodología que estamos desarrollando y que está soportada por estándares internacionales tanto del sector sanitario, como de la ingeniería del software. Esta metodología pretende ser un estándar que permita a los hospitales conocer de una forma rápida y económica fallos en calidad y seguridad de los datos que conforman su HIS, así como detectar los procesos que ocasionan los fallos y dar una solución rápida a los mismos.

Actualmente, esta metodología se está aplicando en un caso de estudio, sobre uno de los procesos clásicos que todos los hospitales tienen como es "*la gestión de turnos de los pacientes*", así como las problemáticas asociadas a los procesos que conforman esos sistemas. Este caso que se presento en la anterior edición del CIBSI en el articulo denominado "*Cumplimiento de la LOPD y los requerimientos legales de la ISO27001 en la citación de pacientes en Hospitales*", demuestra la complejidad de los procesos en los hospitales y cómo se deben ir abordando uno por uno para poder entenderlos y realizar una metodología que sea útil. El caso de estudio también está sirviendo para demostrar que, hasta que no se ha realizado el estudio, la Dirección del hospital no era consciente completamente del potencial que tenía el conocimiento que se estaba perdiendo en la organización, así como lo necesario que era el poder contar con métricas para controlar la seguridad y la calidad de los datos. Desde el punto de vista de la gerencia, los mayores hallazgos obtenidos hasta el momento han sido:

- Comprobar que los informes que manejaban se basaban en información incompleta. A la vista de los problemas detectados, se ha visto la posibilidad de desarrollar nuevas métricas sobre la información que se añadirán al sistema y que serán capaces de detectar problemas de funcionamiento en consultas o con médicos concretos: Baja tasa de consultas, tiempos de espera elevados, tiempos muertos entre pacientes, etc.
- Permitir encontrar de forma muy evidente la manera de mejorar uno de los procesos más problemáticos en el hospital como era la gestión de las consultas y salas de espera. Las soluciones propuestas conllevan una mejora del proceso, un aumento de la eficiencia del personal

implicado y una mayor automatización de los elementos del proceso que hasta el momento habían sido más anárquicos y caóticos.

La investigación continuará aplicando el ciclo completo de la metodología sobre diferentes procesos sanitarios y extrayendo métricas que permitan medir la calidad y seguridad de los datos incluidos en dichos procesos. Además, se verificaran estos procesos en diferentes hospitales para garantizar que la metodología sirva para ambientes heterogéneos.

AGRADECIMIENTOS

Esta investigación es parte del proyecto PROMETEO financiado por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) del Gobierno de Ecuador, y los proyectos MEDUSAS (IDI-20090557) y ORIGIN (IDI-2010043) financiado por el CDTI y el FEDER, BUSINESS (PET2008-0136) concedido por el Ministerio Español de Ciencia y Tecnología y MARISMA (HITO-2010-28), SISTEMAS (PII2I09-0150-3135) y SERENIDAD (PII11-0327-7035) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-la Mancha.

Referencias

[1] Smith, E. and J.H.P. Eloff, *Security in health-care information systems—current trends.* International Journal of Medical Informatics, 1999. **54**(1): p. 39-54.

[2] Chiba, Y., M.A. Oguttu, and T. Nakayama, *Quantitative and qualitative verification of data quality in the childbirth registers of two rural district hospitals in Western Kenya.* Midwifery, 2011(0).

[3] Fernando, J.I. and L.L. Dawson, *The health information system security threat lifecycle: An informatics theory.* International Journal of Medical Informatics, 2009. **78**(12): p. 815-826.

[4] Michael Rigby, et al., *Verifying quality and safety in health informatics services.* BMJ, 2001. **2001 September 8**(323(7312)): p. 552-556.

[5] Winter, A., et al., *Quality of Health Information Systems. Health Information Systems*, 2011, Springer London. p. 201-236.

[6] Campillo, C., *Integration of information for health interventios: from data to information and from information to action. Report SESPAS 2008.* Gaceta Sanitaria, 2008. **22, Supplement 1**(0): p. 14-18.

[7] Mäenpää, T., et al., *The outcomes of regional healthcare information systems in health care: A review of the research literature.* International Journal of Medical Informatics, 2009. **78**(11): p. 757-771.

[8] Martínez Costa, C., M. Menárguez-Tortosa, and J. Fernández-Breis, *Clinical data interoperability based on archetype transformation.* Journal of Biomedical Informatics, 2011. **44**(5): p. 869-880.

[9] Häyrinen, K., K. Saranto, and P. Nykänen, *Definition, structure, content, use and impacts of electronic health records: A review of the research literature.* International Journal of Medical Informatics, 2008. **77**(5): p. 291-304.

[10] Reding, V., *Commission recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number (C(2008) 3282)*, O.J.E. Union, Editor 2008.

[11] HL7-4, *HL7 Standards - Section 4: EHR Profiles*, 2012: Health Level Seven International.

[12] OpenEHR-Foundation, *ADL language, Adl*, 2007.

[13] OpenEHR-specification, *OpenEHR Specification*, 2011.

[14] ISO13606-4, *ISO/TS 13606-4:2009. Health informatics -- Electronic health record communication -- Part 4: Security*, 2009.

[15] ISO13606-1, *ISO 13606-1:2008. Health informatics -- Electronic health record communication -- Part 1: Reference model*, 2008.

[16] ISO13606-2, *ISO 13606-2:2008. Health informatics -- Electronic health record communication -- Part 2: Archetype interchange specification*, 2008.

[17] ISO13606-3, *ISO 13606-3:2010. Health informatics -- Electronic health record communication -- Part 3: Reference archetypes and term lists*, 2010.

[18] ISO13606-5, *ISO 13606-5:2010. Health informatics -- Electronic health record communication -- Part 5: Interface specification.* 2010.

[19] ISO/TS22220, *ISO/TS 22220:2011. Health informatics -- Identification of subjects of health care*, 2011.

[20] ISO/TS14265, *ISO/TS 14265:2011. Health Informatics - Classification of purposes for processing personal health information*, 2011.

[21] Wang, P., *Information systems management issues in the Republic of China for the 1990s.* Information & Management, 1994. **26**(6): p. 341-352.

[22] ISO/HL727953-1, *ISO/HL7 27953-1:2011. Health informatics -- Individual case safety reports (ICSRs) in pharmacovigilance -- Part 1: Framework for adverse event reporting*, 2011.

[23] ISO/HL727953-2, *ISO/HL727953-2:2011. Health informatics -- Individual case safety reports (ICSRs) in pharmacovigilance -- Part 2: Human pharmaceutical reporting requirements for ICSR*, 2011.

[24] ISO/HL7-10781:2009, *Electronic Health Record-System Functional Model, Release 1.1*, 2009.

[25] ISO/HL7-CD10781, *Electronic Health Record-System Functional Model, Release 2.0 (EHR FM)*, 2012.

[26] ISO/HL7-DIS-13449, *Health informatics -- Clinical genomics pedigree topic*, 2011.

[27] ICD-9-CM, *International Classification of Diseases, Ninth Revision, Clinical Modification* 2011.

[28] ISO/FDIS1828, *Health informatics -- Categorial structure for classifications and coding systems of surgical procedures*, 2012.

[29] ISO/IEEE11073-10101:2004, *Health informatics -- Point-of-care medical device communication -- Part 10101: Nomenclature*, 2008.

[30] ISO/IEEE11073-10201:2004, *Health informatics -- Point-of-care medical device communication -- Part 10201: Domain information model*, 2008.

[31] ISO/IEEE11073-10404:2010, *Health informatics -- Personal health device communication -- Part 10404: Device specialization -- Pulse oximeter*, 2010.

[32] ISO/IEEE11073-10407:2010, *Health informatics -- Personal health device communication -- Part 10407: Device specialization -- Blood pressure monitor*, 2010.

[33] ISO/IEEE11073-10408:2010, *Health informatics -- Personal health device communication -- Part 10408: Device specialization -- Thermometer*, 2010.

[34] ISO/IEEE11073-10415:2010, *Health informatics -- Personal health device communication -- Part 10415: Device specialization -- Weighing scale*, 2010.

[35] ISO/IEEE11073-10417:2010, *Health informatics -- Personal health device communication -- Part 10417: Device specialization -- Glucose meter*, 2010.

[36] ISO/IEEE-FDIS-11073-10420, *Health informatics -- Personal health device communication -- Part 10420: Device specialization -- Body composition analyzer*, 2012.

[37] ISO/IEEE-FDIS-11073-10421, *Health informatics -- Personal health device communication -- Part 10421: Device specialization -- Peak expiratory flow monitor (peak flow)*, 2012.

[38] ISO/IEEE11073-10471:2010, *Health informatics -- Personal health device communication -- Part 10471: Device specialization - Independant living activity hub*, 2010.

[39] ISO/IEEE-FDIS-11073-10472, *Health Informatics -- Personal health device communication -- Part 10472: Device specialization -- Medication monitor*, 2012.

[40] ISO/IEEE11073-20101:2004, *Health informatics -- Point-of-care medical device communication -- Part 20101: Application profiles -- Base standard*, 2008.

[41] ISO/IEEE11073-20601:2010, *Health informatics -- Personal health device communication -- Part 20601: Application profile -- Optimized exchange protocol*, 2010.

[42] ISO/IEEE11073-30200:2004, *Health informatics -- Point-of-care medical device communication -- Part 30200: Transport profile -- Cable connected*, 2008.

[43] ISO/IEEE11073-30300:2004, *Health informatics -- Point-of-care medical device communication -- Part 30300: Transport profile -- Infrared wireless*, 2008.

[44] ISO/IEEE-FDIS-11073-30400, *Health informatics -- Point-of-care medical device communication -- Part 30400: Interface profile -- Cabled Ethernet*, 2012.

[45] ISO11073-90101:2008, *Health informatics -- Point-of-care medical device communication -- Part 90101: Analytical instruments -- Point-of-care test*, 2011.
[46] ISO11073-91064:2009, *Health informatics -- Standard communication protocol -- Part 91064: Computer-assisted electrocardiography*, 2009.
[47] ISO/TS11073-92001:2007, *Health informatics -- Medical waveform format -- Part 92001: Encoding rules*, 2007.
[48] 11073-92001, I.D., *Health informatics -- Medical waveform format -- Part 92001: Encoding rules*, 2012.
[49] ISO/FDIS11238, *Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated information on substances*, 2012.
[50] ISO/FDIS11239, *Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated information on pharmaceutical dose forms, units of presentation, routes of administration and packaging*, 2012.
[51] ISO/FDIS11240, *Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of units of measurement*, 2012.
[52] ISO/FDIS11615, *Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated medicinal product information*, 2012.
[53] ISO/FDIS11616, *Health informatics -- Identification of medicinal products -- Data elements and structures for the unique identification and exchange of regulated pharmaceutical product information*, 2012.
[54] ISO/DTR12300, *Health informatics - Principles of mapping between terminological systems*, 2012.
[55] ISO/TR12309:2009, *Health informatics -- Guidelines for terminology development organizations*, 2009.
[56] ISO/DIS13119, *Health informatics -- Clinical knowledge resources -- Metadata*, 2012.
[57] ISO/DIS13120, *Health informatics - Syntax to represent the content of healthcare classification systems - Classification Markup Language (ClaML)*, 2012.
[58] ISO/DTR13128, *Health Informatics -- Clinical document registry federation*, 2012.
[59] ISO/CD13940, *Health informatics -- System of concepts to support continuity of care*, 2012.
[60] ISO12967-1:2009, *Health informatics -- Service architecture -- Part 1: Enterprise viewpoint*, 2009.
[61] ISO12967-2:2009, *Health informatics -- Service architecture -- Part 2: Information viewpoint*, 2009.
[62] ISO12967-3:2009, *Health informatics -- Service architecture -- Part 3: Computational viewpoint*, 2009.
[63] ISO/IEC27799, *ISO/IEC 27799, Health informatics - Information security management in health using ISO/IEC27002.*, 2008.
[64] ISO/IEC27000, *ISO/IEC FDIS 27000, Information Technology - Security Techniques - Information security management systems.*, 2009.
[65] ISO/IEC27002, *ISO/IEC 27002:2005, the international standard Code of Practice for Information Security Management (en desarrollo).* 2007.
[66] ISO/TS21298, *ISO/TS 21298:2008. Health informatics -- Functional and structural roles*, 2008.
[67] ISO/TS21091, *ISO/TS 21091:2005. Health informatics -- Directory services for security, communications and identification of professionals and patients.* 2005.
[68] ISO/TR11633-1:2009, *Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 1: Requirements and risk analysis*, 2009.
[69] ISO/TR11633-2:2009, *Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 2: Implementation of an information security management system (ISMS)*, 2009.
[70] ISO/DTS14441, *Health Informatics: Security and privacy requirements for compliance testing of EHR systems*, 2012.
[71] ISO/AWI-TR17791, *Health informatics - Guidance on Standards for Enabling Safety in Health Software*, 2011.
[72] ISO/TS21547:2010, *Health informatics -- Security requirements for archiving of electronic health records -- Principles*, 2010.
[73] ISO/TR21548:2010, *Health informatics -- Security requirements for archiving of electronic health records -- Guidelines*, 2010.
[74] HIPAA, *Health Insurance Portability and Accountability Act, 1996: US Public Law 141-190, USC 1320d*, 1996.
[75] ISO/DIS22857, *Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health data*, 2011.
[76] ISO22857:2004, *Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information*, 2008.
[77] ISO/TS25238:2007, *Health informatics -- Classification of safety risks from health software*, 2010.
[78] IEC80001-1:2010, *Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities*, 2010.
[79] IEC/DTR80001-2-1, *Application of risk management for IT-networks incorporating medical devices -- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples*, 2012.
[80] IEC/DTR80001-2-2, *Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls*, 2012.
[81] IEC/DTR80001-2-3, *Application of risk management for IT-networks incorporating medical devices -- Part 2-3: Guidance for wireless networks*, 2012.
[82] ISO/TS22600-1:2006, *Health informatics -- Privilege management and access control -- Part 1: Overview and policy management*, 2009.
[83] ISO/TS22600-2:2006, *Health informatics -- Privilege management and access control -- Part 2: Formal models*, 2009.
[84] ISO/TS22600-3:2009, *Health informatics -- Privilege management and access control -- Part 3: Implementations*, 2009.
[85] ASTM-E1762-95, *ASTM E1762-95 Standard Guide for Electronic Authentication of Health Care Information*, 2003.
[86] ASTM-E1985-98, *ASTM E1985-98 Standard Guide for User Authentication and Authorization*, 2003.
[87] ASTM-E1986-98, *ASTM E1986-98 Standard Guide for Information Access Privileges to Health Information*, 2005.
[88] ASTM-E1869-04, *Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records*, 2010.
[89] ASTM-E1988-98, *Standard Guide for Training of Persons who have Access to Health Information (Withdrawn 2007)*, 2007.
[90] ASTM-E2147-01, *Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*, 2009.
[91] ISO/TS17090-1, *ISO/TS 17090-1:2002. Health informatics -- Public key infrastructure -- Part 1: Framework and overview.* 2002.
[92] ISO17090-2, *ISO 17090-2:2008. Health informatics -- Public key infrastructure -- Part 2: Certificate profile.* 2008.
[93] ISO17090-3, *ISO 17090-3:2008. Health informatics -- Public key infrastructure -- Part 3: Policy management of certification authority.* 2008.
[94] ISO/DTS13131, *Health Informatics -- Quality criteria for services and systems for telehealth*, 2012.
[95] ISO/HL7-CD13972-1, *Health Informatics -- Detailed Clinical Models -- Part 1: Quality processes regarding detailed clinical model development, governance, publishing and maintenance*, 2012.
[96] ISO/HL7-CD13972-2, *Health Informatics -- Detailed Clinical Models -- Part 2: Quality attributes of detailed clinical models*, 2012.
[97] ISO/NP-TS16279, *Health Informatics - Alert information in health records*, 2010.
[98] ISO/TR27809:2007, *Health informatics -- Measures for ensuring patient safety of health software*, 2007.
[99] Neubauer, T. and J. Heurix, *A methodology for the pseudonymization of medical data.* International Journal of Medical Informatics, 2011. **80**(3): p. 190-204.
[100] Posthumus, S. and R. von Solms, *A framework for the governance of information security.* Computers & Security, 2004. **23**(8): p. 638-646.
[101] Feng, N. and M. Li, *An information systems security risk assessment model under uncertain environment.* Applied Soft Computing, 2011. **11**(7): p. 4332-4340.
[102] Bagheri, E. and A.A. Ghorbani, *Astrolabe: A Collaborative Multiperspective Goal-Oriented Risk Analysis Methodology.* IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, 2009. **39**(1): p. 66-85.
[103] Committee, I.R.M., *Report of the Study Group on Risk Assessment and Management Advice (SGRAMA).* 2006.
[104] BS7799, *BS 7799: Information security management systems.* , 2002, British Standards Institute (BSI).
[105] Farn, K.-J., S.-K. Lin, and A.R.-W. Fung, *A study on information security management system evaluation--assets, threat and vulnerability.* Computer Standards & Interfaces, 2004. **26**(6): p. 501-513.
[106] Caballero, I., et al. *A Data Quality Measurement Information Model based on ISO/IEC 15939*. in *12th International Conference on Information Quality*. 2007. MIT, Cambridge, MA.

[107] Hewett, R. and R. Seker, *A Risk Assessment Model of Embedded Software Systems.* 29th Annual IEEE/NASA Software Engineering Workshop (SEW'05), 2005: p. 8.
[108] Mainz, J., *Defining and classifying clinical indicators for quality improvement.* Int J Qual Health Care, 2003. **15**(6): p. 523-530.
[109] Konus, J. and D. Minoli, *Information Technology Risk Management in Enterprise Environments.*, N.J.W. Hoboken, Editor 2010.
[110] von Solms, R., et al., *A framework for information security evaluation.* Information & Management, 1994. **26**(3): p. 143-153.
[111] Deming, W.E., *Out of Crisis*1986, Cambridge: MA: MIT Center for Advanced Engineering Study.
[112] Sarsfield, S., *The Data Governance Imperative*. First ed2009: IT Governance Publishing.

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

Ismael Caballero has an MSc and PhD in Computer Science from the Escuela Superior de Informa´tica of the Castilla-La Mancha University in Ciudad Real. He actually works as an assistant professor in the Department of Information Systems and Technologiesat the University of Castilla-La Mancha, and he has also been working in the R&D Department of Indra Sistemas since 2006. His research interests are focused on information quality management, information quality in SOA, and Global Software Development.

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

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

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