Actas de los Talleres de JISBD

- JISBD
- Talleres

Volumen 1. Número 2
PNIS 2007: I Taller sobre Procesos de Negocio e Ingeniería del Software [TOC]
Actas del Iº Taller sobre Procesos de Negocio e Ingeniería del Software.

Zaragoza, España
11 de septiembre de 2007
Editores:
Francisco Ruiz
Universidad de Castilla-La Mancha (España)
Félix Óscar García
Universidad de Castilla-La Mancha (España)

Tabla de Contenidos

Última actualización 20 de Julio de 2007.

Elicitación de Requisitos de Seguridad en Procesos de Negocio

Alfonso Rodríguez
Departamento Auditoría e Informática
Universidad del Bio Bio
Chillán
Chile
alfonso@ubiobio.cl

Eduardo Fernández-Medina y Mario Piattini
Grupo de investigación ALARCOS
Departamento de Tecnologías y Sistemas de Información
Universidad de Castilla-La Mancha
Ciudad Real
España
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es

Resumen

La temprana obtención de requisitos en un proceso de desarrollo de software permite mejorar la calidad del producto. Aunque existen muchos métodos para elicitar requisitos, pocos de ellos son específicos para elicitar requisitos de seguridad. En este artículo se describe un método, M-BPSec, que permite elicitar los requisitos de seguridad que han sido incorporados en la descripción de un proceso de negocio. M-BPSec está compuesto de etapas, trabajadores, herramientas y artefactos que, aplicados de manera coordinada, permiten especificar un proceso de negocio, incorporarle requisitos de seguridad y obtener clases de análisis y casos de uso a partir de dicha especificación. Adicionalmente presentamos un caso de estudio que permite mostrar la forma en que M-BPSec es aplicado.

1. Introducción

La elicitación de requisitos es la actividad que se considera como el primer paso en un proceso de ingeniería de requisitos. Debido a que existen muchas técnicas disponibles para elicitar requisitos, es necesario contar con un método que sirva de guía para su aplicación, teniendo en cuenta que, cada método tiene fortalezas y debilidades y que además está orientado hacia un dominio específico [10].

En el caso específico de los métodos para la elicitación de requisitos de seguridad, éstos son escasos. Adicionalmente, las organizaciones no tratan de manera específica la elicitación de requisitos de seguridad. Este tipo de requisito se considera como cualquier otro requisito y es incluido en los métodos tradicionales de elicitación [8].

Por su parte, los procesos de negocio ya no sólo se consideran importantes para el desempeño y la competitividad de la empresa, sino que además constituyen un punto de partida para un proceso de construcción de software ya que son una importante fuente de requisitos.

El escenario en que se desenvuelven las organizaciones hoy en día, se caracteriza por un incremento de los participantes y el uso intensivo de tecnologías de información y comunicaciones. Esto ha permitido que las organizaciones puedan crecer y abarcar nuevos mercados. Como contrapartida su vulnerabilidad también se ha incrementado.

Aunque la importancia de la seguridad en procesos de negocio es ampliamente aceptada, hasta ahora, la perspectiva de los expertos del negocio en relación con la seguridad, había sido escasamente tratada. En trabajos previos hemos propuesto una extensión, BPSec-Profile, que permite incorporar requisitos de seguridad en el Diagrama de Actividad de UML 2.0 (UML 2.0-AD) y en el Diagrama de Procesos de Negocio de BPMN (BPMN-BPD). Usando esta extensión es posible describir un Proceso de Negocio Seguro (SBP, Secure Business Process) [14, 15].

En este trabajo, describiremos un método mediante el cual es posible elicitar requisitos de seguridad desde una especificación de un proceso de negocio seguro. Para ello hemos organizado este artículo de la siguiente forma: en la Sección 2 presentaremos un resumen de nuestra propuesta, en la Sección 3 abordaremos los trabajos relacionados, en la Sección 4 describiremos el método M-BPSec, en la Sección 5 mostraremos un caso de estudio y finalmente, en la Sección 6, presentaremos nuestras conclusiones.

2. Nuestra propuesta

Nuestra propuesta es un método para elicitar requisitos de seguridad que serán capturados junto con la especificación de un proceso de negocio.
Debido a que M-BPSec incluye modelos (en diferentes niveles de abstracción) y artefactos (piezas de información que son producidas, modificadas o usadas en un método), hemos utilizado la Arquitectura Dirigida por Modelos (MDA, Model-Driven Architecture) [11] y el Proceso Unificado (UP, Unified Process) [6, 13] como marco de referencia.
En la Figura 1 se muestra una vista general de nuestra propuesta. En la primera columna (al lado izquierdo) se muestran los tres tipos de modelos considerados en el marco de trabajo de MDA. En la última columna se puede ver los flujos de trabajo de UP. En la parte central se muestra M-BPSec y los artefactos que son derivados de su aplicación. Con este método es posible describir un proceso de negocio seguro (SBP) y obtener, a partir de esa descripción, un conjunto de clases de análisis y casos de uso que se usarán en un proceso de construcción de software. La especificación del SBP corresponde a un modelo independiente de computación (CIM, Computation Independent Model) y las clases de análisis y los casos de uso corresponden modelos independientes de plataforma (PIM Platform Independent Model).

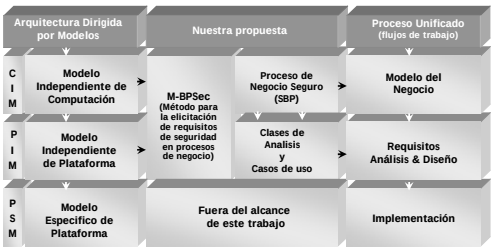

Figura 1. Vista general de nuestra propuesta

En M-BPSec se consideran transformaciones [16, 17] desde CIM hacia PIM que han sido descritas con reglas QVT (Query View Transformation) [12], reglas de refinamiento y listas de comprobación.
Finalmente, los artefactos que se obtienen a partir de la aplicación de M-BPSec pueden ser utilizados en un proceso de construcción de software. En este caso hemos elegido UP. De manera que la descripción del SBP complementará el flujo de trabajo *Modelo del Negocio* y las clases de análisis y los casos de uso complementarán los flujos de trabajo *Requisitos* y *Análisis & Diseño*.

3. Trabajos relacionados

En la revisión de los trabajos relacionados con métodos para la elicitación de requisitos de seguridad hemos encontramos (i) en [8] un análisis comparativo de nueve métodos. Para realizar la comparación, la autora usó los siguientes criterios: adaptabilidad, soporte computacional por medio de una herramienta CASE, nivel de aceptación por parte de los interesados, facilidad de implementación, salidas gráficas, velocidad de implementación, curva de aprendizaje, nivel de madurez y escalabilidad; (ii) en [9] los autores analizan siete propuestas orientadas a establecer requisitos de seguridad en el ámbito de desarrollo de sistemas de información. Los criterios de comparación utilizados fueron: grado de agilidad, soporte de ayudas, grado de integración con otros requisitos, familiaridad con los usuarios y nivel de contribución de la propuesta en relación con los requisitos de seguridad y finalmente, (iii) en [2], se presenta un estudio comparativo que considera tres enfoques: Common Criteria, casos de mal uso y árboles de ataques. Los criterios empleados fueron: dificultad de aprendizaje, usabilidad, grado de aporte a la solución final, y claridad y facilidad de análisis de la salida.
Sin embargo, ninguna de las propuestas revisadas considera la obtención de requisitos de seguridad desde especificaciones de procesos de negocio descritos con UML 2.0-AD o BPMN-BPD. Nuestra propuesta considera esta situación y también facilita la obtención automática de artefactos UML que contienen requisitos de seguridad y que complementan un proceso de creación de software.
En cuanto a los trabajos relacionados con la especificación de requisitos de seguridad en procesos de negocio [1, 4, 5, 7, 18], ellos coinciden en señalar que es necesario capturar tempranamente requisitos de seguridad y que se deben incluir en un proceso de desarrollo de software.
En trabajos previos hemos abordado este problema proponiendo la extensión, BPSec-

Profile, que considera una representación gráfica de un conjunto de requisitos de seguridad. Estos requisitos son comprensibles para los analistas de negocios y no ambiguos para los expertos en seguridad. Hemos tomado como referencia la taxonomía propuesta en [3]. Desde allí seleccionamos un subconjunto de requisitos tomando en cuenta (i) la claridad de la definición, (ii) el potencial significado en el ámbito de los negocios y (iii) la medida en que la definición no esté vinculada con alguna solución específica de seguridad. El subconjunto, no limitado, de requisitos de seguridad está compuesto por: Detección de Ataques y Amenazas, Control de Acceso, Integridad, Privacidad y No repudio.
Para la representación gráfica de un requisito de seguridad hemos asociado un candado, estándar *de facto*, que es individualizado con las iniciales de cada requisito. Adicionalmente, se puede indicar que un requisito de seguridad tenga registro de auditoría, en ese caso se debe usar un candado con una esquina doblada.

4. El método M-BPSec

Para la aplicación de BPSec-profile y la obtención artefactos útiles en un proceso de desarrollo de software, hemos diseñado M-BPSec (ver Figura 2).

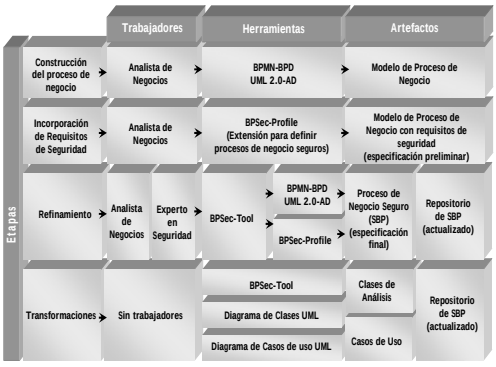

Figura 2. Esquema general de M-BPSec

Este es un método que facilita la elicitación de requisitos de seguridad que han sido especificados en un proceso de negocio. Es una guía que permite aplicar la extensión BPSec-Profile en forma ordenada y no ambigua. Está compuesto por un conjunto de etapas, trabajadores, herramientas y artefactos que, en un enfoque ingenieril y sistemático, permite crear procesos de negocio seguros y obtener artefactos útiles para el desarrollo de software.
Las tres primeras etapas de M-BPSec están directamente relacionadas con la definición de un proceso de negocio seguro. La cuarta y última etapa es un complemento que permite generar automáticamente clases de análisis y casos de uso.
En las secciones siguientes se describirán los elementos que componen M-BPSec.

4.1. Etapas

Las etapas que componen el método tienen como principal objetivo establecer una relación entre trabajadores, herramientas y artefactos. De manera que cada etapa se describirá como un conjunto de actividades que deben ser llevadas a cabo por trabajadores que utilizan herramientas y producen artefactos útiles para la creación de software. Las etapas son:

- *Construcción del proceso de negocio*: en esta etapa el objetivo es crear un modelo del proceso de negocio independiente de computación. El trabajador de esta etapa es el analista del negocio quien es responsable por la especificación del proceso de negocio. Las herramientas utilizadas en la construcción del proceso de negocio son el UML 2.0-AD o BPMN-BPD. El artefacto resultante es la descripción de un proceso de negocio. Aunque no existe un conjunto de reglas que definan la forma en que se construye un proceso de negocio algunas de las siguientes actividades pueden ser realizadas en esta etapa: (i) identificar los actores que participan en el proceso de negocio, (ii) identificar las actividades que llevan a cabo los actores, (iii) identificar almacenes de datos, flujos de datos y mensajes y (iv) establecer la secuencia de actividades, decisiones y puntos de inicio y término de los flujos de trabajo que permiten describir el proceso de negocio
- *Incorporación de Requisitos de Seguridad*: el objetivo de esta etapa es agregar, a la especificación anterior, los requisitos de seguridad. Es necesario que el analista de negocios mantenga el punto de vista independiente de computación y, de este modo, incorpore esta perspectiva en relación con la

seguridad. El único trabajador en esta etapa es el analista de negocios. Las herramientas utilizadas son las propias para la construcción del proceso de negocio, BPSec-Profile y BPSec-Tool. El artefacto resultante es la descripción preliminar del proceso de negocio que incluye especificaciones de seguridad. Las actividades más importantes que se llevan a cabo en esta etapa son: (i) identificar los puntos vulnerables en el proceso de negocio. Esta actividad debe ser ejecutada considerando el punto de vista del negocio, (ii) identificar el o los requisitos de seguridad que satisfacen la necesidad de protección de los puntos vulnerables identificados anteriormente, (iii) establecer los permisos en relación con las especificaciones de control de acceso (iv) definir la prioridad requisitos de seguridad que han sido identificados

- *Refinamiento*: el objetivo de esta etapa es hacer una revisión de las especificaciones de los requisitos de seguridad indicados en la etapa anterior para determinar su pertinencia y consistencia. En esta etapa participan el analista de negocios y el experto en seguridad. Debido a que el rol principal lo desempeña el experto en seguridad, que revisa las especificaciones de seguridad realizadas en la etapa anterior, se debe poner especial atención en evitar un sesgo técnico en las especificaciones finales. Las herramientas utilizadas son las mismas de la etapa anterior, esto es, UML 2.0-AD o BPMN-BPD, BPSec-Profile y BPSec-Tool. Los artefactos resultantes son la especificación final del proceso de negocio seguro y el repositorio de procesos de negocio seguro actualizado. Las actividades más importantes que se llevan a cabo en esta etapa son: (i) revisar la especificación de cada requisito de seguridad realizada por el analista de negocios con el objeto de eliminar aquellas que en una segunda revisión parezcan innecesarias, (ii) revisar las prioridades establecidas para los requisitos especificados, (iii) revisar los permisos otorgados a los objetos en el ámbito de la especificación de un requisitos de seguridad de control de acceso
- *Transformaciones*: el objetivo de esta etapa es obtener, desde la especificación de un proceso de negocio seguro, un subconjunto de las clases de análisis y casos de uso. Esta etapa no requiere trabajadores puesto que se realiza en forma automática a través de BPSec-Tool. Los artefactos resultantes son: clases de análisis, casos de uso y el repositorio de SBP actualizado.

4.2. Trabajadores

Los tipos de trabajadores que se identifican en M-BPSec son el analista de negocios y el experto en seguridad.

El *analista de negocio* es el responsable por la especificación del proceso de negocio. El énfasis de dicha especificación está sobre el negocio propiamente dicho. Se debe evitar, en la medida de lo posible, las especificaciones que contengan elementos propios de soluciones tecnológicas. Esto porque se espera que, en este nivel de abstracción, se tenga un punto de vista independiente de computación en relación con el problema que se está describiendo. El analista de negocios también es el responsable por las especificaciones de los requisitos de seguridad, que de acuerdo con su punto de vista.

El segundo trabajador es el *experto en seguridad*. Este trabajador es el responsable por refinar las especificaciones de seguridad que ha indicado el analista del negocio. El perfil del experto en seguridad corresponde a un trabajador que sea capaz de verificar, validar y completar las especificaciones hechas por el analista de negocios, de manera que dichas especificaciones se puedan transformar en soluciones concretas.

4.3. Herramientas

En esta sección se describen las herramientas que son utilizadas durante la aplicación de M-BPSec. Hemos incluido en esta categoría lenguajes que permiten especificar procesos de negocio y elementos propios del desarrollo de software. Las herramientas son:

- una *notación* que permita describir un proceso de negocio, este caso, UML 2.0-AD o BPMN-BPD
- la extensión, *BPSec-Profile*, que permite incorporar requisitos de seguridad en procesos de negocio descritos con UML 2.0-AD o BPMN-BPD
- el *diagrama de clases* de UML que será obtenido en forma automática desde la

especificación de un proceso de negocio seguro
- el *diagrama de casos de uso* de UML que será obtenido de manera automática a partir del proceso de negocio seguro
- *BPSec-Tool* una herramienta que se ha diseñado con el objeto permitir: (i) la especificación de requisitos de seguridad usando UML 2.0-AD o BPMN-BPD, (ii) obtener automáticamente clases de análisis y casos de uso y (iii) actualizar los datos contenidos en el repositorio de SBP. Desde el punto de vista tecnológico, BPSec-Tool se implementó como una arquitectura de tres capas en que la capa de de presentación se construyó con Microsoft Visio®, la capa de aplicación con C# y la capa de almacenaje con Microsoft-Access®.

4.4. Artefactos

Los artefactos que se describen en esta sección son los que se obtienen a partir de la aplicación de M-BPSec. Estos son:

- una descripción de un proceso de negocio que puede ser construida con UML 2.0-AD o BPMN-BPD
- una descripción de un *proceso de negocio seguro* que corresponde a una especificación de un proceso de negocio que contiene especificaciones de seguridad. Estas especificaciones ha sido incorporadas mediante el uso de BPSec-Profile
- una descripción de las *clases de análisis* que corresponde a un subconjunto de las clases que permiten describir el problema modelado en el SBP. Este modelo clases de análisis se obtiene en forma automática e incluye las clases que se relacionan con especificaciones de seguridad
- una descripción de los *casos de uso* que se obtienen en forma automática desde la especificación del SBP. Estos casos de uso corresponden a un subconjunto de los casos de uso que permiten describir el problema modelado en el SBP
- un *repositorio* que contiene información acerca del proceso de negocio seguro y de los artefactos que son derivados automáticamente desde dicha especificación. Es creado en forma automática a partir de la especificación del SBP. Se actualiza con la información derivada de las transformaciones que se hacen para obtener clases de análisis y casos de uso. Puede ser actualizado en la etapa de Refinamiento sólo en relación con las prioridades y los permisos de control de acceso. Adicionalmente, el repositorio puede ser utilizado para la obtención de información histórica acerca de las especificaciones de SBPs.

5. Un caso de estudio

Este caso de estudio ha sido desarrollado en una cooperativa dedicada a la distribución de energía eléctrica en sectores rurales. La cooperativa Coopelan Ltda. (www.coopelan.cl), opera desde al año 1957 y en la actualidad mantiene 2.200 Km. de línea eléctrica con los que abastece a más de 12.000 clientes. En los últimos años ha incorporado la comercialización de bienes y servicios, tanto para sus clientes de energía eléctrica (socios de la cooperativa) como para el público en general. Desde el punto de vista organizacional, la cooperativa está compuesta por el área técnica, relacionada con la distribución de energía eléctrica, el área comercial que tiene que ver con la comercialización de bienes y servicios y el área administrativa. En total cuenta con 70 trabajadores.

Debido a que los principales clientes de la cooperativa viven en sectores rurales, la forma en que actualmente se realiza el cobro por consumo de energía eléctrica presenta dos problemas: (i) la distribución del recibo o boleta en que se detalla el consumo de energía eléctrica y (ii) el cobro de dicha deuda. Los analistas del negocio han modificado la forma tradicional del proceso de negocio asociado a la recuperación de deudas por consumo de energía, incorporando un aviso electrónico de las deudas y el pago electrónico. Con esta medida complementaria incrementarán los índices de recuperación de deudas. La cooperativa no cuenta con la capacidad técnica y operativa para la recepción de pagos electrónicos (a través de Internet). Por esta razón ha decidido incorporar un cobrador externo que lleve a cabo esta tarea.

El proceso de negocio que describiremos como parte de nuestro caso de estudio se denomina *Pagos de consumos de energía eléctrica.* Este caso de estudio se realizó con la colaboración de analistas de negocio de la cooperativa. Para el desarrollo del caso de estudio hemos aplicado M-

BPSec. El resultado es de las tres primeras etapas es el SBP "*Pagos de consumos de energía eléctrica*" que se muestra en la Figura 3.

El detalle de la aplicación de las etapas de M-BPSec es:

- La etapa *Construcción del proceso de negocio*, básicamente consiste en elaborar el proceso de negocio y es realizada por el analista de negocio. En este caso se utilizó UML 2.0-AD para describir el proceso de negocio. Se identificaron las particiones "Institución Externa", "Cliente", y "Área de Administración" dividida en "Facturación" y "Caja". El proceso de negocio se inicia cuando se lleva a cabo la actividad "Emitir Factura Consumo" y termina cuando se han recibido los pagos y se actualizan las deudas de los clientes.
- En la etapa *Incorporación de Requisitos de Seguridad*, el analista de negocio, desde su perspectiva, identifica áreas vulnerables del proceso de negocio. Previamente se llevó a cabo una reunión en que se explicó el significado de los requisitos de seguridad que están considerados en BPSec-Profile. El analista de negocio identificó vulnerabilidades en: (i) la información que es enviada desde "Cobrador de e-pagos" hacia "Facturación" para lo cual se especificó No Repudio (ii) en la información relacionada con los pagos recibidos en "Caja" para lo cual se especificó Integridad en grado alto y (iii) en las actividades y la información relacionada con la partición "Facturación" para lo cual se especificó Control de Acceso.
- La etapa de *Refinamiento* fue llevada a cabo por el analista de negocio en conjunto con el experto en seguridad. Se analizaron y consensuaron las especificaciones de requisitos de seguridad. Se agregó Registro de Auditoría sobre las especificaciones de No Repudio y Control de Acceso.
- Finalmente, la etapa *Transformaciones*, fue aplicada sobre la especificación del SBP. Esta etapa se lleva a cabo en forma automática utilizando BPSec-Tool. Los resultados obtenidos fueron el diagrama de clases de análisis que se muestra en la Figura 4, el caso de de uso relacionado con el proceso de negocio propiamente dicho y los casos de uso relacionados con las especificaciones de Integridad sobre *Pagos*, No Repudio sobre el mensaje *e-pagos* (ver Figura 5) y Control de Acceso sobre Facturación.

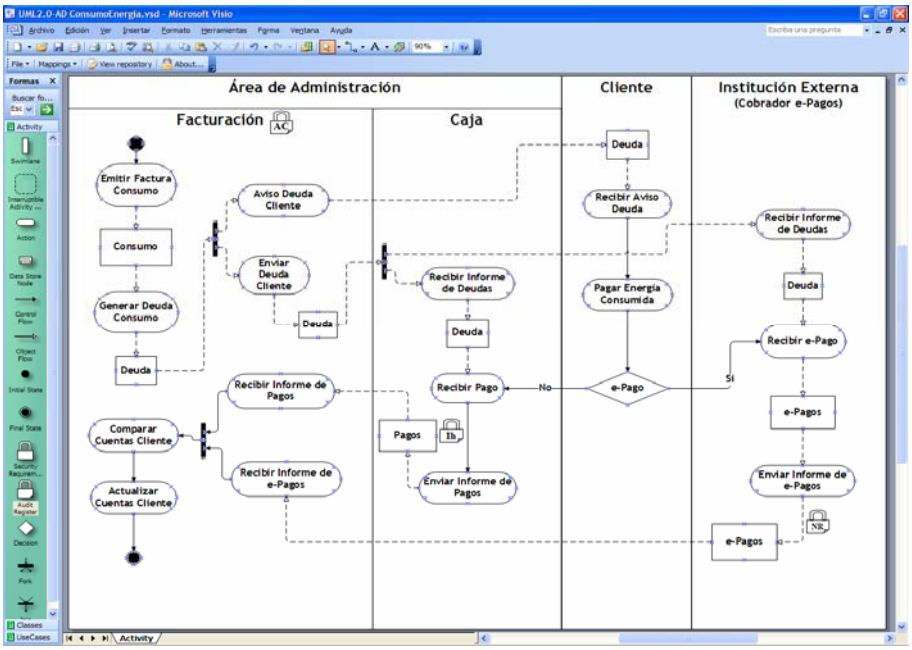

Figura 3. Pagos de consumos de energía eléctrica

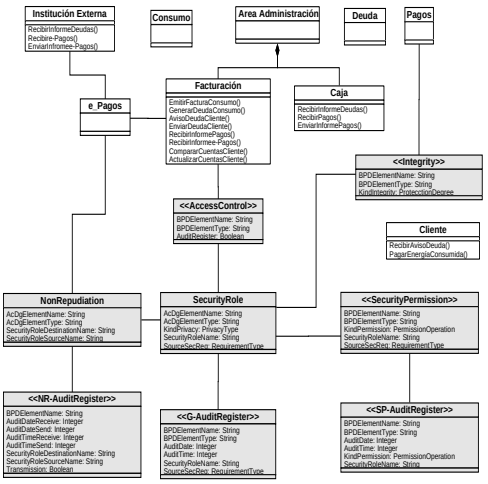

Figura 4. Clases de análisis derivadas del SBP

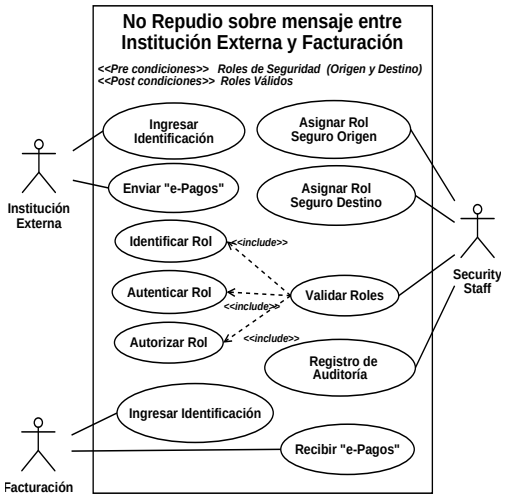

Figura 5. Caso de uso para No Repudio

Tanto el proceso de negocio seguro como las clases de análisis y los casos de uso han sido utilizados como entradas en el proceso de desarrollo de software con el que Coopelan lleva a cabo la creación de software.

6. Conclusiones

Un proceso de negocio que contiene requisitos de seguridad permite incorporar una nueva perspectiva con respecto a la seguridad en un proceso de la creación del software. No obstante, esta especificación en sí misma no es suficiente. La obtención de requisitos de seguridad en este nivel de abstracción se debe enmarcar un método que permita que garantizar la adquisición de requisitos y uso adecuado de los artefactos derivados.

M-BPSec, aplicado de manera regular y sistemática permite: (i) hacer una especificación de requisitos de seguridad en un proceso de negocio descrito con UML 2.0-AD o BPMN-BPD y (ii) obtener artefactos UML, clases de análisis y casos de uso, a través de los cuales es posible alcanzar modelos más concretos que incluyan la seguridad.

Creemos que M-BPSec satisface los criterios de evaluación de los métodos del elicitación de requisitos, como por ejemplo: contar con una herramienta automatizada que dé soporte al método, tener un alto nivel de aceptación por parte de los interesados, producir salidas gráficas, y tener una baja curva de aprendizaje.

Los pasos siguientes en nuestra investigación se orientan hacia la aplicación de M-BPSec sobre problemas de mayor complejidad para observar resultados que nos permitan enriquecer el método y mejorar los artefactos.

Agradecimientos

Agradecemos al señor Eduardo Robba de Coopelan Ltda. por su valiosa colaboración en el desarrollo del caso de estudio. Esta investigación es parte de los proyectos DIMENSIONS (PBC-05-012-1) y MISTICO (PBC06-0082), ambos parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha, España; COMPETISOFT (506AC287) concedido por CYTED y ESFINGE (TIN2006-15175-C05-05/) otorgado por la Dirección General de Investigación del Ministerio de Ciencia y Tecnología, España.

Referencias

[1] Backes, M., Pfitzmann, B., y Waider, M. Security in Business Process Engineering, International Conference on Business Process Management (BPM), Eindhoven, Netherlands., (2003), pp. 168-183.

[2] Diallo, M. H., Romero-Mariona, J., Sim, S. E., Alspaugh, T. A., y Richardson, D. J. A Comparative Evaluation of Three Approaches to Specifying Security Requirements, 12th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ), Luxembourg, (2006).

[3] Firesmith, D. Specifying Reusable Security Requirements, Journal of Object Technology, Vol. 3 (1), January-February., (2004), pp. 61-75.

[4] Herrmann, G. y Pernul, G. Viewing Business Process Security from Different Perspectives, 11th International Bled Electronic Commerce Conference, Slovenia., (1998), pp. 89-103.

[5] Herrmann, P. y Herrmann, G. Security requirement analysis of business processes, Electronic Commerce Research, Vol. 6 (3-4), (2006), pp. 305-335.

[6] Jacobson, I., Booch, G., y Rumbaugh, J. The Unified Software Development Process, (1999) 463 p.

[7] Maña, A., Montenegro, J. A., Rudolph, C., y Vivas, J. L. A business process-driven approach to security engineering, 14th. International Workshop on Database and Expert Systems Applications (DEXA). Prague, Czech Republic., (2003), pp. 477-481.

[8] Mead, N. R. Experiences in Eliciting Security Requirements, CrossTalk: The Journal of Defense Software Engineering, Vol. 19 (12), (2006).

[9] Mellado, D., Fernández-Medina, E., y Piattini, M. A Comparative Study of Proposals for Establishing Security Requirements for the Development of Secure Information Systems, Computational Science and Its Applications (ICCSA), Glasgow, UK, (2006), pp. 1044-1053.

[10] Nuseibeh, B. y Easterbrook, S. M. Requirements Engineering: A Roadmap, ICSE 2000, 22nd International Conference on on Software Engineering, Future of Software Engineering Track., Limerick Ireland. ACM., (2000), pp. 35-46.

[11] Object Management Group. MDA Guide Version 1.0.1, 2003.

[12] QVT. Meta Object Facility (MOF) 2.0 Query/View/Transformation Specification, (2005) 204 p.

[13] Rational Software. Rational Unified Process, Best Practices for Software Development Teams, (2001) 21 p.

[14] Rodríguez, A., Fernández-Medina, E., y Piattini, M. Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes, 3rd International Conference on Trust, Privacy and Security in Digital Business (TrustBus), Krakow-Poland, (2006), pp. 51-61.

[15] Rodríguez, A., Fernández-Medina, E., y Piattini, M. A BPMN Extension for the Modeling of Security Requirements in Business Processes, IEICE Transactions on Information and Systems, Vol. E90-D (4), (2007), pp. 745-752.

[16] Rodríguez, A., Fernández-Medina, E., y Piattini, M. Analysis-Level Classes from Secure Business Processes through Models Transformations, 4th International Conference on Trust, Privacy and Security in Digital Business (TrustBus), Regensburg, Germany, (2007).

[17] Rodríguez, A., Fernández-Medina, E., y Piattini, M. Towards CIM to PIM transformation: from Secure Business Processes defined by BPMN to Use Cases, 5th International Conference on Business Process Management (BPM), Brisbane, Australia, (2007).

[18] Röhm, A. W., Pernul, G., y Herrmann, G. Modelling Secure and Fair Electronic Commerce, 14th. Annual Computer Security Applications Conference, Scottsdale, Arizona, (1998), pp. 155-164.