Una Aproximación basada en i* para el análisis de Requisitos de Seguridad en Almacenes de Datos

E. Soler, V. Stefanov, J. N. Mazón, J.Trujillo, E. Fernández-Medina y M. Piattini

***Resumen*— Las propuestas de análisis de requisitos para almacenes de datos (AD) se centran únicamente en las necesidades de información de los usuarios, sin tener en cuenta otro tipo de requisitos como la seguridad o el rendimiento. Sin embargo, el modelado de estos aspectos en etapas tempranas del desarrollo es fundamental para obtener un AD que satisfaga las expectativas del usuario. En este artículo, se definen dos tipos de requisitos a considerar en el diseño del AD: requisitos de información y de calidad de servicio. Estos requisitos se definen dentro del marco de MDA (*Model Driven Architecture*), lo que permite su *traceability* hacia etapas posteriores de diseño conceptual y lógico. Cabe destacar que este artículo se centra en proponer un modelo de requisitos de seguridad (como un tipo concreto de requisitos de calidad de servicio), así como un proceso en tres fases para su modelado conjuntamente con los requisitos de información.**

***Palabras clave*— Almacén de datos, seguridad, requisitos.**

I. Introducción

El objetivo de un almacén de datos AD) es facilitar el análisis del estado y el desarrollo de una organización con el fin de mejorar el proceso de toma de decisiones [1]. Para ello, el AD integra, en un modelo multidimensional (MD), enormes cantidades de datos procedentes de fuentes de datos heterogéneas. Este tipo de modelo permite obtener fácilmente información como el número de transacciones por cliente o el incremento de ventas durante una promoción. Esta información se usa para descubrir tendencias o decidir sobre futuras inversiones.

Los modelos MDs permiten el acceso a los datos de forma más natural para los analistas. Los datos se localizan en un espacio n-dimensional, con las dimensiones representando las diferentes maneras de ver y clasificar los datos (p.e. según fecha, tienda, cliente, producto, etc.). Los diseñadores de modelos MD especifican un modelo conceptual estructurando la información en hechos y dimensiones. Los hechos son medidas de un proceso de negocio (p.e. cantidad de producto vendida, número de pacientes tratados, etc.), mientras que las dimensiones representan el contexto de análisis de esas medidas.

Hoy en día el análisis de requisitos en AD se centra en el modelo de datos [2]. Como entrada para definir el modelo conceptual MD, se usa el esquema de las fuentes de datos disponibles junto con los requisitos de información del usuario con el fin de obtener un modelo conceptual MD que sea compatible con ambos [3], [4], [5]. El problema es que el producto final que se debe obtener en un proceso de diseño para ADs no es únicamente un modelo de datos sino un sistema de AD completo, donde los usuarios necesitan que la información obtenida cumpla con algunas características (seguridad, rendimiento, visualización, etc.). Estas características son restricciones que el AD debe cumplir al suministrar la información requerida para satisfacer las expectativas de los usuarios, por lo que las hemos denominado requisitos de calidad de servicio (QoS). Estos requisitos son, por tanto, características adicionales que el AD debe cumplir para añadir calidad al uso de la información suministrada por el AD. Informalmente, los requisitos de información se relacionan con qué información se espera que el AD suministre, mientras que los requisitos de QoS se relacionan con cómo la información debe ser suministrada para su correcto uso.

Los requisitos de QoS influyen en el modelo de datos y también entre ellos, por lo que deben considerarse de manera conjunta en etapas tempranas del diseño. Incluso siendo externos a los requisitos de información, los requisitos de QoS están íntimamente ligados a aquellos. Por lo tanto, existe una necesidad de tener una aproximación donde se consideren los requisitos de QoS junto con los requisitos de información, y desde etapas tempranas del desarrollo.

En este artículo, se presenta una aproximación global para el análisis de requisitos en ADs. Se describe la integración de requisitos de QoS en nuestra aproximación para el análisis de requisitos de información en ADs [6]. La inclusión de nuestra propuesta en esta aproximación, basada en MDA (*Model-Driven Architecture*), permite al diseñador [7] (i) derivar no sólo el esquema de la base de datos, sino otras partes del AD como la configuración del control de acceso y (ii) analizar de manera independiente requisitos de información y requisitos de QoS sin perder la conexión entre ambos, mediante el modelado en un CIM (*Computation Independent Model*).

Los requisitos de QoS abarcan muchos aspectos: cómo se deben presentar los datos para una correcta visualización,

Este trabajo ha sido financiado por los proyectos METASIGN (TIN2004-00779) del Ministerio de Educación y Ciencia y DADS (PBC-05-012-2) de la Consejería de Educación y Ciencia de Castilla-La Mancha. Jose-Norberto Mazón dispone de una beca FPU (AP2005-1360) del Ministerio de Educación y Ciencia de España.

cómo se debe acceder a los datos de una manera segura, cómo se debe realizar la implementación para suministrar los datos con un adecuado rendimiento, etc. Debido a esta amplia variedad de requisitos de QoS y la limitada longitud del artículo, nos centramos en un único aspecto: la seguridad. La parte IV describe en detalle cómo se definen los requisitos de seguridad y cómo se integran con los requisitos de información. Se presenta un modelo para requisitos de seguridad en ADs y un proceso en tres etapas para su especificación en un CIM mediante una aproximación basada en objetivos. Todo ello se ilustra con un ejemplo procedente del dominio farmacéutico. El trabajo relacionado se trata en la parte II, seguido de nuestra propuesta para modelar requisitos de información y de QoS (parte III). Finalmente, la parte V presenta las conclusiones y el trabajo futuro.

II. TRABAJO RELACIONADO

Hasta ahora, sólo unas pocas propuestas han considerado el análisis de requisitos como una tarea crucial a realizar en las etapas tempranas del desarrollo del AD. En [5], se propone un método para determinar los requisitos de información de los usuarios del AD y emparejar dichos requisitos con las fuentes de datos disponibles. La propuesta de [8] presenta un proceso de obtención de requisitos específico para ADs en el cual se identifican los objetivos del usuario y la información que se necesita para llevarlos a cabo. Finalmente, en [3] los autores presentan una aproximación en la que definen los requisitos del AD mediante el modelado de objetivos.

Sin embargo, estas propuestas sólo consideran requisitos de información (medidas de interés y su contexto de análisis) relacionados con el proceso de toma de decisiones. Solamente la propuesta llamada *data warehouse requirements definition* (DWARF) [9], [10] adapta el proceso tradicional de ingeniería de requisitos para la definición y gestión de requisitos para el AD, teniendo en cuenta la especificación de otros requisitos además de los de información, tales como seguridad o rendimiento (de manera similar a los requisitos de QoS). Los autores describen una clasificación de estos requisitos (llamados no-funcionales) con el fin de facilitar su especificación mediante el uso de *softgoals*. Desafortunadamente, el modelado de estos requisitos se considera como un aspecto aislado, sin tener en cuenta los requisitos de información relacionados. No obstante, con el fin de obtener un modelo MD conceptual que guíe el desarrollo del AD, satisfaciendo necesidades de información y expectativas de QoS, ambos tipos de requisitos deben modelarse juntos. Además en este trabajo, los autores se centran únicamente en la operacionalización de las *softgoals*. Por lo tanto, en el presente trabajo proponemos un análisis de requisitos para ADs como una etapa fundamental de una aproximación global basada en MDA, en la cual se defina cómo modelar de manera conjunta tanto los requisitos de información como los requisitos de QoS.

QoS es un concepto relacionado con el uso del AD, tal y como se describe en [11]. Los modelos de uso describen cómo se utiliza un AD, p.e. los grupos de usuarios, la flexibilidad de los requisitos, la disponibilidad de ciertos servicios que suministra el AD, etc. Los modelos de uso pueden (i) derivarse de un AD existente con el fin de encontrar mejoras potenciales o (ii) crearse a la vez que se diseña el nuevo AD. Los diferentes aspectos del uso pueden reflejarse en los requisitos de QoS, ya que ambos conceptos intentan capturar no solamente qué información suministra el AD sino también cómo se utiliza el AD.

III. ANÁLISIS DE REQUISITOS EN ALMACENES DE DATOS

Al igual que las bases de datos el diseño de un AD se basa en las fases análisis de requisitos, nivel conceptual, lógico y físico. En la Fig. 1 mostramos cómo puede ser alineado el diseño de los AD seguros con el marco MDA, la cual toma como base la aproximación descrita en [7]. La fase análisis de requisitos coincide con un CIM seguro cuya especificación debe estar dirigida por un análisis de (i) los requisitos de información, (ii) los requisitos de QoS (seguridad) y un análisis conjunto de los requisitos de información y de QoS. Este CIM seguro se modela mediante una adaptación del marco i* [12].

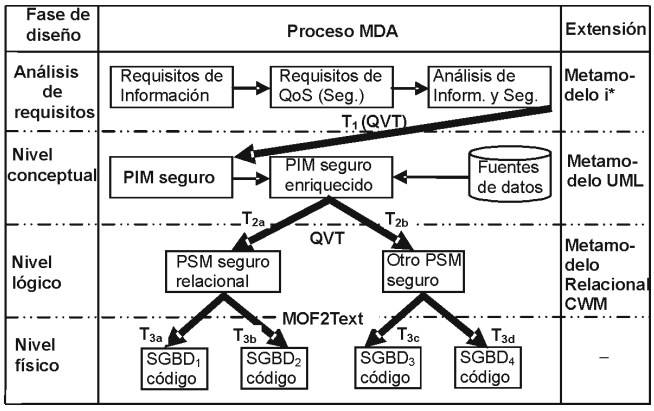

Figura 1 Proceso de diseño de un AD seguro utilizando MDA.

La transformación T_1 permite obtener un PIM seguro que se enriquece con las fuentes de datos[1], de este modo, el PIM seguro enriquecido se corresponde con el nivel conceptual. Este PIM seguro se modela A partir de este PIM se pueden aplicar diferentes transformaciones QVT (T_{2a} y T_{2b} en la Fig. 1) para obtener dos o más PSM seguros, aunque especificamos un PSM relacional pues nos basamos en la extensión del metamodelo relacional presentado en [13]. Por ello, el PSM representa al nivel lógico. Finalmente, a partir de cada uno de los PSM obtenidos es posible obtener código para un Sistema de Gestión de Bases de Datos (SGBD) en específico (vea las transformaciones T_{3a} , T_{3b}, T_{3c} y T_{3d} en la Fig. 1) mediante la aplicación de la propuesta *MOF2Text*. Luego, el código obtenido se corresponde con el nivel físico en el diseño de AD. Puede encontrar más información acerca de nuestra aproximación para el desarrollo de ADs seguros en [4], [6], [7], [14] y [15].

En todo lo que sigue nos centraremos únicamente en la fase

[1] En [4] se puede encontrar más información acerca del análisis de las fuentes de datos operacionales.

análisis de requisitos del AD, es decir, cómo definir un CIM seguro a partir del análisis de requisitos de QoS. La aproximación global para el análisis de requisitos consta de dos partes:

1. **Análisis de requisitos de información**, cuyo objetivo es obtener los requisitos de información que tienen los usuarios para el apoyo a la toma de decisiones, i.e. medidas interesantes y el contexto para su análisis. Estos requisitos deben especificarse en un modelo de requisitos de información.
2. **Análisis de requisitos de QoS**, los cuales enriquecen el modelo de requisitos de información con el fin de reflejar bajo qué restricciones se suministra la información. La razón de este análisis es que el modelo de requisitos de información sólo refleja requisitos para un modelo MD "simple", es decir, que sólo suministra la información adecuada a los usuarios e ignora cómo se debe suministrar esa información para usarse de manera correcta.

A. Análisis de requisitos de información

Los usuarios del AD con frecuencia ignoran como describir de manera apropiada los requisitos de información, ya que son más conscientes de los objetivos que el AD les ayudará a cumplir. Por lo tanto, una fase de análisis de requisitos para ADs debe comenzar por el descubrimiento de estos objetivos. Los requisitos de información pueden descubrirse a partir de estos objetivos de manera más sencilla.

Los objetivos relacionados con el AD pueden especificarse a tres niveles [16]: objetivos estratégicos, los cuales son objetivos principales del proceso de negocio: "incrementar ventas", "incrementar el número de clientes", "decrementar costes", etc. Objetivos de decisión, cuya finalidad es realizar las acciones apropiadas para cumplir un objetivo estratégico, por ejemplo "definir algún tipo de promoción" o "abrir nuevas tiendas". Finalmente, los objetivos de información se relacionan con la información necesaria para cumplir con los objetivos de decisión; ejemplos de este tipo de objetivos serían "analizar las compras de los clientes" o "examinar existencias". Una vez que se definen estos objetivos, los requisitos de información se obtienen directamente de los objetivos de información. Los diferentes elementos MD, tales como hechos o dimensiones, se pueden descubrir a partir de estos requisitos de información con el fin de derivar el correspondiente modelo MD conceptual del AD.

Para modelar todos estos elementos en un CIM, se ha definido un perfil de UML (*Unified Modeling Language*) para i* [12] (ver Fig. 3), pudiendo representar así los diferentes actores del AD, sus dependencias y objetivos. En i* se definen dos modelos: el modelo SD (*strategic dependency*) que describe las relaciones de dependencias entre diferentes actores en el contexto organizacional y el modelo SR (*strategic rationale*), usado para describir los intereses de los actores y cómo deben ser alcanzados.

Los requisitos de información de cada actor se describen en modelos SR. El modelo SR (definido con el estereotipo SR y representado como) permite el modelado de elementos intencionales y sus relaciones de cada actor (*IActor*,). Para definir modelos SR para ADs, los objetivos (*Goal*,), tareas (*Task*,) y recursos (*Resource*,) se representan como elementos intencionales de cada actor del AD, tal y como se puede ver en la Fig. 2. Entre estos elementos intencionales (*IActor*, *Goal*, *Task* y *Resource*) puede haber dos tipos de relaciones: medio-fin (*MeansEnd*,) o tarea-descomposición (*Decomposition*,).

Además, nuestro perfil para i* se ha extendido con el fin de poder modelar características propias de requisitos para ADs. En concreto, los objetivos para el AD pueden definirse usando los estereotipos *Strategic*, *Decision* e *Information*, los cuales especializan el anteriormente definido estereotipo *Goal*. A partir de los objetivos de información, se pueden derivar los requisitos de información (*Requirement*) como tareas. Por otro lado, el análisis de requisitos para ADs necesita de la definición de algunos conceptos MD [3], los cuales se añaden como recursos estereotipados en el CIM: procesos de negocio relacionados con los objetivos de los usuarios del AD (*BusinessProcess*), medidas relevantes relacionadas con los requisitos de información de los usuarios del AD (*Measure*) y el contexto de análisis para analizar dichas medidas (*Context*). El uso de estos elementos se muestra en la Fig. 2.

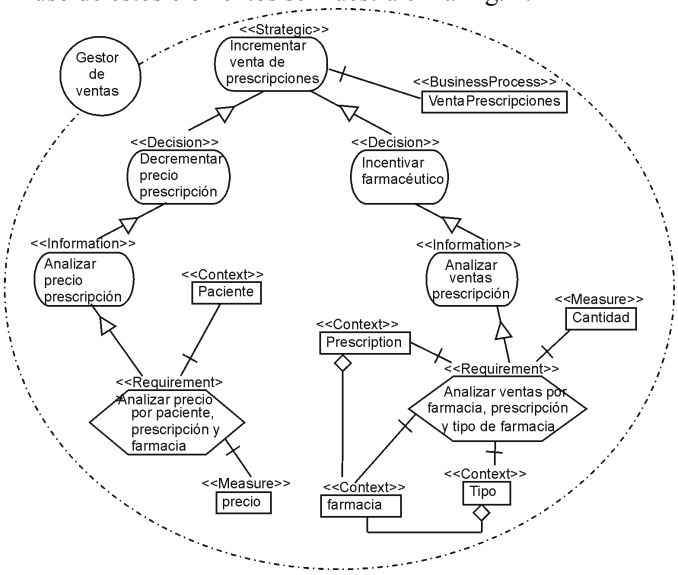

Fig. 2 Modelo de requisitos de información.

Además, se pueden modelar relaciones entre contextos de análisis. Por ejemplo, el contexto farmacia y el contexto tipo están relacionados porque las farmacias pueden agruparse según su tipo. Para modelar estas relaciones se añade a la notación de i* la agregación de UML (metaclase *Association*, representada como). Todos los elementos descritos se

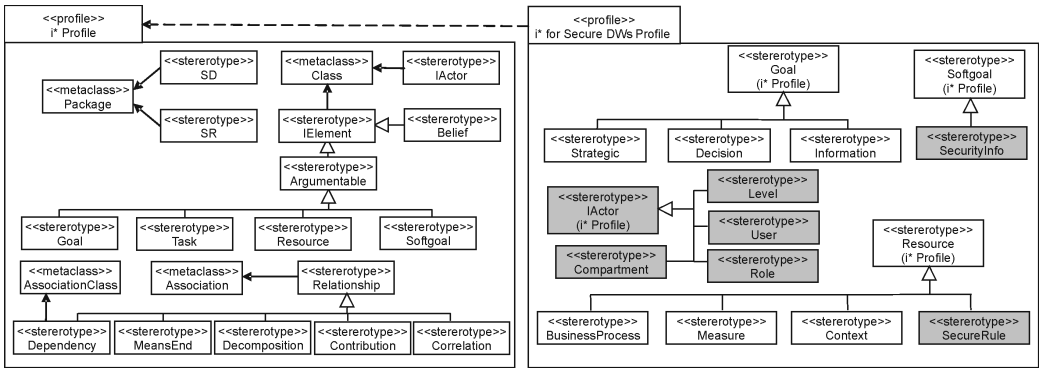

Fig. 3 Perfiles de i* para definir requisitos de seguridad en ADs.

han especificado en un perfil UML para i extendido para ADs [6] (ver Fig. 3).*

Los diferentes tipos de objetivos y los requisitos de información para el AD se modelan y se relacionan con elementos MD en un CIM mediante diferentes pasos: (i) descubrir los diferentes actores (usuarios del AD), definiendo modelos SR para cada uno, (ii) descubrir los diferentes tipos de objetivos, (iii) derivar los requisitos de información de los objetivos de información y (iv) obtener los conceptos MDs relacionados con los requisitos de información.

B. Análisis de requisitos de QoS

Una vez que los requisitos de información han sido especificados en el CIM, el modelo debe enriquecerse mediante la adición de requisitos de QoS. Estos requisitos son múltiples, por lo que para no pasar por alto ningún aspecto importante, es necesario definir una clasificación de requisitos de QoS para ADs. La Fig. 4 muestra una clasificación para capturar los diferentes aspectos que deben considerarse cuando se diseña un AD. Esta clasificación está basada en un catálogo de requisitos no-funcionales para el diseño del AD presentada en [9]:

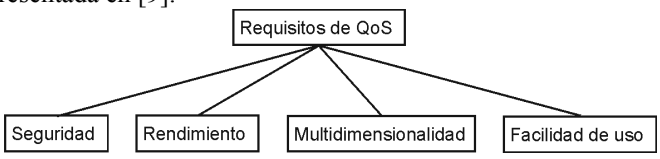

Fig. 4 Aspectos a tener en cuenta durante el diseño del AD.

Seguridad, incluye requisitos relacionados con la protección de recursos valiosos en el AD. Los requisitos de seguridad describen cómo se gestiona el acceso, a qué información se puede acceder y por quién y bajo qué condiciones se puede acceder a esa información

Rendimiento, puede dividirse en rendimiento relacionado con el tiempo (tiempo de proceso o tiempo de respuesta) y con el espacio (cantidad de memoria usada, memoria principal o secundaria).

Multidimensionalidad, cubre aspectos relacionados con el acceso a datos multidimensionales como interpretación o integración.

Facilidad de uso, que requiere flexibilidad y facilidad de aprendizaje.

Cabe destacar que esta lista de requisitos de QoS no es exhaustiva, sino que pretende ser una lista representativa cuyo propósito es mostrar la necesidad de modelar requisitos de QoS junto con los requisitos de información en una aproximación global para el desarrollo del AD. Cada concepto en esta clasificación debe analizarse a nivel de requisitos. Deben desarrollarse nuevas técnicas para especificar tales requisitos de QoS en el CIM junto con los requisitos de información. En este artículo, nos centramos en uno de los requisitos de QoS más importantes para ADs: la seguridad.

IV. REQUISITOS DE SEGURIDAD PARA ALMACENES DE DATOS

Cada tipo de requisito de QoS necesita un tipo especial de técnica para poder ser especificado en un CIM. En este artículo, nos centramos en los requisitos de seguridad. Los requisitos de seguridad son requisitos de QoS asociados con la protección de recursos valiosos del sistema. Estos requisitos de seguridad describen cómo se gestiona el acceso, a qué información se puede acceder y por quién y bajo qué condiciones se puede acceder a la información. Por ello, son denominados con frecuencia políticas de control de acceso (*Access Control Policies*, ACP).

Nuestra aproximación ACP para ADs se describe en [17] y [18], donde se define un modelo de control de acceso y auditoría (*Access Control and Audit*, ACA) con el fin de especificar los aspectos de seguridad para ADs. Sin embargo, esta aproximación está aislada de la fase de análisis de requisitos para el AD y puede causar incongruencias entre las políticas de seguridad y la implementación del AD. Muchos investigadores han reconocido la necesidad de integrar el análisis de requisitos y la definición del control de acceso mediante la especificación de requisitos de seguridad en el desarrollo de sistemas de información [19]. A continuación, nos centramos en describir cómo alinear el modelo ACA con el análisis de requisitos de QoS.

A. Modelo de auditoría y control de acceso (ACA)

El modelo ACA [17], [18] describe un mecanismo de control de acceso, permitiendo representar confidencialidad y auditar medidas del AD mediante la clasificación de sujetos y objetos del sistema. En concreto, se usan clases de acceso

basadas en tres maneras diferentes pero compatibles de clasificar usuarios: por su nivel de seguridad, por su rol y por su categoría. Una clase de acceso es un elemento de un conjunto de clases parcialmente ordenado, donde una clase de acceso c_1 domina una clase de acceso c_2 si y sólo si el nivel de seguridad de c_1 es mayor o igual que el nivel de seguridad de c_2, las categorías de c_1 incluyen a las de c_2 y, al menos, uno de los roles de usuario de c_1 se define para c_2. Para poder especificar un modelo ACA, se deben definir las siguientes clases:

Roles de seguridad de usuario, usados para organizar usuarios según una estructura jerárquica, dependiendo de sus responsabilidades. Cada usuario puede tener más de un rol.

Niveles de seguridad, indican el nivel de acreditación del usuario. Usualmente, corresponde a un elemento de un conjunto ordenado jerárquicamente, tal como *TopSecret* (TS), *Secret* (S), *Confidential* (C) y *Unclassified* (U), donde TS > S > C > U.

Categorías de seguridad de usuario, indican una clasificación horizontal de usuarios atendiendo a ciertos criterios como localización geográfica o área de trabajo. Cada usuario puede pertenecer a una o más categorías.

B. Modelado de requisitos de seguridad

Para poder especificar requisitos de seguridad en un CIM, se necesita extender el perfil de i* para ADs definido en la sección III-A. Nuestra nueva extensión (ver elementos sombreados de la Fig. 3) ofrece mecanismos para representar un actor especial llamado gestor de seguridad (*SecurityManager*,), el cual representa a un encargado de la seguridad de la organización. Los requisitos de seguridad son requisitos de QoS y deben modelarse usando *softgoals* (*SSoftgoal*,). Estas *softgoals* representan y refinan la política de seguridad de la organización. Los elementos del modelo ACA se consideran como recursos etiquetados como <<*SCompartment*>> (categorías), <<*SLevel*>> (niveles) y <<*SRole*>> (roles). Además, con el fin de especificar restricciones a los recursos, se introduce una tarea especial etiquetada como <<SConstraint>>, la cual contribuye a cumplir con las *softgoals* a través de asociaciones de contribución (*Contribution*,). El proceso de refinamiento de *softgoals* se realiza mediante asociaciones medio-fin (*MeansEnd*). Finalmente, cada *softgoal* se asocia con procesos de negocio (*BusinessProcess*), medidas (*Measure*) o contexto de análisis de las medidas (*Context*).

Con el análisis de los requisitos de información descrito en la sección III-A obtenemos modelos SR para cada uno de los actores (usuarios del AD), cada uno de los cuales tendrá conceptos MD relacionados con los requisitos de información. Sin embargo, para modelar los requisitos de seguridad utilizamos otro modelo SR para un único actor (gestor de seguridad). Hay varias razones que justifican este hecho. Primero, si modelamos conjuntamente los requisitos de información y de seguridad el modelo resultante puede ser demasiado grande y complejo, lo que afecta su correcta visualización. Segundo, las medidas de seguridad se modelan siguiendo el modelo ACA, por ello, tenemos que identificar los tipos de información de seguridad que serán utilizados (roles de seguridad de usuarios, niveles de seguridad y categorías de seguridad de usuarios) mediante un refinamiento de las *softgoals* para finalmente asociarlos a éstas, lo que evidencia un proceso algo complejo que resulta independiente de los conceptos MD obtenidos en la fase de análisis de requisitos de información. Tercero, resulta conveniente utilizar modelos independientes para facilitar la definición de una transformación MDA entre el CIM seguro y el PIM seguro, así como garantizar la *traceability*.

Para poder definir un modelo de requisitos de seguridad compatible con el modelo ACA, se proponen los siguientes dos pasos, a realizar una vez se ha obtenido el modelo de requisitos de información (ver sección III-A):

Análisis de requisitos de seguridad. Durante esta fase se especifica un modelo de requisitos de seguridad que consiste en tres pasos:

1. Detectar vulnerabilidades y necesidades del sistema según las políticas de la organización, leyes y regulaciones.
2. Obtener los requisitos de seguridad del gestor de seguridad mediante técnicas de obtención de requisitos como entrevistas. Estos requisitos se modelan mediante *softgoals* y se refinan en *softgoals* de más bajo nivel. Durante este refinamiento, se descubren diferentes responsabilidades y tareas (i.e. roles y categorías) y los niveles que podrán usarse.
3. Asociar las *softgoals* con los correspondientes recursos (i.e. *SCompartment*, *SRole* y *SLevel*).

Análisis conjunto de información y seguridad. Hasta ahora hemos obtenido un modelo de requisitos de información y un modelo de requisitos de seguridad. El próximo paso consiste en relacionar ambos modelos:

1. Cada *softgoal* refinada se asocia con los correspondientes elementos del modelo de requisitos de información (i.e. *BusinessProcess*, *Measure* y *Context*).
2. Considerar otros posibles aspectos de seguridad para los requisitos de información, adicionales a los establecidos con anterioridad. En concreto, se definen tareas *SConstraint* asociadas a *softgoals* para indicar que contribuyen positivamente a su cumplimiento.

C. Caso de estudio

En esta sección se describe un ejemplo de aplicación de nuestra propuesta. Un consorcio farmacéutico gestiona varias farmacias. Este consorcio desea analizar las ventas de medicinas por medio de prescripciones médicas. Por tanto, nos centramos en el proceso de negocio relacionado con las ventas. Dentro del consorcio existen varios grupos: (i) un grupo de vigilancia de fármacos que comprueba el correcto uso de ciertas medicinas, (ii) un comité que vela por la salud de los clientes y (iii) un grupo comercial que gestiona la venta de medicamentos.

Análisis de requisitos de información La primera fase se desarrolla mediante la aproximación para el modelado de requisitos de información descrita en la sección III-A. El modelo i* definido se muestra en la Fig. 2. El proceso de negocio venta de prescripciones se relaciona con el actor principal, gestor de ventas, mediante el objetivo estratégico "incrementar ventas de prescripciones". A partir de este objetivo estratégico, se obtienen dos objetivos de decisión:

"decrementar el precio de la prescripción" e "incentivar al farmacéutico". A partir de estos objetivos de decisión, se obtienen los siguientes objetivos de información: "analizar el precio de las prescripciones" y "analizar las ventas de las prescripciones". Los requisitos de información que se derivan son los siguientes (mostrados como tareas en la figura 2): "analizar el precio por paciente, prescripción y farmacia" y "analizar ventas por farmacia, prescripción y tipo de farmacia". Además, se deben asociar varios recursos a los requisitos de información (medidas y contexto de análisis). Las medidas son cantidad vendida y precio. Los elementos que representan el contexto de análisis son paciente, prescripción y farmacia. El tipo de farmacia también pertenece al contexto de análisis y representa una manera de agregar los datos de las farmacias.

Análisis de requisitos de seguridad Esta fase se lleva a cabo según la propuesta descrita en la sección IV-B. El modelo resultante se muestra en la Fig. 5. Nos centramos en la política de seguridad del proceso de negocio de las ventas de prescripciones, la cual es llevada a cabo por el actor gestor de seguridad mediante la *softgoal* "garantizar la seguridad en las ventas con prescripciones". Mediante un refinamiento se obtienen tres nuevas *softgoals*: "proteger el uso de ciertos medicamentos y el derecho de los consumidores", "mantener la privacidad de las ventas, el precio y los datos del paciente" e "imponer niveles de autorización al proceso de prescripción". Durante este proceso se descubren varias responsabilidades y se asocian a sus *softgoals* correspondientes (ver Fig. 5):

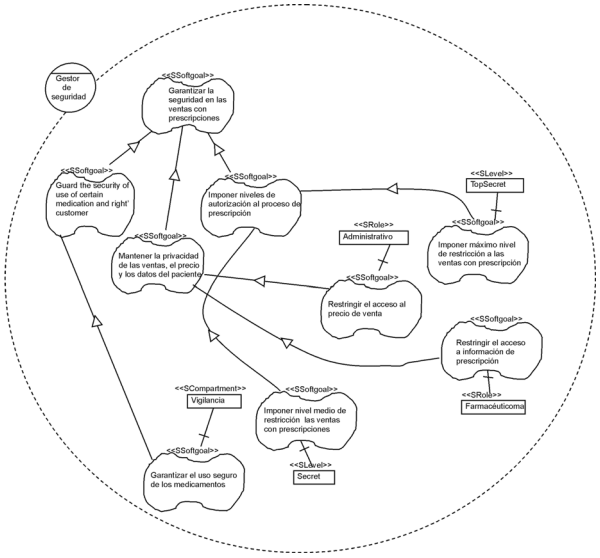

Fig. 5 Modelo de requisitos de seguridad.

1. Se obtienen relaciones jerárquicas: empleado, que se especializa en dos roles: farmacéutico y administrativo.
2. Se detectan las categorías (grupos horizontales): departamento de vigilancia de fármacos y departamento comercial.
3. Se establecen los niveles de restricción: *TopSecret* y *Secret*.

Análisis conjunto de información y seguridad Una vez obtenidos los modelos de requisitos de información y de seguridad, se necesita relacionar los recursos asociados a los requisitos de información (i.e. venta de prescripciones, cantidad vendida, precio, paciente, prescripción, farmacia y tipo de farmacia) con las *softgoals* definidas en el modelo de requisitos de seguridad (p.e. "garantizar el uso seguro de los medicamentos" o "imponer máximo nivel de restricción a las ventas con prescripciones"). El gestor de seguridad depende del gestor de ventas para poder alcanzar dichas *softgoals* (ver Fig. 6). Ventas de prescripciones se asocia con la *softgoal* "imponer máximo nivel de restricción a las ventas con prescripciones", la cual tiene *TopSecret* como *SLevel*. Análogamente, el contexto prescripción se asocia con la *softgoal* "garantizar el uso seguro de los medicamentos", por lo que tiene Vigilancia como *SCompartment*. Debido a que ventas y prescripción permiten un futuro refinamiento del modelo, se necesitan restricciones adicionales: la figura 6 muestra cómo la *SConstraint SRule* contribuye a cumplir con las tres *softgoals* obtenidas anteriormente, por lo que se asocia con el proceso de negocio ventas de prescripciones. El mismo razonamiento asegura que el contexto prescripción se relacione con la *SConstraint Audit*.

El beneficio de aplicar nuestra propuesta es que los niveles, roles y categorías de seguridad para cada usuario del AD se modelan fácilmente en un CIM. Concretamente, en nuestro ejemplo se puede concluir que un usuario tiene acceso a las ventas si su clase de acceso domina la clase de acceso de ventas, i.e. su nivel de seguridad es *TopSecret*. Este CIM puede usarse para derivar un PIM [6] que refleje cada requisito de seguridad a nivel conceptual [17] y [18], asegurando que la implementación del AD satisfará las expectativas de los usuarios.

V. Conclusiones

En este artículo proponemos el modelado conjunto de requisitos de información y de QoS en una etapa explícita del desarrollo de ADs, como paso previo a la derivación de un modelo MD conceptual del AD que satisfaga las expectativas del usuario. Concretamente, este artículo se centra en los requisitos de seguridad. Hasta ahora, hemos propuesto un marco de trabajo general [14] y [15] basado en MDA en el cual se usan nuestras propuestas para el diseño de un AD seguro a nivel conceptual [17], [18] y lógico [13]. En este artículo, se amplía este marco de trabajo para considerar una etapa de análisis de requisitos de seguridad a nivel CIM. Los elementos de seguridad definidos a este nivel deben reflejarse en un PIM que sirva de base a la implementación final. Por ejemplo, los elementos *SConstraint*, deben definirse a nivel PIM siguiendo los patrones definidos en el modelo ACA (*AuditRule*, *SecurityRule* o *AuthorizationRule*).

Por otro lado, la seguridad es únicamente un aspecto de los requisitos de QoS, por lo que nuestro trabajo futuro inmediato se centra en definir mecanismos para modelar otros tipos de requisitos de QoS, estudiar las relaciones y dependencias entre estos requisitos. Otro trabajo a medio plazo consiste en la definición de mecanismos formales que sirvan de base para facilitar el modelado conjunto de cada uno de los modelos necesarios para el análisis de requisitos.

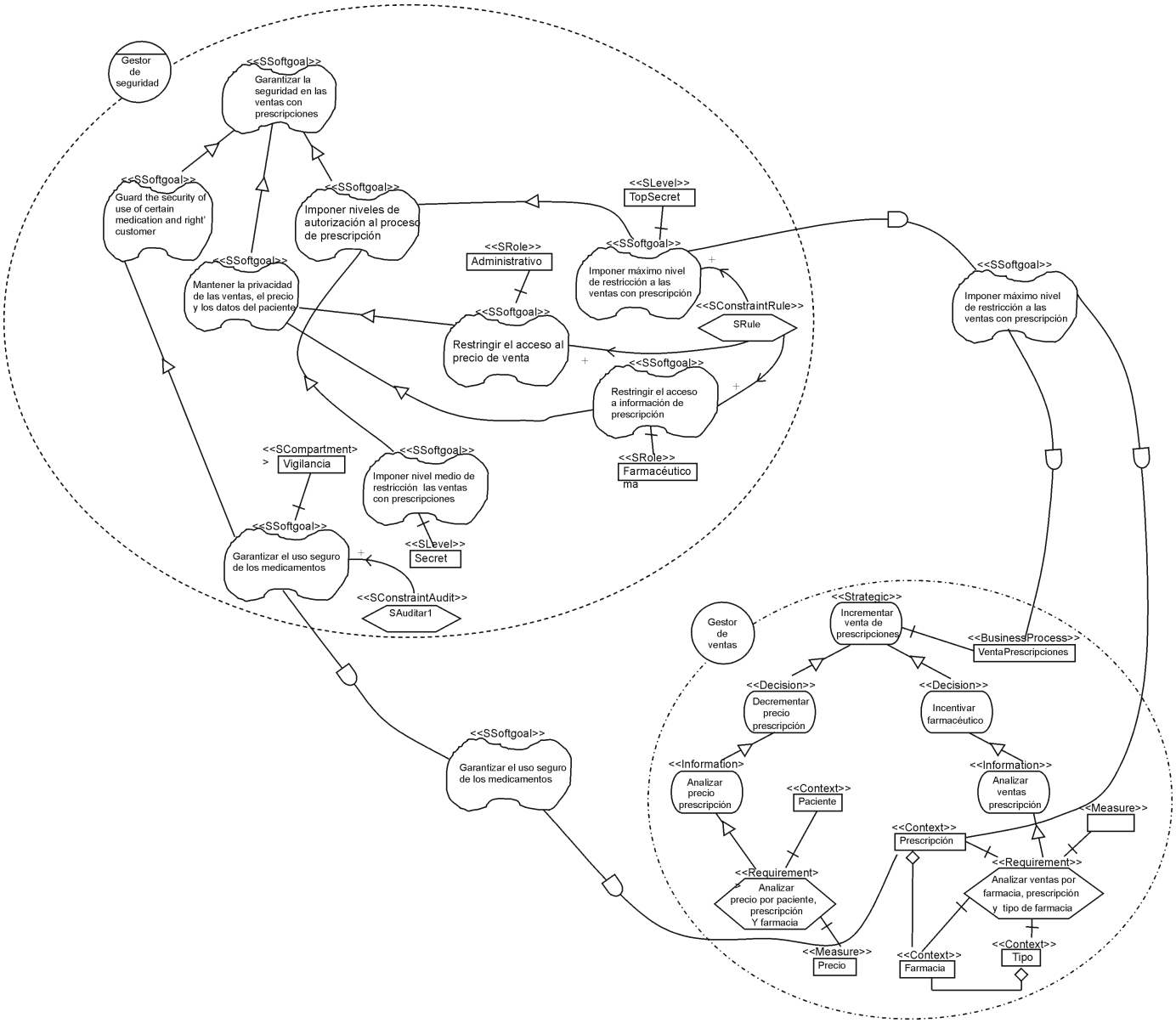

Fig. 6 Modelo integrado de requisitos de información y seguridad.

REFERENCIAS

[1] Kimball, R., Ross, M. The Data Warehouse Toolkit. Wiley & Sons (2002).

[2] Rizzi, S., Abelló, A., Lechtenbörger, J., Trujillo, J. Research in data warehouse modeling and design: dead or alive? In: DOLAP'06, pp. 3–10, Arlington, Virginia, USA, nov. 10. 2006.

[3] Giorgini, P., Rizzi, S., Garzetti, M. Goal-oriented requirement analysis for data warehouse design. In: DOLAP'05, pp. 47-56, Bremen, Germany, nov. 4-5, 2005.

[4] Mazón, J.N., Trujillo, J., Lechtenbörger, J. Reconciling requirement-driven data warehouses with data sources via multidimensional normal forms. Data and Knowl. Eng., vol. 63, no. 3, pp. 725-751, 2007.

[5] Winter, R., Strauch, B. A method for demand-driven information requirements analysis in data warehousing projects. HICSS'03, pp 231, 2203.

[6] Mazón, J.N., Pardillo J., Trujillo, J. A Model-Driven Goal-Oriented Engineering Approach for Data Warehouses. Workshop on Requirements, Intentions and Goals in Conceptual Modeling (RIGiM). ER'07 Workshops, Lecture Notes in Computer Science, vol. 4802, pp. 255-264, Auckland, New Zealand, nov. 5-9, 2007.

[7] Mazón, J.N., Trujillo, J. An MDA approach for the development of data warehouses. Decision Support Systems, vol 45, no. 1, pp. 41–58, 2008.

[8] Prakash, N., Singh, Y., Gosain, A. Informational scenarios for data warehouse requirements elicitation. ER'04, Lecture Notes in Computer Science, vol. 3288, pp. 205–216, Shanghai, China, nov. 8-12, 2004.

[9] Paim, F.R.S., Castro, J. Enhancing Data Warehouse Design with the NFR Framework. In WER'02, pp.40–57, Valencia, España, nov.11-12, 2002.

[10] Paim, F.R.S., Castro, J. DWARF: An approach for requirements definition and management of data warehouse systems. In RE'03, pp. 75–84, Monterey Bay, CA, USA, sept. 8-12, 2003.

[11] Stefanov, V, List, B. A UML Profile for Modeling Data Warehouse Usage. In: 3rd International Workshop on Foundations and Practices of UML (FP-UML 2007). ER'07 Workshops, Lecture Notes in Computer Science vol. 4802, pp. 137-147, Auckland, New Zealand, nov. 5-9, 2007.

[12] Yu, E. Towards modeling and reasoning support for early-phase requirements engineering. RE'97, pp. 226-235, Annapolis, MD, USA, enero 5-8. 1997.

[13] Soler E., Villarroel R., Trujillo J., Fernández-Medina E., Piattini M. Building a secure star schema in data warehouses by an extension of the relational package from CWM. Computer Standards & Interfaces. doi:10.1016/j.csi.2008.03.002.

[14] Soler E., Trujillo J., Fernández-Medina E., Piattini M. A Framework for the Development of Secure DWs based on MDA and QVT. ARES'07, pp. 294-300, Viena, Austria, 10-13 abril. 2007.
[15] Soler E., Trujillo J., Fernández-Medina E., Piattini M. Aplicación de QVT al Desarrollo de Almacenes de Datos Seguros: Un Caso de Estudio. IDEAS'07, pp. 209-222, Isla Margarita, Venezuela, 7-11 mayo. 2007.
[16] Mazón, J.N., Trujillo, J., Serrano, M., Piattini, M. Designing data warehouses: from business requirement analysis to multidimensional modeling. REBNITA'05, pp.44-53, Paris, France, Agosto, 2005.
[17] Fernández-Medina, E., Trujillo, J., Villarroel, R., Piattini, M. Access control and audit model for the multidimensional modeling of data warehouses. Decis. Support Syst., vol. 42, no.3, pp 1270–1289, 2006.
[18] Fernández-Medina E., Trujillo J., Villarroel R., Piattini M. Developing secure data warehouses with a UML extension. Information Systems, vol. 32, no. 6, pp. 826-856, 2007.
[19] Antón, A.I., Earp, J.B., Carter, R.A. Precluding incongruous behavior by aligning software requirements with security and privacy policies. Information and Software. Information & Software Technology, vol. 45, no.14, pp. 967-977, 2003.

Emilio Soler es graduado de matemática de la Universidad Pedagógica de Matanzas (Cuba) y profesor auxiliar del departamento de Informática de la Universidad de Matanzas (Cuba). Soler actualmente es estudiante de doctorado del departamento de sistemas informáticos de la universidad de Alicante (España). Sus actividades de investigación incluyen seguridad en almacenes de datos, MDA y sistemas de información. Ha publicado y presentado artículos en conferencias nacionales e internacionales de ciencias de la computación tales como ICCSA, ARES, JISBD, WOSIS e IDEAS. Su correo de contacto es emilio.soler@umcc.cu.

Verónica Stefanov es graduada de Master y Doctor por la Universidad Tecnológica de Viena, Austria. Sus intereses de investigación incluyen almacenes de datos e inteligencia del negocio, data warehousing, modelado de la empresa, ingeniería de modelos y recuperación de información. Ha publicado varios artículos en conferencias y talleres internacionales, como DAWAK, CAiSE, ECIS y EDOC en los que participa además, como miembro del Comité de Programa. Su correo es stefanov@wit.tuwien.ac.at.

Jose Norberto Mazón es estudiante de doctorado en la Universidad de Alicante (España). Actualmente dispone de una beca FPU del Ministerio de Educación y Ciencia de España. Es ingeniero informático por la Universidad de Alicante. Ha publicado varios trabajos en congresos nacionales e internacionales como DAWAK, ER, DOLAP, BNCOD, JISBD, etc. Sus líneas de investigación son: modelado de bases de datos, diseño conceptual de almacenes de datos, modelado multidimensional y desarrollo dirigido por modelos. Su dirección de correo electrónico es jnmazon@dlsi.ua.es.

Juan Trujillo es profesor en la Escuela de Informática de la Universidad de Alicante, España. Trujillo obtuvo su Doctorado en Informática en la Universidad de Alicante (España) el año 2001. Sus intereses de investigación incluyen modelado de bases de datos, diseño conceptual de almacenes de datos, bases de datos multidimensionales, OLAP, y análisis y diseño orientado a objetos con UML. Ha publicado artículos en conferencias internacionales y revistas tales como ER, UML, ADBIS, CaiSE, WAIM, *Journal* de Gestión de Bases de Datos (JDM) e IEEE *Computer*. Participa como miembro de Comité de Programa de varios talleres y conferencias tales como ER, DOLAP, DSS, y SCI. También ha participado como revisor de varias revistas tales como JDM, KAIS, ISOFT y JODS. Su correo es jtrujillo@dlsi.ua.es.

Eduardo Fernández-Medina es Doctor y Master en Informática. Es profesor asistente en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha (España). Su actividad de investigación es seguridad en bases de datos, almacenes de datos, servicios web y sistemas de información. Y también en métricas de seguridad. Es coeditor de varios libros y capítulos de libros en estos temas, y tiene varias docenas de artículos en conferencias nacionales e internacionales. Participa en el grupo de investigación ALARCOS del Departamento de Informática en la Universidad de Castilla-La Mancha (España). Pertenece a varias asociaciones de investigación y profesionales (ATI, AEC, AENOR, IFIP WG11.3 etc.). Su correo es eduardo.fdezmedina@uclm.es.

Mario Piattini es Master y Doctor en Informática por la Universidad Politécnica de Madrid. Auditor de Sistemas de (*Information System Audit and Control Association*). Actualmente es Catedrático de Universidad en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha (España). Autor de varios libros y artículos sobre bases de datos, ingeniería de software y sistemas de información. Pertenece al grupo de investigación ALARCOS del Departamento de Informática en la Universidad de Castilla-La Mancha (España). Sus intereses de investigación son: diseño de bases de datos avanzadas, calidad de bases de datos, métricas de software, métricas orientadas a objeto, mantenimiento de software. Su correo es mario.piattini@uclm.es.