Requisitos de Seguridad en Procesos de Negocios

Alfonso Rodríguez Ríos[1], Eduardo Fernández-Medina[2], Mario Piattini[2]

[1] Universidad del Bio Bio, Departamento de Auditoría e Informática,
La Castilla S/N, Chillán Chile.
alfonso@ubiobio.cl

[2] Universidad Castilla-La Mancha, Departamento de Informática,
Ronda de la Universidad 5, Ciudad Real, España.
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen: Los Procesos de Negocios son considerados un recurso esencial para que las empresas puedan optimizar y asegurar su calidad obteniendo ventajas respecto de sus competidores. El modelado de Procesos de Negocios, en consecuencia, resulta relevante ya que permite representar la esencia del negocio. Una notación para modelar negocios debe ser capaz de capturar la mayor parte de los requisitos del negocio. Hemos podido comprobar que los requisitos de seguridad han sido poco considerados en las notaciones más utilizadas actualmente para modelar procesos de negocios. En este trabajo presentamos los aspectos de seguridad que han sido escasamente abordados en el modelado de procesos de negocios, una revisión de las principales notaciones utilizadas para el modelado y una propuesta para representar los requisitos de seguridad considerando el dominio de los expertos en el negocio.

1 Introducción

Los procesos de negocios, entendidos como un conjunto de procedimientos o actividades que, colectivamente, llevan a cabo los objetivos o políticas del negocio [34], constituyen la esencia de la competitividad en las organizaciones contemporáneas. Cada etapa en la construcción de los mismos cobra, por lo tanto, especial relevancia. De ellas la especificación de requisitos, concebida como un proceso de facilitación efectiva de la comunicación que se necesita entre los diferentes interesados [23], permite asegurar, en buena medida, que el proceso de negocios será útil y funcional para los objetivos de la organización.

Sin embargo, la noción de seguridad ha sido a menudo descuidada en los modelos de procesos de negocios, ya que usualmente se concentran en el modelado del proceso propiamente dicho [4]. Esto se debe a que el experto en el dominio del proceso de negocios no es un especialista en seguridad [15]. Tampoco los ingenieros de requisitos están entrenados del todo en seguridad y los pocos que han sido entrenados, sólo tienen una idea general de los mecanismos de la arquitectura de seguridad tales como claves de acceso y encriptación, en lugar de los requisitos reales de seguridad [11]. No obstante, muchos aspectos de seguridad pueden ser modelados desde la visión del usuario o el analista de negocios ya que está demostrado que es común que los usuarios finales sean capaces de expresar sus necesidades de seguridad en ese nivel [21], consecuentemente, durante la fase de modelado del negocio los propietarios de los procesos deberían abordar también los requisitos de seguridad [26].

Nuestra propuesta permite a los analistas de negocio especificar tempranamente requisitos de seguridad, sin tener que ahondar en detalles de implementación y/o arquitectura. Creemos que una adecuada notación facilitará esta labor; para ello hemos extendido la notación propuesta por BPMI (Business Process Management Initiative), incorporándole determinados aspectos de seguridad que resultan comprensibles y pertinentes.

El artículo está organizado como sigue: en la sección 2 presentamos el modelado de la seguridad en los procesos de negocios considerando las principales notaciones utilizadas en la industria. En la sección 3, mostraremos la extensión propuesta que permita representar requisitos de seguridad desde la perspectiva del analista del negocio y finalmente en la sección 4 presentamos un ejemplo donde se puede apreciar la aplicación de la propuesta.

2 Modelado de seguridad en procesos de negocios

A pesar de la importancia que supone la seguridad para los procesos de negocios, el modelado de la seguridad en éstos presenta dos problemas fundamentales. Por una parte, el modelado propiamente tal ha resultado inadecuado porque generalmente quienes especifican los requisitos de seguridad son ingenieros de requisitos que han tendido, accidentalmente, a reemplazarlos por restricciones específicas de arquitectura [11]. Por otro

lado, y esto ha resultado ser lo más común, la seguridad ha sido integrada en forma tardía, a menudo durante la implementación real del proceso [4] o más tarde aún, en la fase de administración del sistema. Esto se explica, en parte, porque, a pesar de ser la seguridad un aspecto transversal que afecta tempranamente a los componentes de una aplicación, no es bien entendida y además hay carencia de herramientas que soporten la ingeniería de seguridad [19].

Por otra parte, resulta más o menos evidente que un enfoque orientado al proceso también debiera considerar la información de seguridad en la gestión de los procesos de negocios [1]. En este sentido, modelar la seguridad en un proceso de negocios, implicará capturar los requisitos de seguridad, lo cual debiera hacerse considerando las perspectivas: *estática*, sobre la seguridad de la información procesada, *funcional,* sobre los procesos del sistema, *dinámica,* sobre los requisitos de seguridad considerando el ciclo de vida de los objetos involucrados en el proceso de negocio, *organizacional,* usada para relacionar las responsabilidades de los actores con los procesos de negocios y de *procesos de negocios*, la que corresponde a una visión integrada de todas las perspectivas con un alto grado de abstracción [15].

Si bien los requisitos funcionales de seguridad tienden a variar entre aplicaciones de diverso tipo, no se puede decir lo mismo de los requisitos de seguridad, ya que cualquier aplicación en un alto nivel de abstracción tendrá la misma clase de valoración y potencialmente vulnerabilidad de sus activos [12]. De allí que los requisitos de seguridad que nos interesa representar sean del mismo tipo para todas las organizaciones ya que en este nivel no se está pensando en la implementación. Además es claro que la identificación temprana de requisitos, en este caso específico los requisitos de seguridad, permite ahorrar costes de desarrollo y mantenimiento, por tanto, resulta evidente la utilidad de contar con una notación en la que sea posible especificar requisitos de seguridad.

Nuestra propuesta se centra en dos puntos fundamentales. Por una parte es necesario establecer qué notación se utilizará y por otro lado será necesario decidir sobre los aspectos de seguridad que van a ser considerados.

2.1 Notaciones para el modelado de procesos de negocios

En el modelado de proceso de negocios el objetivo principal es producir una descripción de la realidad, por ejemplo la forma en que se lleva a cabo una transacción comercial, que permita entenderla y eventualmente modificarla con el propósito de incorporar mejoras. En consecuencia, es importante contar con una notación que permita modelar con la mayor claridad posible la esencia del negocio. Esta notación debe permitir incorporar diversas perspectivas, lo que puede dar origen a diversos diagramas, en que queden reflejadas reglas, metas, objetivos del negocio y tanto relaciones como interacciones [9]. Una buena parte del éxito del modelado tiene que ver con la capacidad de expresar las diversas necesidades del negocio y disponer de una notación en que puedan ser descritas. De ahí que la elección de un enfoque y/o una notación de modelado deba hacerse considerando las propiedades del objeto a modelar, es decir, del proceso de negocios, las características del entorno y las razones subyacentes para el uso [6].

Entre las técnicas que se han usado para el modelado de negocios se encuentran: diagramas de flujo, la familia de técnicas denominadas IDEF (Integration DEfinition for Function modeling), redes de Petri, simulación, técnicas basadas en el conocimiento (inteligencia artificial) y diagramas de actividad de roles (Rol Activity Diagrams) [14].

En la actualidad, y de acuerdo con el estado de la industria del modelado de procesos de negocios [20, 22], es posible identificar a Unified Modeling Language (UML) [24] y Business Process Modeling Notation (BPMN) [8] entre los principales estándares, por lo que concentraremos nuestro análisis en ambas notaciones.

El uso de UML se encuentra bastante difundido en relación al modelado de procesos de negocios [9, 17, 19, 21, 30, 32], ya que es un lenguaje consolidado, fácil de aprender y que permite una comunicación fluida entre los diversos actores acerca del modelo. Sin embargo, UML presenta tres problemas que pueden menoscabar el modelado de procesos de negocios [13]; ya que, (i) como UML no ha sido diseñado para modelar procesos de negocios puede suceder que algunos aspectos del modelado no sean tratados adecuadamente o sean vistos con una orientación distinta de la que necesita un experto en el dominio del negocio, por otra parte, (ii) predispone un enfoque orientado a objetos en la concepción de los procesos de negocios en que los objetos del negocio debieron ser definidos de antemano limitando así la visión de los procesos

orientados al negocio en que primero se identifican los flujos de control y de mensajes para luego definir, implícitamente, los objetos del modelo de negocios, y por último (iii) UML suele estar más orientado a los arquitectos de sistemas y diseñadores de software, ya que UML ha sido desarrollado para facilitar la creación de software pensando en un público eminentemente técnico.

Por su parte, BPMN es una propuesta nueva cuya notación considera un único diagrama para la representación de los procesos (BPD, Business Process Diagram), el cual fue diseñado pensando en facilitar su uso y entendimiento y para ofrecer una fuerza expresiva que permita modelar complejos negocios, asignándolos con naturalidad a lenguajes de ejecución como BPEL4WS (Business Process Execution Language For Web Services). Para ello complementa la notación con un lenguaje de modelado (BPML, Business Process Modeling Language) y un lenguaje de consulta (Business Process Query Language, BPQL) [25].

En este trabajo usaremos BPMN porque consideramos que, si bien existe más de una razón para usar esta notación [25] la más importante es que ofrece una técnica de modelado que resulta rápidamente entendible por todos los usuarios del negocio, desde los analistas de negocios que crean borradores de los procesos hasta los desarrolladores técnicos responsables de la implementación tecnológica de esos procesos y finalmente la gente de negocios que administrará y controlará esos procesos. Además, crea una estandarización que conecta el diseño con la implementación de procesos de negocios [8, 35].

2.2 Requisitos de seguridad en el modelado de procesos de negocios

Para modelar requisitos de seguridad en procesos de negocios hay que tener presente dos aspectos que estimamos importantes. Primero, no hay que perder de vista que quien modela el proceso es un experto en el dominio del negocio y que por lo tanto tiene una idea de seguridad exenta de tecnicismo y perturbaciones propias de quien está pensando en la implementación o en soluciones tecnológicas, y segundo, que por la misma razón anterior, hay que considerar la parte de seguridad que esté más consensuada a nivel de usuarios no especialistas y cuyo significado y representación sea más o menos estándar.

Los trabajos que se relacionan con especificaciones de seguridad por parte de los expertos en el dominio del negocio son; (i) escasos [4, 15,

21], (ii) se orientan a la seguridad en la transacción [28] o (iii) apuntan directamente a los sistemas de información en general [31].

Como existe una estrecha relación entre los procesos de negocios y los flujos de trabajo (workflows) [27, 33], hemos puesto revisado los trabajos que se relacionan con seguridad y workflow [2, 3, 7, 36] y los de sistemas de gestión de workflow (WfMS) [16, 18]. Hemos podido constatar que la mayoría de ellos pone énfasis en el control de acceso mediante la utilización del acceso basado en roles, RBAC [5, 7, 10, 29].

Consecuentemente, y teniendo en cuenta que los requisitos de seguridad deben resultar asimilables de manera sencilla por parte de los analistas del negocio y a su vez tener un significado claro para los expertos en seguridad, hemos considerado (i) *control de acceso*, que se entenderá como el grado en que el sistema limita el acceso a sus recursos sólo a los externos autorizados[1], (ii) *auditoría de seguridad*, que corresponde al grado en que el personal de seguridad recogerá, analizará e informará acerca del estado y uso de mecanismos de seguridad y (iii) *privacidad*, que es el grado en que las partes no autorizadas están impedidas de obtener información sensible[2] [11, 12].

3 Extensión de BPMN para el modelado de seguridad

Para capturar los requisitos de seguridad en el modelado de procesos de negocios es conveniente contar con una notación, que deberá ser soportada por un conjunto de conceptos gráficos, que permita representar la semántica de seguridad [15]. Como ya hemos indicado, BPMN ofrece una orientación hacia el dominio de los analistas de negocios, por lo que sería posible capturar requisitos de seguridad en este nivel de abstracción. BPMN no considera explícitamente mecanismos para representar estos requisitos, sin embargo, de entre el conjunto de símbolos utilizados para la construcción del diagrama de procesos de negocios (BPD) [8], los *artefactos* pueden servir para expresar dichos requisitos. Estos fueron diseñados para extender la notación básica del modelado agregándoles la posibilidad de representar situaciones específicas [35]. No obstante, consideramos que una identificación explícita de ellos facilita el modelado y contribuye a una mejor interpretación por parte de los especialistas en seguridad.

[1] Por ejemplo: usuarios, programas, procesos, dispositivos u otros sistemas.
[2] Por ejemplo: identidad de usuarios, datos o comunicaciones privadas.

El mecanismo de extensión previsto por BPMN permite agregar marcas o indicaciones a los elementos gráficos ya definidos [8]. En nuestra propuesta (ver Figura 1) hemos asociado a cada requisito de seguridad, explicados en la sección 2.2, un símbolo para representarlo de manera relativamente estándar.

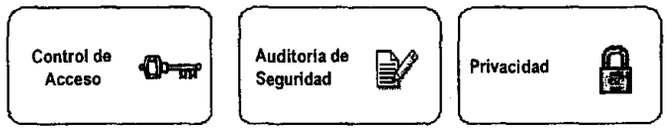
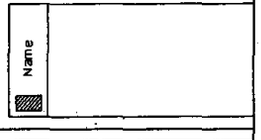
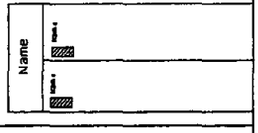


Figura 1: Notación asociada a requisitos de seguridad

La representación de esos requisitos de seguridad en un modelo de procesos de negocios, por parte de los expertos de negocios, se entenderá como la necesidad de incorporar (a través del proceso de desarrollo de sistemas) los mecanismos y la tecnología que permita satisfacer la intención de control de acceso, auditoría de seguridad y privacidad que ha sido especificada.

Los elementos del BPD sobre los cuales proponemos considerar la representación de los requisitos de seguridad son los que se muestran en la Tabla 1. El rectángulo remarcado que hemos incorporado a la notación de BPD indica el lugar en que el requisito de seguridad debe ser representado.

Elemento	Notación
Participante: Representa a un actor o rol en un proceso de negocios. Gráficamente, es una banda en que están contenidos otros elementos del BPD como por ejemplo una Actividad.	
División: Corresponde a subdivisiones de un Participante y se extienden a lo largo de él en forma horizontal o vertical. La División es utilizada para organizar y categorizar Actividades.	
Actividad: Es el término genérico que se usa para identificar el trabajo que realiza una empresa. Esta categoría incluye procesos, subprocesos y tareas	

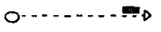
<table>
<tr><td colspan="2">Flujo de Mensajes: Corresponde a información que es transferida durante un proceso de negocios entre dos Participantes que están preparados para enviar o recibir mensajes. Un flujo de mensaje puede ser representado entre dos actividades siempre y cuando se encuentren en distintos Participantes.</td><td>  </td></tr>
<tr><td rowspan="2">Artefacto: Es usado para entregar información adicional acerca del proceso de negocios y no tiene incidencia en la secuencia o flujo del mismo</td><td>Objeto de datos: Proporciona información acerca de lo que hace el proceso. Puede tomar la forma de documentos, datos y otros objetos que son usados y actualizados por el proceso. Por lo general aparece asociado a Actividades o Flujos de Secuencia.</td><td>  </td></tr>
<tr><td>Agrupación: Es un mecanismo visual que reúne elementos de un proceso de negocios. El objetivo principal es destacar ciertas secciones del diagrama con propósitos de documentación y/o análisis.</td><td>  </td></tr>
</table>

Tabla 1: Elementos de BPD en que se incorporan requisitos de seguridad

A continuación describiremos la relación entre cada uno de los elementos del BPD (ver tabla 1) con los requisitos el control de acceso, auditoría de seguridad y privacidad.

- *Participante / División*: Estos elementos serán descritos juntos pues ambos especifican roles. Debido a que *Participante* y *División* incluyen a otros elementos del BPD, en los que también se puede indicar requisitos de seguridad, es necesario verificar la coherencia entre las especificaciones que se hagan en *Participante* o *División* y los elementos que contiene.
  - *Control de Acceso*: Indica que, para este proceso de negocios en particular, las actividades asociadas al *Participante* o *División* son más sensibles por lo que es necesario intensificar los mecanismos de control de acceso. Dicha especificación debe complementarse

con el artefacto *Anotaciones* para indicar el grado de seguridad requerido (alto, medio o bajo)[3].

- *Auditoría de Seguridad*: Indica que todos eventos *relacionados* con *Participante* o *División* serán registrados para posterior análisis en relación a la auditoría de seguridad. Si se usa el artefacto *Anotación*, la auditoría de seguridad se limitará sólo a los eventos allí indicados.
- *Privacidad*: Este requisito indica la necesidad de impedir la obtención de información sensible (por ejemplo la identidad del *Participante* o *División*) por partes no autorizadas. Es necesario agregar información a través del artefacto *Anotación* en donde se especificará el grado de protección de la privacidad que se desea (alta, media o baja).

- *Actividad*: Cuando se especifica algún requisito de seguridad para este elemento del BPD, se tiene que poner atención en las especificaciones de seguridad que tengan los elementos que la contienen (*Participantes, Divisiones, Agrupaciones u otras Actividades*). De igual forma, se debe tener cuidado con las especificaciones que existan en los elementos que estén contenidos en una *Actividad* (otras *Actividades* u *Objetos de Datos*). Esto con el propósito de mantener la coherencia en las especificaciones de los requisitos de seguridad.
  - *Control de Acceso:* Indica que se debe limitar el acceso a la ejecución de la actividad. Este requisito de seguridad es válido sólo si el *Participante* o *División*, en que está contenida la *Actividad*, no tiene especificación de control de acceso. La especificación de control de acceso se debe complementar con *Anotaciones* en donde se especifique el grado de seguridad requerido (alto, medio o bajo).
  - *Auditoría de Seguridad*: Indica que se requiere registrar los eventos que ocurren en la *Actividad*. Si se usa el artefacto *Anotación* para indicar los eventos sobre los que se hará auditoría de seguridad, se entenderá acotado sólo a aquellos que han sido indicados.
  - *Privacidad:* Este requisito de seguridad no será representado en una Actividad porque nos parece demasiado concreto en relación al nivel de abstracción en que se están haciendo estas especificaciones.

---

[3] Niveles abstractos de seguridad exigida que representan la mayor o menor criticidad que percibe el analista de negocios respecto del control de acceso o privacidad según sea el caso.

- *Flujo de mensaje*: Los requisitos de seguridad que se especifican para este elemento se relacionan con el contenido, origen y destino del Flujo de Mensajes.
  - *Control de Acceso*: La indicación de este requisito de seguridad debe interpretarse como la necesidad de proteger el Flujo de Mensaje. Ello implica que se debe validar a los Participantes cuando se envíe y reciba el flujo de mensajes. Se debe complementar con el artefacto Anotación para indicar el grado de seguridad requerida (alto, medio o bajo).
  - *Auditoría de Seguridad*: La indicación de este requisito de seguridad implica que se desea registrar todos eventos relacionados con el envío y recepción del Flujo de Mensaje.
  - *Privacidad*: Establece la necesidad de proteger la identidad de los participantes y la confidencialidad del contenido del Flujo de Mensaje. Se debe complementar con el artefacto *Anotación* para especificar el grado de protección requerido (alto, medio o bajo).

- *Objeto de Datos:* Los requisitos de seguridad para este elemento están relacionados con el contenido del Objeto de Datos.
  - *Control de Acceso:* Este requisito de seguridad no se especifica directamente sobre Objeto de Datos. El control de acceso puede extenderse desde la especificación que se hizo en el Participante o División que lo contiene o a través de las Actividades que lo envían o reciben.
  - *Auditoría de Seguridad*: La indicación de este requisito de seguridad implica que se desea registrar todos eventos relacionados con el envío y recepción del *Objeto de Datos.*
  - *Privacidad*: Establece la necesidad de mantener la confidencialidad del contenido del *Flujo de Datos.* Se debe complementar con el artefacto *Anotación* para especificar el grado de protección requerido (alto, medio o bajo).

- *Agrupación*: Por definición una *Agrupación* puede incluir a cualquiera de los elementos del BPD descritos en la Tabla 1. Por esto, la indicación de requisitos de seguridad que se haga sobre *Agrupación* se propagará a todos los elementos que involucra. En tal caso se debe considerar las especificaciones particulares de cada elemento que agrupa de manera que no se produzcan inconsistencias ni contradicciones.

4 Caso de estudio usando la propuesta de BPMN extendido

En la Figura 2 se muestra un ejemplo de un diagrama de proceso de negocios, que ha sido especificado usando BPMN y la extensión propuesta, en que se describe un proceso de aceptación, revisión y preparación para publicación de artículos escritos por alumnos del Departamento de Auditoría e Informática (DAI) de la Facultad de Ciencias Empresariales en la Universidad del Bio Bio. Anualmente se edita una revista que contiene los mejores trabajos.

El proceso es llevado a cabo por tres participantes: *Alumno*, que prepara el artículo para enviarlo a la revista y eventualmente lo corrige si el artículo ha sido aceptado, *Editor* que prepara los artículos para ser enviados a revisión, quitándole la información de los autores y agregándole una pauta para evaluación, ordena los artículos de acuerdo a la calificación obtenida, eventualmente los manda para corrección, y prepara un borrador con los artículos que serán publicados y *Revisor* que en el plazo de siete días deberá revisar los artículos y completar una pauta de evaluación con la que deberá devolverlos al *Editor*.

Se han incorporado requisitos de seguridad de control de acceso en el flujo de mensaje que se produce entre los participantes *Alumno/Editor* y *Editor/Revisor*, lo que implica validar a los participantes para que el flujo de mensaje pueda ser enviado y recibido. También se ha especificado control de acceso sobre la actividad "*Revisión de correcciones*" que lleva a cabo el *Alumno* y "*Preparar artículo para revisión*" que ejecuta Editor, con lo que se limita la ejecución sólo a los participantes *Alumno y Editor* respectivamente. Sobre el participante *Editor* se ha especificado control de auditoría acotándolo al envío/recepción de flujos de mensaje y a la actividad "*Preparar artículo para revisión*". Por último se ha especificado privacidad para el participante *Revisor*. indicando que el grado de protección debe ser alto, lo que significa que su identidad debe permanecer protegida.

Si bien los requisitos de seguridad deben tener una expresión concreta en la implementación del proceso de negocios, consideramos que ésta es una primera etapa que debía ser definida. A partir de aquí se podrá establecer la correlación de la especificación en este nivel con la implementación.

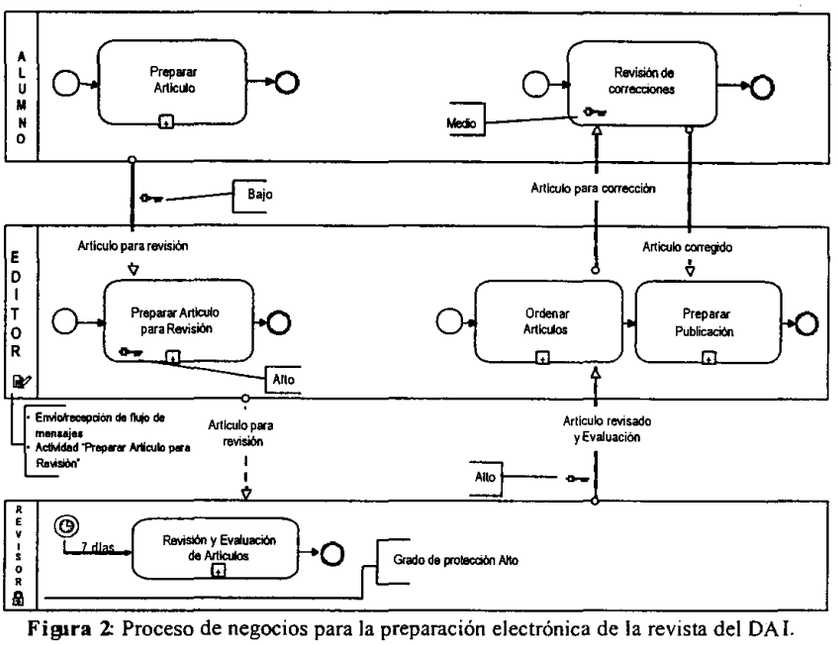


Figura 2: Proceso de negocios para la preparación electrónica de la revista del DAI.

5 Conclusiones

El modelado de procesos de negocios adquiere mayor importancia debido al impacto que puede llegar a tener en la competitividad de la empresa. Nuestro trabajo considera que se debe poner mayor atención en la especificación de requisitos del negocio en altos niveles de abstracción porque creemos que el problema no sólo debe centrarse en una buena solución basada en tecnologías de información. La seguridad es uno de los aspectos que se ha sido considerado más cercano a la implementación que al negocio mismo. Creemos que pue de mejorarse el desempeño de los procesos de negocios si se capturan tempranamente los requisitos de seguridad. Hemos propuesto una extensión a BPMN que entrega a los expertos en negocios un vehículo eficiente para expresar los requisitos de seguridad Los trabajos futuros deberán profundizar sobre aspectos relacionados con la interpretación e implementación de los requisitos de seguridad por parte de los expertos.

Agradecimientos

Esta investigación es parte de los proyectos MESSENGER (PCC-03-003-1) financiado por la "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (España), CALIPO (TIC2003-07804-C05-03) y RETISTIC (TIC2002-12487-E) concedidos por la "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España).

Referencias

[1] Anttila, J., Kajava, J. and Varonen, R.; *Balanced Integration of Information Security into Business Management*, Proceedings of the 30th EUROMICRO Conference. (2004). p:558-564.

[2] Atluri, V.; *Security for Workflow Systems*, Information Security Technical Report Vol. 6 (2) (2001). p:59-68.

[3] Atluri, V. and Huang, W.-K.; *An Authorization Model for Workflow*, Proceedings 4th symposium on Research in Computer Security LNCS, 1146. Rome, Italy. (1996). p:44-64.

[4] Backes, M., Pfitzmann, B. and Waider, M.; *Security in Business Process Engineering*, International Conference on Business Process Management Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). p:168-183.

[5] Bertino, E., Ferrari, E. and Atluri, V.; *A Flexible model Supporting the Specification and Enforcement of Role-Based Authorizations in Workflow Management Systems*, Proceedings of Second ACM Workshop on Role-Based Access Control, Fairfax (Virginia). (1997). p:1-12.

[6] Bider, I.; *Choosing Approach to Business Process Modeling - Practical Perspective*. In http://www.ibissoft.se/english/howto.pdf. (2003).

[7] Botha, R. A. and Eloff, J. H. P.; *A framework for access control in workflow systems*, Information Management & Computer Security Vol. 9/3. (2001). p:126-133.

[8] BPMN; *Business Process Modeling Notation (BPMN)*, Version 1.0 May 3. In http://www.bpmi.org/. (2004).

[9] Castela, N., Tribolet, J., Silva, A. and Guerra, A.; *Business Process Modeling with UML*, Proceedings of the 3st. International Conference on Enterprise Information Systems. Vol. 2. Setubal, Portugal. (2001). p:679-685.

[10] Chaari, S., Ben Amar, C., Biennier, F. and Favrel, J.; *An Authorization and Access Control Model for Workflow*, 1th International Workshop on COmputer Supported Activity Coordination CSAC 2004. Porto, Portugal. (2004). p:31-40.

[11] Firesmith, D.; *Engineering Security Requirements*, Journal of Object Technology Vol. 2 N° 1 January-February 2003. (2003). p:53-68.

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

[13] Ghalimi, I.; *BPMN vs. UML*. In http://www.intalio.com/education/notes/note.xpg?id=BPMN_vs_UML. (2002).
[14] Giaglis, G. M.; *A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques*, International Journal of Flexible Manufacturing Systems Vol. 13 (2). (2001). p:209-228.
[15] Herrmann, G. and Pernul, G.; *Viewing Business Process Security from Different Perspectives* , 11th International Bled Electronic Commerce Conference "Electronic Commerce in the Information Society". Slovenia. (1998). p:89-103.
[16] Hung, P. and Karlapalem, K.; *A Secure Workflow Model*, Australasian Information Security Workshop (AISW2003). Vol. 21. Adelaide, Australia. (2003). p:33-41.
[17] Jürjens, J., *Secure Systems Development with UML*, Springer Verlag, (2004). 309 p.
[18] Kang, M., Froscher, J., Sheth, A., Kochut, K. and Miller, J.; *A Multilevel Secure Workflow Management System*, 11th International Conference on Advanced Information Systems Engineering LNCS (1999). p:271-285.
[19] Lodderstedt, T., Basin, D. and Doser, J.; *SecureUML: A UML-Based Modeling Language for Model-Driven Security*, UML 2002 - The Unified Modeling Language, 5th International Conference. Vol. 2460. Dresden, Germany. (2002). p:426-441.
[20] Lonjon, A.; *Business Process Modeling and Standardization*, BPTrends In http://www.bptrends.com/(2004).
[21] Maña, A., Montenegro, J. A., Rudolph, C. and 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). p:477-481.
[22] Mega; *Business process Modeling and Standardization*. In http://www.bpmg.org/downloads/Articles/Article-MEGA-BusinessProcessModeling&StandardizationEN.pdf. (2004).
[23] Nuseibeh, B. and 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). p:35-46.
[24] OMG; *Object Management Group*. In http://www.omg.org/. (2004).
[25] Owen, M. and Raj, J.; *BPMN and Business Process Management; Introduction to the New Business Process Modeling Standard*, A Popkin Software, W. P. In http://www.bpmn.org/Documents/6AD5D16960.BPMN_and_BPM.pdf. (2003).
[26] Palkovits, S., Rössler, T. and Wimmer, M.; *Process Modelling - Burden or Relief? Living Process Modelling within a Public Organisation*, ICEIS 2004, Proceedings of the 6th International Conference on Enterprise Information Systems. Porto, Portugal. (2004). p:94-102.
[27] Reijers, H. A.; *Business Process Management Attempted Concepticide?*, IRMA International Conference (2004). p:128-131.
[28] Röhm, A. W., Herrmann, G. and Pernul, G.; *A Language for Modelling Secure Business Transactions*, Proceedings 15th. Annual Computer Security Applications Conference. Computer Society Press., Phoenix, Arizona. (1999). p:22-31.
[29] Sandhu, R. and Samarati, P.; *Authentication, Access Control, and Audit*, ACM Computing Surveys Vol. 28 N°1 March 1996. (1996). p:241-243.

[30] Sparks, G.; *An Introduction to UML, The Business Process Model.* In http://www.sparxsystems.com.au/WhitePapers/The_Business_Process_Model.pdf. (2000).

[31] Tryfonas, T. and Kiountouzis, E. A.; *Perceptions of Security Contributing to the Implementation of Secure IS,* Security and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003) Vol. 250. Athens, Greece. (2003). p:313-324.

[32] Vivas, J. L., Montenegro, J. A. and Lopez, J.; *Towards a Business Process-Driven Framework for security Engineering with the UML,* Information Security: Proceedings of the 6th International Conference, ISC 2003, Bristol, U.K. (2003). p:381-395.

[33] W.M.P. van der Aalst, Hofstede, A. H. M. t. and Weske, M.; *Business Process Management: A Survey,* International Conference on Business Process Management (BPM 2003) Volume 2678 (LNCS). Eindhoven, The Netherlands. (2003). p:1-12.

[34] WfMC, *Workflow Management Coalition: Terminology & Glossary.*, Document Number WFMC-TC-1011, Document Number WFMC-TC-1011, (1999). 65 p.

[35] White, S. A.; *Introduction to BPMN.* In http://www.ebpml.org/bpmn.htm. (2004).

[36] Wu, S., Sheth, A., Miller, J. and Luo, Z.; *Authorization and Access Control of Application Data in Workflow Systems,* Journal of Intelligent Information Systems Vol. 18 (1). (2002). p:71-94.