DEPARTAMENTO DE
INFORMÁTICA

Universidad Técnica Federico Santa Maria

Contacto

CIBSI´05
Departamento de Informática - UTFSM
Casilla 110-V
Valparaíso - Chile

Fono: +56(32) 654 429
Fono: +56(32) 654 424
Fax: +56(32) 797 513
e-mail: cibsi@inf.utfsm.cl
cibsi05@inf.utfsm.cl
URL:http://cibsi05.inf.utfsm.cl

≫ AUSPICIA

Microsoft · software AG · IBM · McAfee · Cisco Systems · Impsat · GALA · Grami · NEOSECURE · ORACLE · Guidance Software

≫ PATROCINA

Biblioteca del Congreso Nacional de Chile · Corporación de Capacitación y Empleo SOFOFA · Sociedad Chilena de Ciencia de la computación

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
DEPARTAMENTO DE INFORMATICA

3ER CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA

DEPARTAMENTO DE
INFORMÁTICA

CIBSI05

27 - 25
NOVIEMBRE
2005

ACTAS

CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA

21 - 25 de Noviembre de 2005

Valparaíso, Chile

ISBN 956-7051-10-0
Actas del
3° Congreso Iberoamericano de Seguridad Informática

CIBSI'05

Prólogo

Tenemos el agrado de poner a disposición de los participantes los trabajos aceptados y presentados en el **Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)** realizado entre el 21 y el 25 de Noviembre del 2005 en la ciudad de Valparaíso, Chile, evento que ha sido organizado por el Departamento de Informática de la Universidad Técnica Federico Santa María (Chile) en conjunto con la Universidad Politécnica de Madrid (España).

De un total de 60 artículos enviados al congreso, se seleccionaron un total de 35 trabajos. De este total, 31 de ellos tenían autores de un solo país, y que se distribuyen de la siguiente manera: Argentina (6), Brasil (2), Colombia (3), Chile (1), España (14), México (4) y Uruguay (1). Además se presentaron otros 4 trabajos con autores de diferentes países, donde en cada uno de ellos al menos existe un coautor español y los demás coautores son de Chile, EE.UU., Francia, Polonia y Uruguay.

Los artículos seleccionados cubren las áreas:

- Criptografía, esteganografía y protocolos de seguridad.
- Seguridad en sistemas, redes, comunicaciones y prevención y detección de intrusos.
- Seguridad en sistemas de información, en la Web y en el comercio electrónico
- Modelos de gestión y auditoría en seguridad

Como parte del programa se han incluido tres charlas magistrales sobre voto electrónico, seguridad en entornos ubicuos y tendencias en criptografía.

También como parte del programa, se organizó en conjunto con la Biblioteca del Congreso Nacional de Chile, en el primer día, un evento sobre seguridad informática en el Estado y se incluyeron 5 charlas técnicas de empresas auspiciadoras tales como Cisco Systems, IBM, McCaffee, Neosecure y Software AG.

Deseamos agradecer primero al Comité de Programa por el esfuerzo realizado en la revisión de todos los artículos y en el proceso de selección de éstos. En segundo lugar agradecer a los patrocinadores y auspiciadores que apoyaron de diferentes formas a producir el evento CIBSI'05. Finalmente agradecer a todos los organizadores. Esperamos que la estadía en Valparaíso y la participación en CIBSI'05 haya sido provechosa y de su agrado.

Raúl Monge
Presidente de Comité Organizador

Jorge Ramió
Vicepresidente de Comité Organizador

Valparaíso, Chile

Noviembre, 2005

Organización

Comité Organizador

Dr. Raúl Monge Anwandter (Universidad Técnica Federico Santa María, Chile)
Dr. Jorge Ramió Aguirre (Universidad Politécnica de Madrid, España)
Sr. Javier Cañas Robles (Universidad Técnica Federico Santa María, Chile)

Conferencistas Invitados

Dr. René Peralta (National Institute of Standards and Technology, USA)
Dr. Javier López (Universidad de Málaga, España)

Comité de Programa

Dr. Juan Pedro Hecht (Universidad de Buenos Aires, Argentina)
Dr. Hugo Scolnik (Universidad de Buenos Aires, Argentina)
Dr. Ricardo Dahab (Universidade Estadual de Campinas, Brasil)
Dr. Marco Aurelio Henriques (Universidade Estadual de Campinas, Brasil)
Dr. Adriano Mauro Cansian (Universidade Estadual Paulista, Brasil)
Dr. Routo Terada (Universidade de São Paulo, Brasil)
Dr. Marcos Kiwi (Universidad de Chile, Chile)
Dr. Horst von Brand (Universidad Técnica Federico Santa María, Chile)
Dr. Juan Guillermo Lallinde Pulido (Universidad EAFIT, Colombia)
Dr. Jeimy José Cano Martínez (Universidad de los Andes, Colombia)
Dr. Julio Cesar López (Universidad del Valle, Colombia)
Dr. Jorge Estrada Sarlabous (Academia de Ciencias de Cuba, Cuba)
Dr. Javier Areito Bertolín (Universidad de Deusto, España)
Dr. Joan Borrel Viader (Universidad Autónoma de Barcelona, España)
Dra. Pino Caballero Gil (Universidad de La Laguna, España)
Dr. Jorge Dávila Muro (Universidad Politécnica de Madrid, España)
Dr. Luis Hernández Encinas (Consejo Superior de Investigaciones Científicas CSIC, España)
Dr. Josep Lluís Ferrer-Gomila (Universidad de Las Islas Baleares, España)
Dr. Francisco Javier López Muñoz (Universidad de Málaga, España)
Dra. Amparo Fúster Sabater (Consejo Superior de Investigaciones Científicas CSIC, España)
Dr. Arturo Ribagorda Garnacho (Universidad Carlos III de Madrid, España)
Dr. Miguel Soriano Ibañéz (Universidad Politécnica de Cataluña, España)
Dr. Hugo César Coyote Estrada (Instituto Politécnico Nacional, México)
Dr. Enrique Daltabuit Godas (Universidad Nacional Autónoma de México, México)
Dr. Carlos Mex Perera (ITESM campus Monterrey, México)

Dr. Sergio Rajsbaum Godorezky (Universidad Nacional Autónoma de México, México)
Dr. Horacio Tapia Recillas (Universidad Autónoma Metropolitana, México)
Dr. Edmundo Monteiro (Universidad de Coimbra, Portugal)
Dr. Emilio Hernández (Universidad Simón Bolívar, Venezuela)
Dr. Alfredo Viola Deambrosis (Universidad de la República - Uruguay)

Logística

Srta. Claudia Arancibia (Universidad Técnica Federico Santa María, Chile)
Srta. Carol Castro (Universidad Técnica Federico Santa María, Chile)

Edición y Publicación de Actas

Sr. Pablo Itaim (Universidad Técnica Federico Santa María, Chile)

Auspician

Patrocinan

Índice general

Conferencias Magistrales

Tecnologías de voto electrónico

Martes, 22 de Noviembre 2005, 12:45-14:00

Dr. René Peralta
National Institute of Standards and Technology, USA

Se describirán, en líneas generales, las principales técnicas propuestas que existen hoy en día (algunas ya en uso) para voto electrónico. En EE.UU. existen actualmente dos fuertes controversias con respecto a esta tecnología. El primer punto en discusión es la conveniencia o no de generar, para efectos de auditoria, una copia en papel de cada voto. El segundo punto es la factibilidad del voto por Internet. Se presentarán los principales argumentos en pro y en contra de estas alternativas. Luego se muestra la posición del conferencista al respecto.

Entornos pervasivos y ubicuos: La nueva (in)-seguridad

Miércoles, 23 de Noviembre 2005, 12:45-14:00

Dr. Javier López
Universidad de Málaga, España

Como evolución a las aplicaciones desarrolladas para entornos móviles, las aplicaciones para entornos pervasivos y ubicuos se han establecido firmemente como la próxima frontera en la investigación de Seguridad. Parece obvio que las soluciones de seguridad desarrolladas para la tecnología de hace unos pocos años no resultan adecuadas, dadas las restrictivas características físicas de los nuevos dispositivos y los característicos entornos donde se usan. Aún así, el diseño de las nuevas soluciones preservan muchas de las características de antes, lo que supone un error en multitud de ocasiones. En esta presentación se analizarán los problemas que están abiertos y el abanico de posibles estrategias a seguir para dotar de soluciones seguras a estos nuevos entornos tecnológicos.

Hacia la definición de Procesos de Negocios Seguros basados en una Arquitectura Dirigida por Modelos

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

[1] Universidad del Bío Bío, Departamento de Auditoría e Informática,
La Castilla S/N, Chillán Chile.
alfonso@ubiobio.cl
[2] Universidad Castilla-La Mancha, Departamento de Informática,
Paseo de la Universidad 4, Ciudad Real, España.
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen. Los nuevos escenarios en donde compiten las empresas presentan grandes y nuevos desafíos en variados aspectos. La seguridad es uno de ellos. El comercio electrónico y los trabajos colaborativos exigen mayor y mejor seguridad de los sistemas de información. Otro aspecto importante es el cambio de paradigma en el área de gestión y administración. Los procesos de negocios han pasado a ser un recurso esencial para la competitividad de las empresas. A través de ellos es posible obtener la flexibilidad que les permite optimizar y asegurar la calidad de sus productos y/o servicios. Creemos que la incorporación temprana de la seguridad, por ejemplo en relación a requisitos de seguridad considerando el dominio de los expertos del negocio, repercutirá favorablemente en los sistemas de información. Este trabajo contiene 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 la utilización de una arquitectura dirigida por modelos que permita definir procesos de negocios seguros.

1 Introducción

La necesidad de sobrevivir en entornos competitivos cada vez más complejos e inestables hace que las organizaciones de hoy tengan que ser más flexibles y basen su competitividad en los recursos propios para mantenerse en el mercado con un desempeño financiero superior [19]. En este contexto cobran especial relevancia los procesos de negocios, entendidos como un conjunto de procedimientos o actividades que llevan a cabo, colectivamente, los objetivos o políticas del negocio [51]. En los últimos años han sido el centro de atención de paradigmas en el área de negocios y gestión tan importantes como la reingeniería de procesos de negocios [16, 20, 43] y la gestión de procesos de negocios [38, 49]. Este enfoque ha resultado ser una buena respuesta a la complejidad del entorno, la velocidad con que se requieren nuevos productos y el creciente número de nuevos actores involucrados en las actividades cotidianas de una empresa.

Por otra parte, la introducción del comercio electrónico, con el consecuente uso intensivo de comunicaciones y tecnologías de información, propicia escenarios en que

las empresas junto con ampliar sus negocios, también aumenta su vulnerabilidad. La consecuencia más inmediata es que, debido al creciente número de ataques sobre los sistemas, es altamente probable que tarde o temprano algún intruso tenga éxito [36]. Esta violación de la seguridad causa pérdidas en las organizaciones. Por ello es necesario proteger sus computadores y sus sistemas de la mejor forma posible, lo cual no significa necesariamente seguridad absoluta, pero sí un razonable alto nivel de seguridad en relación a las limitaciones que se tienen [53].

Ya que un proceso de negocios es el punto de partida para el desarrollo del software y en él se definen los requisitos para que el software sea desarrollado [25] creemos pertinente explorar la perspectiva de incorporar la seguridad desde este nivel.

A pesar de que la noción de seguridad es importante en la forma en que se llevan a cabo los negocios en la actualidad, ésta ha sido a menudo descuidada en el modelado 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 [18]. 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 [13].

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 [28], consecuentemente, durante la fase de modelado del negocio los propietarios de los procesos deberían abordar también los requisitos de seguridad [35].

Creemos que es importante contar con herramientas que permitan especificar la seguridad considerando la perspectiva de los analistas de negocios en que sea posible independizar la especificación de requisitos de seguridad de la implementación. Para ello exploramos la utilización del estándar MOF y la definición de arquitecturas dirigidas por modelos (MDA, Model Driven Architecture).

Nuestro artículo se encuentra organizado de la siguiente manera; en la sección 2 presentamos una breve descripción de procesos de negocios, una relación de las principales notaciones utilizadas en el modelado de procesos de negocios, una descripción de cómo se ha modelado la seguridad en relación a los procesos de negocios y la relación que existe entre los procesos de negocios y la arquitectura dirigida por modelos. Finalmente, en la sección 5 se presenta una propuesta para la especificación de requisitos de seguridad usando metamodelos

2 Procesos de negocios.

Los procesos de negocios (BP, Business Process) han cobrado importancia para las empresas ya que representan la manera en que se llevan a cabo las actividades que les permiten alcanzar sus objetivos, dicho de otra forma, son parte de la identidad del negocio mismo [37]. El cambio que las organizaciones han experimentado en la forma en que ven sus negocios, que ha ido desde la tradicional orientación al proyecto, a la función o al producto hasta una orientación al proceso [1, 20], es especialmente

necesario en una economía global [7] y ha colocado a los procesos de negocios en el centro de la atención.

Los procesos de negocios se definen como actividades o procedimientos que en conjunto cumplen un objetivo específico del negocio o metas de más largo alcance, en el contexto de una estructura organizacional, definiendo roles funcionales y relaciones [51]. Estos roles son ejecutados por actores cuyo propósito es alcanzar un conjunto de objetivos predefinidos. Los actores están organizados de manera que sus actividades obedezcan a una representación de los roles en forma coordinada para alcanzar objetivos [5]. La relación entre sistemas de información y procesos de negocios está claramente establecida ya que, estos últimos tienen que operar articulados de manera coordinada (ver Figura 1).

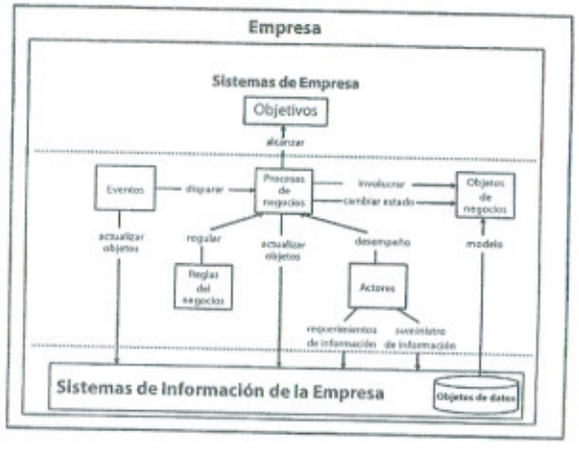

Figura 1 Relación entre Empresa, Sistemas de Negocios y Sistemas de Información Empresariales [5].

Una forma moderna de enfocar los procesos de negocios es a través de la gestión de los mismos (BPM, Business Process Management). BPM tiene claramente identificados sus predecesores y en este sentido no es nuevo, ya que, deriva de los flujos de trabajo (Wf, Workflow) y éstos de la automatización de oficinas [48]. El término BPM puede ser definido como "*el soporte de procesos de negocios usando métodos, técnicas y software para diseñar, representar, controlar y analizar los procesos operacionales que involucran organizaciones, aplicaciones, documentos y otras fuentes de información*" [48, 50].

Tecnológicamente hablando las relaciones entre actores, eventos, reglas y demás componentes de un BPM están soportados por una configuración hardware/software que

se conoce como Sistema de Gestión de Procesos de Negocios (BPMS, Business Process Management Systems) [45, 49]. Los elementos que componen un BPMS son: *(i)* un *motor de procesos*, la pieza central, *(ii)* un *administrador de recursos*, necesarios para el desarrollo de las funciones o actividades, *(iii)* un *programador de tiempos* de ejecución de las tareas con los recursos necesarios, *(iv)* un *administrador de auditoría* y *(v)* un *administrador de seguridad*, siendo este último esencial si se considera que el BPMS es el centro de la competitividad de cada empresa [45]. Adicionalmente, un BPMS deberá tener la capacidad de: *(i)* implementar cambios en las reglas y objetivos del negocio, *(ii)* medir la efectividad de esos cambios, *(iii)* separar el qué y cómo, independencia de administración de recursos y procesos y *(iv)* definir, cambiar e implementar los procesos de negocios de manera consistente. Esto permite afirmar que el mayor valor de los productos BPM es ofrecer la capacidad, a los analistas de negocios, para modificar la manera en que está siendo ejecutado un proceso sin requerir de reprogramación [17].

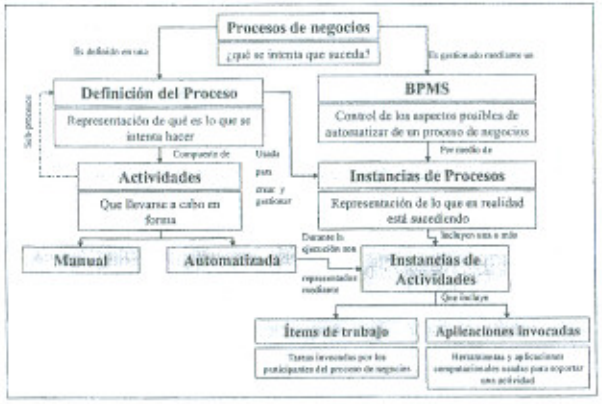

Figura 2: Componentes de un proceso de negocios [22].

En síntesis, un proceso de negocio debe tener una definición del proceso junto con las actividades necesarias para llevarlo a cabo, sean éstas manuales o automáticas. La gestión de procesos de negocios a través de herramientas automáticas (BPMS), permite instanciar los procesos que incluyen una o más actividades que, a su vez, son tareas asignadas a un participante del proceso de negocios o que permiten invocar aplicaciones que son usadas para dar soporte a una actividad (ver Figura 2) [22].

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 [11]. 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 [8].

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) [15].

En la actualidad, y de acuerdo con el estado de la industria del modelado de procesos de negocios [27, 30], es posible identificar a Unified Modeling Language (UML) [33] y Business Process Modeling Notation (BPMN) [10] entre los principales estándares.

El uso de UML se encuentra bastante difundido en relación al modelado de procesos de negocios [11, 23, 25, 26, 28, 42, 47], ya que es un lenguaje consolidado, fácil de aprender y que permite una comunicación fluida entre los diversos actores acerca del modelo.

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 (BPQL, Business Process Query Language) [34].

2.2 Modelado de la 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. Primero, el modelado propiamente dicho ha sido inadecuado porque generalmente quienes especifican los requisitos de seguridad son ingenieros de requisitos que han tendido, accidentalmente, a reemplazarlos por restricciones específicas de arquitectura [13]. Y segundo, que en la práctica ha resultado ser lo más común, la seguridad ha sido integrada en forma tardía, a menudo durante la implementación real del proceso [4] de manera ad-hoc, durante la fase de administración del sistema [26] o simplemente considerada como

un servicio externo que será suministrado por un tercero [29]. 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 [26].

La forma de modelar la seguridad en una organización debe considerar las siguientes perspectivas: *Estática,* sobre la seguridad de la información procesada, *Funcional,* sobre los procesos del sistema, *Dinámica,* sobre los requisitos de seguridad desde 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 [18].

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 [14]. De manera que, es posible establecer que los requisitos de seguridad, que se pueden especificar en un proceso de negocios, sean del mismo tipo para todas las organizaciones, debido a que en este nivel no se está pensando en la implementación.

De acuerdo con [53], es posible definir requisitos de seguridad en función de tres elementos (ver Figura 3), de manera que la combinación de las diferentes fuentes y las interacciones que existen entre ellas permite obtener un conjunto holístico de requisitos de seguridad.

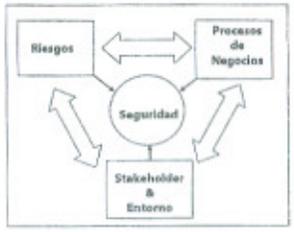

Figura 3: Combinación de las diferentes fuentes para requisitos de seguridad [53]

Los trabajos que se relacionan con especificaciones de seguridad por parte de los expertos en el dominio del negocio son; *(i)* escasos [4, 18, 28], *(ii)* se orientan a la seguridad en la transacción [40], *(iii)* apuntan directamente a los sistemas de información en general [44] o *(iv)* están pensados para ingenieros de seguridad e ingenieros de software [29].

Considerando este escenario y que los procesos de negocios tienen una estrecha relación con el workflow [38, 49] hemos estimado pertinente poner especial atención en los trabajos que relacionan seguridad y workflow [2, 3, 9, 52]. Hemos podido constatar que la mayoría de ellos pone énfasis en el *control de acceso*, considerado como

identificación, autenticación y autorización [14] mediante la utilización del acceso basado en roles, RBAC [6, 9, 12, 41].

2.3 MDA y los Procesos de Negocios

La arquitectura dirigida por modelos es un marco de trabajo para el desarrollo de software cuya idea central es permitir la creación de modelos totalmente independientes de la implementación tecnológica. La propuesta considera un enfoque en que sea posible *(i)* hacer una especificación de un sistema independiente de la plataforma que lo va a soportar, *(ii)* especificar plataformas, *(iii)* seleccionar una determinada plataforma para el sistema y *(iv)* transformar la especificación del sistema en una especificación para una plataforma en particular [31].

MDA tiene que ver con modelos y los trata de dos diferentes maneras [17]: *(i) estandarizándolos:* esto está relacionado con las técnicas que aseguren que todos los modelos usados en el desarrollo del software pueden ser relacionados unos con otros, esto pone énfasis en el uso de MOF (Meta Object Facility) y metamodelos y *(ii) usándolos para el desarrollo del software:* esto tiene que ver con la transición desde modelos abstractos hacia modelos más concretos y las reglas de correspondencia que permitan a un desarrollador transformar un modelo en otro.

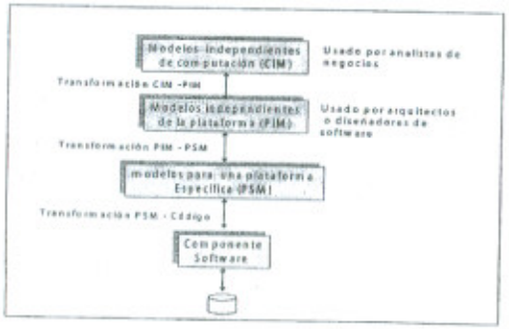

Figura 4: Secuencia de desarrollo de MDA (adaptado de [17])

La propuesta MDA, pone énfasis en el uso del modelo CIM (Computation Independent Model) en que se describe el punto de vista de una aplicación independiente de la computación y provee un modelo comprensible por expertos del domino e ingenieros de sistemas. El PIM (Platform Independent Model) ofrece una definición abstracta de las funciones del negocio y el comportamiento sin detalles de tecnología y el PSM (Platform Specific Model) que define un modelo específico para una plataforma.

La creación de modelos de procesos de negocios por parte de analistas de negocios está considerada en la generación de modelos independientes de computación (ver Figura 4). Para que cada modelo especificado en el enfoque MDA se pueda relacionar con otros, todos deben estar basado en MOF, dicho de otra forma cada modelo MDA tiene su correspondencia hacia MOF, de modo que se pueda comunicar con cualquier otro modelo del tipo MOF-subordinado [17].

Por otra parte, la mayor productividad, portabilidad, interoperabilidad y mantenibilidad y documentación [24] que se le atribuye MDA la hacen una propuesta muy atractiva.

En resumen, los procesos de negocios pueden ser descritos como un modelo CIM para lo cual habría que disponer de lenguaje de modelado que este de acuerdo con MDA. UML y BPMN están en esa dirección por lo que los requisitos de seguridad expresados en una de esas notaciones podrán ser vistos con la perspectiva de la arquitectura dirigida por modelos.

3 Especificación de requisitos de seguridad usando metamodelos

Como ya se estableciera en la sección 2.2 la especificación de requisitos de seguridad en un alto nivel de abstracción, por parte de los analistas del negocio, está prácticamente ausente en los trabajos relacionados.

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. Por otra parte, la identificación temprana de requisitos, a nivel de analista de negocios en la creación de un proceso de negocios, permite ahorrar costes de desarrollo y mantenimiento.

La representación de requisitos de seguridad usando BPMN, la notación propuesta por BPMI (Business Process Management Initiative), fue explorada en [39]. Se consideraron requisitos de seguridad que resultaran asimilables de manera sencilla por parte de los analistas del negocio y que a su vez tuvieran un significado claro para los expertos en seguridad. Los aspectos de seguridad fueron *(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 (Por ejemplo: usuarios, programas, procesos, dispositivos u otros sistemas), *(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 (por ejemplo: identidad de usuarios, datos o comunicaciones privadas) [13, 14]. Podría explorarse su representación utilizando otras notaciones (por ejemplo UML 2).

Sin embargo, y siguiendo la idea subyacente a la arquitectura dirigida por modelos, debiera ser posible especificar los requisitos de seguridad de manera independiente de la notación.

En [46] existe una propuesta para una notación independiente del negocio. Esto tiene sentido si se considera la amplia gama de notaciones para modelado y el no menor número de herramientas que lo soportan. Para los autores resulta necesario contar con un metamodelo que debiera ser *(i)* lo suficientemente simple y natural como para que pueda ser entendido por los no especialistas en tecnologías de información, *(ii)* lo suficientemente amplio como para cubrir todos los aspectos que más o menos se relacionan con procesos de negocios, *(iii)* lo suficientemente detallado como para servir a los objetivos de descripción del sistema, análisis y diseño tanto como lo concerniente al proceso de negocios y *(iv)* servir de base común para las más típicas notaciones de procesos de negocios y debiera ser capaz, en forma más o menos automática, de transformar conceptos de una notación a otra.

Estos conceptos están muy relacionados con la propuesta de un metamodelo para la definición de procesos de negocios (BPDM, Business Process Definition Metamodel) [32]. Este metamodelo se encuentra en etapa de desarrollo y los principales aspectos de su descripción están contenidos en el documento Business Process Definition Metamodel Request for Proposals [21].

El BPDM, es una descripción semántica de la lógica de las relaciones entre varios elementos de cualquier posible descripción de procesos de negocios. No es una notación, simplemente describe las relaciones lógicas [17]. Se encuentra en el contexto de la iniciativa MDA [21], el cual provee los elementos esenciales para cualquier modelado estándar [27].

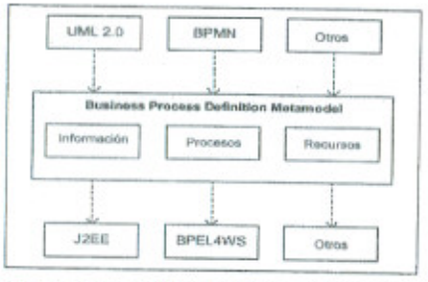

Figura 5: Metamodelo para la definición de procesos de negocios [21].

Como se puede ver en la Figura 5, los principales estándares para el modelado de procesos de negocios están siendo considerados en el metamodelo que propone Object Management Group (OMG). Los estándares para el modelado de procesos de negocios, tales como BPMN o diagramas de actividad de UML 2.0 podrán ser transformados usando este metamodelo. A través de MDA, las empresas estarán en posición de

trasladar sus modelos, creados con herramientas específicas de procesos de negocios, hacia el BPDM y obtener desde allí software en lenguajes como J2EE, BPEL u otro [17].

La unión entre OMG y BPMI, ambas relacionadas con los principales estándares en el modelado de procesos de negocios, UML y BPMN respectivamente, para enfrentar de manera coordinada el modelado de procesos de negocios[1], permite estar optimistas sobre el futuro del metamodelo.

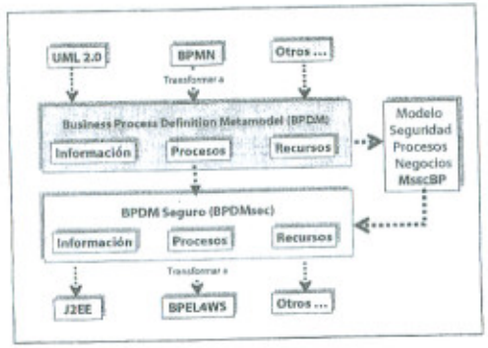

Figura 6: Metamodelo con requisitos de seguridad para procesos de negocios

La aparición de BPDM abre la posibilidad para incorporar las *relaciones lógicas* necesarias que consideren los requisitos de seguridad en el modelado de procesos de negocios. Así se dará origen a un BPDMsec (ver Figura 6) que ya incorpore la seguridad. De manera que, el Modelo de Seguridad de Procesos de Negocios (MsecBP), permita incorporar los requisitos de seguridad especificados a nivel de analistas de negocios en el metamodelo bajo una arquitectura dirigida por modelos. Así, los aspectos de seguridad que quieran ser modelados por los analistas del negocios, por ejemplo, control de acceso, privacidad u otros, van a poder ser contemplados en el metamodelo. El resultado es que, una vez que se haga la transformación de las especificaciones a lenguajes como J2EE , BPEL4WS u otro, ya se tendrán incorporados los aspectos de seguridad.

[1] Ver http://www.omg.org/news/releases/pr2005/06-29-05.htm

4 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 se puede mejorar el desempeño de los procesos de negocios si se capturan tempranamente los requisitos de seguridad. Hemos propuesto un enfoque que considera el diseño dirigido por modelos, de manera que, los expertos en negocios puedan expresar los requisitos de seguridad independiente de computación. Los trabajos futuros deberán profundizar sobre aspectos relacionados con el metamodelo de procesos de negocios para establecer las reglas de transformación de los requisitos de seguridad.

Agradecimientos

Esta investigación es parte de los proyectos DIMENSIONS, parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), 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. Andersson, T., Bider, I. and Svensson, R.; *Introduction of BPS Systems into Operational Practice: Achievements and Setbacks*, The 16th Conference on Advanced Information Systems Engineering, Knowledge and Model Driven Information Systems Engineering for Networked Organisations. Vol. 2. Riga, Latvia. (2004). pp:232-239.
2. Atluri, V.; *Security for Workflow Systems*, Information Security Technical Report. Vol. 6 (2). (2001). pp: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). pp:44-64.
4. Backes, M., Pfitzmann, B. and Waidner, M.; *Security in Business Process Engineering*, International Conference on Business Process Management. Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). pp:168-183.
5. Barrios, J. and Montilva, J.; *Business Modelling Through Roadmaps*, ICEIS 2004, Proceedings of the 6th International Conference on Enterprise Information Systems. Porto, Portugal. (2004). pp:348-355.
6. 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). pp:1-12.
7. Bider, I.; *Business Process Support - from Initial Analysis to Introduction into Operational Practice (Obstacles to Overcome)*. Workshops Proceedings, Information Systems for a

Connected Society In 15th CAiSE '03. Vol. 75. Klagenfurt/Velden, Austria. (2003). pp:398-402.
8. Bider, I.; *Choosing Approach to Business Process Modeling - Practical Perspective*. In http://www.ibissoft.se/english/howto.pdf. (2003).
9. Botha, R. A. and Eloff, J. H. P.; *A framework for access control in workflow systems*, Information Management & Computer Security. Vol. 9/3. (2001). pp:126-133.
10. BPMN; *Business Process Modeling Notation (BPMN)*, Version 1.0 May 3. In http://www.bpmi.org/. (2004).
11. Castela, N., Tribolet, J., Silva, A. and Guerra, A.; *Business Process Modeling with UML*, Proceedings of the 3st. International Conference on Esterprise Information Systems. Vol. 2. Setubal, Portugal. (2001). pp:679-685.
12. 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). pp:31-40.
13. Firesmith, D.; *Engineering Security Requirements*, Journal of Object Technology. Vol. 2 Nº 1 January-February 2003. (2003). pp:53-68.
14. Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology. Vol. 3 (1), January-Febeuary. (2004). pp:61-75.
15. Giaglis, G. M.; *A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques*, International Journal of Flexible Manufacturing Systems. Vol. 13 (2). (2001). pp:209-228.
16. Grant, D.; *A wider view of business process reengineering*, Communications of the ACM (CACM). Vol. 45 (2). (2002). pp:85-90.
17. Harmon, P.; *The OMG's Model Driven Architecture and BPM*. In http://www.bptrends.com/publicationfiles/05%2D04%20NL%20MDA%20and%20BPM%2E pdf. (2004).
18. 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). pp:89-103.
19. Hunt, S., *A General Theory of Competition: Resources, Competences, Productivity, Economic Growth*, Sage Publication Inc., First Edition, (2000). 320 p.
20. Irani, Z., Hlupic, V. and Giaglis, G. M.; *Business process re-engineering: an analysis perspective*, International Journal of Flexible Manufacturing Systems. Vol. 14 (1). (2002). pp:5-10.
21. Iyengar, S., *Business Process Definition Metamodel*, bei/2004-01-02, January 12 th 2004, Version: 1.0.2, Institutions: IBM, Adaptive, Borland, Data Access Technologies, EDS, 88 Solutions. (2004). 172 p.
22. Jennings, N. R., Norman, T. J., Faratin, P., O'Brien, P. and Odgers, B.; *Autonomous Agents for Business Process Management*, Applied Artificial Intelligence. Vol. 14 (2). (2000). pp:145-189.
23. Jürjens, J., *Secure Systems Development with UML*, Springer Verlag, (2004). 309 p.
24. Kleppe, A., Warmer, J. and Bast, W., *MDA Explained: The Model Driven Architecture™: Practice and Promise*, Addison Wesley, (2003). 192 p.
25. List, B. and Korherr, B.; *A UML 2 Profile for Business Process Modelling*, Proceedings of the 1st International Workshop on Best Practices of UML (BP-UML 2005) at the 24th International Conference on Conceptual Modeling (ER 2005). Klagenfurt, Austria. (2005).
26. 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). pp:426-441.
27. Lonjon, A.; *Business Process Modeling and Standardization*, BPTrends. In http://www.bptrends.com/. (2004).

28. 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). pp:477-481.
29. Maña, A., Ray, D., Sánchez, F. and Yagüe, M. I.; *Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software*, Actas de la VIII Reunión Española de Criptología y Seguridad de la Información, RECSI'04. Leganés, Madrid. España. (2004). pp:33-41.
30. Mega; *Business process Modeling and Standardization*. In http://www.bpmg.org/downloads/Articles/Article-MEGA-BusinessProcessModeling&StandardizationEN.pdf. (2004).
31. Object Management Group; *MDA Guide Version 1.0.1*. In http://www.omg.org/docs/omg/03-06-01.pdf. (2003).
32. Object Management Group; *Business Process Definition Metamodel (Revised Submission to BEI RFP bei/2003-01-06)*. In http://www.bpmn.org/Documents/BPDM'OMG-BPD-2004-01-12-Revision.pdf. (2004).
33. OMG; *Object Management Group*. In http://www.omg.org/. (2004).
34. 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).
35. 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). pp:94-102.
36. Quirchmayr, G.; *Survivability and Business Continuity Management*, ACSW Frontiers 2004 Workshops: The Australasian Information Security Workshop (AISW2004), The Australasian Workshop on Data Mining and Web Intelligence (DMWI2004), and The Australasian Workshop on Software Internationalisation (AWSI2004). Dunedin, New Zealand. (2004). pp:3-6.
37. Regev, G. and Wegmann, A.; *Why Do We Need Business Process Support? Balancing Specialization and Generalization with BPS Systems (Introductory note)*, The 15th Conference on Advanced Information Systems Engineering, Workshops Proceedings, Information Systems for a Connected Society. Klagenfurt/Velden, Austria. (2003). pp:361-365.
38. Reijers, H. A. and Heusinkveld, S.; *Business Process Management Attempted Conceptcide?*, IRMA International Conference. (2004). pp:128-131.
39. Rodríguez, A., Fernández-Medina, E. and Piattini, M.; *Towards an integration of Security Requirements into Business Process Modeling*, Security In Information Systems, Proceedings of the Third International Workshop on Security In Information Systems, WOSIS 2005, In conjunction with ICEIS 2005. Miami, USA. (2005). pp:287-297.
40. 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). pp:22-31.
41. Sandhu, R. and Samarati, P.; *Authentication, Access Control, and Audit*, ACM Computing Surveys. Vol. 28 Nº1 March 1996. (1996). pp:241-243.
42. Sparks, G.; *An Introduction to UML, The Business Process Model*. In http://www.sparxsystems.com.au/WhitePapers/The_Business_Process_Model.pdf. (2000).
43. Stoica, M., Chawat, N. and Shin, N.; *An Investigation of the Methodologies of Business Process Reengineering*, Information Systems Education Journal. Vol. 2 (11). (2004).
44. 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). pp:313-324.

45. Van de Putte, G., *Intra-Enterprise Business Process Management*, RedBooks IBM., (2001). 436 p.
46. Vitolins, V. and Kalnins, A.; *Modeling Business*, Modeling and Simulation of Business Systems, Computational Engineering, Finance, and Science. Vilnius, Lithuania. (2003). pp:215-220.
47. 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). pp:381-395.
48. W.M.P. van der Aalst; *Business Process Management: A personal view*, Business Process Management Journal. Vol. 10 (2). (2004). pp:248-253.
49. 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). pp:1-12.
50. Weske, M., W.M.P. van der Aalst and Verbeek, H. M. W.; *Advances in business process management*, Data & Knowledge Engineering. 50. (2004). pp:1-8.
51. WfMC, *Workflow Management Coalition: Terminology & Glossary*., (1999). 65 p.
52. 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). pp:71-94.
53. Zuccato, A.; *Holistic security requirement engineering for electronic commerce*, Computers & Security. Vol. 23 (1). (2004). pp:63-76.

Hacia una Implementación Exitosa de un SGSI

María Eugenia Corti[1], Gustavo Betarte[1], and Reynaldo de la Fuente[2]

[1] Instituto de Computación, Facultad de Ingeniería, Universidad de la República
J. Herrera y Reissig 565, Montevideo, Uruguay
+598 2 7114244 - FAX +598 2 7110469
mcorti@iese.org, gustun@fing.edu.uy
http://www.fing.edu.uy/inco

[2] Datasec
Patria 716, Montevideo, Uruguay
+598 2 7110420
reynaldo@datasec-soft.com
http://www.datasec.com.uy

Resumen La seguridad de la información es un tema que requiere cada vez mayor atención. Las organizaciones, sin importar su tamaño o actividad, se ven en la necesidad de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) para proteger sus activos más sensibles. Asimismo, el surgimiento de estándares internacionales para la implantación y mejora contínua de un SGSI, y su rápida adopción por distintas organizaciones, genera la necesidad de acelerar el proceso de implantación de los mismos.
Este artículo presenta una metodología que complementa el modelo definido en el estándar BS 7799-2:2002 para implementar y gestionar un SGSI. La metodología que se presenta contribuye a obtener una implantación efectiva de las actividades planteadas en el referido modelo.

Keywords: Sistema de Gestión de la Seguridad de la Información, Seguridad de la Información, BS 7799

1. Introducción

La disponibilidad, integridad y privacidad de la información ha sido en todos los tiempos un tema importante para los gobiernos, empresas, organismos y la sociedad en su conjunto. La revolución digital, que ha cambiado la forma de almacenar y transmitir la información, introduce nuevos factores a considerar para el tratamiento de la misma. La disminución de los costos de los PCs y del acceso a la Internet permite que cada vez sea mayor y diverso el público que accede a esta red de redes. Asimismo, las herramientas de ataque son cada vez más sofisticadas, sencillas de usar y se pueden obtener fácilmente en la Internet; los intrusos están mejor preparados y organizados, los administradores de los sistemas informáticos no estan los suficientemente capacitados, debido al aumento