

# Obtaining secure BPEL from Secure Business Process specified with BPMN

G. Márquez, A. Rodríguez and E. F. Medina

**Abstract**— Business Processes are an important resource for performance on business competitiveness. The Business Process descriptions made; with BPMN (Business Process Modelling Notation), the de facto standard in the market, can be translated into execution languages; such as BPEL (Business Process Execution Language). Originally, BPMN specification does not include the representation of security aspects. However, there are proposals that incorporate security specifications of Business Processes using BPMN. Among them we have considered for describing a SBP (Secure Business Process), incorporating the business analyst's perspective in relation to security. However, until now, there are no translations of the SBP to execution languages. In this paper we propose a translation of the security requirements, including access control, defined in a SBP to secure Web services using BPEL language.

**Keywords**— Business Process, Secure Business Process, BPEL.

## I. INTRODUCCIÓN

ACTUALMENTE, los Procesos de Negocio se han convertido en un recurso de gran importancia para las empresas, ya que permiten describir las actividades que ocurren dentro de la organización y que conducen al cumplimiento de fines específicos. Adicionalmente, desde el punto de vista de la Ingeniería de Software, ayudan a enfocarse a la práctica durante el desarrollo de software, permitiendo la recopilación de información, análisis de flujos de datos, entre otros [20].

Por otro parte, la ausencia de medidas de seguridad de la información sitúa a la empresas en una posición de vulnerabilidad. Es por que las organizaciones de hoy requieren garantizar la seguridad de la información desde el punto de vista de la integridad, confidencialidad y privacidad, ya que una irrupción a estos datos puede tener efectos económicos tanto en la parte física como en las personas que conforman la organización [3].

Para representar los Procesos de Negocio existen notaciones como UML (*Unified Modeling Language*) [19] y BPMN (*Business Process Modeling Notation*) [13] que describen la funcionalidad del negocio, donde en este último tiempo, BPMN se ha convertido en la notación más usada para representar los Procesos de Negocio [17]. También es posible traducir estas especificaciones de procesos de negocio hechas con BPMN en lenguajes de ejecución convirtiéndolos en Servicios Web.

Por su parte, BPEL (*Business Process Execution Language*) es un lenguaje estandarizado por OASIS para la composición de Servicios Web que está basado en XML cuyo objetivo es el control central de solicitudes de diferentes Servicios Web con cierta lógica de negocio que ayuda a la programación a gran escala [11]. En este sentido, BPEL cumple un rol de orquestador que permite y determinar la ejecución de distintos Servicios Web [2].

La especificación original de BPMN no incluye la representación de aspectos de seguridad en relación con los Procesos de Negocio. Siendo la seguridad un aspecto importante en la especificación de Procesos de Negocio se ha estado tratando de incluirla en las especificaciones de los Procesos de Negocio [18] [9] [16]. Es así que el trabajo de Rodríguez et al. [16] incluye la seguridad en la especificación del Proceso de Negocio, los cuales están especificados con BPMN. La propuesta define Procesos de Negocio Seguro (*Secure Business Process*, SBP) en que se ha considerado el punto de vista del analista de negocio en relación con la seguridad. En esa propuesta se agregan requisitos de seguridad al metamodelo de BPMN tales como control de acceso, auditoría de seguridad, privacidad, integridad, entre otros. Sin embargo, hemos podido constatar [8] que no existen traducciones de estas especificaciones hacia lenguajes de ejecución como BPEL. Por lo tanto, el objetivo principal de este artículo es definir la forma en que es posible traducir los requisitos de seguridad definidos en un SBP hacia BPEL. En dicha traducción se usará solamente el requisito de seguridad Access Control partiendo del SBP que considera el punto de vista del analista de negocio en relación con restricciones de control de acceso hasta un Servicio Web seguro (BPEL).

El resto del artículo se encuentra organizado de la siguiente forma: en la Sección 2 se presentan los conceptos relacionados con nuestra propuesta de este trabajo, en la Sección 3 se mostrarán los trabajos relacionados con la integración de la seguridad en BPEL desde Procesos de Negocio, luego en la Sección 4, se presenta nuestra propuesta pasara la integración de seguridad en BPEL desde un SBP, en la Sección 5 mostrará un ejemplo ilustrativo y, finalmente, en la Sección 6 se presentaran nuestras conclusiones.

## II. CONCEPTOS RELACIONADOS

En esta sección se presentan los conceptos básicos que se consideran en nuestra propuesta, los cuales se describirán de manera concisa: Procesos de Negocio, Procesos de Negocio Seguro, la notación BPMN y BPEL.

### A. Procesos de Negocio

Un Proceso de Negocio (BP, *Business Process*) es un conjunto de tareas unidas que tienen como objetivo la entrega de un

G. Márquez, Universidad del Bio-Bio, Chillán, Chile, gmarquez@ubiobio.cl

A. Rodríguez, Universidad del Bio-Bio, Chillán, Chile, alfonso@ubiobio.cl

E. F. Medina, Universidad de Castilla-La Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

servicio o producto a un cliente. El proceso debe incluir entradas que deben estar claramente definidas y una salida única. Estas entradas están compuestas por factores que contribuyen con el valor del servicio o producto. Además, los BP pueden ser parte de un proceso mayor y pueden incluir otros BP. Por otro lado, los BP están diseñados para ser operados por uno o más unidades funcionales de una organización, enfatizando en hacer cumplir la cadena de valores que representa un BP en una empresa [21].

### B. Proceso de Negocio Seguro

El Proceso de Negocio Seguro (*Secure Business Process*, SBP) es un concepto introducido por Rodríguez et al. [16] que se basa en una extensión al diagrama BPD (*Business Process Diagram*) [13] con estereotipos de seguridad, creando así un diagrama BPMN seguro. La extensión consiste en una clase denominada *Secure Business Process Diagram* la cual contiene a otra clase denominada *Security Requirement*. Esta, a su vez, contiene a todos los requerimientos de seguridad, entre los cuales está *Access Control*. Para visualizar la propuesta de los Procesos de Negocio Seguro se mostrará la extensión del metamodelo BPD con los requisitos de seguridad en la siguiente Fig. 1.

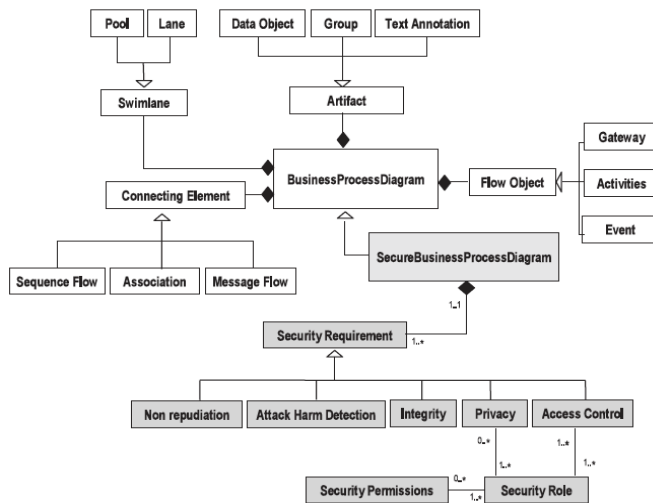



Figura 1. Metamodelo BPMN extendido con requisitos de seguridad [16].

A continuación se mostrará en la Tabla 1 la especificación del requisito de seguridad de *Access Control* detallando su descripción, asociación con el diagrama BPMN-BPD y su notación, ya que se será éste el que se integrará para el ejemplo ilustrativo que será descrito más adelante.

TABLA I. DESCRIPCIÓN DEL REQUISITO DE SEGURIDAD DE *ACCESS CONTROL* DEFINIDO EN UN SBP.

<b>Requisito de seguridad:</b>	Access Control
<b>Descripción:</b>	Corresponde a la limitación de acceso a recursos sólo a usuarios autorizados. Desde la perspectiva de la seguridad, esta especificación supone la definición de

	roles que pueden ser asignados a personas, entidades o sistemas.
<b>Asociación con BPMN-BPD:</b>	Pool, Lane, Activity y Group.
<b>Notación:</b>	

### C. Business Process Modeling Notation

BPMN es una notación gráfica estandarizada que permite representar el modelado de Procesos de Negocio [13]. Esta notación proporciona una forma estándar para describir los Procesos de Negocio tanto para propósitos descriptivos de alto nivel, como para rigurosos entornos de software orientados a procesos [6]. El objetivo principal de BPMN es crear mecanismos simples y entendibles para representar el negocio de una empresa, y paralelamente, entender su complejidad. La utilización de esta notación ha sido creciente en las empresas pues en la definición de BPMN se consideró usar elementos gráficos para mostrar a todos los usuarios cuál es la lógica del negocio en la organización [4].

### D. Business Process Execution Language

BPEL (*Business Process Execution Language*, también llamado WS-BPEL) es un entorno de trabajo basado en XML que permite definir a las empresas los procesos que están conectados dentro o fuera de la organización a través de los Servicios Web [11]. BPEL se ha convertido en el organizador que permite unir los Servicios Web en una solución coherente, facilitando su interacción dentro y fuera de una empresa. A su vez, proporciona una gramática basada en XML para la descripción lógica con el objetivo de controlar y coordinar los Servicios Web que participan en el flujo del proceso.

## III. TRABAJOS RELACIONADOS

En trabajos previos [8] hemos llevado a cabo una revisión de la literatura, basada en las directrices propuestas en [5]. En este artículo presentaremos los trabajos más cercanos a nuestra propuesta. Autores como Souza et al. [18] hacen posible la creación de Servicios Web desde Procesos de Negocio con seguridad. Se utilizan requisitos de seguridad clásicos y no funcionales para probar la propuesta. A partir de lo anterior, se crea el entorno de trabajo llamado Sec-MoSC, el cual está compuesto por cuatro componentes principales: BPMN, un módulo de extensión de seguridad, un módulo de servicio de extensión y un traductor. El módulo de BPMN permite a los desarrolladores definir un Proceso de Negocio utilizando la notación estándar BPMN. La extensión de seguridad brinda apoyo al modelo de los requisitos de seguridad y se unen a los elementos de BPMN. La extensión de servicio es la responsable de la anotación de la información de servicio (por ejemplo, los servicios de candidato para ejecutar una tarea) en BPMN y el traductor transforma los servicios en BPMN.

También la seguridad ha sido tratada en distintos niveles. La Arquitectura Orientada a Servicios (*Service-oriented*

*Architecture*), por ejemplo, ofrece una infraestructura flexible que permite que los componentes que son desarrollados de manera independiente, se puedan comunicar de forma perfecta. En el ámbito de flujos de trabajo de la organización, SOA proporciona una base adecuada para ejecutar Procesos de Negocio como una orquestación de múltiples servicios independientes. Junto con el aumento de la conectividad, los correspondientes riesgos de seguridad aumentan exponencialmente [9]. Sin embargo, los requisitos de seguridad generalmente se definen a nivel técnico, a diferencia a un nivel organizacional que proporcionan un amplio punto de vista sobre los participantes, los activos y sus relaciones en materia de seguridad. Wolter et al. [23] destacan que hay varios tipos de objetivos de seguridad (tales como la autenticación y confidencialidad) que se pueden definir como políticas de Arquitecturas Orientadas a Servicios (SOA) pero, en general, de forma manual.

Por otro lado, en BPMN, los modelos de los Procesos de Negocio son capturados como BPD y éstos a su vez, se componen de elementos que son capaces de representar los aspectos del negocio que se quiere describir. A partir de lo anterior, Ouyang et al. [14] proponen un mecanismo llamado BPMN2BPEL el cual transforma los elementos que están en BPD que representan los Procesos de Negocio en BPEL, usando un algoritmo iterativo que reduce los elementos de BPD a componentes, siendo estos subconjuntos de BPD que solamente tiene un punto de entrada y de salida.

Desde el punto de vista de los Servicios Web, la autonomía, la independencia, entre otras, son características que están siendo cada vez más explotadas por las organizaciones. Las empresas no solo exportan sus funciones como Servicios Web, también exportan sus servicios a otras organizaciones para que puedan usarlos. Dado que estos servicios también pueden ser ofrecidos por otros proveedores, no hay algún mecanismo que asegure la confianza y seguridad de sus datos. Es por eso que en el trabajo de Frankova [2] se aborda la ingeniería de los Procesos de Negocio basados en acuerdos a nivel de servicios desde los requerimientos. Este trabajo complementa las metodologías y el desarrollo de Procesos de Negocio bajo en una arquitectura orientada a servicios, enfatizando la seguridad.

En los trabajos descritos anteriormente, hemos observado que el tema de seguridad tanto en Servicios Web como en Procesos de Negocio es un tema que ha sido tratado. No obstante, la diversidad de trabajos que usan los Procesos de Negocio para especificar la seguridad en BPEL, no hay en la literatura propuesta que describan la seguridad en BPEL desde SBP

#### IV. NUESTRA PROPUESTA PARA INCORPORAR LA SEGURIDAD EN BPEL DESDE UN SBP

Para lograr la integración de la seguridad desde un BPMN seguro a BPEL y obtener un Servicio Web seguro, hay que seguir un recorrido que involucra diversas tecnologías que trabajan en conjunto. El marco general de la propuesta se muestra en la Fig. 2.

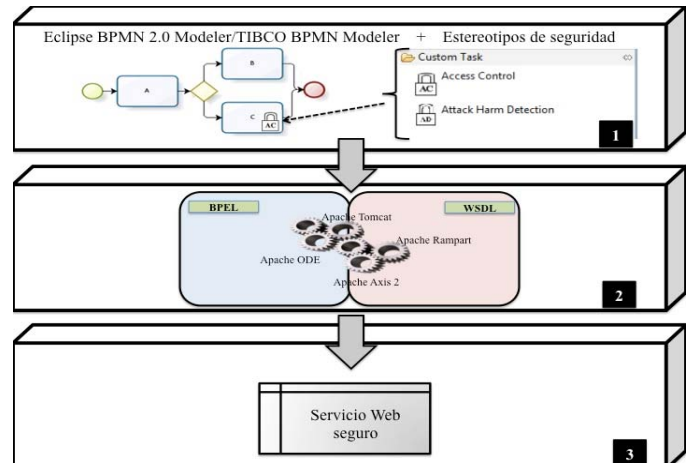


Figura 2. Propuesta de integración de la seguridad en BPEL desde un BPMN seguro.

Como es posible observar en la Fig. 2, se ha dividido el trabajo en tres partes a las que hemos denominado bloques. El Bloque-1 contiene el diagrama BPMN seguro y los estereotipos de seguridad (los que se han denominado *SecurityStereotypes*). Éstos contienen la referencia de los requisitos de seguridad definidos un SBP y que son interpretados en el diagrama BPMN. En este artículo nosotros hemos desarrollado sólo el requisito de Access Control, el que queda representado por un candado con las letras AC en su interior. Luego, el Bloque-2 contiene los lenguajes BPEL/WSDL y las correspondientes tecnologías que hacen posible la integración de la seguridad en BPEL. Por último, el Bloque-3 contiene el Servicio Web seguro, en el cuál ya se ha integrado el Access Control.

Para la adaptación uso del entorno tecnológico que permitiera llevar a cabo la propuesta lo primero que se hizo fue revisar la notación BPMN del entorno Eclipse Indigo considerando extender la funcionalidad del modelador. Para ello en el Bloque-1, se creó un *plugin* que almacena los requisitos de seguridad y posibilita que el analista de negocio pueda hacer la acción de *drag and drop* sobre los requisitos de seguridad que estime conveniente. Nuestra propuesta contempla el desarrollo del requisito de seguridad de Access Control, no obstante, cada requisito de SBP demanda un desarrollo en particular. Una vez creado el BPMN seguro, se obtiene el correspondiente código y modelo BPEL usando BPMN2BPEL y Eclipse BPEL Editor, el cual ofrece todas las facilidades tecnológicas para la creación y manipulación del código BPEL.

Ya que el diagrama contiene información adicional de la seguridad que después se ve reflejada en el código BPEL, no fue necesario modificar la herramienta BPMN2BPEL. Una vez que se obtiene el código BPEL, hay que tener un entorno de ejecución para que funcione. Para ello en el Bloque-2, se eligió el motor Apache ODE [7], considerando que es el entorno más usado por BPEL. Este motor de orquestación ejecuta los Procesos de Negocio siguiendo el estándar WS-BPEL y además, interactúa con los Servicios Web mediante el envío y recibo mensajes, manejo de manipulación de datos y

recuperación de errores. En este punto cabe hacer notar que el motor Apache ODE, donde se ejecuta BPEL, por ahora, no soporta extensiones de seguridad [7]. Ésta se considerará en futuras versiones.

Hasta ahora hemos obtenido un código BPEL desde un BPMN seguro y también se ha dicho que BPEL, debido a las versiones y actualizaciones, no soporta extensiones de seguridad. Es por ello que varios autores [18] [9] [23], que han trabajado con BPEL y Servicios Web, utilizan Web Services Description Language (WSDL) [22] para describir la seguridad. La importancia de WSDL es que, junto con los elementos descritos anteriormente, hacen que BPEL pueda adoptar los Servicios Web como su mecanismo de comunicación externa (red). Así las facilidades de mensajería BPEL dependen del uso del WSDL para describir los mensajes entrantes y, por otro lado, permitir las especificaciones de servicios Web seguros (WS-Security). Estas especificaciones permiten traducir los requisitos de seguridad definidos en [16] en requisitos de seguridad Web y obtener el correspondiente Servicio Web seguro. Los WS-Security son protocolos de comunicaciones que suministran un medio para aplicar seguridad a los Servicios Web, publicados por OASIS [12]. A su vez, estos estándares están contenidos en Apache Rampart [15], que es el módulo de seguridad de Apache Axis2 [1], permitiendo este último la manipulación de WS-Security, razón por la cual se ha seleccionado esta herramienta para el desarrollo de esta investigación.

Finalmente, en este bloque, hay que asociar los requisitos de seguridad especificados en [16] con alguna política o estándar de seguridad. Cada requisito de seguridad cumple un rol y una funcionalidad específica que no necesariamente coincide con las especificaciones de WS-Security, ya que éste se encuentra orientado a la seguridad funcional del Servicio Web. Sin embargo, es posible encontrar similitudes entre ambos mecanismos de seguridad. En el caso específico del requisito de Access Control se ha asociado el estándar WS-Security denominado WS-Security Username Token [10].

Por último, en el Bloque-3, se tiene que generar el Cliente Web para el Servicio Web seguro a partir del archivo WSDL. El entorno Eclipse Ganymede ofrece alternativas tecnológicas (Eclipse Web Tools Platform) para generar el Cliente Web de manera automática (aunque Eclipse Indigo también ofrece herramientas Web, no obstante, la propuesta BPMN2BPEL funciona sólo para Eclipse Ganymede bajo Linux). Una vez realizado lo anterior, es posible obtener un prototipo de Servicio Web seguro con el requisitos de seguridad Access Control a partir de lo definido en un BPMN seguro.

#### V. EJEMPLO ILUSTRATIVO

En esta sección se presenta un ejemplo que permite ilustrar la propuesta. Para ello se construido un diagrama de proceso de negocio seguro usando BPMN extendido. El ejemplo representa el procesamiento de la ficha clínica de un paciente que es atendido en un centro de atención de salud (ver Fig. 3). Cabe mencionar que en esta figura se han omitido los Pools Paciente, Empresa de Seguro, entre otros, ya que la

herramienta BPMN2BPEL sólo transforma a código un proceso descrito en un solo Pool.

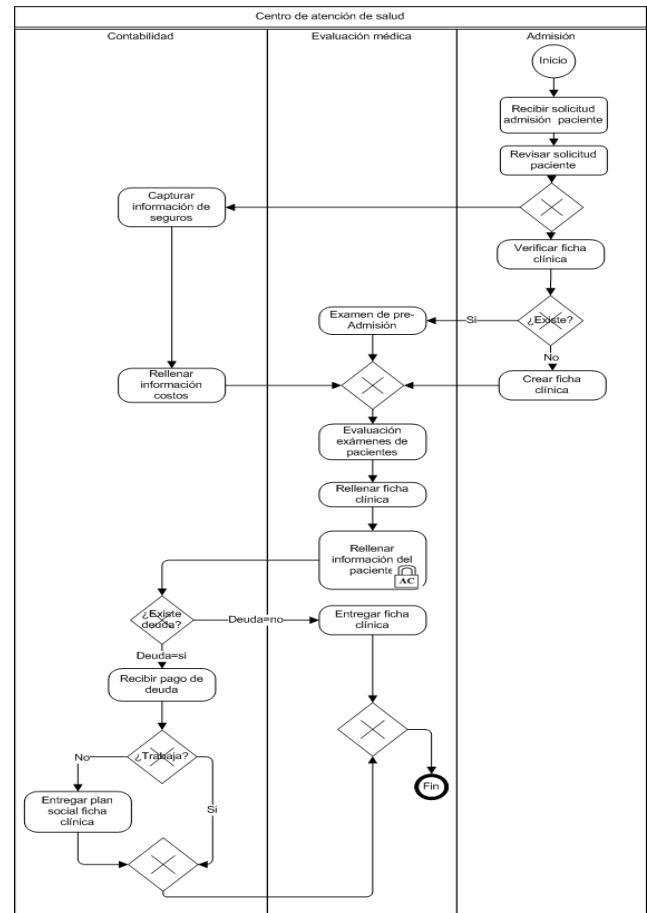


Figura 3. SBP de entrega de ficha a paciente

El proceso descrito en la Fig. 3 comienza cuando al servicio de admisión del centro de atención de salud le llega la solicitud de admisión del paciente para ser revisada. Posteriormente, se hace una recolección de datos que consiste en la verificación de la ficha clínica y la captura de información relacionada con los seguros. Una vez realizada todas las operaciones de recolección de datos, se hacen los exámenes de evaluación al paciente y se rellena la ficha clínica. Luego, se completa la ficha con información del paciente para lo cual se deben ingresar a los datos sociales. El analista del negocio, que ha creado el SBP, ha determinado que la información social del paciente es sensible por lo que ha decidido controlar el acceso a la misma, lo que ha representado a través de un candado con las letras AC en su interior. Como ya se tiene la información médica del paciente, se debe verificar si el paciente posee alguna deuda con el centro de salud, en caso de que el paciente posea deuda, la debe cancelar y posteriormente se verifica si el paciente trabaja o no. En caso de que no trabaje, se debe registrar que se encuentra en riesgo social y se le entrega la ficha clínica con esa información. Si el paciente trabaja, se le entrega la ficha clínica sin ninguna observación de riesgo social. En caso de que el paciente no posea ninguna deuda, se le entrega la ficha clínica.



### A. Integración de la seguridad en BPEL

La integración de la seguridad en BPEL se resume en la Fig. 4. En esta figura, que es análoga a la Fig. 2, se describe el recorrido que es necesario para obtener el Servicio Web Seguro desde un SBP, detallando los principales elementos permiten tal recorrido. En los siguientes párrafos se explicará los pasos más importantes para obtener el Servicio Web seguro desde un SBP.

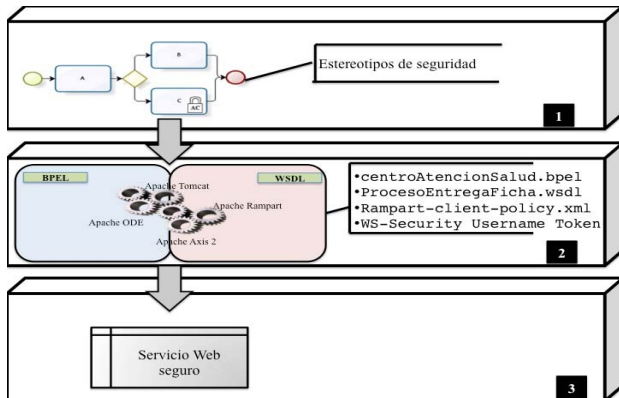


Figura 4. Aspectos técnicos para obtener servicios Web Seguro desde un SBP

**Bloque-1.** Para este bloque se ha creado una extensión para Eclipse Indigo la que se ha denominado SecurityStereotypes que permite al analista de negocio arrastrar el requisito de Access Control al diagrama BPMN para crear un SBP.

**Bloque-2.** Se utiliza la herramienta BPMN2BPEL y se obtiene el archivo centroAtencionSalud.bpel, el cual contiene la información de que la actividad Rellenar Información del paciente posee un requisito de seguridad. Luego, se crea el archivo ProcesoEntregaFicha.wsdl el cual contiene la información generada por el código BPEL y se le especifica en el encabezado del código que se utilizarán las propiedades de WS-Security Username Token, esto se ve reflejado en la Fig. 5.

```

1: <wsp:Policy xmlns:wsp=
2:   "http://docs.oasis-open.org/wss/2004/01/"
3:   oas:200401-wss-wssecurity-utility-1.0.xsd"
4:   xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
5:   <wsp:ExactlyOne>
6:     <wsp:All>
7:       <ramp:RampartConfig xmlns:ramp=
8:         "http://ws.apache.org/rampart/policy">
9:         <ramp:user>alice0112</ramp:user>
10:        <ramp:passwordCallClass>
11:          PWCHandler</ramp:passwordCallClass>
12:        </wsp:Policy>

```

Figura 5. Política de seguridad de Access Control

A su vez, también se especifica la seguridad en el documento rampart-client-policy.xml, donde se detalla que el usuario al que hemos denominado alice0112 (ver línea 9 de la Fig. 6) y la contraseña que será utilizada para acceder a la

```

1: <wsp:Policy wsu:Id="UsernameToken" xmlns:wsp=
2:   "http://docs.oasis-open.org/wss/2004/01/"
3:   oas:200401-wss-wssecurity-utility-1.0.xsd"
4:   ...
5:   <sp:SupportingTokens
6:     xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
7:       securitypolicy/200702">
8:     <sp:UsernameToken sp:IncludeToken=
9:       "http://docs.oasis-open.org/ws-sx/ws-securitypolicy
10:        /200702/IncludeToken/AlwaysToRecipient"/>
11:   </sp:SupportingTokens>
12: </wsp:Policy>

```

información. Esta contraseña será administrada por una clase Java (ver línea 10 de la Fig. 6).

Figura 6. Código de rampart-client-policy.xml

Por último, en este bloque se programan las clases Java necesarias para crear el Servicio Web seguro. Estas clases deben contener la información que fue descrita en el archivo WSDL y que están almacenadas en el documento XML.

**Bloque-3.** A continuación, hay que obtener un prototipo donde se debe mostrar la ventana inicial del Servicio Web seguro que describe la actividad Rellenar información del paciente. Por ahora, sólo se ha desarrollado esta actividad como prueba para determinar que es posible obtener el Servicios Web seguro. Además, en el prototipo deben estar las variables Login y Password que contiene las restricciones de acceso a un usuario al momento de rellenar la ficha de un cierto paciente. En la Fig. 7 se ilustra el prototipo que describe la actividad Rellenar información del paciente.

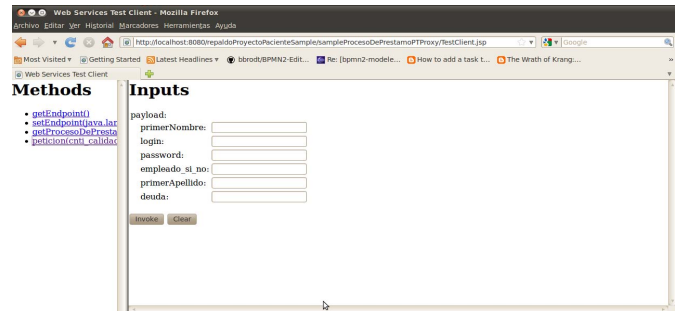


Figura 7. Ventana del prototipo de un Servicio Web seguro.

## VI. CONCLUSIONES Y TRABAJO FUTURO

En este artículo se ha descrito el trabajo que apunta obtener Servicios Web seguros partiendo de la especificación de un SBP usando BPEL. En primer lugar, se han descrito los elementos más importantes que se relacionan con la propuesta, los cuales son: Procesos de Negocio, BPMN, BPEL y WSDL. La base de este artículo es BPEL ya que tiene el propósito de representar los Procesos de Negocio a gran escala. Para obtener un Servicio Web seguro, fue necesario utilizar los archivos WSDL que describen la funcionalidad de los Servicios Web usando la información contenida en un código BPEL y permiten la especificación de estándares de seguridad WS-Security. Por lo tanto, la propuesta descrita en este artículo propone una primera aproximación de obtención de Servicios Web seguros desde un SBP utilizando un conjunto de herramienta relacionadas entre si.

El trabajo futuro se debería centrar en refinar las tecnologías utilizadas, ya que el plugin SecurityStereotypes fue creado para Eclipse Indigo bajo el Sistema Operativo Windows 7 y el resto de la propuesta fue creado en Eclipse Ganymede en Ubuntu, versión 10.4. Por último, se debe desarrollar todos los requisitos de seguridad descritos en un SBP.

## REFERENCIAS

- [1] Axis2. (2011). *Apache Axis2*. Available: <http://axis.apache.org/axis2/java/core/>
- [2] G. Frankova, "Engineering Business Process with Service Level Agreements," International Doctorate School in Information and Communication Technologies, 2010.
- [3] J. Jürjens, *Secure Systems Development with UML*: Springer-Verlag, 2005.
- [4] F. Kamoun, "A Roadmap towards the Convergence of Business Process Management and Service Oriented Architecture," *Ubiquity*, vol. 2007, 2007.
- [5] B. Kitchenham, "Guideline for performing Systematic Literature Review in Software Engineering," *Software Engineering Group, Department of Computer Science, Keele University*, vol. 2.7, 2007.
- [6] R. Ko, S. Lee, and E. W. Lee, "Business process management (BPM) standars: a survey," *Emerald*, vol. 15, pp. 744-791, 2009.
- [7] T. v. Lessen, "Business Process Management with BPMN & BPEL," *International Workshop BPM III*, 2011.
- [8] G. Márquez, A. Rodríguez, and E. Fernández-Medina, "Revisión de la literatura sobre integración de especificaciones de seguridad en BPEL/XPDL desde Procesos de Negocio Seguro," *Congreso Internacional de Computación e Informática del Norte de Chile INFONOR-CHILE*, vol. 2, 2011.
- [9] M. Menzel, I. Thomas, and C. Meinel, "Security Requirements Specification in Service-oriented Business Process Management," *International Conference on Availability, Reliability and Security*, 2009.
- [10] OASIS, "Web Services Security Username Token Profile 1.1," OASIS Standard Specification 2006.
- [11] OASIS, "Web Services Business Process Execution Language Version 2.0," *OASIS*, 2007.
- [12] OASIS. (2011). *Open stAndarS for the Information Society*. Available: <http://www.oasis-open.org/>
- [13] OMG. (2011). *Business Modeling Model and Notation*.
- [14] C. Ouyang, M. Dumas, and A. H. M. T. Hofstede, "Translating BPMN to BPEL," *BPM Center Report*, 2006.
- [15] Rampart. (2011). *Apache Rampart*. Available: <http://axis.apache.org/axis2/java/rampart/>
- [16] A. Rodríguez, E. Fernández-Medina, and M. Piattini, "A BPMN Extension for the Modeling of Security Requirements in Business Processes," *IEICE trans. Information and Systems*, vol. E90-D, pp. 745-752, 2007.
- [17] R. Shapiro, "XPDL 2.2: Incorporating BPMN 2.0 Process Modeling Extensions," 2010.
- [18] A. Souza, B. L. B. Silva, F. Lins, J. Damasceno, N. Rosa, P. Maciel, R. Medeiros, B. Stephenson, H. Motahari-Nezhad, J. Li, and C. Northfleet, "Incorporating Security Requirements into Service Composition: From Modelling to Execution," *Service-Oriented Computing*, vol. 5900, pp. 373-388, 2009.
- [19] UML. (2011). *UML Resource Page*.
- [20] B. Warboys, "Software Process Technology, Third European Workshop, EWSPT '94, Villard de Lans, France, February 7-9, 1994, Proceedings," vol. 772, p. 252, 1994.
- [21] S. White, *Guía de Referencia y modelado BPMN. Comprendiendo y utilizando BPMN.*, 2009.
- [22] C. Wolter, M. Menzel, and C. Meinel, "Modelling Security Goals in Business Processes," *Computer and Information Science*, 2008.
- [23] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel, "Model-driven business process security requirement specification," *Journal of Systems Architecture*, pp. 211-223, 2009.



**Alfonso Rodríguez** es doctor en informática y magister en dirección de empresas. Actualmente es profesor asociado en el Departamento de Ciencias de la Computación y Tecnologías de la Información en la Universidad del Bio-Bio, Chillán, Chile. La actividad de investigación está concentrada en las áreas de ingeniería de software y sistemas de información, siendo la seguridad en procesos de negocio, el principal tema de investigación que ha desarrollado en los últimos años. Ha co-organizado el taller internacional de seguridad en sistemas de información en los años 2007 y 2008 formando actualmente parte del comité de programa así como también varias conferencias tales como International Conference on Enterprise Information Systems (ICEIS), ACM International Conference on Security of Information and Networks (SIN), Ibero-American Workshop on Data Quality (IAWDQ), Encuentro Chileno de Computación (ECC), entre otras.



**Eduardo Fernández-Medina** es doctor e ingeniero en informática. Es profesor contratado doctor a tiempo completo en la Escuela Superior de Informática de la Universidad de Castilla La-Mancha en Ciudad Real (España). Su actividad investigadora se centra en la seguridad de bases de datos, seguridad de servicios Web, requisitos de seguridad, métricas de seguridad y seguridad de sistemas de información avanzados. Es co-editor de varios libros y capítulos de libros sobre los anteriores temas y ha escrito varias docenas de artículos en conferencias nacionales e internacionales. Es miembro del grupo de investigación Alarcos del Departamento de Sistemas y Tecnologías de Información de la Universidad de Castilla La-Mancha en Ciudad Real (España). Así como de varias asociaciones profesionales y de investigación (ATI, AEC, AENOR, IFIP, WG11.3, etc.).



**Gastón Márquez** es Ingeniero Civil en Informática y Magister candidato en Ciencias de la Computación de la Universidad del Bio-Bio (Chile). Su actividad de investigación se centra en la Ingeniería de Software, siendo lo Procesos de Negocio, Servicios Web, seguridad en Procesos de Negocio y Servicios Web sus temas de interés. Ha participado en varias conferencias tales como Encuentro de Computación e Informática del Norte (INFONOR), Encuentro Chileno de Computación (ECC) y Encuentro Tesistas (ET), estos dos últimos pertenecientes a las Jornadas Chilenas de Computación.