Universidad del Bío-Bío
Facultad de Ciencias Empresariales
Departamento de Ciencias de la Computación y Tecnologías de la Información

Tesis de Magíster en Ciencias de la Computación

Integración de la Seguridad en la Capa de Negocio y la Interfaz de Usuario a través de ArchiMate, BPMN-BPSec e IFML

Chillán, Chile, Julio 2018

Estudiante: Luis Alfredo San Martín Muñoz
Director de Tesis: Dr. Alfonso Rodríguez Ríos

Resumen

Dentro de las organizaciones, la seguridad es un punto importante que tratar. Una manera de identificar y comprender las necesidades de seguridad de una organización es a través del uso de modelos que representan los diversos elementos de la organización. En la literatura existen múltiples trabajos que han establecido formas de modelar las necesidades de seguridad en algunos estándares de modelado. Dentro de los modelos utilizados por las organizaciones, se encuentran los modelos de arquitectura empresarial, de proceso de negocio y de interfaz de usuario, los cuales son modelados, en esta Tesis, con los lenguajes ArchiMate, BPMN e IFML, respectivamente. Éstos fueron seleccionados por ser los lenguajes estándar para modelar cada uno de estos modelos. Pese a que, en el estándar BPMN, no es posible especificar necesidades de seguridad, existen extensiones que lo permiten, siendo BPMN-BPSec una de ellas. Por otro lado, a través de la realización de una revisión sistemática de la literatura, se ha podido concluir que también es posible modelar algunas de las necesidades de seguridad en los estándares ArchiMate e IFML.

El enfoque de la Arquitectura Dirigida por Modelos define distintos niveles de abstracción de modelos y la transformación entre estos. Ya que parte del modelo ArchiMate considera el negocio de la organización, éste puede ser complementado con los procesos de negocio modelados con BPMN. Por esto, existe la posibilidad de establecer una correspondencia entre ambos modelos. Por otro lado, los modelos IFML permiten modelar interfaces de usuario de aplicaciones que integran los procesos de negocio de las empresas en el mundo digital. Esto permite mantener cierta relación entre los procesos de negocio modelados con BPMN y las interfaces de usuario modeladas con IFML, lo cual posibilitaría establecer una correspondencia entre ambos tipos de modelos.

En la literatura se han propuesto correspondencias de elemento a elemento entre ArchiMate y BPMN, pero a la fecha no se ha realizado una correspondencia modelo a modelo, lo cual implica reglas de transformación complejas. De igual manera no se han considerado los requisitos de seguridad en estas transformaciones. Por otro lado, las correspondencias entre BPMN e IFML no han sido abordadas en la literatura hasta ahora.

Debido a lo anterior, el objetivo de esta Tesis es definir un mecanismo que permita integrar la seguridad descrita a nivel de negocio, el cual es abordado por ArchiMate y BPMN, y la interfaz de usuario, la cual es abordada por IFML. Para ello, se establece una correspondencia entre los elementos que modelan los requisitos de seguridad, ya expresados en BPMN-BPSec, con los elementos de arquitecturas empresariales, definidos con ArchiMate, y los elementos de interfaz de usuario, definidos con IFML.

Así, durante esta investigación y con apoyo del conocimiento adquirido por medio de la realización de una revisión sistemática de la literatura, se ha logrado establecer reglas de transformación para modelos de arquitectura empresarial, procesos de negocio e interfaz de usuario, teniendo en consideración la seguridad como elemento central. Estas reglas han sido debidamente validadas a través de la experimentación y el análisis de las correspondencias propuestas. Además, se ha construido un prototipo de herramienta para la transformación desde ArchiMate hacia BPMN-BPSec, permitiendo una transformación automática y sin la intervención directa del modelador.

Abstract

Among organizations, security is an important point to treat. A way of identifying and comprehending the security needs of an organization is through the use of models that represent distinct elements of the organization. Multiple works that establish ways for modeling the security needs in some modeling standards exist in literature. Enterprise Architecture, Business Process and User Interface models exist among the models utilized by organizations, which are modeled, in this Thesis, with the ArchiMate, BPMN and IFML languages, respectively. These were selected due to their status as the standard languages for modeling each of these models. Although it is not possible to specify security needs in the BPMN standard, there are extensions that allow it, such as BPMN-BPSec. On the other hand, through the realization of a systematic literature review, it has been possible to conclude that it is also possible to model some security needs in the ArchiMate and IFML standards.

The Model-Driven Architecture approach defines distinct abstraction levels of models and the transformation between them. Since part of the ArchiMate model considers an organization´s business, this can be complemented by business processes modeled with BPMN. Due to this, it is possible to establish a correspondence between both models. On the other hand, IFML models allow modeling user interfaces of applications that integrate business processes of enterprises in the digital world. This allows maintaining a certain relationship between business processes modeled with BPMN and user interfaces modeled with IFML, which would allow stablishing a correspondence between both kinds of models.

Correspondences between elements of ArchiMate and BPMN have been proposed in literature, but, up to date, no correspondence between the models themselves, which implies complex transformation rules, has been done. Similarly, security requirements have not been considered in these transformations. On the other hand, correspondences between BPMN and IFML have not yet been tackled in literature.

Due to the above, the objective of this Thesis is to define a mechanism that allows the integration of security described at a business level, which is tackled by ArchiMate and BPMN, and the user interface, which is tackled by IFML. For this, a correspondence between the elements that model security requirements, which are already expressed in BPMN-BPSec, with the elements of enterprise architectures, defined with ArchiMate, and the user interface elements, defined with IFML, is established.

Thus, during this research and supported by the knowledge acquired through the realization of a systematic literature review, it has been possible to establish transformation rules for enterprise architecture, business processes and user interface models. This considering security as a core element. These rules have been adequately validated through the experimentation and the analysis of the proposed correspondences. Moreover, a tool prototype for the transformation from ArchiMate to BPMN-BPSec has been constructed, allowing an automatic transformation without the need of a modeler’s direct intervention.

Índice General

Índice de Tablas

Índice de Figuras

Capítulo 1: Introducción

La importancia de la seguridad aumenta cada día con el avance de la globalización y el uso cada vez más intensivo del Internet. La información que gestionan las organizaciones está en constante peligro, por lo que es fundamental establecer medidas de seguridad para resguardar dicha información. Frente a las cada vez mayores amenazas de seguridad que afectan a las organizaciones, adquiere valor la Ingeniería de Seguridad, área de la ingeniería que tiene que ver con la reducción del riesgo del daño intencionado no autorizado a los activos valiosos, a un nivel que es aceptable para los actores del sistema (Ahmed y Matulevičius, 2014). El aspecto fundamental de la ingeniería de seguridad es la gestión de riesgos que resultan de las amenazas potenciales que pueden afectar los activos de la empresa, es decir, crear contramedidas para combatir las amenazas (Menzel *et al.*, 2009). Los elementos que conforman la empresa son activos que deben ser protegidos, pero para proteger algo lo principal es identificarlo. En este sentido, los modelos usados en las organizaciones facilitan la identificación de los elementos que forman la empresa y de esta forma se hace más fácil establecer mecanismos de seguridad para dichos elementos.

En la última década la necesidad de abarcar la seguridad en el inicio de los proyectos ha traído consigo la idea de representar la seguridad en diversas notaciones y lenguajes, entre los que se encuentran los modelos de procesos de negocio. La creación de BPMN-BPSec (Rodríguez *et al.*, 2007), UMLSec (Saleem *et al.*, 2012), SecureBPMN (Brucker, 2013) y otras notaciones que utilizan los estándares existentes para modelar la seguridad en procesos de negocio da cuenta de esto (Menzel *et al.*, 2009).

Por su parte, la importancia que se le ha dado a los modelos en los últimos años ha provocado el surgimiento de distintos métodos, enfoques, metodologías y/o marcos de trabajo que buscan integrar estos modelos en el proceso de desarrollo de software. Entre los enfoques propuestos destaca la Arquitectura Dirigida por Modelos (MDA por las siglas en inglés de Model Driven Architecture) (OMG, 2017) propuesta por la Object Management Group (OMG) que pretende dar solución al problema de las plataformas cambiantes y a la portabilidad de los sistemas de información. MDA propone la definición de modelos con distintos niveles de abstracción: modelos independientes de la computación (CIM, siglas en inglés Computation Independent Model), modelos independientes de plataforma (PIM, por sus siglas en inglés Platform-Independent Model) y modelos para plataformas específicas (PSM, por sus siglas en inglés Platform-Specific Model) y la generación automática de código a través de transformaciones entre estos modelos (Jacho *et al.*, 2015).

Existen diferentes lenguajes para modelar los distintos ámbitos de las organizaciones, algunos propios y otros han llegado a ser estándares que incluso entregan mecanismos de extensibilidad permitiendo agregar elementos al lenguaje. Dentro de estos ámbitos se encuentra la arquitectura empresarial, los procesos de negocio y las interfaces de usuario de sus aplicaciones. Los dos primeros son muy destacados a nivel de negocio en las empresas y las interfaces de usuario son un aspecto relevante en el desarrollo de software.

Como se expone en Feltus *et al.* (2014), la arquitectura empresarial define los elementos que conforman la organización, el modo en que estos elementos interactúan entre ellos y el entorno, y el modo en que se organizan y son fuente de información para la toma de decisiones. Los modelos de arquitectura empresarial permiten representar los sistemas de información de las empresas en un conjunto de esquemas denominados puntos de vista. Aunque existen varios

estándares y herramientas para crear modelos de arquitectura, en esta Tesis se utiliza ArchiMate (The Open Group, 2013), un estándar muy usado en la industria para el modelado de arquitecturas empresariales.

Por su parte, los procesos de negocio son la combinación del conjunto de actividades que las empresas deben realizar siguiendo una estructura que describe su orden operativo y dependencias, para perseguir un objetivo o resultado deseado (Paja *et al.*, 2011). Los modelos de procesos de negocio permiten un entendimiento común y el análisis de un proceso de negocio (Paja *et al.*, 2011). También existe más de un estándar para representar procesos de negocio, no obstante, BPMN (Business Process Modeling and Notation) (OMG, 2011) es un estándar de *facto* en la industria (Harmon y Wolf, 2008). En esta Tesis se utilizará un trabajo previo (Rodríguez *et al.*, 2007) en el que se extiende la notación de BPMN con BPSec (Business Process Security), el cual permite integrar seguridad en la descripción de procesos de negocio.

Finalmente, hasta ahora en el área de las interfaces de usuario, el diseño y construcción se realiza en su mayoría de forma manual. Comúnmente no se usan modelos, a diferencia de la arquitectura empresarial y los procesos de negocio donde sí son usados. En los últimos años los investigadores vieron la necesidad de contar con una notación para modelar interfaces de usuario y crearon un estándar llamado IFML (Interaction Flow Modeling Language), sucesor formal de otra notación anterior llamada WebML (Web Modeling Language) (Wazlawick, 2014). IFML es el estándar para modelar interfaces de usuario utilizado en esta Tesis.

Puesto que la idea central de esta Tesis es modelar la seguridad integrando arquitecturas empresariales, procesos de negocio e interfaces de usuario, se ha considerado que modelar la seguridad en la capa de negocio de un modelo de arquitectura empresarial significa que por lógica si existe un modelo de proceso de negocio de la misma empresa, dicho modelo debe ser consistente a lo expresado en el modelo de arquitectura empresarial, es decir debe modelar los procesos de negocio y la seguridad de los mismos al igual que en el modelo de arquitectura empresarial (puesto que son abstracciones de una misma realidad). De igual forma, las interfaces de usuario de aplicaciones que integran los procesos de negocio al mundo digital, tienen relación con estos ultimos, por ello, si existe un modelo de interfaz de usuario de una aplicación computacional para la misma empresa mencionada anteriormente, entonces esta interfaz de usuario debe ser consistente al modelo de proceso de negocio de la empresa incluyendo la seguridad modelada en él. Es importante no perder la lógica del negocio relacionada a la seguridad en los distintos modelos, para lo cual debe existir una trazabilidad de los requisitos que permita hacer el seguimiento de los requisitos y su evolución a través de los modelos.

ArchiMate puede ser complementado con BPMN, es decir, se puede modelar la lógica del negocio con muy poco detalle en un modelo de arquitectura empresarial y complementarlo con un modelo más detallado en un modelo BPMN. Hasta el momento no se han encontrado trabajos que permitan establecer una transformación desde la capa de negocio de ArchiMate considerando las necesidades de seguridad (requisitos de seguridad) a BPMN y luego a IFML. Por esto, esta Tesis se enfoca en modelar requisitos de seguridad en la capa de negocio de ArchiMate, establecer una correspondencia que permite transformar la capa de negocio de un modelo de arquitectura empresarial ArchiMate con requisitos de seguridad a un modelo de proceso de negocio seguro BPMN-BPSec, y luego usar dicho modelo obtenido en BPMN-BPSec y realizar una correspondencia hacia IFML. La idea detrás de esto se basa en que, tener una correspondencia

entre los estándares mencionados anteriormente ayuda a mantener los objetivos de seguridad alineados entre el negocio y las Tecnologías de la Información.

1.1 Hipótesis y Objetivos

Los objetivos de las organizaciones son la base de estas, y una de las premisas más fundamentales en la gestión de la organización es el avanzar en dirección hacia los objetivos. Hoy en día es primordial que dentro de los objetivos de las organizaciones se encuentren algunos que tengan relación con la seguridad y que éstos se apliquen no solo en el negocio, sino que también en las TI (Tecnologías de la Información). No obstante, es difícil que los objetivos de seguridad entre el negocio y las TI estén en perfecta sincronía. Así, la hipótesis detrás de esta investigación es que:

"Es posible establecer una correspondencia entre los requisitos de seguridad a nivel de arquitectura empresarial, procesos de negocio e interfaz de usuario para mantener alineados los objetivos de seguridad entre el negocio y las TI de la organización".

Para demostrar esto, en esta Tesis se tiene como objetivo general:

"Definir un mecanismo para integrar la seguridad en la capa de negocio y la interfaz de usuario, estableciendo una correspondencia entre los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec y los elementos de ArchiMate e IFML".

Se debe tener claro que una correspondencia puede implicar transformaciones entre modelos o búsqueda de equivalencias. Esto no implica necesariamente transformaciones descritas a nivel de los metamodelos de los estándares involucrados.
La Figura 1 muestra de forma gráfica el objetivo de la Tesis. Considerando los niveles de abstracción que establece la Arquitectura Dirigida por Modelos (MDA), tanto ArchiMate como BPMN se encuentran a nivel de CIM, e IFML a nivel de PIM, tal como se muestra en el costado derecho de la Figura 1.

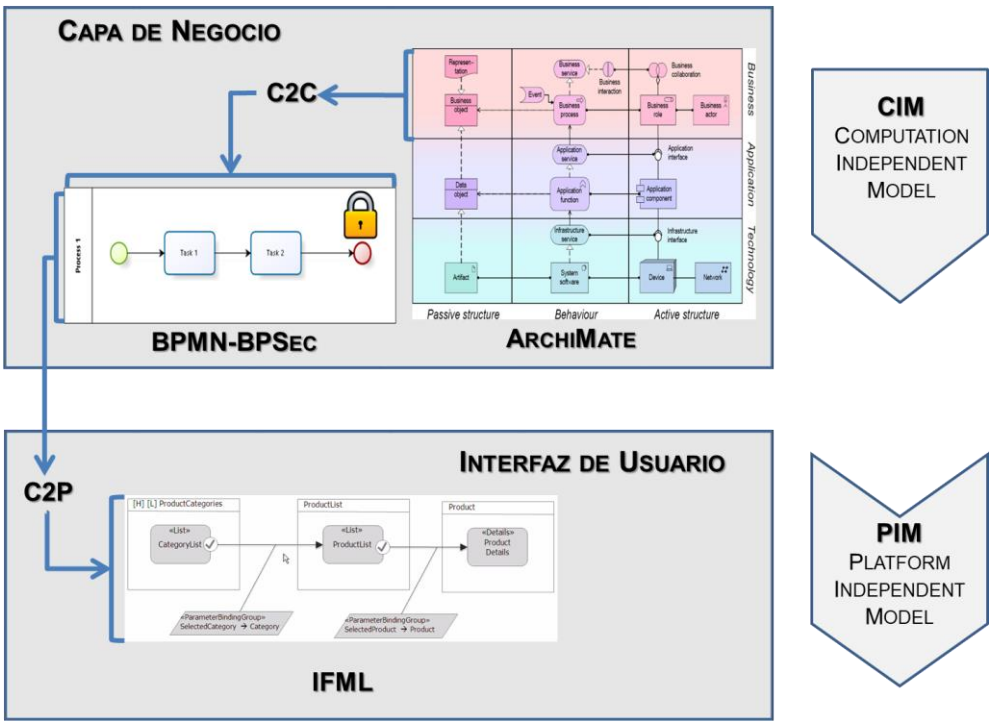


Figura 1: Modelo de la propuesta de Tesis.

Una de las tres capas más importantes de ArchiMate es la capa de negocio y ésta puede ser complementada con BPMN para su descripción más detallada. La capa de negocio es la capa superior en la imagen que representa ArchiMate y BPMN, se representa con un modelo de ejemplo a su lado en la Figura 1. Se puede decir que un modelo BPMN está dentro de la capa de negocio de la empresa. Una parte del objetivo de esta Tesis consiste en definir la forma en que se modelan los requisitos de seguridad en la capa de negocio de ArchiMate para así poder establecer una correspondencia hacia BPMN-BPSec en una correspondencia que se identifica como C2C (de CIM a CIM), lo cual se muestra en la parte superior de la Figura 1. La otra parte de esta Tesis consiste en definir cómo se modelan los requisitos de seguridad en IFML para establecer una correspondencia del modelo BPMN-BPSec a IFML, correspondencia que se identifica como C2P (de CIM a PIM), lo que se muestra en la parte inferior de la Figura 1.
Los objetivos específicos, establecidos para lograr el objetivo general son:

- Revisar la literatura para buscar especificaciones de seguridad en los estándares ArchiMate e IFML.
- Revisar la literatura para buscar mapeos o transformaciones entre ArchiMate-BPMN y BPMN-IFML (con y sin elementos de seguridad).
- Establecer una correspondencia entre los elementos de ArchiMate y los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec.
- Establecer una correspondencia entre los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec y los elementos de IFML.
- Validar la pertinencia de los resultados del punto anterior mediante un grupo de expertos.

Aunque la identificación de los requisitos de seguridad en ArchiMate e IFML no se establece en los objetivos específicos, es necesario primero identificar cómo modelar éstos en ambos lados para poder realizar la correspondencia.
El alcance de la investigación considera solo los estándares ArchiMate e IFML y la extensión BPMN-BPSec. La investigación está centrada en requisitos de seguridad a nivel de arquitectura empresarial, procesos de negocio e interfaces de usuario. Para el conjunto de requisitos de seguridad se tienen en cuenta solo los que son cubiertos por la extensión BPMN-BPSec.

1.2 Organización de la Tesis de Magíster

Esta Tesis de Magíster se organiza de la siguiente manera: en el Capítulo 2 denominado "Conceptos Relacionados", se presenta una serie de conceptos que fueron utilizados para establecer el contexto en el cual se desarrolla esta Tesis; en el Capítulo 3 denominado "Trabajos Relacionados", se presenta una revisión sistemática de la literatura que da como resultado los principales trabajos en donde se integra la seguridad en ArchiMate e IFML, así como también trabajos en que se desarrollan transformaciones desde modelos ArchiMate hacia BPMN y desde BPMN hacia IFML; en el Capítulo 4 denominado "Correspondencia de ArchiMate a BPMN-BPSec" se plantea la correspondencia de la capa de negocio de un modelo ArchiMate con requisitos de seguridad hacia un modelo de proceso de negocio seguro descrito con BPMN-BPSec; en el Capítulo 5 denominado "Correspondencia de BPMN-BPSec a IFML", se plantea la correspondencia de un modelo de proceso de negocio seguro BPMN-BPSec hacia un modelo de interfaz de usuario modelado con IFML; en el Capítulo 6 denominado "Prototipo de Herramienta", se plantea un prototipo de una herramienta que permite transformar la capa de negocio de un modelo ArchiMate a un modelo BPMN-BPSec de forma automática usando reglas de transformación establecidas con el lenguaje ATL; en el Capítulo 7 denominado "Experimentación y Análisis de Resultados", se desarrolla un cuasi experimento con el objetivo de confirmar que lo propuesto en los Capítulo 4 y 5 es válido; y, finalmente, en el Capítulo 8 denominado "Conclusiones", se verifica si los objetivos propuestos en esta Tesis han sido cumplidos y se presentan las conclusiones respecto del trabajo realizado.

Capítulo 2: Conceptos Relacionados

En este capítulo se introducirán los conceptos que se asocian a esta Tesis. En la Sección 2.1 se describe la Arquitectura Empresarial con el estándar ArchiMate, en la Sección 2.2 se describen los procesos de negocio con el estándar BPMN, además de los modelos de proceso de negocio seguro descritos en la extensión BPMN-BPSec, para finalmente en la Sección 2.3, concluir con una descripción de los modelos de interfaz de usuario descritos con el estándar IFML.

2.1 Arquitectura Empresarial con ArchiMate

El estándar IEEE 1471-2000 define la arquitectura como la organización fundamental de un sistema basado en sus componentes, la interrelación entre éstos y el entorno, y los principios que guían su diseño y evolución (Maier *et al.*, 2004). Una Arquitectura Empresarial (EA, por sus siglas en inglés de Enterprise Architecture) se define como una arquitectura en la que el sistema abarca toda una organización, cuyos componentes fundamentales son los procesos del negocio, las tecnologías y los sistemas de información de la empresa y sus respectivas relaciones (Escobar *et al.*, 2013). Uno de los propósitos principales de la Gestión de la Arquitectura Empresarial (EAM, por las siglas en inglés de Enterprise Architecture Management) es alinear una empresa con sus objetivos de negocio y requerimientos, y específicamente en el contexto de metas de servicios de negocio. La EAM ayuda a diseñar y garantizar una coherente estructura organizacional de la empresa, procesos de negocio y la infraestructura a través de un conjunto de modelos (Grandry *et al.*, 2013a).

ArchiMate es un estándar de The Open Group y un lenguaje que complementa TOGAF (The Open Group Arquitecture Framework) (The Open Group, 2011), el esquema (o marco de trabajo) de arquitectura empresarial que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial. ArchiMate está constituido por un metamodelo y un lenguaje de modelado común para describir la construcción y operación de los procesos del negocio, estructuras organizacionales, flujos de información, sistemas de TI e infraestructura técnica (Escobar *et al.*, 2013). Este lenguaje está en constante mejora puesto que cuenta con un foro donde los investigadores adscritos a The Open Group realizan aportes, los cuales posteriormente son incluidos en las versiones oficiales de ArchiMate (Grandry *et al.*, 2013a).

ArchiMate 2.1 introduce una representación en capas de la arquitectura empresarial, organizado en 3 capas de abstracción: negocio, aplicación y tecnología. Las capas se ajustan a estrictas dependencias que van de capa superior (negocio) a capa inferior (tecnología), es decir, los elementos de la capa de negocio tiene dependencias en los elementos de la capa de aplicación, que tienen dependencias en los elementos de la capa de tecnología (The Open Group, 2013). En ArchiMate 3.0 (versión actual) se introducen otras capas que se observan en la Figura 2, pero las capas de negocio, aplicación y tecnología siguen siendo las capas del núcleo (The Open Group, 2016).

El núcleo del lenguaje consiste en tres tipos principales de elementos o también llamados aspectos del lenguaje para representar: una estructura pasiva (un objeto en el que se lleva a cabo el comportamiento), el comportamiento (una unidad de actividad realizada por uno o más elementos activos de estructura) y una estructura activa (una entidad que es capaz de realizar comportamiento) (The Open Group, 2013) . En ArchiMate 3.0 y como se muestra en la Figura 2

estos tipos de elementos son llamados aspectos, a los cuales se agrega la anteriormente llamada extensión de motivación (motivation aspect del inglés, que modela el "porqué" de la arquitectura), aunque los otros tres anteriores siguen siendo los aspectos del núcleo (The Open Group, 2016).

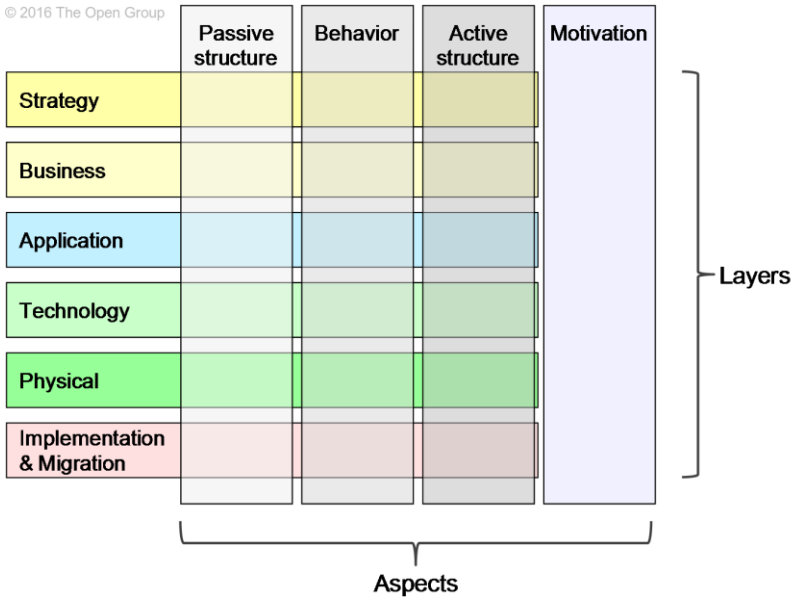


Figura 2: Capas y aspectos de ArchiMate (The Open Group, 2016)

ArchiMate cuenta con un metamodelo que contiene sólo los conceptos básicos y las relaciones que sirven a los propósitos de modelado de la arquitectura de la empresa en general. A través de su metamodelo ArchiMate facilita mecanismos de extensión del lenguaje a dominios más específicos (The Open Group, 2013).

ArchiMate es utilizado por las empresas pues existe un conjunto de herramientas comerciales que le da soporte. Entre ellas se puede mencionar: Archi, Sparx Enterprise Architect y BiZZdesign Architect (Korman *et al.*, 2014).

Como ya se ha dicho, existe más de un estándar para representar Arquitectura Empresarial, sin embargo, en esta Tesis se usa ArchiMate por su amplio uso (Korman *et al.*, 2014), su relación con TOGAF (The Open Group, 2011) y su metamodelo basado en el estándar MOF (OMG, 2002).

Aunque no se encontraron trabajos donde se relacione ArchiMate de forma explícita con su correspondencia en los niveles del enfoque MDA, se puede decir (y así se ha interpretado en esta Tesis) que su capa de negocio al igual que BPMN (solo la parte de modelado), se encuentra en el nivel de modelo independiente de la computación (CIM) del enfoque de la Arquitectura Dirigida por Modelos.

2.2 Procesos de negocio con BPMN

Los procesos de negocio permiten describir las actividades que ocurren dentro de la organización y que conducen al cumplimiento de fines específicos. Un proceso de negocio es un conjunto de tareas unidas que tienen como objetivo la entrega de un servicio o producto a un cliente (Weske, 2008).

Los procesos de negocio pueden ser modelados a través de los estándares BPMN 2.0 (versión actual), los Diagramas de Actividad de UML 2.5 (OMG, 2015b), entre otros. No obstante en la industria, BPMN es el estándar preferido para modelar procesos de negocio (Harmon y Wolf, 2008). En la versión 2.0 de BPMN se incorpora un metamodelo robusto basado en MOF y mecanismos de extensibilidad fortaleciendo que sea un estándar *de facto* en la industria (OMG, 2011). A nuestro juicio, razones suficientes, para que sea elegido como el estándar de modelado de procesos de negocio a usar en esta Tesis.

BPMN fue publicado por primera vez en el año 2004 por el Business Process Management Iniciative (BPMI) y, posteriormente, adoptado por la OMG como especificación en el año 2006. BPMN es un lenguaje formal que permite modelar, simular y, eventualmente, ejecutar procesos de negocio (Curto, 2013).

BPMN es una notación para modelamiento de procesos de negocio cuyo objetivo es proveer de una notación gráfica estandarizada en formato de flujo de trabajo, fácil de entender y de comunicar entre usuarios de todo nivel. Con esto se busca que los usuarios del negocio y los desarrolladores técnicos les sea fácil entender el flujo y el proceso. BPMN 2.0 incorpora características nuevas para la construcción de modelos ejecutables, que permite la construcción de diagramas, que puedan ser ejecutados sobre un motor de procesos (Jacho *et al.*, 2015). Los modelos creados con BPMN se consideran modelos independiente de la computación (CIM) según los niveles de abstracción establecidos por MDA (Rodríguez *et al.*, 2010). BPMN 2.0 introduce un mecanismo de extensibilidad que permite agregar elementos estándar BPMN con atributos adicionales. Este mecanismo puede ser utilizado por modeladores y herramientas de modelado para añadir elementos no estándar o artefactos para satisfacer una necesidad específica (OMG, 2011).

2.2.1 BPMN-BPSec

BPSec es una extensión para BPMN (Rodríguez *et al.*, 2007) y diagramas de actividad UML (Rodríguez *et al.*, 2011) a través de la cual es posible modelar la seguridad en procesos de negocio. La extensión BPSec contempla los siguientes requisitos de seguridad: control de acceso, detección de amenazas y ataques, auditoria de seguridad, integridad, no repudio y privacidad. Su notación y descripción se muestra en la Tabla 1. La extensión está compuesta por 17 estereotipos, definidos con una descripción y una notación que pretenden dejar claro su uso y que sea entendible por expertos del negocio.

Notación	Requisito de Seguridad	Descripción
	Access Control	Establece la necesidad de intensificar y definir mecanismos para restringir el acceso a cierto recurso.
	Attack Harm Detection	Detección de ataques o amenazas
	Audit Register (AR)	Necesidad de registrar los eventos de seguridad con el propósito de su posterior análisis.
	Integrity	Protección de la intencional y no autorizada corrupción de componentes. En la notación se usa una x que se reemplaza por una "w", una "m" o una "h", para indicar la especificación de integridad baja (w), integridad media (m) e integridad alta (h).
	Non Repudiation	Necesidad de evitar la negación de cualquier aspecto de la interacción.
	Privacy	Necesidad de evitar que entidades no autorizadas obtengan información. En la notación se usa una x que se reemplaza por una "a" o una "c", para indicar anonimato (a) o confidencialidad (c).

Tabla 1: Requisitos de seguridad incluidos en BPMN-BPSec (Rodríguez *et al.*, 2011)

En Rodríguez *et al.* (2010) se presenta un conjunto de reglas de transformación QVT (Query View Transformations) bajo el enfoque de la Arquitectura Dirigida por Modelos que permiten obtener diagramas de casos de uso y diagramas de clases UML a partir de un modelo de negocio seguro modelado en BPMN y UML-AD (UML Activity Diagram) con la extensión BPSec.

2.3 Interfaz de Usuario con IFML

El objetivo del estándar IFML (OMG, 2015a) es proporcionar a los arquitectos de sistemas, ingenieros de software y desarrolladores de software las herramientas para la definición de modelos de flujo de interacción que describen las principales dimensiones de un Front End de una aplicación. Fue publicado como estándar oficialmente en el año 2013.

Una de las principales ventajas de IFML es que no es una iniciativa independiente aislada de otros métodos de modelado. Por el contrario, IFML está profundamente arraigado dentro del enfoque MDA de la OMG. Está considerado como un modelo independiente de plataforma (PIM) (OMG, 2015a; Wazlawick, 2014).

IFML presta especial atención a la facilidad de uso y entendimiento de los modelos (OMG, 2015a; Wazlawick, 2014). Es conciso, evitando la redundancia y reduciendo el número de tipos de diagramas y conceptos necesarios para expresar la interfaz y la interacción de las decisiones de diseño más destacadas. Incluye extensibilidad en la definición de nuevos conceptos (por ejemplo nuevos tipos de eventos). Se asegura de la aplicabilidad, es decir, que apoya la construcción de marcos de transformación de modelos y generadores de código que pueden transformar PIM en un modelo para plataforma específica (PSM) adecuado y, en última instancia, en las aplicaciones ejecutables para una amplia gama de plataformas tecnológicas y dispositivos (OMG, 2015a).

IFML es adecuado para modelar interfaces de usuario, especialmente aquellas que hacen uso de datos, tales como los sistemas de información (Wazlawick, 2014).

IFML utiliza los mecanismos de extensibilidad de UML para permitir la definición de estereotipos, valores etiquetados y restricciones. Las extensiones están destinadas a perfeccionar la semántica de los conceptos básicos o para proporcionar casos específicos de los conceptos básicos como tal, por lo tanto, deben perfeccionar la semántica de los conceptos IFML y no modificarlo (Brambilla y Fraternali, 2014; OMG, 2015a).
En la Tabla 2 se presentan algunos de los elementos del núcleo más usados.

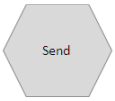
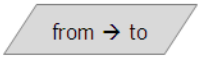
Notación	Nombre	Definición
	View Container	Un elemento de la interfaz que comprende elementos que muestran el contenido y soportando la interacción y otros ViewContainers
	View Component	Un elemento de interfaz que muestra contenido o acepta entradas.
	Event	Una ocurrencia que afecta el estado de la aplicación.
	Action	Una pieza de lógica empresarial desencadenada por un evento.
	Navigation Flow	Actualización de los elementos de la interfaz en la vista o activación de una acción causada por la ocurrencia de un evento. Los datos pueden estar asociados con el flujo a través de enlaces de parámetros.
	Data Flow	Datos pasando entre ViewComponents o Acciones como consecuencia de una acción previa del usuario.
	Parameter Binding	Especificación de que un parámetro de entrada de una fuente está asociado con un parámetro de salida de un objetivo.
	Activation Expression	Expresión booleana asociada con un ViewElement, ViewComponentPart or Event: si es verdadero el elemento está habilitado.

Tabla 2: Algunos de los elementos del núcleo de IFML (OMG, 2015a)

IFML ha sido usado en esta Tesis por ser el único lenguaje estándar de modelado de interfaz de usuario que produce modelos independientes de plataforma y por tener un metamodelo basado en MOF, lo que permite realizar una transformación de modelos basados en este último.
IFML en su especificación cuenta con 18 elementos del núcleo y 8 elementos de extensión (OMG, 2015a).

Capítulo 3: Trabajos Relacionados

Existen múltiples formas originales para realizar una investigación sobre un tema o interrogante de investigación, no obstante también existen metodologías formales. En el año 2004, Barbara Kitchenham (Kitchenham, 2004) introdujo el concepto de "Revisión Sistemática de la Literatura" (RSL), como una metodología que formaliza las etapas para el desarrollo de una revisión de la literatura que es aplicable a distintos ámbitos o áreas. Desde ese entonces algunos investigadores han utilizado dicha estructura para realizar sus revisiones de la literatura obteniendo muy buenos resultados. Una RSL es un método para identificar, evaluar, interpretar y sintetizar las investigaciones científicas existentes con respecto a un tema. Este tipo de revisiones se realizan de forma rigurosa e imparcial para que tengan un alto valor científico (Pino *et al.*, 2006). Se definen protocolos de búsqueda y revisión, se busca toda la información relevante sobre un tema y se documenta el proceso.

El método formalmente consta de 3 etapas. Una primera etapa de "planificación de la revisión" que tiene como propósito definir los parámetros más importantes que serán tomados en cuenta cuando se lleve a cabo la revisión, más específicamente, tiene como objetivo identificar y definir formalmente el objetivo de la investigación y los protocolos de revisión. La siguiente etapa es el "desarrollo de la revisión" donde se lleva a cabo la revisión. En esta etapa se aplican los protocolos definidos en la etapa de planificación por lo que se dice que el desarrollo es guiado por la planificación pero no es que sean un proceso rígido, ya que en la etapa de desarrollo se pueden llevar a cabo modificaciones de la planificación. Finalmente se encuentra la etapa de "presentación de resultados" que como su nombre lo indica, consiste en presentar los resultados obtenidos en la etapa de desarrollo.

En esta sección se presenta la aplicación de cada uno de los pasos de la revisión sistemática de la literatura que tienen como propósito cumplir los 2 primeros objetivos específicos de esta Tesis.

3.1 Primera etapa: Planificación de la Revisión

El objetivo de la investigación consta de dos partes estrechamente relacionadas, por un lado se busca identificar en la literatura especificaciones de seguridad en los estándares ArchiMate e IFML y transformaciones o correspondencia de elementos entre ArchiMate-BPMN y BPMN-IFML con y sin elementos de seguridad. Y por otro lado se busca identificar los elementos de ArchiMate e IFML con los que se pueden representar los requisitos de seguridad que contempla la propuesta BPMN-BPSec o brindar las bases para ello. Para la realización de la RSL se han utilizado principalmente los motores de búsqueda de material científico: Google Scholar, Scopus, ScienceDirect y SpringerLink, la página Web de WebRatio y en menor proporción Google.

Como protocolo de búsqueda se utilizaron combinaciones de los términos "Security", "non-functional requirement", "transformation", "mapping", "derivation", "correspondence", "BPMN", "Archimate" e "IFML". Bajo el criterio de que IFML posee una estrecha relación con su antecesor "WebML", se consideró este término también.

La estrategia de búsqueda aplicada consistió en el uso principalmente de los motores de búsqueda de material científico nombradas anteriormente. Cuando los artículos no estaban disponibles se buscó en Internet en general a través de Google y en páginas Web de los autores de los artículos. Y se consideró la búsqueda de los artículos relacionados con los que ya habían sido seleccionados. En el caso particular de IFML, también se realizó una búsqueda en la página

Web de WebRatio (https://www.webratio.com/) ya que este sitio provee una serie de documentos relacionados a IFML dentro de los cuales era posible que existiera información importante para esta Tesis. Los registros de las búsquedas se hicieron en un documento Excel y los artículos aceptados fueron agregados al gestor de referencias bibliográficas.

Como criterio de inclusión se consideraron todos aquellos trabajos o estudios realizados considerando un rango de año que depende del estándar y el año de su primera publicación (desde el año 2008 para ArchiMate y 2012 para IFLM). Se buscó en inglés y español considerando las especificaciones de seguridad u otro requisito no funcional en ArchiMate, IFML y transformaciones o correspondencias de elementos entre los estándares BPMN, ArchiMate e IFML con y sin elementos de seguridad u otro requisito no funcional y que se enmarquen en algunos de los siguientes tópicos: i) propuestas de mejora de estándares, extensiones, especificaciones y perfiles para integrar y/o especificar seguridad u otro requisito no funcional en ArchiMate o IFML y ii) aplicación de transformaciones entre modelos BMPN, ArchiMate e IFML con y sin elementos de seguridad u otro requisito no funcional. Los artículos relacionados con WebML se relacionan a los tópicos de IFML.

Se estableció que se excluirían todos aquellos estudios que, a pesar de contener los términos de búsqueda o combinaciones de ellos, no aporten información relevante sobre el tema.

La idea de incluir trabajos que traten otros requisitos no funcionales se basa en que pueden existir similitudes entre la forma de modelar requisitos de seguridad y cualquier otro requisito no funcional. Además, contar con trabajos que modelen otros requisitos no funcionales puede ser de ayuda para definir la forma de modelar los requisitos de seguridad.

Se estableció una estrategia de extracción de datos que consiste en tener en cuenta:

- Comunidad a que está orientado el artículo (introducción, trabajos relacionados, referencias)
- Contribuciones (resumen, introducción, conclusión).
- Posibles consecuencias de las contribuciones (aplicaciones directas, nuevas técnicas, introducción)
- Información detallada necesaria para la revisión y los fundamentos de un marco de trabajo, las características de un modelo, etc. (preliminares, cuerpo del artículo).

Finalmente se estableció una estrategia de síntesis de datos de acuerdo a los siguientes temas:

- Integración o especificaciones de seguridad u otro requisito no funcional en ArchiMate.
- Integración o especificaciones de seguridad u otro requisito no funcional en IFML.
- Transformación o correspondencia de elementos entre ArchiMate y BPMN
- Transformación o correspondencia de elementos entre BPMN e IFML.
- Transformación o correspondencia de elementos entre ArchiMate y BPMN con seguridad u otro requisito no funcional.
- Transformación o correspondencia de elementos entre BPMN e IFML con seguridad u otro requisito no funcional.

3.2 Segunda etapa: Desarrollo de la Revisión

En base a la planificación se realizó la etapa de desarrollo donde se estableció la Tabla 3 en la cual se muestran las combinaciones buscadas para ArchiMate y la Tabla 4 donde se muestran las combinaciones buscadas para IFML. Para la búsqueda en la página Web de WebRatio no se consideró ningún término sino que se revisó todo, ya que la página no provee una herramienta de búsqueda por términos o combinaciones de términos.

ID	Combinación de Términos	Criterio de Año
1	"Security" OR "non-functional requirement" AND "ArchiMate"	2008 (ArchiMate fue estandarizado en el 2008)
2	"transformation" OR "mapping" OR "derivation" OR "correspondence" AND "BPMN" AND "Archimate"	2008 (ArchiMate fue estandarizado en el 2008)

Tabla 3: Combinación de términos para la búsqueda en ArchiMate

ID	Combinación de Términos	Criterio de Año
3	"Security" OR "non-functional requirement " AND "IFML"	2012 (IFML es estandarizado en el 2013, se desarrolló entre el 2012 al 2013)
4	"transformation" OR " mapping " OR " derivation" OR "correspondence" AND "BPMN" AND "IFML"	2012 (IFML es estandarizado en el 2013, se desarrolló entre el 2012 al 2013)
5	"patterns" AND "IFML"	2012 (IFML es estandarizado en el 2013, se desarrolló entre el 2012 al 2013)
6	"requirement" AND "IFML"	2012 (IFML es estandarizado en el 2013, se desarrolló entre el 2012 al 2013)
7	"requirement" AND "WebRatio"	2012 (IFML es estandarizado en el 2013, se desarrolló entre el 2012 al 2013)
8	"Security" OR "requirement "AND "WebML"	1999 (aproximadamente en esa fecha se generó WebML)

Tabla 4: Combinación de términos para la búsqueda en IFML

En base a las búsquedas se construyó la Tabla 5 de resumen, en la que se presentan los resultados de todas las búsquedas realizadas por cada combinación de términos y motor de búsqueda.

ID	Motor de Búsqueda	Combinación de Términos	Número de Resultados	Total Revisados	Total Revisión Preliminar	Total Revisión en Profundidad	Fecha Búsqueda
1	Google Scholar	1	820	78	16	13	01-07-2016
2	Scopus	1	14	14	0	0	11-07-2016
3	ScienceDirect	1	26	26	0	0	11-07-2016
4	SpringerLink	1	144	20	0	0	17-07-2016
5	Google Scholar	2	484	58	4	4	17-07-2016
6	Scopus	2	39	39	0	0	24-07-2016
7	ScienceDirect	2	21	21	0	0	25-07-2016
8	SpringerLink	2	113	20	0	0	25-07-2016
9	Google Scholar	3	38	38	4	3	21-05-2016
10	Scopus	3	4	4	0	0	30-05-2016
11	ScienceDirect	3	22	22	0	0	30-05-2016
12	SpringerLink	3	1	1	0	0	06-06-2016
13	Google Scholar	4	32	32	0	0	23-05-2016
14	Scopus	4	3	3	0	0	30-05-2016
15	ScienceDirect	4	5	5	0	0	31-05-2016
16	SpringerLink	4	7	7	0	0	06-06-2016
17	Google Scholar	5	85	85	0	0	27-05-2016
18	Scopus	5	19	19	0	0	30-05-2016
19	ScienceDirect	5	41	41	0	0	04-06-2016
20	SpringerLink	5	8	8	0	0	06-06-2016
21	Google Scholar	6	46	46	0	0	05-06-2016
22	Scopus	6	16	16	0	0	05-06-2016
23	ScienceDirect	6	38	38	0	0	06-06-2016
24	SpringerLink	6	12	12	0	0	06-06-2016
25	Google Scholar	7	117	117	6	2	11-06-2016
26	Scopus	7	40	40	1	0	21-06-2016
27	ScienceDirect	7	20	20	0	0	21-06-2016
28	SpringerLink	7	49	49	1	1	25-06-2016
29	Google Scholar	8	1.610	24	4	1	27-06-2016
			3.887	**916**	**36**	**24**	

Tabla 5: Resumen de Búsquedas

Es necesario dejar claro que se hablará de artículos revisados, pero algunos de estos en realidad son secciones o capítulos de libros. Se revisó un total de 916 artículos. El que un artículo fuera seleccionado en un determinado motor de búsqueda con una determinada combinación de términos, no significa que solo se encontró con esa combinación de motor de búsqueda y combinación de términos, el artículo pudo estar repetido en otras combinaciones, es decir, algunos de los artículos encontrados se repiten al realizar la búsqueda con otras de las combinaciones de términos.

No se revisaron todos los resultados, solo se revisó una proporción la cual correspondió a 916 artículos. Para cada uno de los motores de búsqueda se revisó un total proporcional a la cantidad

y la calidad de los resultados para dicho motor de búsqueda. La calidad de los resultados se determinó que puede ser apreciada en relación a la aparición de más de 20 artículos consecutivos que no tenían ninguna relación con lo que se está buscando. Esto indicó que muy probablemente el resto no tendrían relación, algo que sucede con bastante frecuencia en mayor medida en el motor de búsqueda Google Scholar, y la revisión del resto de los artículos muy probablemente no proveería resultados por lo cual no se seguía revisando.
Para las búsquedas relacionadas con IFML se revisaron todos los artículos ya que no se encontraban buenos resultados. Para la búsqueda particular de la combinación 8 solo se registró la búsqueda en Google Scholar ya que no dio resultados relevantes con el resto de los motores de busqueda.
Para todos los resultados de las búsquedas se realizó un pequeño resumen de lo que trata el artículo (esto es distinto del tópico de aceptación que es más corto). La idea fundamental de este resumen es utilizarlo en caso de dudas que puedan surgir al respecto de un determinado artículo y en caso de disminuir los criterios de aceptación.
En general la estrategia de revisión de cada resultado de la búsqueda se basó en lo establecido en la planificación. Se revisó a través de la lectura principalmente del resumen y las conclusiones, si habían dudas se revisaba el resto del artículo según la estrategia de extracción de datos.
Durante una primera revisión se seleccionó preliminarmente un total de 36 artículos en base a una lectura superficial de estos. Estos 36 fueron revisados en profundidad en una segunda etapa y se seleccionó 24 de ellos. Se observó que los 12 artículos descartados no tenían relevancia en el tema o no contenían la información que se buscaba obtener. Luego se revisaron las referencias de estos artículos en busca de nuevos artículos pero estas referencias solo apuntaban a los artículos ya seleccionados o los descartados en la segunda etapa.
En las siguientes subsecciones se presenta una breve reseña de cada uno de los 24 artículos seleccionados, los que son presentados teniendo en cuenta la estrategia de síntesis considerada en la RSL. Para ello se debe tener en cuenta que algunos de los temas no produjeron resultados. Solo tres temas presentados produjeron resultados y el tema 4, sobre transformaciones IFML en general, fue agregado durante el desarrollo de la revisión. A modo de resumen la Tabla 6 da cuenta de la cantidad de artículos seleccionados por cada tema.

Tema	Artículos
Tema 1: Elementos de Seguridad en ArchiMate	12
Tema 2: Transformaciones ArchiMate-BPMN	5
Tema 3: Elementos de Seguridad en IFML	4
Tema 4: Transformaciones IFML	3
	24

Tabla 6: Resumen artículos por tema

Se debe recordar que todos los artículos seleccionados son anteriores a ArchiMate 3.0 por lo tanto las reseñas están basadas en ArchiMate 2.1 y ArchiMate 2.0, lo cual significa que solo consideran la existencia de las capas de negocio, aplicación y tecnología, y el aspecto motivacional es tratado por el nombre de la extensión de motivación o extensión motivacional.

3.2.1 Tema 1: Elementos de Seguridad en ArchiMate

Con respecto a los elementos de seguridad en ArchiMate se encontraron un total de 12 artículos, los cuales corresponden a la mitad del total de artículos seleccionados (24 artículos seleccionados en total). Estos serán analizados en forma detallada en las siguientes subsecciones.

3.2.1.1 Modelado de gestión de riesgos y seguridad en ArchiMate

Grandry *et al.* (2013b) exponen que la Gestión de Riesgos de Seguridad en Sistemas de Información (ISSRM del inglés, Information System Security Risk Management) establece que las amenazas de seguridad son tan numerosas que es imposible actuar en todas ellas, porque todas las soluciones de seguridad tecnológica tienen un costo y las empresas cuentan con recursos limitados. Por lo tanto, las empresas quieren asegurarse de que sólo adoptan soluciones para el cual el Retorno de la Inversión de Seguridad (ROSI, siglas del inglés Return On Security Investment) sea positivo. Para ello, diversas variables deben ser evaluadas. Existen varios enfoques ISSRM y la mayoría habla de diferentes conceptos y terminologías. Se propone una integración de la gestión de riesgos de seguridad y la gestión de arquitectura empresarial usando ArchiMate. Para ello se establece una correspondencia entre los elementos de ambos dominios, la cual se muestra en la Tabla 7.

Concepto ISSRM	Concepto ArchiMate
Business Asset	Business Process, Business Object, Business Actor, Business Role
IS Asset	Application Component, System Software, Node, Device, Network
Security Objective	Driver
Risk	Assessment
Event	Assessment
Impact	Assessment
Threat	Assessment
Vulnerability	Assessment
Risk Treatment	Goal
Security Requirement	Requirement
Control	Core Element

Tabla 7: Correspondencia elementos ISSRM-ArchiMate (Grandry *et al.*, 2013b)

La propuesta (Grandry *et al.*, 2013b) se presenta como una extensión de gestión de riesgos para ArchiMate. Abarca la capa de aplicación y de negocio haciendo uso de los elementos introducidos en la extensión Motivación de ArchiMate 2.0. En dicha extensión de ArchiMate se abstrae *"la razón que está detrás de la arquitectura de una empresa"*, o en otras palabras, porqué razón existen ciertos elementos de la arquitectura. La extensión de Motivación se ha desarrollado para apoyar una dimensión adicional de la arquitectura, con la cual se intenta responder el porqué (la causa, motivo o razón de existencia de los otros elementos). La motivación es relevante en cada una de las 3 capas de abstracción (negocio, aplicación y tecnología) y permite trazar la razón de ser de los elementos de la arquitectura.
Además la propuesta cuenta con un caso de estudio y un metamodelo en base a ArchiMate que se muestra en la Figura 3. El metamodelo básicamente muestra a qué elemento de ArchiMate le

corresponde cada uno de los elementos que componen la gestión de riesgos y cómo estos se relacionan entre sí usando las relaciones de ArchiMate.

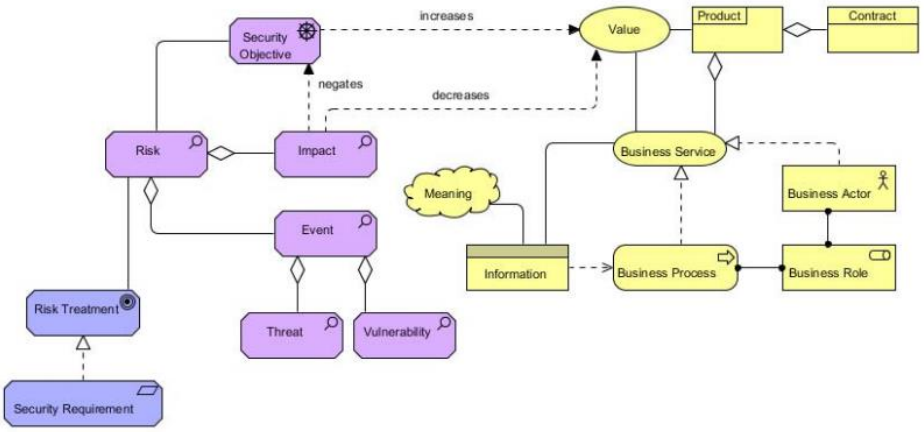


Figura 3: Metamodelo propuesta ISSRM- ArchiMate (Grandry *et al.*, 2013b)

3.2.1.2 Seguridad en ArchiMate a través de políticas de seguridad

Blangenois *et al.* (2013) y Feltus *et al.* (2014) presentan el concepto de política de ArchiMate, necesario para modelar los sistemas SCADA (Supervisory Control And Data Acquisition). SCADA es un software de infraestructura crítica que permite controlar procesos a distancia, en el que se reciben datos que se usan para facilitar la retroalimentación del sistema. Los sistemas SCADA tienen una organización por capas, similar a la organización por capas de ArchiMate. Uno de los enfoques de la infraestructura crítica es el uso de agentes, los cuales necesitan de políticas que den cuenta de las responsabilidades del agente y le permitan actuar. Aquí se menciona que una política se puede expresar en un contexto de seguridad y que existen políticas en la capa organizacional y en la capa de la aplicación de ArchiMate. En base a lo anterior, se establece una relación con políticas de seguridad en que se indica que en cada elemento "Business Service" de ArchiMate se puede representar una política de seguridad.

3.2.1.3 El control de acceso con RBAC en ArchiMate

Gaaloul y Proper (2013), Gaaloul *et al.* (2014a) y Gaaloul *et al.* (2014b) exponen que las técnicas e idiomas de EA no se ocupan de los problemas de seguridad de manera satisfactoria. Por ejemplo, los artefactos de control de acceso son simplemente representados en el nivel de TI sin tener en cuenta la definición del proceso y la gestión de recursos de las organizaciones. En estos trabajos se propone un modelo de control de acceso para apoyar la gestión de la organización en la arquitectura empresarial. La novedad de este enfoque consiste en cerrar la brecha entre los modelos de arquitectura empresarial y el control de acceso con RBAC (Role-Based Access Control), que permite restringir el acceso al sistema solo a usuarios autorizados. El enfoque es adecuado para ser usado en aplicaciones en la nube. Se establece una correspondencia entre el metamodelo de RBAC y el metamodelo de la capa de negocio de ArchiMate que se muestra en la Figura 4.

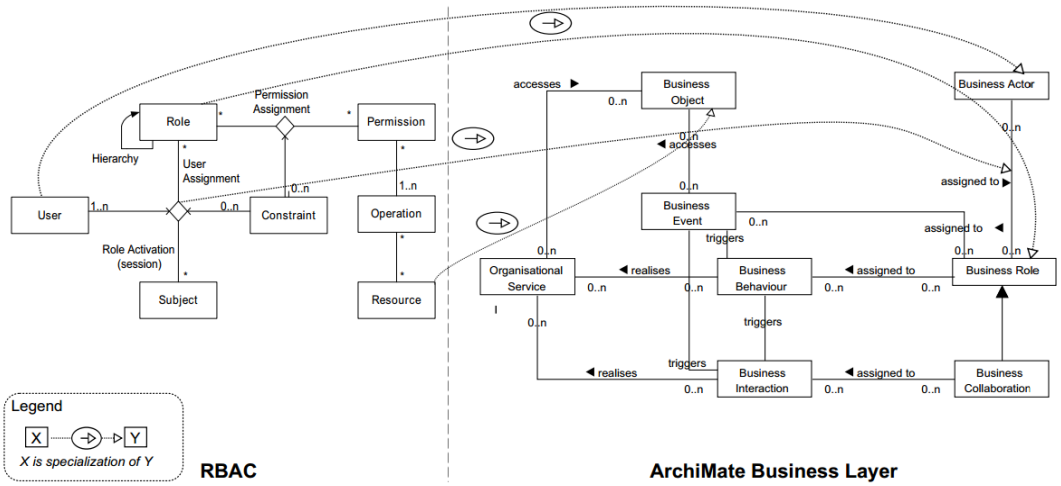


Figura 4: Correspondencia de elementos RBAC y la capa de negocios de ArchiMate (Gaaloul y Proper, 2013)

Además se presenta un marco de control de acceso (ACF-Access Control Framework) para apoyar las políticas de autorización dentro de la arquitectura empresarial. ACF se define como un conjunto de componentes de software que aceptan las solicitudes de acceso a los recursos, analizan éstas contra las políticas que representan los derechos de acceso reales a los recursos y entrega una respuesta en base a este análisis. Para esto se define el componente de aplicación en ArchiMate que regula el control de acceso (Figura 5) y por otro lado el modelo del Framework de control de acceso ACF (Figura 6).

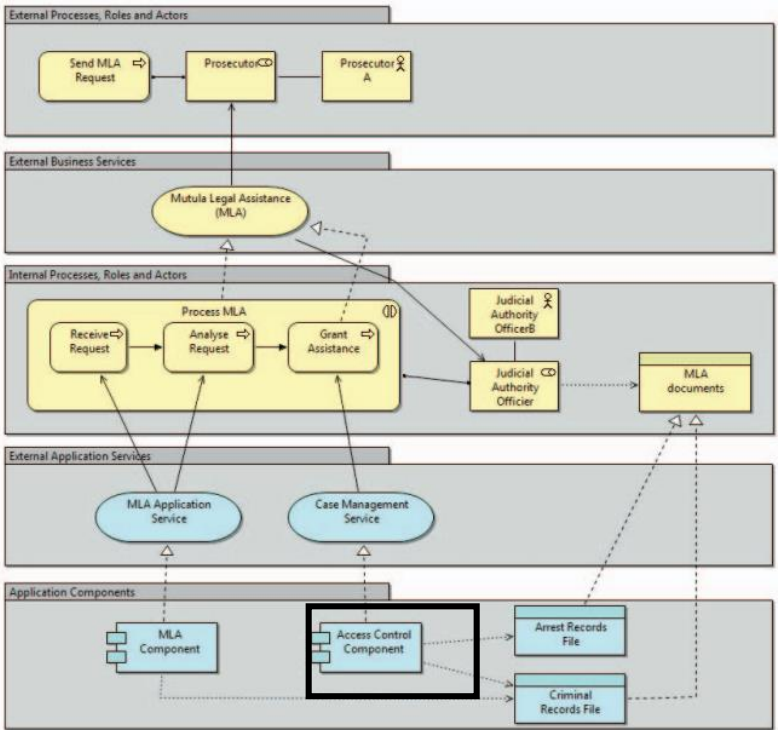


Figura 5: Componente de control de acceso en ArchiMate (Gaaloul y Proper, 2013)

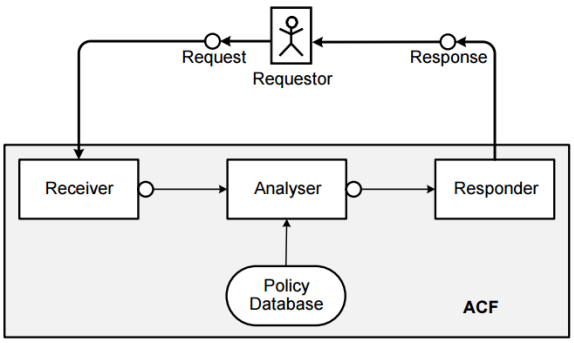


Figura 6: Framework de control de acceso ACF (Gaaloul y Proper, 2013)

Además Gaaloul *et al.* (2014a) realizan una correspondencia de elementos de RBAC a DEMO (Design and Engineering Methodology for Organizations) con el fin de establecer un enlace entre ArchiMate, RBAC y DEMO. Este último ofrece una perspectiva teórica para el pensamiento y el diseño asociado a la manera de trabajar junto con una metodología.

3.2.1.4 Métodos de evaluación de riesgos usando ArchiMate

Korman *et al.* (2014) seleccionan métodos de evaluación de riesgos de la seguridad de la información. Dichos métodos consideran un conjunto de información de entrada a los cual los autores proponen asignar a elementos de ArchiMate, de tal forma que la arquitectura empresarial se transforme en una fuente de entrada para dichos métodos. La idea detrás de esto es que, dado el amplio uso de ArchiMate, podría ser una fuente de orientación para la realización de evaluaciones de riesgos, así como una manera de hacer más eficiente el proceso de evaluación de riesgos de la seguridad de la información. El estudio muestra que, aunque ArchiMate versión 2.0 no es capaz de describir directamente los asuntos que se relacionan de manera explícita a la seguridad de la información (por ejemplo, vulnerabilidades, perfiles de amenazas, contramedidas), si puede modelar gran parte de la información sugerida por los métodos. No se muestra cuáles son los elementos que forman parte de la correspondencia o sus relaciones.

3.2.1.5 Modelado de seguridad en ArchiMate (The Open Group)

Band *et al.* (2015) exponen que a través de su extensión de Motivación, el lenguaje ArchiMate hace posible el vínculo entre las medidas de control de los requisitos de seguridad, principios y objetivos, así como a los resultados de un análisis de riesgos. Por otro lado, los modelos ArchiMate se pueden vincular con lenguajes para los procesos de negocio y soluciones de TI, tales como BPMN y UML. Se extiende el contenido del riesgo y de seguridad existente del Framework TOGAF utilizando el lenguaje de modelado visual ArchiMate. Se realiza una correspondencia de los conceptos de riesgo y seguridad con los conceptos y componentes de ArchiMate 2.1. La Figura 7 muestra la correspondencia de los conceptos de riesgos y seguridad con el lenguaje ArchiMate, en otras palabras, muestra un metamodelo de cómo los elementos de seguridad y riesgos deben ser modelados en ArchiMate (con qué elemento de ArchiMate debe ser representado cada uno de los elementos de seguridad). La extensión de riesgos se basa en gran medida en la propuesta presentada anteriormente en la sección 3.2.1.1.

Es interesante destacar que en esta propuesta un requerimiento de seguridad es modelado como un elemento llamado Requerimiento.

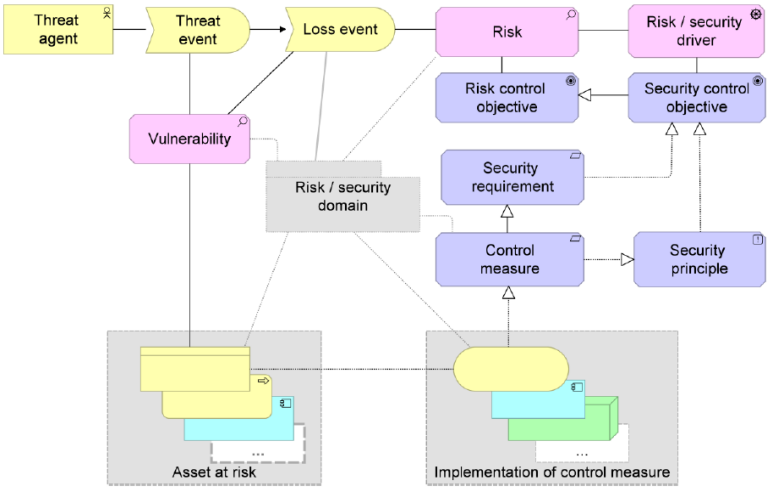


Figura 7: Correspondencia de conceptos de riesgo y seguridad a ArchiMate (Band *et al.*, 2015)

3.2.1.6 Comparando otro modelo con la seguridad de ArchiMate

Coles-Kemp *et al.* (2015) exponen la existencia del informe analizado en el punto anterior (Sección 3.2.1.5) y muestran una manera de modelar seguridad, específicamente gestión de riesgos, con el modelo TREsPASS. El modelo TREsPASS no usa ArchiMate, sino que se basa en una notación propia. La idea expuesta es que los conceptos que modela ArchiMate en gestión de riesgos también pueden ser modelados por el modelo TREsPASS. La Figura 8 muestra los conceptos que se pueden modelar con el modelo TREsPASS. Al realizar una comparación se puede apreciar que realmente este modelo TREsPASS abarca menos conceptos que el informe de Band *et al.* (2015), los conceptos que abarca el informe de Band *et al.* (2015) son 12 conceptos de seguridad y riesgos, mientras que el modelo de Coles-Kemp *et al.* (2015) solo abarca 9.

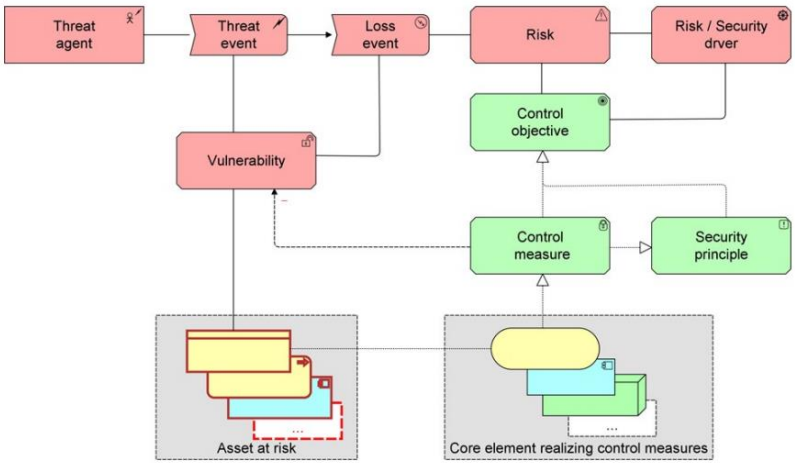


Figura 8: Correspondencia de conceptos de riesgo y seguridad en TREsPASS (Coles-Kemp *et al.*, 2015)

3.2.1.7 Riesgos de seguridad en un automóvil modelados con ArchiMate

Blommendaal (2015) realizó un estudio que tiene como objetivo identificar los riesgos de seguridad de la información en un automóvil que está conectado a una red. Se utiliza ArchiMate como estándar de modelado y para especificar los riesgos se utiliza la propuesta de Band *et al.* (2015) presentada en la sección 3.2.1.5, la cual está oficializada por The Open Group. En la Tabla 8 se muestra la correspondencia entre los elementos según la propuesta de Band *et al.* (2015).

Risk Concept	ArchiMate elements
Threat agent	Business actor
Threat event	Bussiness event
Risk	Assessment
Risk Metrics	Atributes of assessment
Vulnerability	assessment
Risk Control, treatment and migration	Driver
Control requirement	Requirement
Asset at risk	Value/Other
Policy	Principle

Tabla 8: Correspondencia de conceptos de Riesgos a elementos de ArchiMate (Blommendaal, 2015)

3.2.1.8 Riesgos de seguridad de edificios inteligentes representados con ArchiMate

Dubois y Mauger (2015) presentan un trabajo que se enmarca en la arquitectura empresarial de edificios inteligentes, donde una parte importante del modelado es la gestión de riesgos de seguridad. Un edificio inteligente es definido en el trabajo como un edificio de alojamiento de varios sistemas de información que proveen servicios de gestión energética, seguridad, bienestar, comunicación, etc. El modelado se realiza con ArchiMate y para la gestión de riesgos de seguridad se utiliza la propuesta de Grandry *et al.* (2013b) presentada en la sección 3.2.1.1.

3.2.1.9 Gestión de riesgos en ecosistemas usando ArchiMate

Por último, en el trabajo de Feltus *et al.* (2015) se expone que existen ecosistemas que reúnen a las empresas que colaboran para lograr un objetivo sistémico común, como por ejemplo garantizar la asistencia sanitaria nacional, las telecomunicaciones o la estabilidad financiera. Se propone un metamodelo para el modelado de las capacidades y recursos de los ecosistemas, un enfoque de gestión de riesgos en base a este metamodelo y un lenguaje de extensión de ArchiMate para sostener la gestión del riesgo sistémico. Se utiliza la propuesta de Grandry *et al.* (2013b) presentada en la sección 3.2.1.1, para representar la gestión del riesgo sistémico. El enfoque se lleva a cabo en dos etapas: primero se diseña el modelo de dominio y segundo se modela el riesgo basado en el modelo de dominio. Se presenta un caso de estudio donde se aplica la propuesta de Grandry *et al.* (2013b).

3.2.2 Tema 2: Transformaciones ArchiMate-BPMN

Con respecto a las transformaciones de ArchiMate a BPMN existen algunas propuestas que aunque no abarcan todos los elementos, si lo hacen de forma general. Estas propuestas se exponen en 5 de los 24 artículos seleccionados, los cuales son analizados a continuación.

3.2.2.1 Vinculación entre ArchiMate y BPMN por Penicina

Penicina (2013) afirma que una vinculación entre modelos de proceso de negocio y modelos de EA permitiría mirar los procesos en detalle en diferentes capas de la empresa. BPMN tiene sus limitaciones cuando se trata de modelar otros aspectos de la organización tales como la estructura organizativa y funciones, datos, reglas de negocio, los sistemas técnicos, etc. lo cual si puede ser modelado en modelos de EA. La autora también afirma que durante el modelado de la capa de negocio, un proceso de negocio se puede ampliar usando un lenguaje de diseño de procesos de negocio; por ejemplo, BPMN. Esto indica a la vez que un modelo de proceso de negocio en BPMN permite representar abstracción con más detalles del proceso que ArchiMate, en otras palabras, BPMN permite representar más detalles de los procesos de negocio que ArchiMate.
La autora define una vinculación entre BPMN y ArchiMate a nivel de metamodelos, mapeando los elementos de las diferentes capas de ArchiMate con los correspondientes elementos del metamodelo de BPMN 2.0 (Tabla 9, Tabla 10 y Tabla 11). La autora en este artículo habla de la "integridad de los modelos de proceso" para referirse a que los modelos deben contener todos los elementos necesarios desde el punto de vista del sistema de información y la "legalidad de los modelos de proceso" como el cumplimiento de las leyes relacionadas con el sistema. Luego, se propone usar el modelo BWW (por sus autores Bunge, Wand y Weber) (Bunge, 1979; Wand y Weber, 1993) para evaluar la integridad y legalidad de los modelos de proceso de negocio en ArchiMate y BPMN. El modelo BWW describe los conceptos necesarios para la construcción o descripción de un sistema de información. Finalmente, la autora concluye que los modelos no son suficientes para poder cumplir con todos los elementos del modelo BWW y plantea la idea de complementar los modelos BPMN y ArchiMate.

Elementos de la capa de negocios de ArchiMate	Elementos BPMN
Business Process	Business Process Diagram, Pools, Lanes
Function	Task, Sub-Process
Business Interaction	Collaboration Diagram
Business Event	Event
Business Object	Data Object
Business Role	Lane

Tabla 9: Correlación entre elementos de la capa de negocios de ArchiMate y BPMN (Penicina, 2013)

Elementos de la capa de aplicación de ArchiMate	Elementos BPMN
Data Object	Data Object
Application Function	Service Task, Script Task

Tabla 10: Correlación entre elementos de la capa de aplicación de ArchiMate y BPMN (Penicina, 2013)

Elementos de la capa tecnológica de ArchiMate	Elementos BPMN
Device	Data Store
Artefact	Data Objects

Tabla 11: Correlación entre elementos de la capa tecnológica de ArchiMate y BPMN (Penicina, 2013)

3.2.2.2 Correspondencia entre ArchiMate y BPMN por Gill y Qureshi

Gill y Qureshi (2015) presentan una lista de elementos ArchiMate y su correspondencia con elementos BPMN. La lista se obtuvo del análisis de distintas métricas como el grado de similitud sintáctica, análisis semántico y el análisis estructural y similitud global de los elementos. Dicha lista se encuentra en la Tabla 12.

ArchiMate	BPMN
Business Actor	Participant
Business Role	Partner Role
Business Collaboration	Colaboration
Business Interface	Interface
Location	Pool
Business Event	Event
Data Object	Data Object
Business Service	Activity
Business Process	Activity
Artefact	Artefact

Tabla 12: Mapeo elementos ArchiMate con BPMN (Gill y Qureshi, 2015)

3.2.2.3 Relacionando los elementos de ArchiMate con BPMN por Gill

Gill (2015) evalúa la aplicabilidad e integración del estándar de modelado de alto nivel ArchiMate con cinco estándares de modelado de nivel de detalle como BPMN (Business Process Model and Notation), UML (Unified Modelling Language), FAML (FAME [Framework for Agent-Oriented Method Engineering] Language), SoaML (Service Oriented Architecture Modelling Language), y BMM (Business Motivation Model).

La idea es aplicar e integrar ArchiMate de alto nivel con estándares de bajo nivel para el modelado de arquitectura empresarial ágil.

Un resumen de la relación entre los elementos se presenta en la Tabla 13.

ArchiMate	BPMN
Active Structure: Business Actor Business Role Business Colaboration Business Interface Location	Pool Swimlane
Behavioral: Business Process Business Function Business Interaction Business Event Business Service	Activity Task Gateway Sequence Event Pool Swimlane
Passive Structure: Business Object Representation Meaning Value Product Contract	Data Object Data Store

Tabla 13: Mapeo elementos ArchiMate a BPMN (Gill, 2015)

3.2.2.4 Otra vinculación entre ArchiMate y BPMN

Kirikova *et al.* (2015) presentan un trabajo que se enfoca en la necesidad de representar el tiempo en los modelos de las empresas, por ello proponen una vinculación entre los modelos de arquitectura empresarial, de proceso de negocio y de tiempo. Dejando de lado el aspecto del tiempo, el mapeo de elementos entre BPMN y ArchiMate se muestra en la Tabla 14.

BPMN Element	ArchiMate Element
Lane, Participant (Pool), Data Object, Data Store	Business actor, Business role, Business interface, Location, Business object, Contract, Product Application component, Application interface, Data object, Node, Device, Infrastructure interface, System software, Artifact
Start event, Intermediate event, End event	Business Event

Tabla 14: Mapeo elementos BPMN a ArchiMate (Kirikova *et al.*, 2015)

3.2.2.5 Patrones para representar seguridad

Kirikova *et al.* (2016) proponen una extensión del método de elicitación de requisitos de seguridad de proceso de negocio (SREBP por sus siglas en inglés Security Requirements Elicitation from Business Processes). Se muestra que (i) el marco de modelo de empresa abarca prácticamente todos los conceptos de definiciones relacionadas con la seguridad de la

información y que (ii) el uso de la estructura con el método SREBP cumple con el modelado de la empresa común y el enfoque de la arquitectura empresarial.
La idea es relacionar los patrones de SREBP con la arquitectura empresarial representada con ArchiMate, para lo cual se realiza un análisis de los conceptos y elementos de seguridad con el modelo empresarial y se propone un mapeo de elementos entre BPMN y ArchiMate (Tabla 15). No se detectan elementos que representen seguridad por sí mismo, sino que la seguridad es representada por el conjunto de actividades del patrón.

Capa ArchiMate	Concepto ArchiMate	Concepto BPMN
Negocio	Business Process	Business Process Diagram, Pools
Negocio	Function	Task
Negocio	Business Object	Data Objects
Negocio	Business Event	Event
Negocio	Business Role	Lane
Aplicación	Data Object	Data Objects
Tecnología	Artefact	Data Objects

Tabla 15: Mapeo elementos ArchiMate a BPMN (Kirikova *et al.*, 2016)

3.2.3 Tema 3: Elementos de Seguridad en IFML

Con respecto a artículos relacionados a elementos de seguridad en IFML, se encontraron un total de 4 artículos. En estos artículos aunque no se identifican los elementos de seguridad en IFML, si se entregan pistas e información que fue relevante para las siguientes etapas de esta Tesis.

3.2.3.1 Permisos de control de acceso en WebML

Wright y Dietrich (2008) analizan y comparan los lenguajes de modelado de aplicaciones Web teniendo en cuenta las opciones y propiedades que proveen las aplicaciones Web hoy. Se pone una mayor atención sobre WebML y UWE (UML-based Web Engineering, modelos de interfaz de usuario modelados usando diagramas UML). Se expone que WebML tiene soporte para usuarios y grupos de usuarios, pero solo como miembros del modelo estructural (modelo entidad-relación). Los usuarios pertenecen a un grupo y a un grupo se le permite el acceso a solo una vista del sitio. WebML no puede apoyar el modelado de interacción entre múltiples usuarios (el modelo asume que solo un usuario interactúa con el modelo en un tiempo dado). El único permiso representado en el modelo es la capacidad de los grupos para ver ciertas páginas y si se quiere especificar permisos de seguridad adicionales se deben modelar de forma explícita a través de cadenas de operación (el flujo de los elementos).

3.2.3.2 Permisos de seguridad en WebML

Ingle y Meshram (2012) analizan y comparan las distintas notaciones de modelado Web dentro de los cuales se encuentra WebML. Se dice que WebML tiene soporte incorporado para grupos de usuarios y los únicos permisos de seguridad representados en el modelo tienen relación con la capacidad de los grupos de ver ciertas páginas; de manera que los permisos de seguridad adicionales se deben comprobar de forma explícita a través de cadenas de operación. Los grupos

de usuarios en realidad no son representados por la notación WebML sino que son representados en los modelos de base de datos.

3.2.3.3 Patrones de diseño con IFML que representan seguridad

Brambilla y Fraternali (2014) muestran definiciones formales y discuten distintos elementos de IFML. Dentro de los aportes de su libro se encuentran los patrones de Front End con IFML. Se presentan distintos patrones de Front End, elementos recurrentes a la hora de modelar Front End de aplicaciones. Dentro de estos patrones se encuentra el patrón de Logout y Login (control de acceso) en distintas situaciones: Control de Acceso a la aplicación, Control de Acceso a una determinada vista y Control de Acceso por roles (dependiendo del rol se obtiene acceso a una vista). Siendo estos modelos muy similares, solo se muestra el más completo en la Figura 9. Se habla de la extensibilidad del lenguaje para abarcar dominios más específicos y se muestran los elementos de una extensión para dispositivos móviles. Se indica que la herramienta de WebRatio permite crear plugins de extensiones IFML.

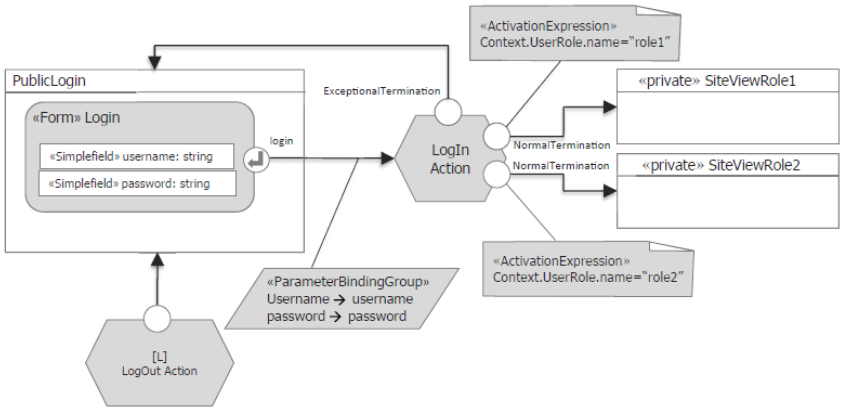


Figura 9: Modelo IFML de Login (Brambilla y Fraternali, 2014)

En cuanto a la relación entre IFML con otros estándares se expone que: *"gracias a su integración en el marco MDA, IFML permite una estrecha integración con otras perspectivas de modelado del sistema. En particular, tres aspectos se definen explícitamente en la norma: la integración con el modelo de contenido, integración con la lógica de negocio, y la integración con modelos de procesos de negocio. Integraciones adicionales son posibles, por ejemplo, con los modelos específicos de la plataforma, modelos de implementación de sistemas y modelos de arquitectura empresarial"* (Brambilla y Fraternali, 2014).

3.2.3.4 Requisito de control de acceso en IFML

Pizarro Zea (2015) plantea la construcción de una aplicación Web para automatizar y administrar pruebas psicológicas a individuos, y almacenar y procesar los resultados a través de la plataforma o ambiente de desarrollo WebRatio que modela interfaz de usuario en lenguaje estándar IFML. Usa la herramienta de WebRatio para generar código de forma automática a partir de los modelos Front End.

Dentro de los requerimientos de la aplicación se considera el requisito no funcional de "control de acceso", el cual se modela como se muestra en la Figura 10.

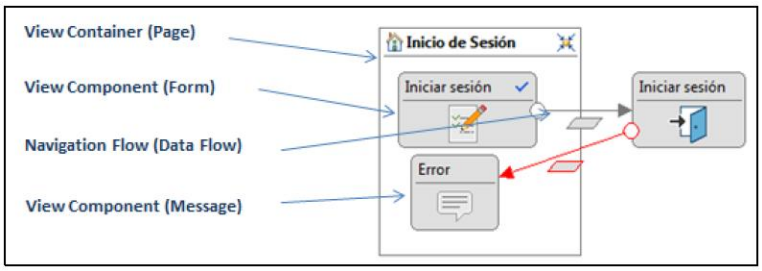


Figura 10: Modelo IFML de requisito control de Acceso (Pizarro Zea, 2015)

3.2.4 Tema 4: Transformaciones IFML

En la literatura revisada no se encontraron trabajos en que se abordará en forma directa transformaciones desde BPMN a IFML por lo que en esta sección se presentarán aquellos trabajos que puedan proveer ideas para abordar las transformaciones definidas en esta Tesis.

3.2.4.1 Modelo para transformar BPMN con SBP en WebML

Brambilla y Fraternali (2013) presentan la arquitectura de la propuesta BPM4People. Esta propuesta consta de dos partes importantes desde el punto de vista del modelado, el modelo del proceso de negocio social (SBP por sus siglas en inglés de Social Business Process) extensión de BPMN y el modelo WebML. La idea de la propuesta es crear un modelo BPMN con la extensión de SBP y transformarlo en un modelo WebML, posteriormente transformar el modelo WebML en código. El problema es que no se muestra cómo se realiza la transformación, es solo una arquitectura de la propuesta.

3.2.4.2 De BPMN a IFML usando al modelador

En la OMG (2015a), la especificación de IFML no considera el dominio de la seguridad. La especificación muestra la estrecha relación entre el modelo de datos, el modelos de negocio y el modelo de interfaz de usuario pero no da lineamentos o una relación o mapeo de cómo debe ser la interpretación de los elementos de BPMN en IFML de forma exacta. El modelo Front End es más bien una interpretación del modelo BPMN sin una relación exacta entre los elementos. No se presenta una transformación sino que se expone que es posible realizar la transformación, pero todo depende del modelador. No se establecen correspondencias de elementos o patrones ni nada.

3.2.4.3 Traduciendo patrones CTT en IFML

Blanckaert (2015) investiga si IFML puede ser integrado dentro de métodos de diseño de la Web semántica (WSDM por sus siglas en inglés Web Semantics Design Method). Se concluye que es posible la integración pero no es viable.
En WSDM se utilizan modelos ConcurTaskTrees (CTT) los cuales se centran en cómo avanzan las tareas del usuario y en qué momentos la interacción de usuario es requerida. CTT consiste de

una notación cuyo fin es apoyar los enfoques de ingeniería para el modelado de tareas. El objetivo principal de CTT en WSDM es especificar la interacción de usuario.
En WSDM, ORM (Object-Role Modelling) se utiliza para modelar la información requerida por el modelo de tarea CTT.
Se presenta una serie de patrones CTT (en algunas ocasiones enriquecido con ORM) los cuales son traducidos a elementos IFML.

3.3 Tercera etapa: Publicación de los Resultados de la Revisión

Los resultados de esta revisión sistemática de la literatura fueron utilizados principalmente para conocer el estado del arte de los temas relacionados a esta Tesis y para la elaboración de los artículos que son derivados de esta Tesis.

3.4 Conclusiones

Existen varias propuestas que pretenden establecer los elementos que modelan la gestión de riesgos y seguridad en ArchiMate, no obstante, la que tiene mayores referencias y, por tanto, es más aceptada por la comunidad relacionada es la que presenta The Open Group (Band *et al.*, 2015). Esta propuesta considera lo expuesto en el marco de trabajo TOGAF para realizar gestión de riesgos y seguridad, lo cual le da más puntos a su favor.
Aunque en esta RSL solo se buscaba tener una base para definir la forma de modelar requisitos de seguridad en ArchiMate, se ha encontrado mucha más información relevante para el modelado de la gestión de riesgos que puede ser de ayuda para otros trabajos futuros.
Del lado de las transformaciones de ArchiMate a BPMN se encontraron algunas correspondencias de elementos que pueden ser de ayuda. Aunque en algunos casos no coinciden en la correspondencia de un mismo elemento, se pueden comparar y obtener un resultado en base a la mayor cantidad de propuestas que presentan dicha correspondencia de elemento. No todas las correspondencias están completamente definidas. Por ejemplo, al existir correspondencias de un elemento con más de un elemento y viceversa no queda claro con precisión la correspondencia final. Además, no fue posible encontrar un caso de estudio que muestre una correspondencia entre un modelo modelado con ArchiMate y un modelo modelado con BPMN, lo que hace que la mayoría de las correspondencias sean presentadas a nivel de elementos y no a nivel de modelos.
En cuanto a IFML no se encontró información sobre cómo modelar la seguridad en este estándar. La idea de usar los grupos de usuarios como un elemento de Control de Acceso (Wright y Dietrich, 2008; Ingle y Meshram, 2012) aunque puede ser aplicada en IFML al igual que WebML, no es muy apropiada ya que realmente los grupos de usuarios no existen dentro de los elementos de IFML y los grupos de usuarios en la plataforma WebRatio se representan en el modelo de la base de datos. La existencia del patrón de Front End de Login (Brambilla y Fraternali, 2014) que corresponde a un requisito de Control de Acceso puede indicar que es posible que el resto de los requisitos que abarca la extensión BPMN-BPSec también tienen una correspondencia con un patrón de Front End.
En cuanto a las transformaciones entre estándares BPMN e IFML, al inicio se pensó que usar los modelos CTT (Blanckaert, 2015) como intermediario podría ser una buena idea, pero resulta que estos modelos al igual que IFML son usados para representar Front End, por lo cual no es muy claro que se puedan usar estos modelos como guía de transformación de BPMN-BPSec a IFML. El

resto de los artículos seleccionados no realizan una transformación con correspondencias de elementos o patrones establecidos, ya que suele ser una interpretación que cambia cuando cambia el modelador.
No se encontraron resultados de transformaciones utilizando elementos de seguridad.

Capítulo 4: Correspondencia de ArchiMate a BPMN-BPSec

ArchiMate es un lenguaje que permite modelar la arquitectura de la empresa en un alto nivel de abstracción y entre las capas que permite describir se encuentra la de negocio. BPMN, por su parte, es un lenguaje dedicado al modelado de procesos de negocio. En este capítulo se analiza la coincidencia que existe entre ambos lenguajes. En particular, se abordan los aspectos de seguridad teniendo en cuenta aquellos que son posibles de representar por medio de la extensión de BPMN-BPSec. Para llevar a cabo esta tarea se ha tomado como base los resultados de la RSL (ver en Sección 3.2.2), en donde se constata que es posible encontrar equivalencias entre ambos lenguajes aunque ninguno de los trabajos encontrados aborde la seguridad. La relación entre ArchiMate y BPMN ha sido tratada mediante el establecimiento de algunas correspondencias entre elementos de ambos lenguajes de modelado (Gill, 2015; Gill y Qureshi, 2015; Kirikova *et al.*, 2016; Kirikova *et al.*, 2015; Penicina, 2013), pero no se han encontrado trabajos que aborden la transformación automática de modelos.

Debido a lo anterior, en este capítulo se busca complementar la capa de negocio de un modelo de Arquitectura Empresarial para que incluya la seguridad a través de requisitos de seguridad en ArchiMate. Para, posteriormente partiendo de ese modelo obtener de manera automática un modelo de proceso de negocio que incluya la seguridad, el cual será representado usando la propuesta BPMN-BPSec.

Este capítulo se encuentra organizado de la siguiente forma: en la Sección 4.1 se detalla cómo modelar cualquier requisito de seguridad en ArchiMate; en la Sección 4.2 se establece la forma de modelar los requisitos usados en la extensión BPMN-BPSec en ArchiMate considerando que los requisitos de seguridad no se relacionan con todos los elementos de la capa de negocio de ArchiMate; en la Sección 4.3 se detalla la forma en que se debe realizar la correspondencia desde la capa de negocio de ArchiMate con requisitos de seguridad hacia BPMN con la extensión BPSec; y, finalmente, en la Sección 4.4 se presentan las conclusiones de este capítulo.

4.1 Seguridad en ArchiMate

En Ingeniería de Requisitos, el concepto de requisito de seguridad se refiere a una necesidad de seguridad que debe ser cumplida. Por otro lado, en ArchiMate los conceptos relacionados con la seguridad pueden ser modelados a través del *Aspecto Motivacional.* Entre estos conceptos de seguridad, de acuerdo con Band *et al.* (2015) y The Open Group (2016), se encuentra el "*Requisito de Seguridad*" que puede ser modelado con el elemento "*Requisito*" y el "*Principio de Seguridad*" que puede ser modelado con el elemento "*Principio*". Se debe tener en cuenta que estos dos elementos representan necesidades de seguridad, solo que un Principio es menos concreto o más abstracto que un Requisito. Por consiguiente, para modelar requisitos de seguridad es necesario modelar Requisitos y Principios. De la misma forma, un Principio puede ser realizado por uno o más Requisitos. En la Figura 11 se muestra esta relación instanciada como principios y requisitos de seguridad.

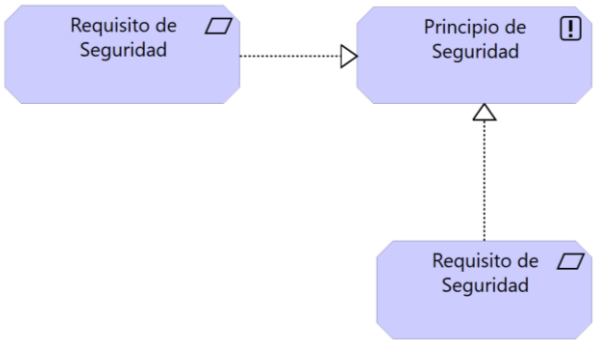


Figura 11: Estructura de Principios y Requisitos en ArchiMate

En la Tabla 16, se muestran los 28 principios de seguridad obtenidos desde la literatura evaluando su descripción con respecto a aspectos relacionados a la seguridad. Los principios cuentan con la referencia del artículo de origen, el nombre del principio y su descripción. Se encuentran ordenados por el año de publicación del artículo, desde el más actual al más antiguo. Los primeros 7 principios corresponden a los seleccionados de los 21 principios de TOGAF y el resto corresponde a principios mencionados en la literatura general.

N°	Artículo	Principio	Descripción
1	The Open Group, 2011	Continuidad del negocio	Las operaciones de la empresa se mantienen a pesar de las interrupciones del sistema.
2	The Open Group, 2011	Aplicaciones de uso común	Se refiere al desarrollo de aplicaciones utilizadas en toda la empresa, uso de las mismas fuentes de datos.
3	The Open Group, 2011	Los datos son un activo	Los datos son un activo que tiene valor para la empresa y deben ser administrados como corresponde. Los datos son la base de la empresa, por lo tanto, deben ser administrados con cuidado para obtener los datos cuando y donde se requieran.
4	The Open Group, 2011	Los datos se comparten	Los usuarios tienen acceso a los datos necesarios para llevar a cabo sus funciones, por lo tanto, los datos se comparten a través de las funciones de las organizaciones.

Tabla 16: Principios de seguridad en la literatura

N°	Artículo	Principio	Descripción
5	The Open Group, 2011	Los datos son accesibles	Los datos son accesibles para que los usuarios puedan llevar a cabo sus funciones. Existe una propiedad de los datos.
6	The Open Group, 2011	Administrador de datos	Cada elemento de datos tiene un administrador responsable de la calidad de datos. Puesto que los datos pueden perder su integridad cuando se introducen varias veces, el administrador de datos será el único responsable de eliminar la entrada de datos redundantes del esfuerzo humano y recursos de datos almacenados.
7	The Open Group, 2011	Seguridad de datos	Los datos deben estar protegidos contra el uso no autorizado y la divulgación. Además, de los aspectos tradicionales de la clasificación de seguridad nacional, esto incluye, pero no se limita a, la protección de la información previa a la toma de decisiones, sensible a la selección de origen, y propietaria.
8	Whitman y Mattord, 2011	Los propietarios de los sistemas tienen responsabilidades de seguridad fuera de sus propias organizaciones	Cuando un sistema almacena y usa información de los clientes, pacientes, socios, u otros, la seguridad de esta información se convierte en la responsabilidad de los propietarios de los sistemas.
9	Stonebur ner *et al.*, 2004	Ofrecer garantías de que el sistema es, y sigue siendo, resistente frente a las amenazas que se esperan	La seguridad es la base para la confianza de que un sistema cumpla con sus expectativas de seguridad. Estas expectativas típicamente se pueden resumir como proporcionar suficiente resistencia a la penetración tanto directa como los intentos de eludir los controles de seguridad.
10	Stonebur ner *et al.*, 2004	Aislar los sistemas públicos de acceso a los recursos de misión crítica (por ejemplo, datos, procesos, etc.)	En los casos en que la sensibilidad o criticidad de la información es alta, las organizaciones pueden querer limitar el número de sistemas en los que se almacena esos datos y aislarlos, ya sea física o lógicamente.
11	Stonebur ner *et al.*, 2004	Proteger la información mientras está siendo procesada, en tránsito y en el almacenamiento	El riesgo de la modificación no autorizada o destrucción de datos, la divulgación de información, y la negación de acceso a los datos en tránsito debe ser considerado junto con los riesgos asociados a los datos que están en almacenamiento o en trámite.
12	Stonebur ner *et al.*, 2004	Identificar y prevenir errores y vulnerabilidades comunes	Muchos errores se vuelvan a producir con regularidad. Aprender del pasado mejorará los resultados futuros.
13	Stonebur ner *et al.*, 2004	Implementar la seguridad a través de una combinación de medidas distribuidas física y lógicamente	A menudo, un único servicio de seguridad se consigue mediante elementos existentes en equipos independientes que cooperan. Es importante asociar todos los elementos con el servicio de seguridad que proporcionan.
14	Stonebur ner *et al.*, 2004	Autenticar a los usuarios y procesos para garantizar que las decisiones de control de acceso sean adecuadas, tanto dentro como fuera de los dominios	La autenticación es el proceso en el que un sistema establece la validez de una transmisión, un mensaje o un medio de verificar la elegibilidad de un individuo, proceso o máquina para llevar a cabo una acción deseada, asegurando así que la seguridad no se ve comprometida por una fuente no confiable.
15	Stonebur ner *et al.*, 2004	Utilizar identidades únicas para asegurar la rendición de cuentas	Una identidad puede representar un usuario real o un proceso con su propia identidad, por ejemplo, un programa que permite realizar un acceso remoto.
16	Stonebur ner *et al.*, 2004	Diseñar y operar un sistema de TI para limitar el daño y ser resistente en respuesta	Los sistemas de información deben ser resistentes a los ataques, deben limitar los daños, y deben recuperarse rápidamente cuando se producen ataques. Se reconoce la necesidad de tecnologías de protección adecuadas a todos los niveles para asegurar que cualquier posible ataque cibernético será contrarrestado de manera efectiva.

Tabla 16 : Principios de seguridad en la literatura (Continuación)

N°	Artículo	Principio	Descripción
17	Stoneburner *et al.*, 2004	Desarrollar y ejercitar procedimientos de contingencia y recuperación de desastres para asegurar la disponibilidad adecuada	La continuidad de los planes de operaciones o procedimientos de recuperación de desastres frente a la continuidad de la operación de una organización en el caso de un desastre o interrupción del servicio prolongada que afecta a la misión de la organización. Tales planes deben contemplar una fase de emergencia de respuesta, una fase de recuperación, y un retorno a la fase de funcionamiento normal. Personal responsable durante un incidente y los recursos disponibles deben ser identificados.
18	Stoneburner *et al.*, 2004; Tipton y Krause, 2003; Wood, 1990	Diseñar e implementar mecanismos de auditoría para detectar el uso no autorizado y para apoyar las investigaciones de incidentes	Las organizaciones deben monitorizar, grabar y revisar periódicamente los registros de auditoría para identificar el uso no autorizado y garantizar que los recursos del sistema están funcionando correctamente.
19	Stoneburner *et al.*, 2004; Tipton y Krause, 2003; Wood, 1990	Implementar mínimo privilegio	El concepto de limitar el acceso, o "menor privilegio", es simplemente proporcionar no más autorizaciones que las necesarias para realizar las funciones requeridas. Esto es quizás lo que más a menudo se aplica en la administración del sistema. Su objetivo es reducir el riesgo mediante la limitación del número de personas con acceso a los controles críticos de seguridad del sistema.
20	Tipton y Krause, 2003	Responsabilidad individual	Los individuos se identifican de forma única en los sistemas de seguridad, y los usuarios son responsables de sus acciones.
21	Tipton y Krause, 2003	Autorización	Los mecanismos de seguridad deben ser capaces de conceder autorizaciones para el acceso a la información o los sistemas específicos basados en identificación y autentificación del usuario.
22	Tipton y Krause, 2003; Ozier, 1997	Proporcionalidad	Los controles de seguridad de la información deben ser proporcionales a los riesgos de la modificación, la negación del uso o divulgación de la información.
23	Dhillon y Backhouse, 2000; Ozier, 1997	Disponibilidad	Se refiere al hecho de que los sistemas utilizados por una organización siempre están disponibles cuando se necesitan.
24	Dhillon y Backhouse, 2000; Ozier, 1997	Integridad	Se refiere al mantenimiento de los valores de los datos almacenados y manipulados, tales como el mantenimiento de los signos y símbolos correctos.
25	Dhillon y Backhouse, 2000; Ozier, 1997	Confidencialidad	Se refiere principalmente a la restricción del acceso a los datos solo a aquellos que están autorizados.
26	Ozier, 1997	La continuidad operativa y planes de contingencia	La dirección debe planificar y operar tecnología de la información de tal manera que se preserve la continuidad de las operaciones de la organización.
27	Wood, 1990	Atrapamiento	Atrapamiento se refiere al proceso por el cual alguien es inducido a realizar un acto ilegal o abusivo. Una forma de establecer controles que utilizan atrapamiento es la creación de un "agujero" en el sistema de control de acceso y observar los penetradores que intentar aprovechar este agujero.
28	Wood, 1990	Controlar la periferia	Se refiere a establecer una especie de valla o muro en la periferia que impida el acceso a entidades no autorizadas.

Tabla 16 : Principios de seguridad en la literatura (Continuación)

Para la representación de la seguridad se puede personalizar el lenguaje ArchiMate a través de la especialización de elementos (estereotipos) lo que permite definir nuevos elementos o relaciones. Este mecanismo, que ya ha sido usado en Band *et al.* (2015), permite modelar un *Requisito de Seguridad* o un *Principio de Seguridad* utilizando estereotipos que serán identificados entre los símbolos "« »". Adicionalmente, la relación que existe entre los principios de seguridad y los requisitos de seguridad se establece en ArchiMate a través de una relación de ***realización***, cuya simbología se muestra en la Figura 12 y que en este caso se refiere a que entidades más abstractas (Principios) se realizan por medio de entidades más tangibles (Requisitos).

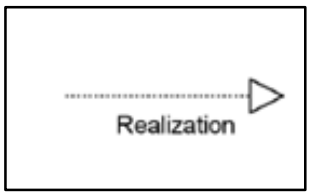


Figura 12: Simbología relación Realización en ArchiMate

En la Figura 13 se muestra el principio *Seguridad de Datos* realizado por los requisitos *Control de Acceso a los datos* y *Privacidad de los Datos*.

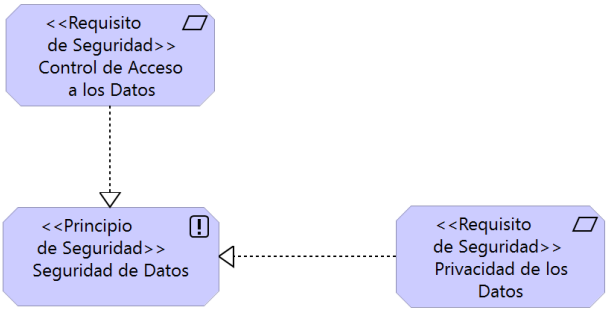


Figura 13: Ejemplo relación principio de seguridad - requisitos de seguridad

Una vez definida la forma de modelar Principios y Requisitos de seguridad de la capa motivacional de ArchiMate 3.0, es necesario indicar la manera en que éstos se relacionan con los elementos de la capa de negocio. La especificación de ArchiMate 3.0 establece que tanto el elemento "Principio" como el elemento "Requisito" se pueden relacionar con casi cualquier elemento del lenguaje a través de la relación de ***realización*** o ***asociación***, cuya simbología se muestra en la Figura 14. Esto incluye ya sea un elemento de comportamiento o uno estructural, solo el elemento Stakeholder no permite estas relaciones (The Open Group, 2016).

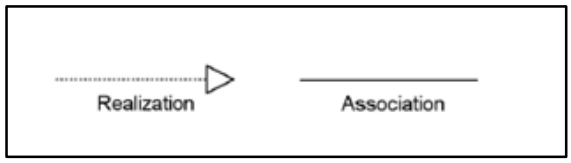


Figura 14: Simbología para relaciones entre elementos de estructura y comportamiento

Lo anterior muestra que existen dos formas de representar o modelar los requisitos de seguridad especificados en la capa de negocio. Un ejemplo básico de estas relaciones entre las capas de negocio y los requisitos de seguridad se muestra en la Figura 15 y en la Figura 16. En la primera de ellas el proceso de negocio "*Pagar multa/factura a biblioteca*" especificado en la capa de negocio requiere de especificaciones de seguridad, más concretamente se especifica "Control de Acceso" y "Privacidad". Para ello ha sido necesario ***asociar*** a dicho proceso los requisitos de seguridad que realizan el principio "Seguridad de datos" especificados en la capa Motivacional.

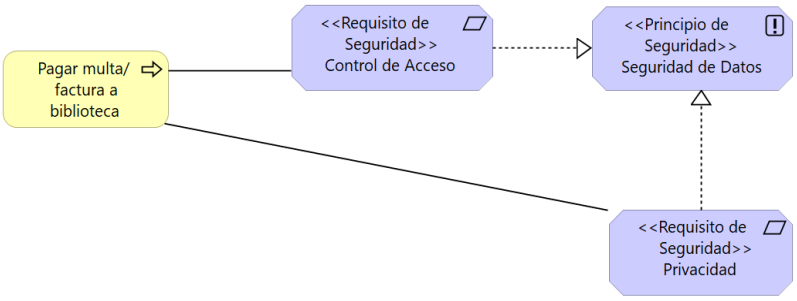


Figura 15: Parte 1 de un modelo de Arquitectura Empresarial segura

Otra posible relación es la mostrada en la Figura 16, donde se muestra la relación de ***realización***, donde el mismo proceso de "*Pagar multa/factura a biblioteca*" ***realiza*** un requisito de seguridad denominado "Control de acceso" y otro denominado "Privacidad", los cuales a su vez ***realizan*** un principio de seguridad denominado "Seguridad de datos".

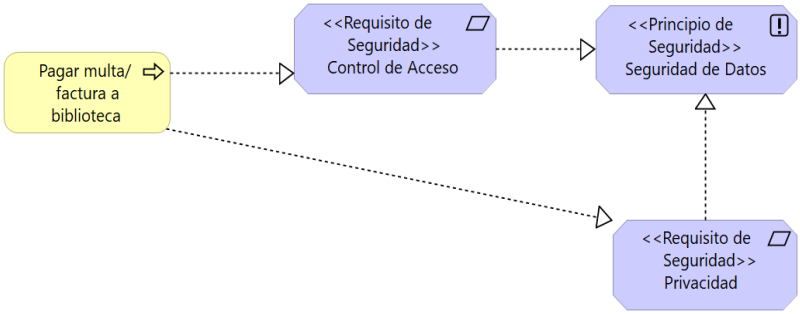


Figura 16: Parte 2 de un modelo de arquitectura empresarial segura

En síntesis, un requisito de seguridad puede ser representado en ArchiMate usando la capa motivacional mediante los elementos requisito/principio que pueden ser vinculados por la relación **realización**. Puesto que los requisitos están especificados en capa motivacional, éstos pueden ser asociados a los elementos de cualquier otra capa a través de las relaciones de **realización** o **asociación**, con la sola excepción del elemento stakeholder (The Open Group, 2016). No obstante, estas son solo las relaciones permitidas por el lenguaje, hay que tener en cuenta la relación lógica que puede existir entre el concepto del negocio representado y el requisito de seguridad asociado o realizado. Por ejemplo, el requisito de seguridad relacionado a los datos denominado "Integridad", solo se relaciona lógicamente a elementos relacionados a datos, un elemento "Rol de Negocio" instanciado como "bibliotecario" no tiene una relación lógica

con este requisito de seguridad. Dicho lo anterior, aunque la relación de la seguridad es posible en ArchiMate del modo descrito, es necesario poner atención en la especificación lógica y contextual de la misma.

4.2 Requisitos de BPMN-BPSec en ArchiMate

En la Sección anterior se presentó la forma de modelar los requisitos de seguridad en ArchiMate. En esta Sección se muestra cómo modelar los requisitos de seguridad que incluye la propuesta BPMN-BPSec en ArchiMate, considerando la especificación lógica y contextual de dichos requisitos.

En la Sección 4.2.1 se introduce la propuesta BPMN-BPSec y los requisitos de seguridad que esta incluye. En la Sección 4.2.2 se presenta la relación de dichos requisitos con los principios de seguridad presentados en la Tabla 16 de la sección anterior, para luego exponer la relación que es posible de establecer entre los requisitos de seguridad incluidos en la propuesta BPMN-BPSec y modelados en ArchiMate y los elementos de la capa de negocio de éste, logrando una especificación de requisitos de seguridad en ArchiMate que considera la lógica y el contexto.

4.2.1 Especificación de la seguridad en BPMN

BPMN-BPSec (Rodríguez *et al.*, 2007) es una extensión de BPMN y como tal integra nuevos conceptos a la notación, en este caso requisitos de seguridad. Los requisitos de seguridad posibles de representar fueron tomados de (Firesmith, 2003) y corresponden a:

- Control de acceso: El control de acceso se refiere a limitar el acceso a sus recursos solo a las entidades externas autorizadas (por ejemplo, usuarios humanos, programas, dispositivos u otros sistemas).
- Detección de ataques y amenazas: es el grado con el que un atentado o ataque exitoso (o su resultado de daño) es detectado, grabado y notificado.
- Integridad: es el grado con el que un componente es protegido de intencional o no autorizada corrupción.
- No repudio: es el grado con el que una parte de una interacción (por ejemplo un mensaje, transacción o transmisión de datos) es impedida del repudio exitoso (o negado) de un aspecto de la interacción.
- Privacidad: es el grado con el que una parte no autorizada (entidad) es impedida de obtener información sensible. Incluye anonimato y confidencialidad.

Existen trabajos con BPMN-BPSec en los que se han elaborado reglas de transformación bajo el enfoque de la Arquitectura Dirigida por Modelos, permitiendo obtener diagramas de casos de uso y diagramas de clases UML. Esto indica que es posible realizar reglas de transformación hacia otros lenguajes de modelado usando esta extensión de BPMN, por lo cual es apropiado usarla para realizar la correspondencia que se tiene como objetivo realizar en esta Tesis.

En el metamodelo de BPMN-BPSec se representan estos requisitos y la relación de cada uno de ellos con los elementos de BPMN. En la Tabla 17 se muestra, de manera resumida, la relación de los elementos de BPMN que tienen una relación con los requisitos de seguridad incluidos en la propuesta BPSec. En la Tabla 17, una “X” representa la relación entre el requisito y el elemento de BPMN. Por ejemplo el “Control de Acceso” tiene una relación con todos los elementos de

BPMN que se muestran en la Tabla 17, mientras que el "No repudio" solo tiene una relación con el elemento MessageFlow de BPMN.

Requisito de seguridad	Elementos de BPMN					
	Activity	DataObject	Group	Lane	MessageFlow	Pool
Control de Acceso	X	X	X	X	X	X
Detección de ataques y amenazas		X	X	X	X	X
Integridad		X			X	
No repudio					X	
Privacidad			X	X		X

Tabla 17: Relación BPMN con requisitos de seguridad de BPSec

A partir de esta especificación se deben definir los criterios para relacionar los requisitos de seguridad descrita en BPMN-BPSec con los elementos de la capa de negocio de ArchiMate.

4.2.2 Modelado de Requisitos de Seguridad en ArchiMate-BPMN-BPSec

Antes de especificar la correspondencia entre ArchiMate y BPMN-BPSec, es necesario establecer los fundamentos que guían el modelado de los requisitos de seguridad de BPMN-BPSec en el modelo de Arquitectura Empresarial con ArchiMate, logrando una especificación de requisitos que considera la lógica y contexto de éstos. Para lo cual se requiere realizar dos importantes pasos:

1. Asociar los principios de seguridad de la literatura con los requisitos de seguridad que son posibles de representar en BPMN-BPSec.
2. Vincular los elementos de la capa de negocio de ArchiMate en donde es posible representar la seguridad con los requisitos incluidos en la propuesta BPMN-BPSec.

En la Tabla 18 se muestra la relación entre los requisitos de seguridad posibles de representar en BPMN-BPSec y los principios de seguridad mostrados en la Tabla 16. En la Tabla 18, los principios se identifican como [Pp N° X], donde x corresponde al número del principio en la Tabla 16. Se establece el Tipo de Relación entre los requisitos de seguridad de BPMN-BPSec como una relación "Directa" cuando la definición o descripción del "Principio" lo vincula al "Requisito" y la relación "Indirecta" cuando el "Principio" puede tener una interpretación que lo vincula al "Requisito" o dicho de otra forma, se puede interpretar de cierta manera que permite tener una cercanía o un vínculo con el "Principio", la cual no está especificada en su descripción.

Requisito de Seguridad de BPMN-BPSec	Principio de Seguridad	Tipo de Relación
Control de acceso	Los datos son un activo [Pp N° 3]	Indirecta
	Los datos se comparten [Pp N° 4]	Indirecta
	Los datos son accesibles [Pp N° 5]	Indirecta
	Administrador de datos [Pp N° 6]	Indirecta
	Seguridad de datos [Pp N° 7]	Indirecta
	Los propietarios de los sistemas tienen responsabilidades de seguridad fuera de sus propias organizaciones [Pp N° 8]	Indirecta
	Ofrecer garantías de que el sistema es, y sigue siendo, resistente frente a las amenazas que se esperan [Pp N° 9]	Indirecta
	Aislar los sistemas públicos de acceso a los recursos de misión crítica (por ejemplo, datos, procesos, etc.) [Pp N° 10]	Directa
	Proteger la información mientras está siendo procesada, en tránsito y en el almacenamiento [Pp N° 11]	Directa
	Autenticar a los usuarios y procesos para garantizar que las decisiones de control de acceso sean adecuadas, tanto dentro como fuera de los dominios [Pp N° 14]	Directa
	Implementar mínimo privilegio [Pp N° 19]	Directa
	Responsabilidad individual [Pp N° 20]	Directa
	Autorización [Pp N° 21]	Directa
	Confidencialidad [Pp N° 25]	Directa
	Controlar la periferia [Pp N° 28]	Indirecta
Detección de ataques y amenazas	Diseñar y operar un sistema de TI para limitar el daño y ser resistente en respuesta [Pp N° 16]	Directa
	Atrapamiento [Pp N° 27]	Indirecta
Integridad	Aplicaciones de uso común [Pp N° 2]	Indirecta
	Los datos son un activo [Pp N° 3]	Indirecta
	Administrador de datos [Pp N° 6]	Directa
	Proteger la información mientras está siendo procesada, en tránsito y en el almacenamiento [Pp N° 11]	Directa
	Integridad [Pp N° 24]	Directa
No Repudio	Utilizar identidades únicas para asegurar la rendición de cuentas [Pp N° 15]	Indirecta
	Responsabilidad individual [Pp N° 20]	Directa
Privacidad	Los datos son accesibles [Pp N° 5]	Indirecta
	Seguridad de datos [Pp N° 7]	Indirecta
	Los propietarios de los sistemas tienen responsabilidades de seguridad fuera de sus propias organizaciones [Pp N° 8]	Directa
	Proteger la información mientras está siendo procesada, en tránsito y en el almacenamiento [Pp N° 11]	Indirecta
	Confidencialidad [Pp N° 25]	Indirecta

Tabla 18: Relación de los requisitos de BPMN-BPSec con los principios de seguridad

Para vincular los requisitos de la capa de negocio de ArchiMate con los requisitos de seguridad de BPMN-BPSec, se deben establecer criterios de relación. Los criterios usados se basan en los mismos usados para la especificación de estos requisitos en BPMN. Estos criterios son:

- Control de acceso: Tiene una relación con elementos que pueden modelar acciones o tareas (individuales o compuestas), datos almacenados o datos en tránsito (el flujo), agrupaciones de acciones o tareas y participantes.
- Detección de ataques y amenazas: Tiene una relación con elementos que modelan los datos grabados o datos en tránsito, grupos de acciones o tareas y participantes.
- Integridad: Tiene una relación solo con elementos que modelan datos grabados y en tránsito.
- No repudio: Tiene una relación solo con elementos que modelan los datos en tránsito, es decir transacción o transmisión.
- Privacidad: Tiene una relación solo con elementos que modelan agrupaciones de acciones o tareas y participantes.

Los elementos de la capa de negocio que cumplen con el criterio de relación del requisito son aquellos elementos de ArchiMate en los que se permite la especificación de dicho requisito.
En la Tabla 19 se muestra la relación entre los elementos de la capa de negocio de ArchiMate con los requisitos de BPMN-BPSec basados en los criterios definidos. Una "X" significa que un elemento de la capa de negocio de ArchiMate "puede" (pero no está obligado a) tener una relación lógica con el requisito de seguridad.

Elemento de la capa de negocio de ArchiMate	**Requisitos de Seguridad BPMN-BPSec**				
	Control de acceso	**Detección de amenazas y ataques**	**Integridad**	**No repudio**	**Privacidad**
Business Actor	X	X			X
Business Role	X	X			X
Business collaboration	X	X			X
Business interface					
Business Process	X	X			X
Business function	X	X			X
Business interaction	X	X			X
Business event					
Business service					
Business object	X	X	X		
Contract	X	X	X		
Representation	X	X	X		
Product	X				X

Tabla 19: Relación elementos ArchiMate con requisitos BPSec

En base a esta información se puede observar que, exceptuando el requisito de No Repudio, todos los otros requisitos de BPMN-BPSec se relacionan con alguno de los elementos de la capa de negocio de ArchiMate. El requisito No Repudio no puede ser representado pues no existe algún elemento en la capa de negocio de ArchiMate que pueda representar flujos de datos entre actores o participantes.

Los elementos de la capa de negocio de ArchiMate que no tienen relación con los requisitos de seguridad BPMN-BPSec son aquellos que no cumplen con los criterios de relación. (i) Una *Business Interface* debe ser preferentemente un sustantivo, no puede representar un participante ya que expone la funcionalidad de un servicio de negocio a un rol o actores y tampoco puede representar una agrupación o un dato, se puede decir que es un canal o un medio (por ejemplo un teléfono o el Internet) por lo cual no es posible que tenga una relación con los requisitos de seguridad; (ii) Un *Business Event* puede originarse en el entorno de la organización (por ejemplo, desde un cliente), pero también pueden producirse eventos internos generados por otro elemento de estructura activa como por ejemplo un Business Process, no puede ser clasificado dentro de algunos de los criterios definidos anteriormente, ya que es un comportamiento que ocurre instantáneamente; (ii) Un *Business Service* expone el comportamiento, pero no es el comportamiento.

Los requisitos de BPMN-BPSec son usados con la finalidad de indicar que un determinado elemento de BPMN debe implementar el requisito de seguridad. En ArchiMate, esto sería equivalente a exponer la relación donde un elemento realiza un requisito, por ello *la relación más ideal para representar este vínculo entre los requisitos de BPMN-BPSec y los elementos en ArchiMate sería la* ***realización*** *mostrada en la Figura 16.*

De esta forma, en esta sección se ha mostrado cómo especificar los requisitos de seguridad incluidos BPMN-BPSec en ArchiMate, considerando la lógica y contexto de estos.

4.3 Equivalencias entre ArchiMate y BPMN-BPSec

Dado que el propósito de este trabajo es encontrar una equivalencia entre la capa de negocio de ArchiMate y BPMN en relación a la seguridad, en esta sección se analiza primeramente la equivalencia entre los elementos de la capa de negocio de ArchiMate y BPMN (sin considerar la seguridad), y luego la equivalencia de la seguridad a través de los requisitos de seguridad. Finalmente, se establece el conjunto de equivalencias especificadas como reglas de transformación entre ambos modelos.

4.3.1 Correspondencia entre elementos de ArchiMate y BPMN

En la literatura existen varias propuestas sobre correspondencia entre modelos ArchiMate y BPMN (Penicina, 2013; Gill y Qureshi, 2015; Kirikova *et al.*, 2016). En estos trabajos se proponen correspondencias de elemento a elemento que se basan principalmente en la semántica de los mismos. Adicionalmente, y como parte de esta Tesis, se proponen otras correspondencias teniendo en cuenta que en ArchiMate la combinación de elementos y el nivel de abstracción en el que se modela podría tener una correspondencia hacia más de un elemento en BPMN.

Las correspondencias se muestran en la Tabla 20, donde, por cada elemento de ArchiMate, se presenta el o los elementos de BPMN con los que tiene correspondencia, el origen de la

correspondencia, vale decir, si es tomada de la literatura o si es una propuesta propia de esta investigación y, finalmente, una explicación de por qué se plantea dicha correspondencia.

ArchiMate	BPMN	Origen	Explicación
Business Actor	Pool	Gill y Qureshi, 2015	Un Pool puede representar procesos o participantes y un Business Actor puede ser interpretado como un participante en la capa de negocio de ArchiMate, por ello semánticamente estos elementos tienen una correspondencia.
	Lane	Propia	Un Lane al igual que un Pool puede representar participantes con la diferencia que solo puede representar participantes. Como un Business Actor puede ser interpretado como un participante en la capa de negocio de ArchiMate entonces semánticamente estos elementos tienen una correspondencia.
Business Role	Pool	Propia	Un Business Role puede ser clasificado como participante y como un Pool puede representar un participante, entonces, semánticamente ambos elementos tienen una correspondencia.
	Lane	Penicina, 2013; Kirikova *et al.*, 2016	Un Business Role es similar a un business actor, puede ser clasificado como un participante del proceso y como tal puede ser modelado con un Lane.
Business collaboration	Pool	Propia	Una Business Collaboration puede ser clasificada como un participante en el entorno del negocio, y un Pool puede representar un participante, entonces, una business collaboration semánticamente puede tener una correspondencia con un Pool.
	Lane	Propia	Una Business Colaboration puede ser clasificada como un participante, y como un Lane representa participantes, entonces, semánticamente una business colaboration puede tener una correspondencia con un Lane.
Business Process	Pool	Penicina, 2013; Kirikova *et al.*, 2016	En BPMN un Pool puede representar un proceso de negocio, además de participantes. Por ello, semánticamente un Business Process puede tener una correspondencia con un Pool en BPMN.
	Activity	Gill y Qureshi, 2015	Un Business Process representa una secuencia de comportamientos de negocio que logra un resultado específico. Una Activity representa una unidad de trabajo a realizar, pero también puede representar una tarea un poco más compleja a través de un sub-proceso (extensión de una Actividad pero que sigue siendo una actividad). ArchiMate tiene un nivel de abstracción mucho mayor que BPMN, así que lógicamente es muy poco probable que un Business Process en ArchiMate sea usado para representar una unidad de trabajo simple, pero sí es muy probable que pueda ser usado para representar un sub-proceso. Sigue existiendo la posibilidad de que sea una tarea simple o algo más complejo en un sub-proceso, pero al final ambos son una actividad.
Business Event	Event	Penicina, 2013; Gill y Qureshi, 2015; Kirikova *et al.*, 2016	Un Business Event es un elemento de la conducta empresarial que indica un cambio de estado de la organización. Desencadenan o interrumpen el comportamiento y son instantáneos. Los eventos de BPMN representan algo que ocurre o que puede ocurrir durante el curso de un proceso. Por lo anterior, un business Event de ArchiMate es semánticamente similar a un evento en BPMN.

Tabla 20: Correspondencia de elementos ArchiMate a BPMN

ArchiMate	BPMN	Origen	Explicación
Business Object	Data Object	Penicina, 2013; Gill y Qureshi, 2015; Kirikova *et al.*, 2016	Un Business Object podría ser usado para representar los activos de información que son relevantes desde un punto de vista comercial y puede ser realizada por los objetos de datos. Un Data Object permite mostrar la información que una actividad necesita, como las entradas y las salidas. Es decir, representan los documentos, la información y otros objetos que son usados o actualizados durante el proceso. Semánticamente ambos elementos tienen una correspondencia.
Contract	Data Object	Propia	Un Contract generalmente se refiere a un documento donde se presenta información de un acuerdo entre dos o más partes, por lo cual semánticamente solo puede tener una correspondencia con un Data Object en BPMN.
Representation	Data Object	Propia	Una Representation es una forma perceptible de la información transportada por un objeto de negocio, puede decirse que se refiere a una parte de un objeto de negocio, por lo cual puede tener una correspondencia semantica con un Data Object al referirse a información a fin de cuentas.

Tabla 20: Correspondencia de elementos ArchiMate a BPMN (Continuación)

En cuanto a los requisitos de seguridad, las correspondencias básicas se establecen como que un requisito de seguridad de ArchiMate tendrá una correspondencia con su homólogo en BPSec, como se muestra en la Tabla 21.

Nombre del elemento en ArchiMate	Notación del elemento en ArchiMate	Nombre del elemento en BPMN-BPSec	Notación del elemento en BPMN-BPSec
Requisito de Seguridad instanciado como Control de Acceso	<<Requisito de seguridad>> Control de acceso	Requisito de seguridad Control de Acceso	AC
Requisito de Seguridad instanciado como Detección de Ataques y Amenazas	<<Requisito de seguridad>> Detección de ataques y amenazas	Requisito de seguridad Detección de Ataques y Amenazas	AD
Requisito de Seguridad instanciado como Integridad	<<Requisito de seguridad>> Integridad	Requisito de seguridad Integridad	I_x
Requisito de Seguridad instanciado como No Repudio	<<Requisito de seguridad>> No Repudio	Requisito de seguridad No Repudio	NR
Requisito de Seguridad instanciado como Privacidad	<<Requisito de seguridad>> Privacidad	Requisito de seguridad Privacidad	P_x

Tabla 21: Correspondencia requisitos de seguridad de ArchiMate a BPMN-BPSec

Los principios de seguridad no se muestran en la correspondencia, ya que actualmente no existe una forma de modelarlos en BPMN.

4.3.2 Reglas de transformación

En la sección anterior solo se considera la correspondencia de elemento a elemento y no de modelo a modelo que es el objetivo de esta Tesis. Un modelo de Arquitectura Empresarial no es tan simple como para que las correspondencias entre elementos permitan realizar una correspondencia automática de modelo a modelo. El conjunto de elementos que se relacionan entre si (contexto), tienen un impacto muy significativo al momento de realizar la correspondencia entre modelos. Es por esto que en esta sección se proponen una serie de reglas de transformación que tienen como objetivo permitir la correspondencia entre ArchiMate y BPMN-BPSec considerando el contexto y así liberándose de la interacción con el modelador para realizar la correspondencia.

Las correspondencias entre elementos que han sido definidas en la sección anterior son la guía para proponer reglas de transformación de modelo a modelo donde existe más de un elemento involucrado. Estas reglas se clasifican en casos o escenarios que se pueden presentar al momento de realizar la correspondencia de modelos. Para esto se analizaron varios modelos de Arquitectura Empresarial con ArchiMate presentes en la Web, considerando escenarios reales y repetitivos entre los modelos. Algunas de estas reglas dejan más claro el porqué algunos elementos ArchiMate tienen más de un elemento BPMN como correspondencia.

Al momento de realizar la correspondencia de la capa de negocio de un modelo de Arquitectura Empresarial modelado con ArchiMate a un modelo modelado con BPMN-BPSec se deben de tener en cuenta las reglas de transformación, ya que éstas son las que permiten realizar la correspondencia en base a la realidad de los modelos. Las reglas toman las correspondencias entre elementos como base, pero también dependen del contexto del modelo.

A continuación, se muestra una regla de transformación como una forma de ejemplificar la manera en que éstas se describen, mientras que el total de 19 reglas propuestas se encuentran en el Anexo A. Las reglas se encuentran clasificadas por escenarios y muestran los elementos involucrados en la regla, la regla de transformación en base al lenguaje de transformación de modelos ATL (Atlas Transformation Language) y una representación gráfica de los elementos. La mayoría de estas reglas constan de dos partes importantes. Una parte es la correspondencia de los elementos de ArchiMate a BPMN y la otra es la correspondencia de los requisitos de seguridad específicamente hacia los requisitos de BPSec. Ambas partes están en una sola regla ya que la seguridad está integrada en el modelo. En la parte de la Regla en ATL, la sección de seguridad se encuentra destacada en un recuadro. No todos los elementos conllevan seguridad, y no son los mismos requisitos de seguridad para todos, estos se basan en la Tabla 19, en la cual se determinó cuáles requisitos se relacionaban a cada elemento de la capa de negocio de ArchiMate. Se debe tener en cuenta que la creación de reglas ATL para la trasformación de modelo a modelo de forma automática es algo considerado posteriormente a la definición de los objetivos de esta Tesis, debido a que facilitan la correspondencia entre los modelos de ArchiMate y BPMN-BPSec.

4.3.2.1 Regla de transformación 1

Escenario 1.- Un proceso de negocio de ArchiMate como Pool o Actividad en BPMN: Un *<proceso de negocio>* en ArchiMate pueden tener relación de *<composición>* o *<agregación>* con este mismo elemento.

Las relaciones de *<composición>* y *<agregación>* se identifica visualmente de dos formas: en la Figura 17 se muestran las relaciones de *<composición>* o *<agregación>*, mientras que en la Figura 18 las relaciones se identifican por el hecho que visualmente los elementos están contenidos dentro de otro. En los siguientes escenarios estas relaciones pueden no ser resaltadas.

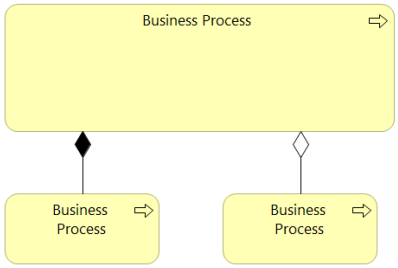


Figura 17: Uso de relación de composición y agregación Alternativa 1

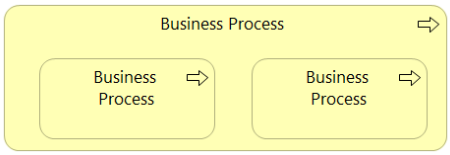


Figura 18: Uso de relación de composición y agregación Alternativa 2

Regla 1.- Cuando un *<proceso de negocio>* de ArchiMate no se encuentra siendo parte de otro *<proceso de negocio>* (se refiere a tener una relación de *<composición>* o *<agregación>*), entonces el *<proceso de negocio>* tiene una correspondencia con un *<Pool>* en BPMN. La seguridad especificada en los elementos tiene una correspondencia como se especifica.

N° de Regla: 1

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>	*<Pool>*

Regla en ATL:

```
rule BusinessPToPool {
        from
                a : ARC!Elemento (a.isBusinessP(a.Tipo) and
                        a.BusinessPIsPool(a.Id))
        to
                b : BPS!Pool (
                        Name <- a.Name,
                        --Requisitos de Seguridad--
                        RequisitoAC <- a.requisitoControlAc(a),
                        RequisitoAD <- a.requisitoDetecAtacAm(a),
                        RequisitoP <- a.requisitoPrivacidad(a)
                )
    }
```

Gráficamente:

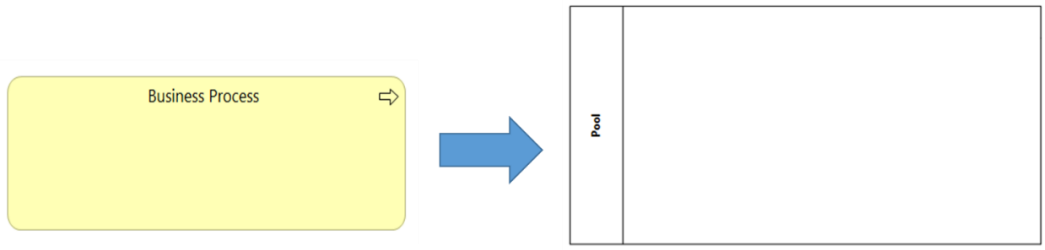


Figura 19: Business Process simple a un Pool

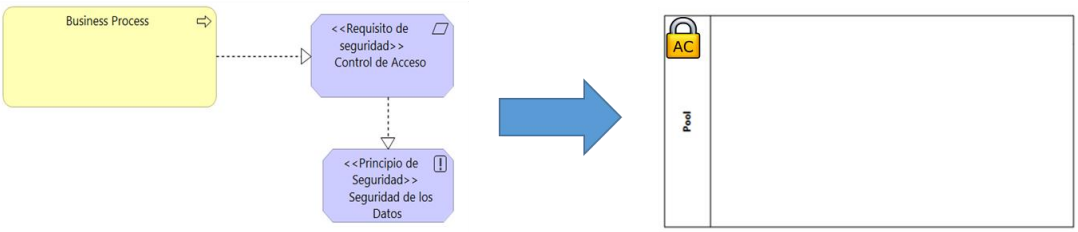


Figura 20: Business Process simple a un Pool (Con Control de Acceso)

4.4 Conclusiones

Actualmente en la literatura existen varias propuestas de transformación de elementos entre ArchiMate y BPMN (Penicina, 2013; Gill y Qureshi, 2015; Kirikova *et al.*, 2016), pero se ha observado que éstas se enfocan en la semántica de los elementos. Esto, si bien es útil para el modelador, no permite abordar adecuadamente las consecuencias que se derivan de las relaciones entre los elementos que son descritas en el modelo. Esto es causado por el hecho de

que, en un modelo, los elementos y las relaciones entre éstos causan un impacto en la transformación. Cuando los elementos poseen más de una posible correspondencia, el poder definir cuál de éstas es la más adecuada depende del contexto, que generalmente se basa en las relaciones de los elementos. Es por esto que las relaciones tienen un impacto importante en la correspondencia final y no se ha logrado identificar un artículo en la literatura que lo aborde. Además, considerar los elementos y sus relaciones mejora la correspondencia entre modelos ArchiMate y BPMN, permitiendo que puedan existir transformaciones autónomas entre modelos, es decir, sin la interacción del modelador mediante el uso de las tecnologías y lenguajes computacionales.

En esta Tesis se han tenido en cuenta las propuestas de la literatura con respecto a la correspondencia de elementos entre los lenguajes ArchiMate y BPMN de forma semántica. Además, se han enriquecido estas propuestas en base al conocimiento que ha sido adquirido durante el desarrollo de esta Tesis, proponiendo correspondencias mucho más completas.

En cuanto a la correspondencia de ArchiMate a BPMN-BPSec, no existe mayor complejidad para realizar la correspondencia debido a que en el modelo un elemento de ArchiMate puede tener una correspondencia con un solo elemento de BPMN. De manera que, los requisitos se relacionan a los elementos y estos tienen un solo elemento de correspondencia, lo cual significa que no existe complejidad adicional en la correspondencia de requisitos entre ambos lenguajes.

La correspondencia de la seguridad se trabaja de forma conjunta con las reglas de transformación de los elementos de la capa de negocio de ArchiMate hacia BPMN-BPSec, evidenciando el hecho de que la seguridad es una parte integrada del modelo y no una parte separada que puede ser tratada como algo externo del modelo.

El objetivo de esta Tesis era solo realizar la correspondencia de la seguridad de modelo a modelo. Sin embargo, debido a que no existía una correspondencia completa de modelo a modelo que pudiera integrarse con la correspondencia de la seguridad, también se desarrolló la correspondencia del modelo de la capa de negocio de ArchiMate junto con los requisitos seguridad de forma integrada hacia BPMN con la extensión BPMN-BPSec.

Capítulo 5: Correspondencia de BPMN-BPSec a IFML

Las interfaces de usuario tienen relación con los procesos de negocio, por ello, si existe un modelo de interfaz de usuario de una aplicación computacional para una empresa, entonces esta interfaz de usuario debe ser consistente al modelo de proceso de negocio de la misma, incluyendo la seguridad modelada en él. El presente capítulo se centra en el cuarto objetivo de esta Tesis, el cual consiste en: "Establecer una correspondencia entre los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec y los elementos de IFML". Por ello, en las siguientes secciones se desarrolla esta correspondencia entre los modelos de proceso de negocio seguro modelados con BPMN-BPSec y los modelos de interfaz de usuario o Front End modelados con IFML.

Se ha realizado una revisión sistemática de la literatura en búsqueda de una correspondencia entre BPMN e IFML, considerando el modelado de requisitos de seguridad. Se revisaron 627 artículos pesquisados de los buscadores Scopus, ScienceDirect, SpringerLink y Google Scholar. No se encontró una transformación directa desde BPMN hacia IFML, no obstante, sí se identificaron patrones de interfaz de usuario modelados con IFML que pueden tener una relación con la seguridad.

Teniendo como base la información obtenida de la revisión sistemática de la literatura, este Capítulo se encuentra estructurado de la siguiente forma: en la Sección 5.1 se muestra un análisis y selección de los patrones de Front End modelados con IFML provenientes de la literatura que tienen relación con la seguridad; en la Sección 5.2 se busca establecer la correspondencia de los elementos de BPMN con IFML; luego, en la Sección 5.3 se muestra un análisis de los requisitos de seguridad de BPMN-BPSec en el Front End sin tener en cuenta los modelos, para luego realizar una relación de los requisitos de seguridad de BPMN-BPSec que tienen una representación en el Front End con los patrones relacionados con la seguridad seleccionados en la Sección 5.1; en la Sección 5.4, se establece la correspondencia entre BPMN-BPSec e IFML a través de la combinación de los resultados de las Secciones 5.2 y 5.3; y, finalmente, en la Sección 5.5 se presentan las conclusiones del Capítulo.

5.1 Patrones Front End modelados con IFML relacionados a la seguridad

Los resultados de la revisión sistemática de la literatura no proveen una correspondencia de BPMN a IFML como base para plantear una correspondencia entre BPMN-BPSec e IFML. No obstante, en la revisión sistemática de la literatura se encontraron patrones de interfaz de usuario con IFML que tienen una relación con la seguridad.

Por lo anterior, en esta sección se presentan los resultados del análisis de los patrones de Front End encontrados en la literatura. Estos se encontraron en inglés y fueron traducidos al español, pero su abreviación originalmente en inglés fue conservada. Se analizaron los 74 patrones encontrados, de los cuales solo los 19 presentados en la Tabla 22 se relacionan de alguna forma con la seguridad, estando la mayoría de ellos relacionados con el control de acceso. La Tabla 22 cuenta con un numero identificador para cada patrón, el nombre del patrón con su abreviación original en inglés, la finalidad del patrón o uso del patrón, y la relación que tiene con la seguridad, ya sea requisitos de seguridad como tal o cualquier otra relación con la seguridad, como la validación de datos, casos de éxito y errores, etc.

N°	Nombre Patrón	Finalidad del Patrón	Relación con la seguridad
1	OW-MFE: Front ends múltiples en el mismo modelo de dominio (Brambilla y Fraternali, 2014)	Se utiliza como una arquitectura técnica para entregar un conjunto de aplicaciones sobre los mismos datos, representados en el modelo de dominio. Una vista que varía dependiendo del usuario que accede.	Permite que los ViewContainers se utilicen como recursos en un control de acceso basado en funciones.
2	A-OCR: Creación de objetos (Brambilla y Fraternali, 2014)	El patrón de creación de objetos permite la creación de un nuevo objeto.	Se crea un identificador único para el nuevo objeto. Se modela el caso de éxito y el de error.
3	A-OACR: Creación de objetos y asociaciones (Brambilla y Fraternali, 2014)	Puede usarse una variante del patrón de creación de objetos para crear un nuevo objeto y establecer sus asociaciones con otros objetos.	Para seleccionar la conexión a otros objetos se usan datos precargados. Se modela el caso de éxito y el de error.
4	A-ODL: Eliminación de Objetos (Brambilla y Fraternali, 2014)	El patrón de eliminación de objetos se utiliza para eliminar uno o más objetos de una clase dada.	Se modela el caso de éxito y el de error. Se muestran las instancias de los objetos a eliminar.
5	A-CODL: Eliminación (o Borrado) en cascada (Brambilla y Fraternali, 2014)	Se utiliza para propagar la eliminación de un objeto a otros objetos dependientes, que están conectados a él por una asociación con cardinalidad mínima de 1, y, por lo tanto, no podría existir sin el objeto que se está eliminando	Esto mantiene la integridad de los datos. Se modela el caso de éxito y el de error.
6	A-OM: Modificación de objetos (Brambilla y Fraternali, 2014)	El patrón de modificación de objeto se utiliza para actualizar uno o más objetos de una clase dada.	Se modela el caso de éxito y el de error. Se muestran las instancias de los objetos a modificar.
7	DE-INPL: Edición en el lugar (Brambilla y Fraternali, 2014)	La edición *in situ* permite al usuario editar el contenido sin abandonar la vista actual para acceder a un formulario de entrada de datos. Es aplicable cuando la autenticación no es necesaria o el usuario ya está autenticado.	Relación de control de acceso para la edición de datos.
8	DE-VAL: Validación de datos de entrada (Brambilla y Fraternali, 2014)	Un patrón recurrente asociado con la entrada de datos es la validación de la entrada proporcionada por el usuario para asegurar que cumple con los requisitos de la aplicación.	Validación de datos
9	IA-LOGIN: Login (Brambilla y Fraternali, 2014)	La identificación y autenticación del usuario son los procedimientos mediante los cuales la aplicación reconoce y verifica la validez de una identidad proporcionada por el usuario. El medio más común para lograr esta funcionalidad es el proceso de inicio de sesión.	Control de acceso
10	IA-LOGOUT: LOGOUT (Brambilla y Fraternali, 2014)	La información sobre la identidad autenticada del usuario preservada en el Contexto puede ser borrada por iniciativa del usuario mediante una Acción de "Logout".	Relacionado al control de acceso
11	IA-CEX: Notificación de expiración del contenido (Brambilla y Fraternali, 2014)	La información de contexto que contiene la identidad autentificada del usuario también puede ser borrada por el sistema (por ejemplo, por razones de seguridad).	Relacionado al control de acceso

Tabla 22: Patrones de Front End modelados con IFML y su relación con la seguridad

N°	Nombre Patrón	Finalidad del Patrón	Relación con la seguridad
12	IA-SPLOG: Login a un viewcontainer específico (Brambilla y Fraternali, 2014)	La autenticación se proporciona en una página pública y a continuación, el usuario autenticado accede a la colección de páginas privadas. Es el mismo patrón de Login[9] pero el flujo direcciona a una vista privada.	Control de acceso
13	IA-ROLE: Mostrando y desplegando los roles de usuario (Brambilla y Fraternali, 2014)	El patrón de inicio de sesión tiene un segundo efecto secundario, además de la identificación: si los usuarios se clasifican en funciones, la acción de inicio de sesión define el rol predeterminado del usuario que inicia sesión.	Control de acceso, Privacidad
14	IA-RBP: permiso basado en los roles para los elementos de la vista (Brambilla y Fraternali, 2014)	Cuando el usuario es autenticado, la información de Contexto se puede utilizar para implementar permisos de acceso que dependen de la función del usuario. Esto permite que los usuarios accedan a vistas dependiendo de sus roles.	Control de acceso
15	IA-NRBP: permisos negativos basados en roles para los elementos de la vista (Brambilla y Fraternali, 2014)	Asociado a la existencia de vistas que pueden ser para distintos roles, pero que conservan su estructura y contenido en general y solo que se diferencian en cuanto a las funciones. Se diseña una vista única para ambos roles, pero se imponen permisos (negaciones) "negativos" para el rol con reglas de acceso más estrictas.	Control de acceso
16	IA-OBP: Permisos basados en objetos (Brambilla y Fraternali, 2014)	Otro tipo complementario de control de acceso se expresa sobre los objetos de contenido utilizando el concepto de asociaciones de personalización. Es una vista donde una acción provoca un cambio.	Control de acceso a objetos
17	IA-PRO: Gestión y despliegue de perfiles de usuario (Brambilla y Fraternali, 2014)	El perfil de usuario es la información dependiente de la aplicación asociada con la identidad de un usuario autenticado. Es un patrón para modificar la información del usuario identificado.	Privacidad
18	IA-IPSI: inicio de sesión *in situ* (Brambilla y Fraternali, 2014)	Es un patrón típico en el cual el usuario puede navegar por el contenido de las vistas sin estar identificado, pero cuando el usuario intenta activar una cierta acción, puede ser advertido de la necesidad de iniciar sesión primero.	Control de acceso
19	SES-EXC: duración de la expiración de los datos de la sesión (Brambilla y Fraternali, 2014)	Trata de la expiración de la sesión a través de cambiar los datos del usuario por datos que son inválidos, de esta forma la sesión expira.	Control de sesión

Tabla 22: Patrones de Front End con IFML y su relación con la seguridad (Continuación)

Hoy en día se realiza una separación de la seguridad entre los conceptos de Security y Safety, Security es el grado de detección, prevención y reacción al daño malicioso, mientras que Safety se relaciona a la detección, prevención y reacción al daño accidental. En la Tabla 22 se puede apreciar que la mayoría de los patrones de seguridad tienen relación con el daño accidental, es decir relacionado al concepto de Safety. Por otro lado, los requisitos de BPMN-BPSec están relacionados al daño intencional y/o malicioso, o en otras palabras se relacionan con Security. En

este caso, de los patrones seleccionados, solo los patrones relacionados al Login como un mecanismo de control de acceso y algunos relacionados a la privacidad tienen relación con los requisitos incluidos en BPMN-BPSec.

5.2 Correspondencia de elementos BPMN a IFML

Los resultados de la RSL realizada con respecto a la existencia de correspondencias de BPMN hacia IFML no arrojaron resultados positivos. No obstante, en esta Sección se realiza un análisis con la intensión de establecer esta correspondencia.

BPMN cuenta con 12 elementos básicos, los cuales se muestran en la Tabla 23, ordenados en el mismo orden presentado en el documento de especificación de BPMN. En esta Tabla, por cada elemento de BPMN se presenta el elemento IFML o un patrón de Front End modelado con IFML que es la posible correspondencia del elemento BPMN. El símbolo "-" significa que no se encontró una correspondencia adecuada. Además, se presenta una explicación del porqué de la correspondencia o la no existencia de esta en algunos casos. Los elementos de IFML nombrados se encuentran detallados en la Sección 2.3 del Capítulo de conceptos relacionados.

Elemento de BPMN	Elemento IFML o patrón de Front End modelado con IFML	Explicación
Event	Elemento Event	Un Event (Evento) de BPMN tiene una relación semántica con un Event de IFML, pero no es una correspondencia completa, solo existe una relación entre los Eventos Intermedios de BPMN y los Event de IFML.
Activity	-	Una Activity (Actividad) de BPMN no tiene relación con algún elemento o patrón específico de IFML, pues la correspondencia depende del contenido de la actividad, por ejemplo, la actividad de "eliminar un usuario" no tiene la misma representación que una actividad de "crear planilla de ventas".
Gateway	-	Una Gateway (Compuerta) de BPMN no tiene relación con algún elemento o patrón específico de IFML.
Sequence Flow	Elemento Navigation Flow	Un Sequence Flow (Flujo de Secuencia) de BPMN tiene una relación semántica con un Navigation Flow de IFML, pero un Navigation Flow no siempre corresponde a una secuencia de flujo.
Message Flow	-	Un Message Flow (Flujo de Mensaje) de BPMN no tiene una relación semántica con algún elemento o patrón específico de IFML. El Data Flow de IFML podría confundirse como una posible relación, pero este elemento se usa para el flujo de variables desde una vista de la aplicación a otra, mientras que un Flujo de Mensaje implica el Flujo de Mensajes que generalmente se administra a través de Bases de Datos.
Association	-	Una Association (Asociación) de BPMN no tiene relación con algún elemento o patrón específico de IFML.
Pool	-	Un Pool de BPMN no tiene relación con algún elemento o patrón específico de IFML, en IFML no existe una manera de realizar agrupaciones de elementos en el modelo o algo por el estilo.
Lane	-	Ocurre lo mismo que con un Pool, no existe una manera de realizar agrupaciones de elementos en el modelo o algo por el estilo.

Tabla 23: Correspondencia de BPMN a IFML

Elemento de BPMN	Elemento o patrón de Front End modelado con IFML	Explicación
Data Object	Elemento ViewComponent	Un DataObject (Objeto de Dato) de BPMN tiene una correspondencia con un ViewComponent de IFML. Por ejemplo, el contenido de un archivo de información puede estar representando por un ViewComponent en un ViewContainer. Este elemento sigue teniendo una parte de Back End en cuanto a transacciones para manipularlo, debe estar guardado en alguna parte.
Message	Elemento ViewComponent	Un Message (Mensaje) de BPMN se utiliza para representar el contenido de una comunicación entre dos participantes, este contenido puede ser representado a través de un ViewComponent en IFML.
Group	-	Ocurre lo mismo que con un Pool y Lane, no existe una manera de realizar agrupaciones de elementos en el modelo o algo por el estilo.
Annotation	Elemento ViewComponent	Una Annotation (Anotación) de BPMN tiene una relación con un ViewComponent en IFML. Un ViewComponent permite mostrar el contenido, al igual que para el caso de un Objeto de Dato o un Mensaje.

Tabla 23: Correspondencia de BPMN a IFML (Continuación)

Las Activities son el elemento más importante de un proceso de negocio y a través del análisis no es posible establecer una correspondencia directa hacia IFML desde este elemento.
Debido a que es posible de representar solo el contenido de algunos elementos de BPMN en IFML, no es posible establecer una correspondencia exacta y completa entre BPMN e IFML. Solo es posible realizar una correspondencia aproximada y se necesita la intervención de un modelador para realizar la correspondencia completa de los modelos.

5.3 Requisitos de seguridad BPMN-Sec en Front End modelado con IFML

En esta sección se establece qué requisitos involucrados en BPMN-BPSec tienen una representatividad y/o relación con el Front End y cuál es la correspondencia de éstos con los patrones de modelado IFML. Por esto, a continuación se presenta un análisis y selección de los requisitos de seguridad que abarca BPMN-BPSec en relación a su posible representatividad y/o relación con el Front End y el Back End, para luego relacionar los requisitos relacionados al Front End con los patrones seleccionados en la Tabla 22.
La estrategia aplicada en esta Sección consiste en que primero se seleccionan los requisitos de seguridad de BPMN-BPSec que tienen una relación con el Front End, y luego éstos se relacionan con un patrón de Front End modelado con IFML.

5.3.1 Relación requisitos de seguridad BPMN-BPSec con el Front End/Back End

En esta subsección se realiza un análisis de cada uno de los requisitos de BPMN-BPSec con respecto a su representatividad y/o relación con el Front End y el Back End, para seleccionar solo los requisitos de seguridad que tienen una relación con el Front End.

Control de Acceso: En el Front End de la mayoría de las aplicaciones actuales, el control de acceso tiene una interpretación que generalmente se traduce en un Login, en el cual se realiza la identificación y autentificación de las entidades externas a fin de comprobar la autorización que estas entidades poseen para acceder a los recursos que provee el sistema. Se pueden identificar 3 casos donde se producen un Login que tiene significado o interpretación en el Front End:

- Control de acceso a través de una página de inicio donde se consulta la identidad del usuario.
- Cuando el usuario está realizando tareas donde no necesita identificarse, pero llega a una actividad donde lo necesita, debiendo identificarse a través de una página como aquella del primer caso.
- Cuando los datos de un usuario ya identificado y autentificado se usan para comprobar la autorización para acceder a recursos del sistema.

El último caso puede no tener necesariamente una interpretación en el Front End, sino más bien en el Back End.

Todo este análisis es realizado considerando que la interfaz de usuario de control de acceso solo se aplica a los seres humanos, mientras que el control de acceso a software involucrado generalmente se trata en el Back End.

Detección de ataques/amenazas: En el Front End, las acciones de detección y grabado de ataques y/o amenazas no tienen una interpretación, pues estas tareas generalmente son ejecutadas en el Back End. El cumplimiento de la necesidad de notificación de este requisito es la única que tiene una representatividad en el Front End, ya que conlleva la existencia de una interfaz de usuario que muestra los resultados de la detección que han sido previamente grabados. Debido a la simpleza de esta actividad, la utilización de un patrón no es necesaria.

Integridad: En una primera instancia se puede identificar la integridad en el Front End: i) a través de la definición de los tipos de datos que se pueden ingresar en un Formulario, ii) a través de los tipos de datos que se pueden seleccionar, iii) a través de la definición de los tipos de datos que se deben mantener al realizar una eliminación (por ejemplo, que no se pueda eliminar la categoría de películas de "horror" si aún existen películas de este género en la base de datos), y iv) a través de la validación de los datos ingresados. Todas estas interpretaciones se basan en presentar a los usuarios opciones válidas para que no ingresen algo que no es coherente con lo que se está pidiendo. Sin embargo, esta interpretación no coincide del todo con aquella presentada por BPMN-BPSec, ya que la integridad que se maneja en esta extensión se relaciona a una “corrupción intencional” y no “una corrupción accidental” que es lo que las anteriores interpretaciones de integridad buscan. En el Front End, la integridad de BPMN-BPSec no tiene una interpretación, es algo que se controla a través del Back End.

No repudio: En el Front End el requisito de No Repudio no tendría una interpretación, ya que las medidas para cumplir este requisito se implementan en el Back End, sin ninguna repercusión en el Front End. Por ejemplo, en el envío de correos electrónicos no se presenta una interfaz al usuario para que ingrese “Su” dirección de correo electrónico o para ingresar la fecha y hora de envío de un mensaje, puesto que es algo que se realiza en el Back End.

Privacidad: La privacidad en el Front End tiene una interpretación en base a qué datos y/o funciones pueden ser visualizados por un cierto usuario. El uso de los roles de usuario en conjunto con el Login de control de acceso permite identificar al usuario para que en base a esta identidad pueda visualizar ciertos datos y funciones que son responsabilidad de él. Si la privacidad se aplica sobre los datos, esto tiene una interpretación en el Front End en los datos y/o en las funciones aplicables sobre los datos a los que puede o no acceder una persona. Teniendo en cuenta los patrones de diseño en IFML identificados anteriormente, los permisos negativos, como la visualización de funciones de modificación dependiendo del usuario y la propiedad de los datos, podrían tener un significado en este requisito. En resumen, el uso de

roles de usuario, donde se crean vistas distintas para cada usuario o los permisos negativos, donde cierta vista o componente de vista no es visualizado para cierto usuario, son una interpretación de la privacidad en el Front End. La simple agregación de un dato o función que se visualiza en la vista para un cierto tipo de usuario es una interpretación de la privacidad en la interfaz de usuario. Dicho esto, se puede concluir que en un modelo de Front End independiente de la plataforma, la privacidad va ligada con el control de acceso. El control de acceso se encarga de presentar la autorización del usuario sobre los datos y funciones y la privacidad tiene que ver con mostrar los datos y funciones que la autorización dispone.
A modo de resumen, en la Tabla 24 por cada requisito de seguridad involucrado en BPMN-BPSec se presenta si es o no posible de representar o relacionar con el Front End y una explicación de porqué se establece esto.

Requisito de Seguridad BPMN-BPSec	Representación o Relación en el Front End	Explicación
Control de acceso	[Si]	Tiene una interpretación que generalmente se traduce en un Login, en el cual se realiza la identificación y autentificación de las entidades externas a fin de comprobar la autorización que estas entidades poseen para acceder a los recursos que provee el sistema.
Detección de ataques/amenazas	[No]	Las tareas relacionadas a este requisito generalmente son ejecutadas en el Back End. El cumplimiento de la necesidad de notificación de este requisito es la única que tiene una representatividad en el Front End, ya que conlleva la existencia de una interfaz de usuario que muestra los resultados de la detección que han sido previamente grabados. Debido a la simpleza de esta actividad, el establecimiento de un patrón no es necesario.
Integridad	[No]	En el Front End, la integridad de BPMN-BPSec no tiene una interpretación, es algo que se controla a través del Back End. Las posibles relaciones se refieren generalmente a "corrupción intencional" y no "una corrupción accidental" que es lo que se busca en el requisito de integridad incluido en BPMN-BPSec.
No repudio	[No]	En el Front End el requisito de No Repudio no tendría una interpretación, ya que las medidas para cumplir este requisito se implementan en el Back End, sin ninguna repercusión en el Front End
Privacidad	[Si]	Representación a través de la administración de la visualización de los datos o funciones (que se pueden aplicar sobre los datos) en relación con el tipo de usuario o roles y la propiedad de los datos. El uso de los roles de usuario en conjunto con el Login de control de acceso permite identificar al usuario para que en base a esta identidad pueda visualizar ciertos datos y funciones que son responsabilidad de él. Por lo anterior se puede concluir que en el Front End la Privacidad tiene una estrecha relación con el Control de Acceso.

Tabla 24: Requisitos BPSec VS Representatividad en el Front End

Como se puede apreciar, solo el control de acceso y la privacidad pueden tener una representación en el Front End, el resto solo tiene una representación a nivel de Back End o una leve representatividad en el Front End, la cual debido su simpleza, el establecimiento de un patrón no es necesario.

5.3.2 Requisitos de seguridad BPMN en el Front End modelados con IFML

En esta subsección se relacionan los requisitos que se pueden representar y/o relacionar con el Front End (los cuales han sido obtenidos en la subsección anterior - control de acceso y

privacidad) con los patrones de Front End seleccionados en la Tabla 22 (patrones de Front End modelados con IFML).

Control de Acceso: De los patrones seleccionados en la Tabla 22 de la sección 5.1, existen varios que tienen una relación con este requisito. Todos estos patrones son similares, pero existen dos que son más generales y cubren lo modelado en el resto de ellos. Estos dos patrones son denominados como: *IA-SPLOG: Login a un viewcontainer específico* (identificado como el número 12 en la Tabla 22) y *IA-RBP: permiso basado en los roles para los elementos de la vista* (identificado como el número 14 en la Tabla 22), los cuales se muestran en las Figura 21 y Figura 22, respectivamente.

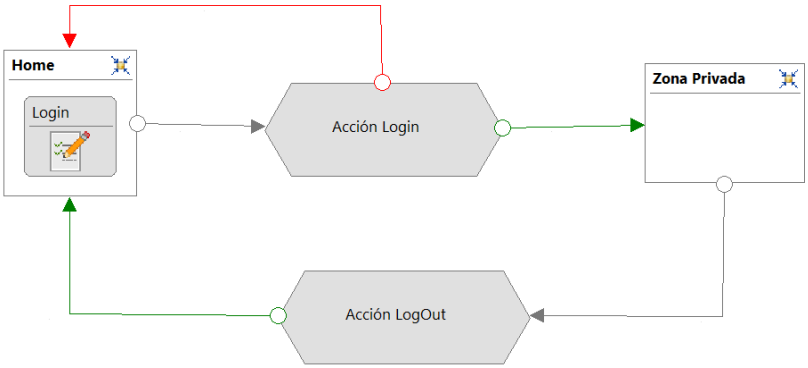


Figura 21: IA-SPLOG: Login a un viewcontainer específico

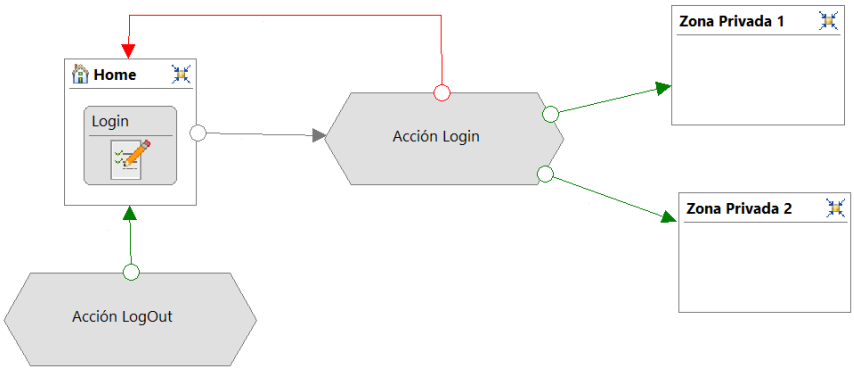


Figura 22: IA-RBP: permiso basado en los roles para los elementos de la vista

La finalidad del control de acceso a través de un Login es mostrar o realizar una cierta parte de la interacción con el usuario a la cual no se puede tener acceso sin poseer la autorización necesaria. Debido a lo anterior, cada vez que se tenga un Login exitoso, como se muestra en las Figura 21 y Figura 22, el flujo de navegación redirigirá a una página (ViewContainer) distinta de la que representa al Login.

Si se quiere reducir el control de acceso a un solo patrón para una mayor simplicidad, entonces se puede decir que el patrón *IA-SPLOG: Login a un viewcontainer* es el mismo patrón *IA-RBP: permiso basado en los roles para los elementos de la vista*, solo que para un solo rol de usuario y, por lo tanto, solo se necesita este último patrón en todos los casos.

Se debe tener en cuenta que, según la definición del requisito de control de acceso, solo los patrones relacionados a la acción de Login son parte del control de acceso, mientras que el Logout (cierre de sesión - eliminación o término de la autorización que brinda el control de acceso) no es parte del control de acceso en sí, pero es mencionado ya que, siempre que existe un Login, debe existir un Logout.

Privacidad: Aunque en la Tabla 22 de la Sección 5.1 los patrones identificados como 13 y 17 se relacionan con la privacidad, para aplicar estos patrones es necesario saber la información específica donde se aplica la privacidad, lo cual no existe en la notación BPMN-BPSec.

La privacidad en el Front End va de la mano del Login y el uso de roles. Es necesario tener conocimiento de la identidad del usuario y su autorización para mantener la privacidad. Por esta razón, se debe establecer hasta dónde se encuentra el control de acceso y dónde comienza la privacidad en un patrón de Login basado en roles. En la Figura 23 se muestra un esquema en el que se usa la definición del requisito control de acceso la que indica la realización de 3 acciones: la identificación, la autentificación y la autorización. Se establece que la identificación se lleva a cabo en el ViewContainer donde se deben introducir las credenciales, mientras que las acciones de autentificación y autorización se realizan en la acción de Login, por lo tanto, la privacidad comienza cuando se realiza la bifurcación del flujo de navegación desde la Acción Login en base a la autorización. Los datos que presenta un modelo BPMN-BPSec con una especificación de privacidad, solo permiten una correspondencia cuando está acompañado con una especificación de control de acceso.

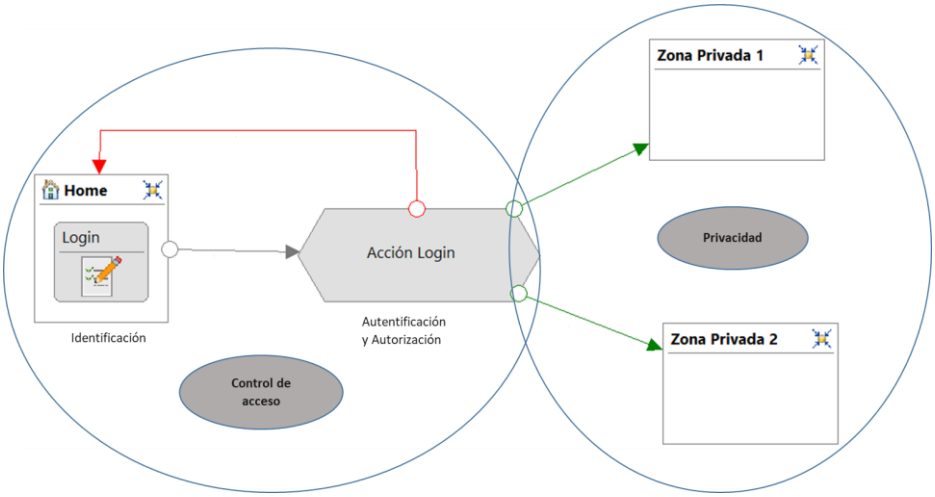


Figura 23: Esquema de identificación del Control de acceso y la Privacidad

5.4 Correspondencia de BPMN-BPSec a IFML

En resumen, de lo presentado en las secciones anteriores, se observa que solo los requisitos de Control de Acceso, a través del patrón de Login, y la Privacidad, a través de la gestión de la visualización de los datos o funciones, tienen una representatividad o relación con el Front End. Por otro lado, los elementos de BPMN y su representatividad en IFML solo se puede observar que el contenido del Objecto de Dato, el Mensaje y la Anotación pueden ser representados como un

ViewComponent, mientras que otros elementos solo tienen una representatividad en casos específicos y muy acotados, por lo que no es posible realizar una correspondencia. Esto no ocurre con los requisitos de seguridad que abarca BPMN-BPSec puesto que éstos son muy específicos, por lo que es posible determinar cuáles tienen una representación en el Front End. Los elementos de BPMN no son iguales ya que no son muy específicos y casi todo depende del contenido de los elementos en el modelo (qué están abstrayendo). Teniendo en cuenta solo los elementos de BPMN relacionados con BPMN-BPSec, el DataObject sería el único con una relación.
El objetivo de esta Sección consiste en establecer la correspondencia entre BPMN-BPSec e IFML a través de la combinación de los resultados de las Secciones 5.2 y 5.3. Debido a que de los elementos de BPMN relacionados a los requisitos de seguridad modelados con BPMN-BPSec solo el elemento Data Object tiene una correspondencia con IFML, para realizar las correspondencias para los otros elementos (Activity, Group, Lane, MessageFlow y Pool) y para dar un contexto a los requisitos de seguridad, se asumirá que su representación siempre comienza con un ViewContainer.
Esta transformación solo tiene el objetivo de realizar la correspondencia de BPMN-BPSec hacia IFML con respecto a los requisitos de seguridad modelados, el resto del modelo necesita la intervención de un modelador.
El alcance de la investigación, definido en base a los objetivos planteados para esta Tesis, no consideraba la realización de una correspondencia automática desde BPMN-BPSec hacia IFML. Debido a esto, no fue necesario definir reglas ATL para esta correspondencia.
A continuación, se muestra la primera regla de transformación de BPMN-BPSec hacia IFML, el resto se encuentra detallada en el Anexo B.

5.4.1 Regla 1.- Actividad con Control de Acceso:

En el caso de una actividad con Control de Acceso, este requisito debe ser implementado antes de realizar la actividad. De los patrones de seguridad que tienen relación con el Control de Acceso, el más adecuado para esta correspondencia es el patrón *IA-SPLOG: Login a un viewContainer específico*. En la Figura 24 se muestra este caso en BPMN-BPSec y en la Figura 25 se muestra su representación en IFML. Se debe tener en cuenta que, en algunos patrones (Como el que se muestra en la Figura 25), se ha integrado el LogOut, que es otro patrón que posee una relación indirecta con el control de acceso, pues representa el término de la autorización que brinda el Login.

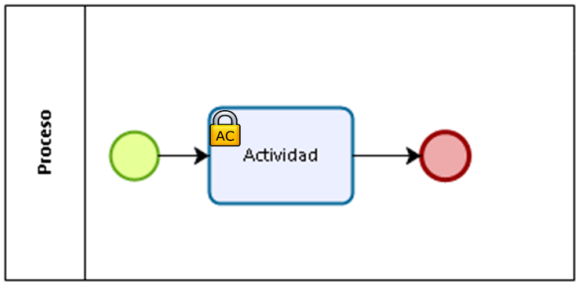


Figura 24: Caso 1 de actividad en BPMN-BPSec

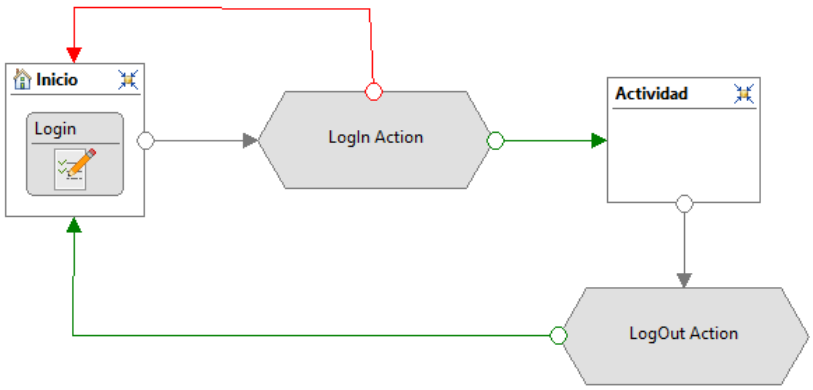


Figura 25: Correspondencia caso 1 de actividad en IFML

Como se aprecia en la Figura 25, se realiza el Login para cumplir con el requisito Control de Acceso especificado en el modelo BPMN-BPSec. Luego el flujo de navegación se dirige al primer elemento que es parte de la actividad, donde se inicia el flujo o representación de la actividad como tal. Dicha representación, con un ViewContainer para la actividad, puede ser un conjunto de viewContainer, flows, events, actions y/o viewComponent que siguen el flujo después de la acción de Login.
Un ejemplo de esta regla se muestra en la Figura 26 en BPMN-BPSec, mientras que en la Figura 27 se muestra la correspondencia en IFML.

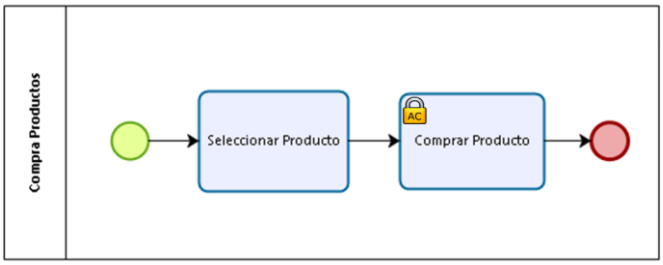


Figura 26: Ejemplo caso 1 de actividad en BPMN-BPSec

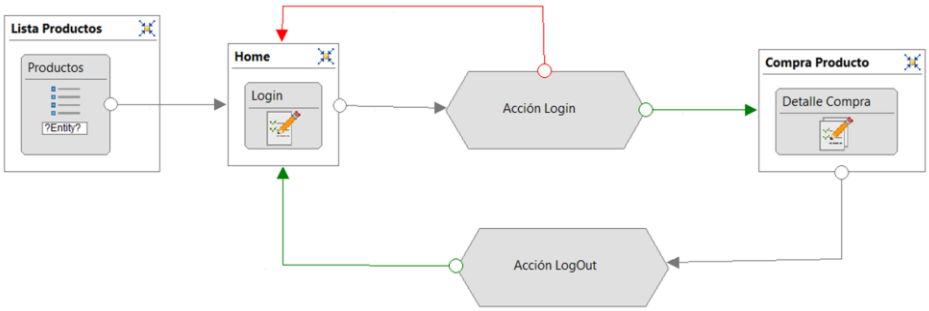


Figura 27: Ejemplo de una actividad con control de acceso en IFML

Para este ejemplo se realizan dos Actividades. La primera no necesita Control de Acceso a través de un Login, pero la segunda actividad lo necesita. Después de realizar el Login el flujo de navegación se divide en un caso donde la acción de Login es correcta y un caso donde ocurre una excepción y el Login es incorrecto, en el primer caso el flujo dirige a la actividad de "Comprar Producto" que se encuentra compuesta por un viewContainer. En el caso de que la acción de Login sea incorrecta, el flujo se dirige a la vista inicial del Login (viewContainer con el Form de Login). El LogOut dirige el flujo a donde el modelador lo defina, puede ser a la actividad anterior a la actividad con Control de Acceso, puede ser a la actividad siguiente sin Control de Acceso o a la vista inicial del Login. La acción de Login no implica la acción de LogOut al finalizar la actividad con Control de Acceso, eso es decidido por el modelador.

5.5 Conclusiones

IFML tiene elementos que permiten modelar un Front End con bastante detalle. Al transformar un modelo de proceso de negocio descrito con BPMN hacia IFML de forma automática se necesita una mayor información que la que provee el modelo descriptivo de BPMN, por ejemplo, una actividad de BPMN al representarla en IFML se necesita información del contenido de la actividad, visualmente una actividad que tiene relación con la eliminación de contenido no es igual a una actividad que tiene relación con la agregación de contenido.

Se debe tener en cuenta que, para algunos de los requisitos de seguridad involucrados en BPSec, sí es posible realizar una correspondencia hacia IFML porque estos requisitos son lo suficientemente específicos.

La finalidad del objetivo abordado en este capítulo es proveer una correspondencia con los requisitos de seguridad incluidos en la propuesta BPMN-BPSec y no establecer una correspondencia completa del modelo entre BPMN e IFML. Una correspondencia más completa del modelo podría necesitar una correspondencia incluyendo la capa de aplicación de ArchiMate.

En base al análisis realizado, se puede concluir que todos los requisitos de seguridad involucrados en BPMN-BPSec tienen una relación con el Back End, mientras que solo algunos de ellos tienen una relación con el Front End.

Capítulo 6: Prototipo de Herramienta

La transformación de modelos consiste en un conjunto de reglas que son aplicadas sobre uno o más modelos de origen y permiten obtener uno o más modelos de destino. Hay diversas propuestas para especificar, implementar y ejecutar transformaciones de modelos. Algunos ejemplos de lenguajes de propósito general para transformación de modelos, son el estándar QVT y otros como ATL y RubyTL (Giandini *et al.*, 2010).

En este Capítulo se presenta un prototipo de herramienta denominado EAS2BPSec-Tool (Enterprise Architecture Secure to BPSec) que tiene como objetivo demostrar que, mediante el uso de las reglas de transformación propuestas en el Capítulo 4 de esta Tesis, es posible realizar la correspondencia de un modelo de la capa de negocio de una Arquitectura Empresarial, modelado con ArchiMate e integrando requisitos de seguridad, hacia un modelo de proceso de negocio seguro, modelado con BPMN-BPSec, sin la interacción de un modelador en la transformación.

Debido a que, en base a lo mencionado en el Capítulo 4, se ha logrado realizar una correspondencia completa, modelo a modelo, entre ArchiMate y BPMN-BPSec, EAS2BPSec-Tool se ha centrado en la transformación entre estos modelos. Sin embargo, debido a que, como se indica en el Capítulo 5, no se logró realizar una correspondencia modelo a modelo, sino que solo una entre algunos elementos de BPMN-BPSec y algunos patrones de seguridad de IFML, la transformación entre estos modelos no ha sido considerada como parte del prototipo de herramienta.

Este Capítulo se encuentra organizado de la siguiente forma: en la Sección 6.1 se presentan las características generales del prototipo de herramienta, en la Sección 6.2 se muestran los principales aspectos gráficos del prototipo y, finalmente, en la Sección 6.3 se presenta un ejemplo de su uso en la transformación de un modelo.

6.1 Características generales del prototipo de herramienta

Para la construcción de EAS2BPSec-Tool se trabajó en el entorno de desarrollo Eclipse, con los lenguajes Java (Oracle, 2018) y ATL (Eclipse, 2018a) y se desarrolló como una aplicación de escritorio en un archivo JAR (Java Archive). Java se usa para la construcción general de la herramienta y ATL para las reglas de transformación de modelos entre ArchiMate y BPMN-BPSec. Tanto el modelo de entrada (ArchiMate) como el modelo de salida generado por el prototipo de herramienta (BPMN-BPSec) están definidos en formato XML.

La sintaxis abstracta de ATL es especificada mediante un metamodelo usando el estándar Meta-Object Facility (MOF), y provee de lenguajes en modo textual y gráfico para representar las reglas de transformación del lenguaje. ATL es un proyecto con constantes actualizaciones, foros, ejemplos, reportes de bugs, etc., y es muy usado. La semántica de la ejecución de las reglas es, resumidamente, la siguiente: dada una parte reconocida del modelo de origen, mediante los patrones de origen, son creadas sus correspondientes partes en el modelo de destino (Lopez *et al.*, 2009).

ATL aplica un patrón de transformación de modelos que se muestra en la Figura 28. Con *MMa* se refiere al metamodelo del lenguaje de modelado de origen, *MMb* se refiere al metamodelo del lenguaje de modelado de destino, *Ma* se refiere al modelo de origen basado en el metamodelo *MMa*, *Mb* se refiere al modelo de destino basado en el metamodelo *MMb* y *mma2mmb.atl* se

refiere a las reglas de transformación ATL que permiten transformar el modelo de origen (*Ma*) en el modelo de destino (*Mb*) basándose en los metamodelos de ambos (*MMa* y *MMb*).

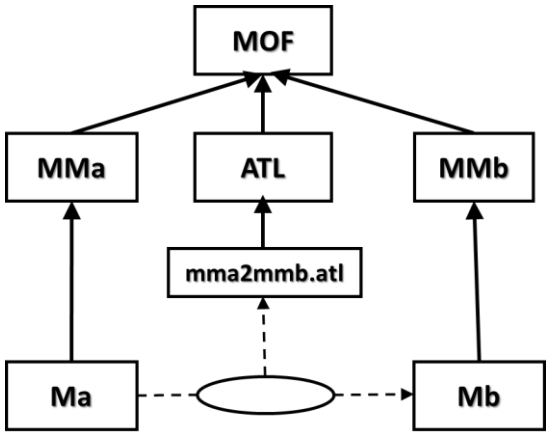


Figura 28: Esquema enfoque de ATL (Lopez *et al.*, 2009)

Entonces, para realizar las reglas de transformación con ATL se debió definir los correspondientes modelos y metamodelos utilizados por el prototipo de herramienta:

- *MMa* corresponde al metamodelo de ArchiMate (*MM ArchiMate*).
- *MMb* corresponde al metamodelo de BPMN-BPSec (*MM BPSec*).
- *Ma* corresponde a un modelo ArchiMate (*M ArchiMate*) basado en el metamodelo *MMa*.
- *Mb* corresponde a un modelo BPMN-BPSec (*M BPSec*) basado en el metamodelo *MMb*.

De este modo, EAS2BPSec-Tool toma como entrada un modelo de ArchiMate y, por medio de su transformación utilizando reglas ATL, genera un modelo de salida de BPMN-BPSec, todo esto tomando de base los metamodelos de ambos estándares, lo cual queda ilustrado en la Figura 29. A continuación, se describe en mayor detalle cada uno de estos elementos.

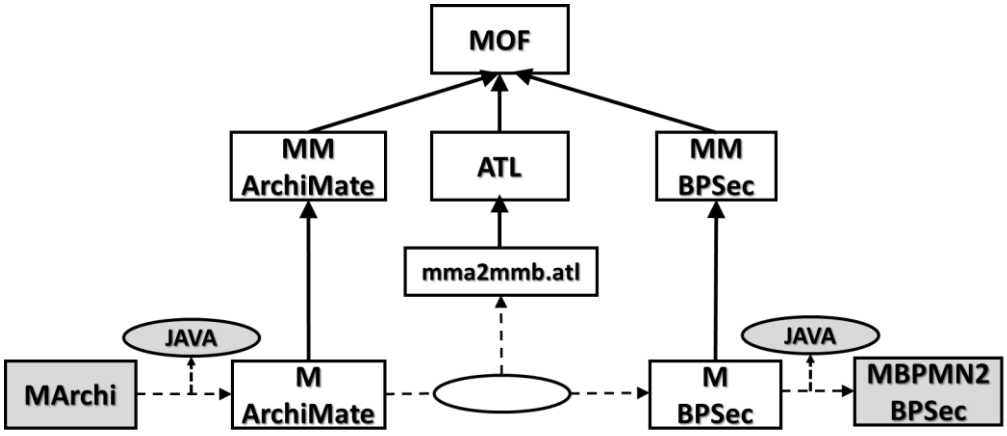


Figura 29: Ámbito de la herramienta EAS2BPSec-Tool

MM ArchiMate corresponde al metamodelo de ArchiMate. The Open Group ha especificado este metamodelo por partes, no en uno solo que exponga los elementos, relaciones y conectores de

relaciones, además de las restricciones de éstos. Específicamente, para las reglas de transformación planteadas en esta Tesis (ver detalle en Anexo A), no se necesita un metamodelo muy completo, puesto que no se está poniendo énfasis en las restricciones más complejas del lenguaje. Teniendo en cuenta esto, se ha construido un metamodelo del lenguaje basado en la especificación de éste, el cual se muestra en la Figura 30.

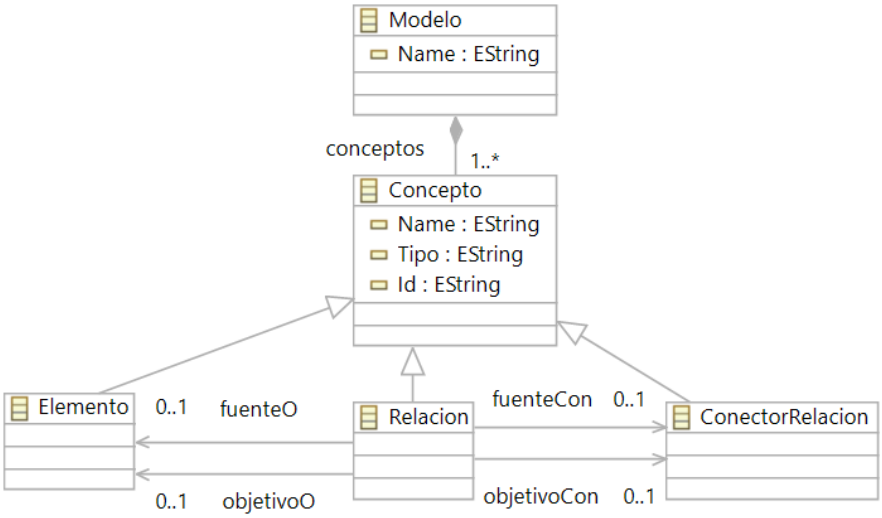


Figura 30: Metamodelo Básico de ArchiMate (*MM ArchiMate*)

MM BPSec corresponde al metamodelo de BPMN-BPSec, el cual es provisto por Rodríguez *et al.* (2007). Un resumen de este metamodelo ha sido mostrado anteriormente, mediante la Tabla 17 en la Sección 4.2.1. *M ArchiMate* corresponde a un modelo ArchiMate, el cual puede ser generado por medio de la herramienta Archi ArchiMate Modelling (MArchi) usando el lenguaje Java (Archi, 2018). Este modelo se encuentra en formato XML. *M BPSec* corresponde al modelo BPMN-BPSec que se genera a través de reglas ATL, el cual puede ser transformado utilizando el lenguaje Java en un modelo visualizable a través de la herramienta BPMN2 Modeler (Eclipse, 2018b), la cual posee un plug-in que implementa la extensión BPMN-BPSec (MBPMN2 BPSec). Al igual que el modelo de entrada, este modelo es generado en formato XML.
Respecto a las reglas ATL definidas para realizar la transformación, éstas se encuentran detalladas en el Anexo A.

6.2 Principales aspectos gráficos del prototipo

Se presentan las pantallas principales del prototipo de herramienta, junto a una breve descripción de cada una de las funciones presentadas en éstas.
La pantalla inicial de EAS2BPSec-Tool se muestra en la Figura 31, donde la opción de "ABRIR RUTA ARCHIVO" permite ingresar la ruta de ubicación del archivo del modelo ArchiMate modelado usando la herramienta Archi.

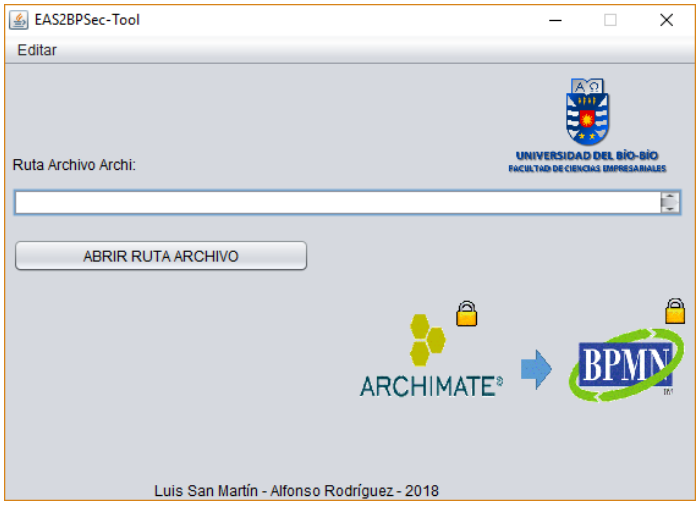


Figura 31: Prototipo de Herramienta - selección de ruta de acceso

Luego, recibiendo la ruta del Archivo Archi, el prototipo de herramienta ofrece la posibilidad de abrir el modelo en la herramienta Archi y transformar el modelo hacia BPMN-BPSec (ver Figura 32).

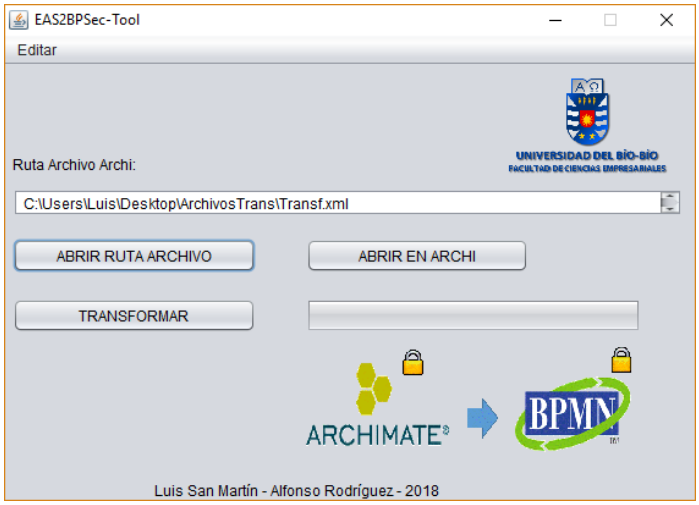


Figura 32: Prototipo de Herramienta - transformación

Finalmente, una vez usada la opción de transformar el modelo, como se muestra en la Figura 33, el prototipo de herramienta permite visualizar el modelo en la herramienta BPMN2 Modeler con el Plug-in de BPMN-BSec. El archivo generado con el modelo de proceso de negocio seguro usando BPMN-BPSec se encuentra en la misma ruta que el archivo original, pero con la extensión .bpmn.

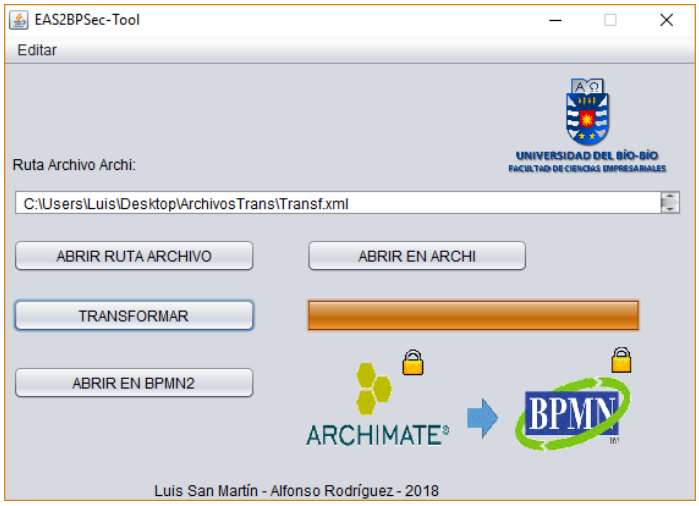


Figura 33: Prototipo de Herramienta - visualizar modelo transformado

El prototipo de herramienta utiliza la ruta que generalmente tienen estas herramientas, pero también brinda la opción para cambiar dicha ruta como se muestra en la Figura 34.

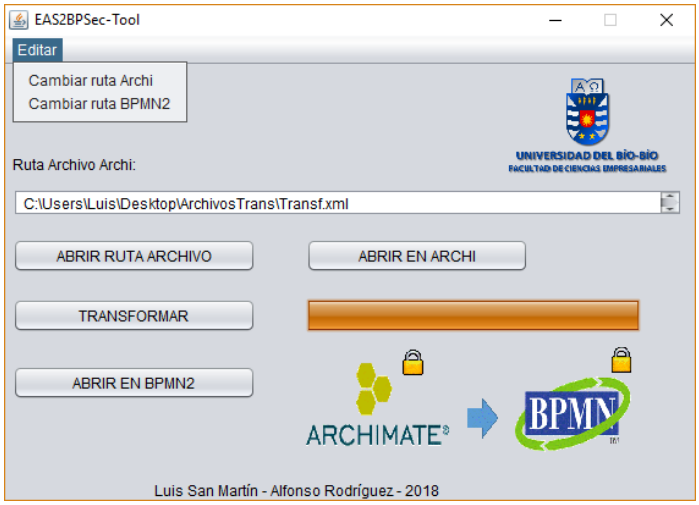


Figura 34: Prototipo de Herramienta - ruta herramientas Archi y BPMN2

6.3 Ejemplo de uso del prototipo de herramienta

En esta Sección se muestra un ejemplo de uso del prototipo de herramienta, usando como modelo de entrada un modelo que ha sido obtenido de un "Reporte de evaluación de arquitectura empresarial de la Universidad de Coventry" (Czechowski *et al.*, 2011), presentado en la Figura 35, y se ha enriquecido con algunos requisitos de seguridad que pueden ser implementados en dicha arquitectura. Dicha arquitectura empresarial corresponde solo a la parte de la biblioteca de la Universidad de Coventry.

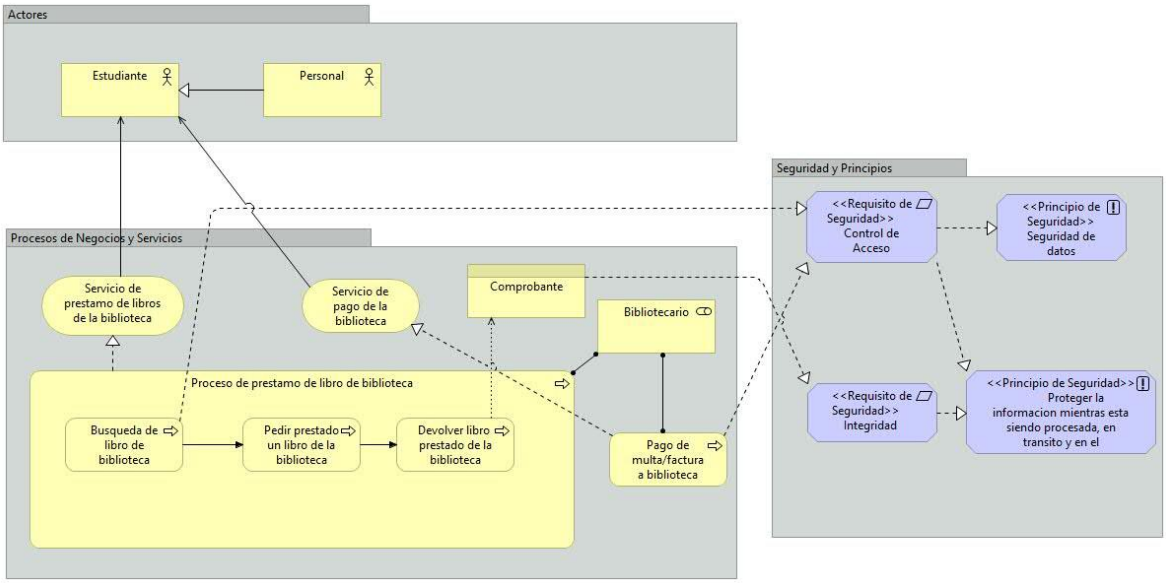


Figura 35: Ejemplo EA de la Universidad de Coventry modelado en la herramienta Archi

Como primer paso, se debe generar este modelo, utilizando la herramienta Archi ArchiMate Modelling, de la cual se obtiene un archivo que será utilizado como la entrada de EAS2BPSec-Tool. Este archivo debe ser seleccionado utilizando la opción "ABRIR RUTA ARCHIVO" del prototipo de herramienta, como se observa en la Figura 31. Una vez que se ha indicado la ruta del modelo de entrada, este puede ser abierto en la herramienta Archi ArchiMate Modelling desde EAS2BPSec-Tool, seleccionado la opción "ABRIR EN ARCHI".

El segundo paso es realizar la transformación de este modelo hacia un modelo BPMN-BPSec. Para ello, se selecciona la opción "TRANSFORMAR", como se observa en la Figura 32. Una barra de progreso indica el avance de la transformación.

Una vez que esta transformación se ha completado, se despliega un mensaje indicándolo, y se da la opción "ABRIR EN BPMN2", que permite abrir el modelo BPMN-BPSec generado, utilizando la herramienta BPMN2 Modeler, como se observa en la Figura 33. La transformación es realizada utilizando reglas de transformación ATL. El modelo BPMN-BPSec resultante para este caso se muestra en la Figura 36.

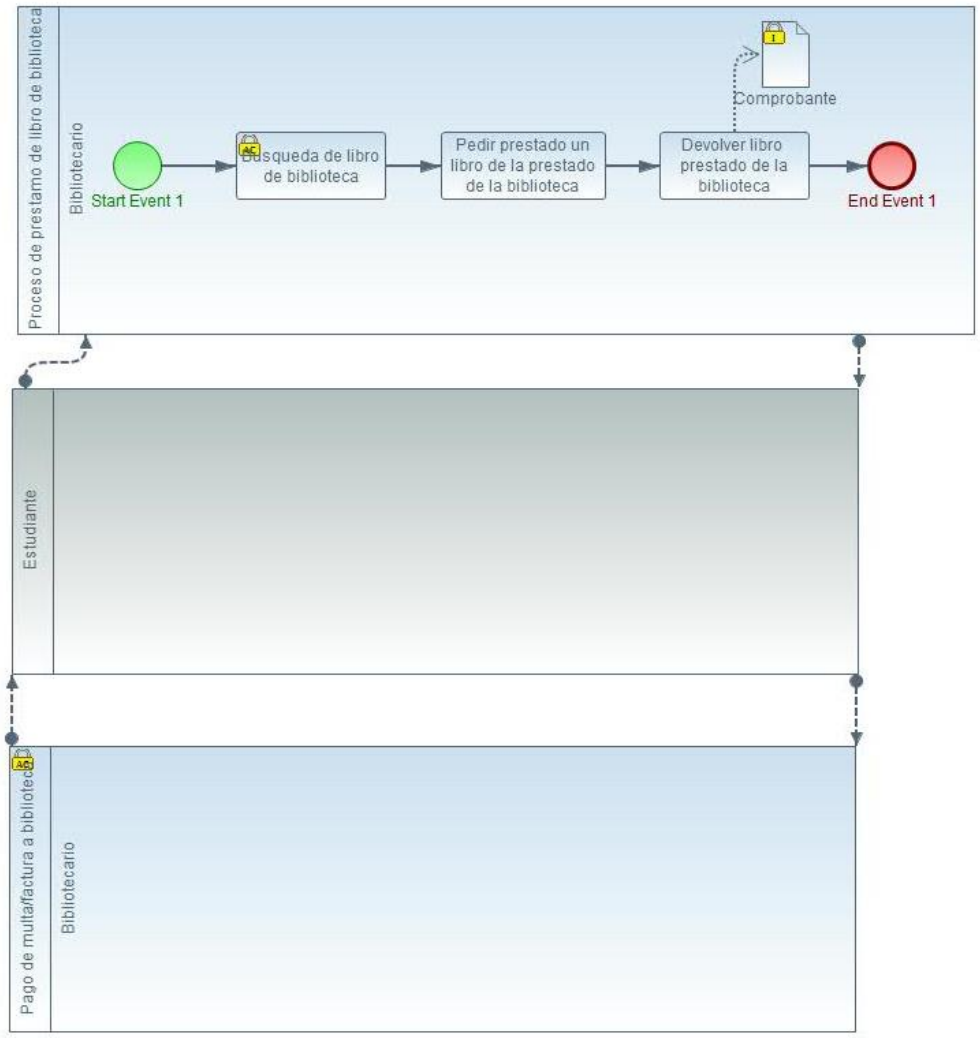


Figura 36: Modelo correspondencia a través de reglas ATL

Se ha confirmado que de acuerdo con las reglas de transformación planteadas en el Capítulo 4: Correspondencia de ArchiMate a BPMN-BPSec, el modelo BPMN-BPSec mostrado en la Figura 36 es la correspondencia del modelo ArchiMate mostrado en la Figura 35. Esto demuestra que el prototipo de herramienta funciona correctamente.

Desde el punto de vista de la interpretación de la realidad modelada en la Arquitectura Empresarial, se debe tener en cuenta que el modelo generado en BPMN-BPSec representa lo mismo, solo que el tipo de modelo y el lenguaje usado para modelarlo es distinto.

Capítulo 7: Experimentación y Análisis de Resultados

Un experimento se define como una prueba o ensayo en la que es posible manipular deliberadamente una o más variables independientes para observar los cambios que ocurren en la variable dependiente en una situación o contexto estrictamente controlado por el experimento. Adicionalmente, un experimento debe poder ser replicado o reproducido por otros y producir los mismos resultados (Baray, 2006).

Existen dos tipos de experimentos, los "Controlados" en los que los tratamientos se asignan a los sujetos de manera aleatoria; y los denominados "Cuasi Experimentos", en los que esta aleatorización no es posible (Genero *et al.*, 2014).

Para llevar a cabo un experimento, es necesario seguir un Proceso Experimental, en el que se detallan las actividades a realizar, qué debe hacerse y cuáles son las entradas y las salidas de cada actividad. En Genero *et al.* (2014), se presenta el proceso experimental como un proceso que consta de 5 actividades: Definición del alcance, Planificación, Operación, Análisis e interpretación y Presentación y difusión.

Para validar las reglas de transformación modelo a modelo de la capa de negocio de ArchiMate a BPMN-BPSec propuestas en esta Tesis, además de las correspondencias que han podido ser identificadas entre elementos de BPMN-BPSec y patrones de seguridad de IFML, se diseñó, aplicó y analizó un "Cuasi Experimento" debido a que el tratamiento de los sujetos no es asignado de forma aleatoria, pues deben poseer cierto conocimiento sobre el tema. Aun así, éste sigue siendo un experimento que requiere las 5 actividades definidas por Genero *et al.* (2014) para su realización.

Este Capítulo se encuentra estructurado de la siguiente forma: en la Sección 7.1 se presentan las actividades para la realización del Cuasi Experimento y en la Sección 7.2 se presentan las Conclusiones de éste.

7.1 Actividades del proceso experimental

Las actividades del Proceso Experimental presentadas en Genero *et al.* (2014) se describen a continuación:

Definición del alcance: En esta actividad se deben definir los objetivos del experimento.

Planificación: Se realiza para tener una noción clara de cómo se va a llevar a cabo el experimento. La planificación se divide en otras 7 sub-actividades:

- **Selección de contexto:** Este determina el entorno en que se desarrolla el experimento.
- **Formulación de la hipótesis:** Una teoría provisional o una suposición que se cree que explica el comportamiento que se pretende explorar.
- **Selección de variables:** Se deben elegir las variables que se van a manipular (variables independientes) y las que se medirán (variables dependientes) en el experimento.
- **Selección de sujetos:** Se deben seleccionar aquellas personas a los que se aplican los tratamientos del experimento.
- **Elección del diseño:** Se elige un buen diseño que permite la realización de réplicas correctas.
- **Instrumentación:** Se dota de los medios para realizar el experimento y para su seguimiento sin afectar el control del experimento.
- **Evaluación de la validez:** Consiste en establecer cómo validar los resultados encontrados.

Operación: Consiste en la recolección de los datos que se han de analizar posteriormente. Durante esta actividad se llevan a cabo 3 tareas:

Preparación: Consiste en la preparación de las personas que serán parte del experimento como sujetos.

Ejecución: Consiste en la realización del experimento.

Validación de los datos: Se comprueba que los datos recogidos son razonables y se han recogido correctamente.

Análisis e interpretación: Se toman los datos recogidos y se analizan e interpretan correctamente.

Presentación y difusión: Se presentan los hallazgos del experimento.

En las siguientes subsecciones se detalla cada una de estas etapas para llevar a cabo el Cuasi Experimento desarrollado en esta Tesis.

7.1.1 Definición del alcance

El objetivo de este cuasi experimento consistió en analizar las correspondencias de modelos realizadas por expertos, con el propósito de comparar éstas con las correspondencias propuestas en esta Tesis (reglas de transformación) y así demostrar la validez de lo propuesto.

7.1.2 Planificación

Para tener una noción clara de la realización del cuasi experimento desarrollado, se definieron cada una de las 7 tareas que forman la planificación:

Selección del contexto: El cuasi experimento se realizó en un entorno académico con estudiantes y profesores de la Universidad del Bío-Bío.

Formulación de la hipótesis: Este cuasi experimento solo cuenta con una hipótesis que consiste en que las reglas de transformación propuestas en esta Tesis coinciden con aquellas que propondrían expertos en el tema.

Selección de variables: En este cuasi experimento, primeramente, la variable independiente corresponde al modelo o los elementos del modelo de la capa de negocio de ArchiMate que se transformarán, y la variable dependiente corresponde al modelo o los elementos del modelo de proceso de negocio seguro con BPMN-BPSec al cual son transformados los elementos o el modelo de la capa de negocio de ArchiMate. En una segunda instancia la variable independiente corresponde al modelo o los elementos del modelo de proceso de negocio seguro modelado con BPMN-BPSec que se transformarán, y la variable dependiente corresponde a los patrones de interfaz de usuario modelados con IFML, al cual se transformarán los elementos del modelo o modelos BPMN-BPSec.

Selección de sujetos: Los sujetos que participaron del cuasi experimento debían contar con cierto nivel de conocimiento para que sean los indicados para la recopilación de información. Para que un sujeto fuera indicado para participar en el cuasi experimento debió: (i) Poseer conocimientos de ArchiMate, (ii) Poseer conocimientos de BPMN, (iii) Poseer conocimientos de BPMN-BPSec, y (iv) Poseer conocimiento sobre diseño de interfaz de usuario o modelado de interfaz de usuario con IFML. El conocimiento sobre BPMN-BPSec pudo ser ignorado si se explicaba al sujeto como funciona BPMN-BPSec.

Elección del diseño: El diseño de este cuasi experimento consistió en un diseño único, es decir se aplica el mismo tratamiento a todos los sujetos ya que no existe la disponibilidad de muchos sujetos a los cuales aplicar el cuasi experimento.

Instrumentación: Este cuasi experimento se realizó por medio de un instrumento de medición donde los sujetos debían realizar tareas manualmente usando lápiz y papel.

Este instrumento de medición (ver en Anexo C) se construyó en base a 3 tareas: (i) una Sección de selección múltiple, (ii) una Sección de construcción de modelos y (iii) una Sección de preguntas de opinión personal. Las dos primeras corresponden a la transformación de ArchiMate a BPMN-BPSec y la última a la transformación de BPMN-BPSec a IFML.

(i) La sección de selección múltiple consistió en preguntas de alternativas donde se presenta un escenario (una cierta configuración u orden de los elementos en el modelo) que se puede encontrar en un modelo ArchiMate, en el cual se debe aplicar una o más reglas de transformación, y diferentes alternativas de posibles correspondencias a BPMN-BPSec, donde una de ellas coincide con la propuesta. Antes de la creación del instrumento, se realizó un sondeo, midiendo posibles respuestas para seleccionar posibles alternativas. Esta Sección tiene como objetivo la validación de las reglas de transformación entre elementos.

(ii) La sección de construcción de modelos consistió en la presentación de dos modelos ArchiMate, uno sin contexto y otro con un contexto, y se pidió al sujeto que, según su opinión, creara un modelo que sea correspondiente usando BPMN-BPSec. En el modelo sin contexto no se modela un problema específico, y tiene como objetivo que el sujeto no proponga una correspondencia basada en su conocimiento con respecto al problema u otros problemas similares. Esta sección tiene como objetivo la validación de las reglas de transformación aplicadas en un modelo, comparando el modelo generado por los sujetos con respecto al modelo donde se aplican las reglas propuestas.

(iii) Finalmente, la sección de preguntas de opinión personal consistió en la presentación de una posible correspondencia entre BPMN-BPSec e IFML o afirmaciones sobre esta transformación de modelos con la finalidad de pedir su opinión con respecto a si está en acuerdo o en desacuerdo con respecto a las correspondencias propuestas y afirmaciones realizadas.

El instrumento de medición realizado y usado en el cuasi experimento se encuentra en el Anexo C.

Además, posterior al análisis de los resultados de la aplicación del instrumento, se planeó y se realizó una discusión con los expertos donde los sujetos discuten sobre los resultados del instrumento de medición y proponen mejoras para las reglas de transformación.

Evaluación de validez: La validación de las reglas en el instrumento de medición se basó en los siguientes criterios divididos por la sección del instrumento:

- **Análisis de resultados selección múltiple:** Las preguntas de selección múltiples se basaron en que solo una alternativa coincide con las reglas planteadas. No fue necesario establecer varios criterios de evaluación de estas preguntas. El único criterio que fue suficiente es el porcentaje de respuestas correctas para una pregunta. Es muy difícil que las respuestas de todos los sujetos coincidan con las reglas de transformación propuestas, por lo que se debió establecer un porcentaje de aceptación.

- **Comparar modelos:** En la comparación de modelos existen muchas posibles respuestas, por ello se establecieron una mayor cantidad de criterios de evaluación.
    - **La misma realidad**: Compara el modelo ArchiMate con el modelo BPMN-BPSec generado. Los elementos deben modelar la misma abstracción en ambos modelos. Ambos modelos modelan la misma realidad o contexto, aunque se pierda información.
    - **Relación de los elementos** (elemento de origen->elemento correspondiente): Los elementos transformados guardan una relación semántica.
    - **Relación entre los elementos** (relación elementos de origen->relación elementos correspondientes): Como se relacionan los elementos en el modelo de origen debe ser correspondiente con cómo se relacionan los elementos en el modelo de destino. Mantenimiento de las relaciones.
    - **Información agregada:** Información que se agrega a la abstracción en base al conocimiento propio o ideas de la realidad que se está representando en el modelo.
- **Preguntas de opinión personal:** Las preguntas de opinión personal se basaron en el acuerdo o desacuerdo con respecto a la afirmación o correspondencia propuesta. Se estableció un porcentaje por el cual se considera que la afirmación o correspondencia ha sido aceptada por parte de los sujetos.

El tiempo usado al responder el instrumento en la sección de selección múltiple consideró un tiempo promedio de 10 min. Para la sección de construcción de modelos se consideró un promedio de 10 min. nuevamente. Finalmente, la sección de preguntas de opinión consideró un tiempo promedio de 4 min. Entonces, el total de tiempo necesario para responder el instrumento fue de aproximadamente 24 min.

Los resultados se basaron en la evaluación de los criterios de validación. En la sección de selección múltiple, el porcentaje aceptable de respuestas que coinciden con lo propuesto por pregunta es de un porcentaje mayor al 55%, considerando que no exista otra alternativa con un porcentaje mayor al 30%. La sección de construcción de modelos se basó en una evaluación del cumplimiento de los criterios del 0 al 100%, donde 0% se consideró muy malo y 100% muy bueno, considerando un 60% como aceptable. En la sección de preguntas de opinión, el porcentaje aceptable de respuesta de acuerdo con la afirmación o correspondencia correspondió a un 60%.

7.1.3 Operación

Preparación: Al seleccionar sujetos con ciertos conocimientos no fue necesario una preparación. El instrumento de medición indicó las instrucciones de forma detallada.

Ejecución: Al momento de la aplicación del instrumento se contó con 7 sujetos que coincidían con las características establecidas en la planificación. Para la ejecución, considerando la extensión del experimento, se entregó individualmente el instrumento a los sujetos y se les pidió su entrega en un tiempo considerable.

Validación de los datos: Se verificó que no se encontraran inconsistencias en las respuestas de los sujetos y que no existan respuestas similares que indiquen la interacción entre los sujetos al realizar el cuasi experimento.

7.1.4 Análisis e interpretación

El resumen de los resultados de la Sección de selección múltiple del instrumento de medición se encuentra en la Tabla 25 donde la columna *Pregunta* corresponde al número de la pregunta incluyendo el número de la página donde se encuentra ésta, la columna de *Resultado* corresponde al porcentaje que obtuvo la respuesta correcta (desde el punto de vista de las propuestas) en la pregunta considerando todos los sujetos, el *Porcentaje de aceptación* corresponde al porcentaje de aceptación de la regla que se aplica en la pregunta y la columna de *Comentario* corresponde a un comentario con respecto al resultado de la pregunta. El *Resultado* se calcula directamente a través de la cantidad de respuestas que son correctas con respecto al total de respuestas. El *Porcentaje de aceptación* se calcula con respecto a la aparición de la regla en las preguntas. Por ejemplo para la pregunta 1, la regla se repite y es aceptado en las preguntas 2, 4, 5, 6, 7, 8, 9, 10, 11 y 12, es decir se acepta la regla en 10 de 11 preguntas lo cual corresponde a un 90,9%, eso sumado al porcentaje de aceptación de la pregunta con respecto al total (el porcentaje de la pregunta sería un 9,09% del total y 3 de los 7 sujetos están de acuerdo lo cual sería un 3,9%) da como resultado un 94,81%. No todas las reglas se repiten dentro de otras reglas.

En general las reglas son aceptadas, con excepción de las preguntas 3, 4, 5 y 6, pues en estas existe conflicto, por lo que fue necesario discutirlas con los expertos.

Pregunta	Resultado	Porcentaje Aceptación	Comentario
1 (Anexo C; Pág. 135)	42.86%	94,81%	Resultado ajustable ya que en las respuestas de las preguntas 2, 4, 5, 6, 7, 8, 9, 10, 11 y 12 se usa la regla correcta en base a la propuesta. (en la 3 no se aplicaba la regla)
2 (Anexo C; Pág. 136)	28,57%	89,80%	Resultado reajustable ya que en las respuestas de las preguntas 6, 8, 9, 10, 11,12 se usa la regla correcta en base a la propuesta
3 (Anexo C; Pág. 136)	0%	0%	Es posible que los business function y business interaction no tengan dicha correspondencia
4 (Anexo C; Pág. 137)	0%	0%	No existe una respuesta aceptable, existe la necesidad de discutir una regla de transformación aceptable.
5 (Anexo C; Pág. 138)	28,57%	28,57%	No existe una respuesta aceptable, existe la necesidad de discutir una regla de transformación aceptable.
6 (Anexo C; Pág. 139)	0%	0%	No existe una respuesta aceptable, existe la necesidad de discutir una regla de transformación aceptable.
7 (Anexo C; Pág. 140)	100%	100%	Completamente aceptable
8 (Anexo C; Pág. 141)	100%	100%	Completamente aceptable
9 (Anexo C; Pág. 142)	100%	100%	Completamente aceptable
10 (Anexo C; Pág. 143)	100%	100%	Completamente aceptable
11 (Anexo C; Pág. 144)	57,14%	57,14%	Aceptable, considerando que según la semántica de los elementos es correspondiente y el porcentaje es mayor que un 55%
12 (Anexo C; Pág. 145)	100%	100%	Completamente aceptable

Tabla 25: Resumen resultados sección de selección múltiple

La sección de construcción de modelos del instrumento se evaluó en base a los criterios establecidos para la evaluación de la validez, de lo cual se obtuvo la Tabla 26 que muestra los porcentajes de aceptación para cada uno de los criterios de evaluación establecidos previamente. En la Tabla 26 la columna "ID Modelo Instrumento" se presenta de la forma "X.Y", donde "X" corresponde al número del instrumento de medición o id del sujeto e "Y" corresponde al modelo que puede ser 1 para el modelo sin contexto (en Pág. 146) y 2 para el modelo con contexto (en Pág. 147), y la columna "Criterios" corresponde a los porcentajes de aceptación para cada modelo en el instrumento. Un "-" significa que el sujeto no realizó el modelo.

	Criterios			
ID Modelo Instrumento	**La misma realidad**	**Relación de los elementos**	**Relación entre los elementos**	**Información agregada**
1.1	90%	100%	95%	100%
1.2	100%	100%	90%	100%
2.1	100%	75%	90%	100%
2.2	100%	95%	90%	100%
3.1	5%	5%	0%	100%
3.2	60%	60%	70%	30%
4.1	60%	50%	10%	100%
4.2	-	-	-	-
5.1	60%	55%	10%	60%
5.2	80%	90%	50%	60%
6.1	95%	75%	90%	100%
6.2	95%	75%	85%	90%
7.1	95%	75%	45%	90%
7.2	100%	95%	75%	100%

Tabla 26: Porcentajes criterios de aceptación de modelos

En general los criterios son aceptables. No existe una respuesta que coincida 100% con la propuesta, pero las reglas son aceptadas en general aunque no exista una respuesta exactamente igual, ya que sí son idénticas en la mayoría de sus partes. Si se debe nombrar un detalle perjudicial, ese seria que los participantes y los servicios de negocio no corresponden con la propuesta, pero estos son solo una parte pequeña de toda la propuesta y el primero es aceptado en la sección de selección múltiple, mientras que el segundo se discute con los expertos.

El resumen de la Sección de preguntas de opinión se presenta en la Tabla 27, donde la columna de *Pregunta* corresponde al número de la pregunta incluyendo el número de la página donde se encuentra ésta y el *Porcentaje de aceptación* corresponde al porcentaje de respuestas de acuerdo a la propuesta por cada pregunta.

Pregunta	Porcentaje Aceptación
1 (Anexo C; Pág. 148)	100%
2 (Anexo C; Pág. 149)	100%
3 (Anexo C; Pág. 150)	71,43%
4 (Anexo C; Pág. 151)	71,43%
5 (Anexo C; Pág. 152)	85,71%

Tabla 27: Resumen resultados sección de preguntas de opinión

La discusión del instrumento se centró en las reglas no aceptadas, dado que la mayoría de los criterios fueron respaldados por las respuestas solo se analizó aquellas reglas que tuvieron menos coincidencia, de lo cual se obtuvo lo siguiente:

- Las Business Function y Business Interaction no tienen la misma correspondencia que un Business Process, además no se logró un acuerdo sobre una posible correspondencia por lo cual no se establecen reglas de correspondencia para estos dos elementos.
- El uso de un servicio de negocio para interactuar con el comportamiento significa que existe una comunicación en ambos sentidos, por lo cual el flujo de mensaje en la regla debe ir en ambos sentidos. La Figura 37 se muestra el cambio.

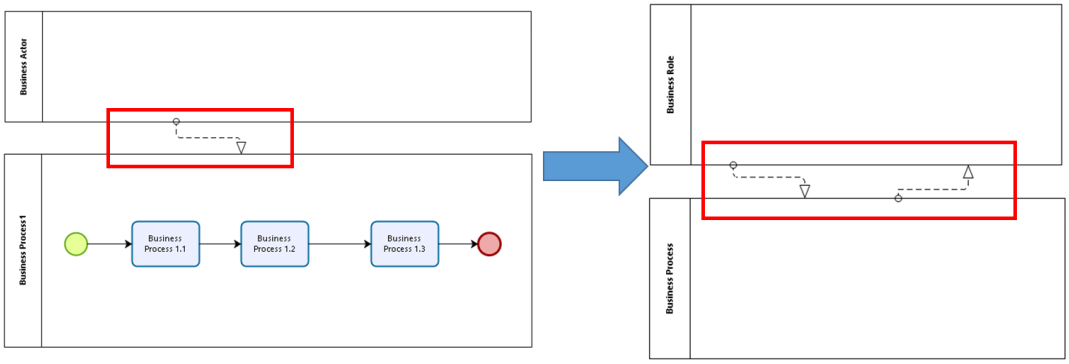


Figura 37: Cambio en regla del servicio de negocio

- El escenario de un proceso de negocio sirviendo a un elemento de estructura activa en la capa de negocio se debería de realizar a través de un servicio por lo cual se cambió lo estipulado el escenario de las preguntas 5 y 6 de la sección de selección múltiple del instrumento. Por lo cual el escenario y las reglas de la Figura 38 cambiaron a lo mostrado en la Figura 39.

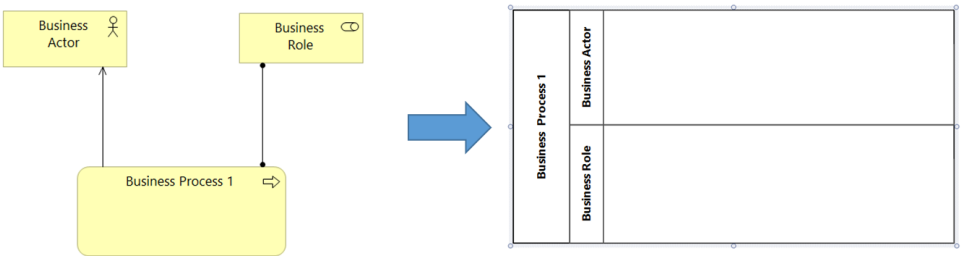


Figura 38: Escenario antiguo

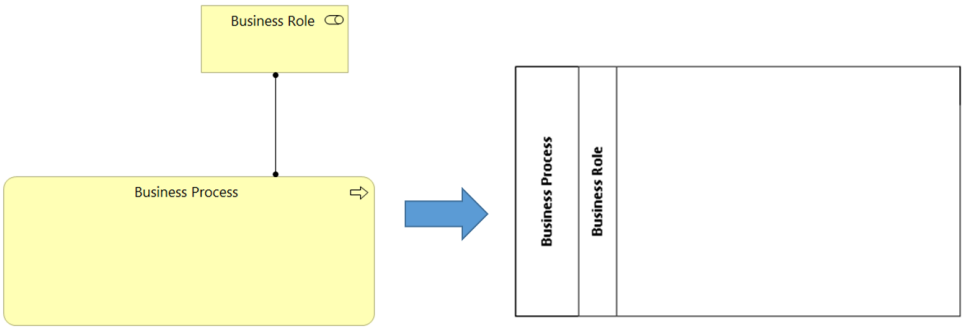


Figura 39: Nuevo escenario

Las modificaciones que resultaron de la discusión con los expertos fueron aplicadas a la propuesta, por lo cual lo mostrado en esta Tesis corresponde a lo aceptado por los expertos.

7.1.5 Presentación y difusión

La presentación y difusión de los resultados de este experimento se realiza a través del presente informe de Tesis.

7.2 Conclusiones

Considerando los resultados de la experimentación se concluye que las reglas de transformación propuestas en esta Tesis son válidas, ya que el grupo de expertos con los que se trabajó aceptan las reglas propuestas, en un 80% para las reglas de ArchiMate a BPMN-BPSec y un 75% para las reglas de BPMN-BPSec a IFML.

No existe una aceptación completa de las reglas por parte de cada experto, pero sí existe en forma general considerando las respuestas y opinión del grupo.

El uso de un instrumento de medición y posterior discusión de los resultados de ésta, ha facilitado la comprensión de la problemática a tratar por parte de los expertos y la discusión se realizó de forma fluida.

Las opiniones de los expertos son relevantes para la retroalimentación de la propuesta. Sin ella, la propuesta solo sería manejada y aceptada por los autores de esta Tesis, los cuales pueden tener un razonamiento errado o sesgado.

Finalmente, se debe tener en cuenta que el pequeño número de expertos participantes en el experimento limita un poco la generalización de los resultados, pero esto es un problema que siempre existirá a causa de los pocos expertos disponibles con el conocimiento necesario.

Capítulo 8: Conclusiones

8.1 Análisis de los objetivos propuestos/cumplidos

Esta investigación buscó establecer una correspondencia entre los requisitos de seguridad modelados a nivel de arquitectura empresarial, procesos de negocio e interfaz de usuario con los lenguajes de modelado ArchiMate, BPMN-BPSec e IFML, como una forma de mantener alineados los objetivos de seguridad entre el negocio y las TI de la organización. El poseer una correspondencia entre estos modelos permite mantener los mismos objetivos de seguridad entre ellos, ya que estos objetivos pasan de un modelo a otro en la correspondencia y se deberían mantener hasta la implementación. Además, la correspondencia misma permite la trazabilidad de los objetivos de seguridad.
Para cumplir con el objetivo de esta Tesis, se buscó cumplir con un conjunto de objetivos específicos, para los cuales a continuación se presenta un análisis de su cumplimiento.

Objetivos 1 y 2: *Revisar la literatura para buscar especificaciones de seguridad en los estándares ArchiMate e IFML. Revisar la literatura para buscar mapeos o transformaciones entre ArchiMate-BPMN y BPMN-IFML (con y sin elementos de seguridad).*

Se realizó una revisión sistemática de la literatura para conocer las especificaciones de seguridad en los estándares ArchiMate e IFML, además de los mapeos o transformaciones entre ArchiMate y BPMN y entre BPMN e IFML, con y sin elementos de seguridad existentes en la literatura.
Se encontraron 12 artículos relacionados a las especificaciones de seguridad en el estándar ArchiMate y 4 artículos que presentan algunos detalles importantes para poder establecer formalmente la forma de especificar la seguridad en IFML. En cuanto a las transformaciones, se encontraron 5 artículos relacionados a la transformación de ArchiMate hacia BPMN, pero ningún artículo con respecto a la transformación de BPMN hacia IFML, por lo que se buscaron transformaciones hacia IFML desde cualquier otro lenguaje de modelado como una forma de encontrar ideas para realizar la correspondencia. De este modo, se encontraron 3 artículos relacionados a ello.
En general, se encontró información concreta que permite establecer cómo modelar las especificaciones de seguridad en ArchiMate, e información sobre la correspondencia semántica entre los elementos de ArchiMate y BPMN, pero dejando de lado las relaciones. En IFML no se encontraron muchos detalles relevantes, solo indicios para establecer cómo especificar la seguridad y ningún trabajo sobre transformaciones de BPMN hacia IFML.

Objetivo 3: *Establecer una correspondencia entre los elementos de ArchiMate y los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec.*

Se logró establecer cómo modelar los requisitos de seguridad en ArchiMate, respaldado por la literatura, y se estableció una correspondencia entre la capa de negocio de ArchiMate, con requisitos de seguridad, y BPMN-BPSec, considerando las relaciones entre los elementos de ArchiMate, lo cual no había sido considerado en la literatura.
Se establecieron reglas de transformación que permiten realizar la correspondencia de forma automática y sin la intervención de un modelador.

Objetivo 4: *Establecer una correspondencia entre los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec y los elementos de IFML.*

Se lograron establecer correspondencias entre los requisitos de seguridad incluidos en BPMN-BPSec hacia IFML usando patrones, pero, por falta de información desde la literatura (una base), esta correspondencia no fue muy extensa. Aun así, este objetivo se cumplió, ya que se estableció la correspondencia desde los elementos que modelan los requisitos de seguridad, expresados en BPMN-BPSec, hacia IFML, a través de patrones existentes en la literatura. Se debe resaltar que el objetivo no consideraba una correspondencia completa del modelo, solo de los requisitos de seguridad.

Objetivo 5: *Validar la pertinencia de los resultados del punto anterior mediante un grupo de expertos.*

Se realizó un cuasi experimento que logró validar las propuestas de transformación. El cuasi experimento contó con la participación de expertos en el tema, a los cuales se les aplicó un instrumento de medición y, posteriormente, se discutieron los resultados del análisis del instrumento y se realimentó la propuesta.

8.2 Principal aporte

El principal aporte de esta Tesis corresponde a las reglas de transformación que permiten obtener un modelo de proceso de negocio seguro, modelado con BPMN-BPSec, a partir de la capa de negocio de un modelo de Arquitectura Empresarial, modelado con ArchiMate. Además, se realizaron las correspondencias desde los requisitos de seguridad de BPMN-BPSec hacia un modelo de interfaz de usuario, modelado con IFML. Este conjunto completo de transformaciones, desde ArchiMate a BPMN-BPSec y desde este último hacia IFML, permiten demostrar que es posible mantener los objetivos de seguridad del negocio en las tecnologías de información, permitiendo una trazabilidad de dichos objetivos. Las transformaciones propuestas en esta Tesis son la base para identificar la trazabilidad de los objetivos de seguridad.
Además, en esta Tesis se construyó un prototipo de herramienta que permite, usando las reglas de transformación de ArchiMate a BPMN-BSec propuestas en esta Tesis, transformar la capa de negocio de un modelo ArchiMate en un modelo BPMN-BPSec, sin la interacción de un modelador.

8.3 Trabajos futuros

Existen varios trabajos que se pueden realizar en el futuro dentro del contexto de esta Tesis, siendo los más destacados:

- Ampliar las reglas de transformación de ArchiMate hacia BPMN-BPSec y proponer nuevas transformaciones de ArchiMate hacia otros modelos, como, por ejemplo, los modelos de actividad o modelos de base de datos de UML. Esto considerando que la Arquitectura Empresarial es la base de la empresa y puede relacionarse a la mayoría de los modelos usados por las empresas.

- Crear una correspondencia más completa desde BPMN hacia IFML a través de la asociación de verbos con patrones, aprovechando el hecho de que una actividad siempre se compone de un verbo y un sustantivo.

8.4 Contraste de resultados

Se participó en el VI Encuentro de Investigaciones de Estudiantes de Postgrado, realizado por la Universidad del Bío-Bío durante el año 2017, donde se presentaron los resultados de la revisión sistemática de la literatura sobre la seguridad en ArchiMate y las correspondencias de ArchiMate a BPMN. Además, se presentaron las propuestas de correspondencia de la capa de negocio de ArchiMate hacia BPMN-BPSec establecidas durante esta Tesis.

Se redactó un artículo sobre la revisión sistemática de la literatura relacionada a la seguridad que se puede modelar en ArchiMate, el cual fue enviado y se encuentra en revisión por parte de la revista Journal of Universal Computer Science (J.UCS).

Se redactó otro artículo relacionado a la transformación de la capa de negocio del modelo de Arquitectura Empresarial modelado con ArchiMate hacia un modelo de proceso de negocio seguro modelado con BPMN-BPSec.

Referencias

Ahmed, N., & Matulevičius, R. (2014). Securing business processes using security risk-oriented patterns. Computer Standards & Interfaces, 36, 723-733.

Archi. (2018). Archi ArchiMate Modelling In. https://www.archimatetool.com/.

Band, I., Engelsman, W., Feltus, C., Paredes, S. G., Hietala, J., Jonkers, H., & Massart, S. (2015). Modeling Enterprise Risk Management and Security with the ArchiMate® Language. The Open Group.

Baray, H. L. Á. (2006). Introducción a la metodología de la investigación: Juan Carlos Martínez Coll.

Blanckaert, J. (2015). Integrating the Interaction Flow Modelling Language (IFML) into the Web Semantics Design Method (WSDM).

Blangenois, J., Guemkam, G., Feltus, C., & Khadraoui, D. (2013). Organizational Security Architecture for Critical Infrastructure. In Availability, Reliability and Security (ARES), 2013 Eighth International Conference on (pp. 316-323): IEEE.

Blommendaal, C. (2015). Information Security Risks for Car Manufacturers based on the in-Vehicle Network.

Brambilla, M., & Fraternali, P. (2013). Human computation for organizations: socializing business process management. In Handbook of Human Computation (pp. 255-264): Springer.

Brambilla, M., & Fraternali, P. (2014). Interaction Flow Modeling Language: Model-Driven UI Engineering of Web and Mobile Apps with IFML: Morgan Kaufmann.

Brucker, A. D. (2013). Integrating security aspects into business process models. it–Information Technology it–Information Technology, 55, 239-246.

Bunge, M. (1979). A World of Systems. 1979. Treatise on Basic Philosophy, 1979. In: Reidel Publishing, Dordrecht, Holland.

Coles-Kemp, L., Bullée, J., Montoya, L., Junger, M., Heath, C., Pieters, W., & Wolos, L. (2015). Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security. In (pp. 22-26).

Curto, J. R. P. (2013). BPM (Business Process Management): Cómo alcanzar la agilidad y eficiencia operacional a través de BPM y la empresa orientada a procesos: BPMteca. com.

Czechowski, N., Padam, S., Anderson, I., & Woodcock, C. (2011). Enterprise Architecture Evaluation Report

Coventry University.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43, 125-128.

Dubois, E., & Mauger, C. (2015). Extended Architectural Models: First Steps Towards the Reconciliation of the'Soft'and the'Hard'Parts of an Enterprise. In 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop (pp. 125-129): IEEE.

Eclipse. (2018a). ATL Transformation Language. In. https://www.eclipse.org/atl/.

Eclipse. (2018b). BPMN2 Modeler. In. https://www.eclipse.org/bpmn2-modeler/.

Escobar, J., Losavio, F., & Ortega, D. (2013). Standard quality model to Enterprise Architecture support tools. In CLEI (pp. 1-12).

Feltus, C., Fontaine, F.-X., & Grandry, E. (2015). Towards Systemic Risk Management in the Frame of Business Service Ecosystem. In International Conference on Advanced Information Systems Engineering (pp. 27-39): Springer.

Feltus, C., Ouedraogo, M., & Khadraoui, D. (2014). Towards cyber-security protection of critical infrastructures by generating security policy for SCADA systems. In Information and Communication Technologies for Disaster Management (ICT-DM), 2014 1st International Conference on (pp. 1-8): IEEE.

Firesmith, D. G. (2003). Common concepts underlying safety security and survivability engineering. In: DTIC Document.

Gaaloul, K., Guerreiro, S., & Proper, H. A. (2014). Modeling access control transactions in enterprise architecture. In 2014 IEEE 16th Conference on Business Informatics (Vol. 1, pp. 127-134): IEEE.

Gaaloul, K., & Proper, H. A. (2013). An access control model for organisational management in enterprise architecture. In Semantics, Knowledge and Grids (SKG), 2013 Ninth International Conference on (pp. 37-43): IEEE.

Gaaloul, K., Yangui, S., Tata, S., & Proper, H. A. (2014). Architecting Access Control for Business Processes in the Cloud. In Proceedings of the 2014 International Workshop on Advanced Information Systems for Enterprises (pp. 8-14): IEEE Computer Society.

Genero, M., Cruz-Lemus, J., & Piattini, M. (2014). Métodos de investigación en ingeniería del software. Editorial RA-MA: Madrid, Spain, 171-199.

Giandini, R., Pérez, G., & Pons, C. (2010). Un lenguaje de Transformación específico para Modelos de Proceso del Negocio. In XXXVI Conferencia Latinoamericana de Informática (CLEI 2010) (Vol. 18).

Gill, A. Q. (2015). Agile enterprise architecture modelling: Evaluating the applicability and integration of six modelling standards. Information and Software Technology, 67, 196-206.

Gill, A. Q., & Qureshi, M. A. (2015). Adaptive enterprise architecture modelling. Journal of Software, 10, 628-638.

Grandry, E., Feltus, C., & Dubois, E. (2013a). Conceptual integration of enterprise architecture management and security risk management. In Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2013 17th IEEE International (pp. 114-123): IEEE.

Grandry, E., Feltus, C., & Dubois, E. (2013b). Conceptual integration of enterprise architecture management and security risk management. In 2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops (pp. 114-123): IEEE.

Harmon, P., & Wolf, C. (2008). The state of business process management. Business Process Trends.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? Computers & Security, 21, 402-409.

Ingle, D., & Meshram, B. (2012). Analyzing Web Modeling Existing Languages and Approaches to Model Web Application Design. International Journal of Advanced Research in Computer Engineering & Technology, 1, 196-204.

Jacho, N., Martínez, S. S., Borrero, L. L., & Rodríguez, R. M. (2015). Análisis de la Transformación de Modelo CIM a PIM en el Marco de Desarrollo de la Arquitectura Dirigida por Modelos (MDA). Revista Politécnica, 36.

Kirikova, M., Matulevičius, R., & Sandkuhl, K. (2016). The Enterprise Model Frame for Supporting Security Requirement Elicitation from Business Processes. In International Baltic Conference on Databases and Information Systems (pp. 229-241): Springer.

Kirikova, M., Penicina, L., & Gaidukovs, A. (2015). Ontology based linkage between enterprise architecture, processes, and time. In East European Conference on Advances in Databases and Information Systems (pp. 382-391): Springer.

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33, 1-26.

Korman, M., Sommestad, T., Hallberg, J., Bengtsson, J., & Ekstedt, M. (2014). Overview of Enterprise Information Needs in Information Security Risk Assessment. In Enterprise Distributed Object Computing Conference (EDOC), 2014 IEEE 18th International (pp. 42-51): IEEE.

Lopez, H., Veresi, F., Viñolo, M., Calegari, D., & Luna, C. (2009). Estado del arte de lenguajes y herramientas de transformación de modelos. Reportes Técnicos 09-19.

Maier, M. W., Emery, D., & Hilliard, R. (2004). ANSI/IEEE 1471 and systems engineering. Systems Engineering, 7, 257-270.

Marquez, G., Rodriguez, A., & Fernandez Medina, E. (2014). Obtaining secure BPEL from Secure Business Process specified with BPMN. Latin America Transactions, IEEE (Revista IEEE America Latina), 12, 315-320.

Menzel, M., Thomas, I., & Meinel, C. (2009). Security requirements specification in service-oriented business process management. In Availability, Reliability and Security, 2009. ARES'09. International Conference on (pp. 41-48): IEEE.

OMG. (2002). Meta Object Facility(MOF) Specification.

OMG. (2011). Business Process Model and Notation Specification. Version 2.0.

OMG. (2015a). Interaction Flow Modeling Language Specification. Version 1.0.

OMG. (2015b). UML Specification. Version 2.5.

OMG. (2017). Model Driven Architecture. In (Vol.).

Oracle. (2018). Java Developer Center. In. http://www.oracle.com/technetwork/es/java/index.html.

Ozier, W. (1997). Generally accepted system security principles(GASSP). COMPUT SECUR J, 13, 69-75.

Paja, E., Giorgini, P., Paul, S., & Meland, P. H. (2011). Security requirements engineering for secure business processes. In Workshops on Business Informatics Research (pp. 77-89): Springer.

Penicina, L. (2013). Linking BPMN, ArchiMate, and BWW: Perfect match for complete and lawful business process models? In PoEM (Short Papers) (pp. 156-165).

Pino, F., García, F., & Piattini, M. (2006). Revisión sistemática de mejora de procesos software en micro, pequeñas y medianas empresas. Revista Española de Innovación, Calidad e Ingeniería del Software, 2, 6-23.

Pizarro Zea, C. N. (2015). Desarrollo de una aplicación web para pruebas psicológicas de respuesta típica con WebRatio.

Rodríguez, A., de Guzmán, I. G.-R., Fernández-Medina, E., & Piattini, M. (2010). Semi-formal transformation of secure business processes into analysis class and use case models: An MDA approach. Information and Software Technology, 52, 945-971.

Rodríguez, A., Fernández-Medina, E., & Piattini, M. (2007). A BPMN extension for the modeling of security requirements in business processes. IEICE transactions on information and systems, 90, 745-752.

Rodríguez, A., Fernández-Medina, E., Trujillo, J., & Piattini, M. (2011). Secure business process model specification through a UML 2.0 activity diagram profile. Decision Support Systems, 51, 446-465.

Saleem, M., Jaafar, J., & Hassan, M. (2012). A domain-specific language for modelling security objectives in a business process models of soa applications. AISS, 4, 353-362.

Stoneburner, G., Hayden, C., & Feringa, A. (2004). NIST Special Publication 800-27 Rev A. A: engineering principles for information technology security (a baseline for achieving security). National Institute of Standards and Technology, Gaithersburg.

The Open Group. (2011). TOGAF specification. Version 9.1.

The Open Group. (2013). ArchiMate Specification. Version 2.1.

The Open Group. (2016). ArchiMate Specification (Vol. Version 3.0).

Tipton, H. F., & Krause, M. (2003). Information security management handbook: CRC Press.

Wand, Y., & Weber, R. (1993). On the ontological expressiveness of information systems analysis and design grammars. Information Systems Journal, 3, 217-237.

Wazlawick, R. S. (2014). Object-oriented analysis and design for information systems: Modeling with UML, OCL, and IFML: Elsevier.

Weske, M. (2008). Business Process Management: Concepts, Languages, Architectures. Springer, Pag. 3-67.

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security: Cengage Learning.

Wood, C. C. (1990). Principles of secure information systems design. Computers & Security, 9, 13-24.

Wright, J., & Dietrich, J. (2008). Survey of existing languages to model interactive web applications. In Proceedings of the fifth Asia-Pacific conference on Conceptual Modelling-Volume 79 (pp. 113-123): Australian Computer Society, Inc.

Anexos

Anexo A. Reglas de Transformación de Modelos de ArchiMate a BPMN-BPSec

A continuación se presentan las reglas de transformación de modelos que se han propuesto en esta Tesis.
Nota: Las reglas ATL presentadas son solo un abstracto y sin las funciones o helper.

Escenario 1.- Un proceso de negocio de ArchiMate como Pool o Actividad en BPMN: Un *<proceso de negocio>* en ArchiMate pueden tener relación de *<composición>* o *<agregación>* con este mismo elemento.

Las relaciones de *<composición>* y *<agregación>* se identifica visualmente de dos formas: en la Figura 40 se muestran las relaciones de *<composición>* o *<agregación>*, mientras que en la Figura 41 las relaciones se identifican por el hecho que visualmente los elementos están contenidos dentro de otro. En los siguientes escenarios estas relaciones pueden no ser resaltadas.

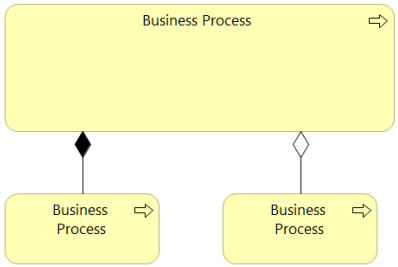


Figura 40: Uso de relación de composición y agregación Alternativa 1

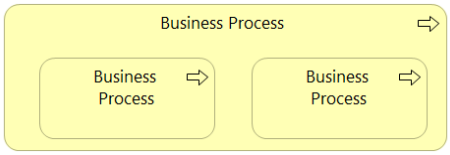


Figura 41: Uso de relación de composición y agregación Alternativa 2

Regla 1.- Cuando un *<proceso de negocio>* de ArchiMate no se encuentra siendo parte de otro *<proceso de negocio>* (se refiere a tener una relación de *<composición>* o *<agregación>*), entonces el <proceso *de negocio*> tienen una correspondencia con un *<Pool>* en BPMN. El requisito de seguridad realizado por el elemento en ArchiMate es también especificado en el elemento correspondiente en BPMN.

N° de Regla: 1

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>	*<Pool>*

Regla en ATL:

```
rule BusinessPToPool {
        from
                a : ARC!Elemento (a.isBusinessP(a.Tipo) and
                        a.BusinessPIsPool(a.Id))
        to
                b : BPS!Pool (
                        Name <- a.Name,
                        --Requisitos de Seguridad--
                        RequisitoAC <- a.requisitoControlAc(a),
                        RequisitoAD <- a.requisitoDetecAtacAm(a),
                        RequisitoP <- a.requisitoPrivacidad(a)
                )
    }
```

Gráficamente:

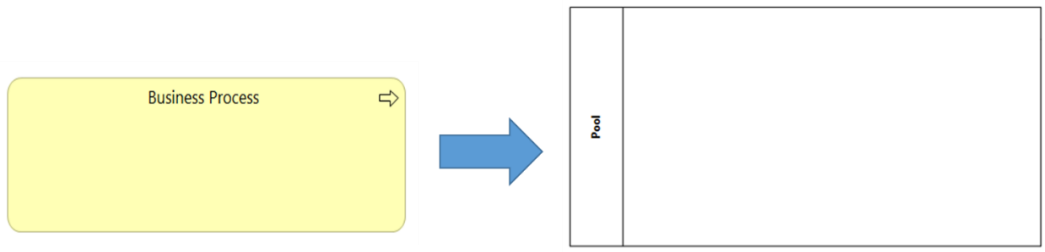


Figura 42: Business Process simple a un Pool

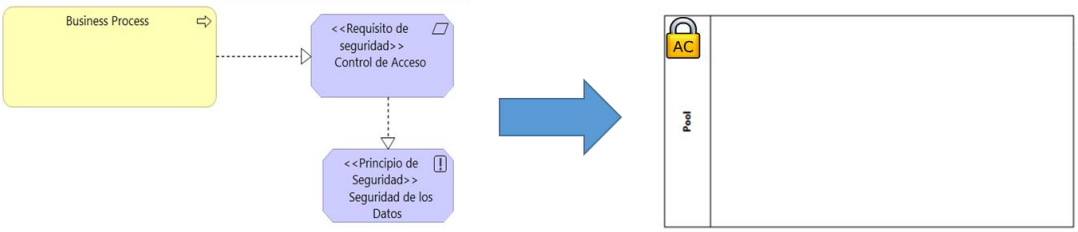


Figura 43: Business Process simple a un Pool (Con Control de Acceso)

Regla 2.- Cuando un *<proceso de negocio>* de ArchiMate es parte de otro *<proceso de negocio>* a través de las relaciones de *<composición>* o *<agregación>*, entonces tiene una correspondencia con una *<actividad>*. Tal vez una de estas actividades es un sub-proceso pero este es una extensión de una actividad así que siendo una actividad está correcto. El requisito de seguridad realizado por el elemento en ArchiMate es también especificado en el elemento correspondiente en BPMN.

N° de Regla: 2

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Agregación relationship>, <Composición relationship>, <Triggering relationship>	*<Actividad>, <Pool>, <Linea de secuencia>, <Asociación>*

Regla en ATL:

```
rule BusinessPToActividad {
        from
                a : ARC!Elemento (a.isBusinessP(a.Tipo) and not a.businessPIsPool(a.Id))
        to
                b : BPS!Activity (
                        Name <- a.Name,
                        PoolO <- a.buscaElementoPool(a.Id),
                        LaneO <- a.laneDeActividad(a.buscarLanes(a.buscaElementoPool(a.Id))),
                        --Requisitos de Seguridad--
                        RequisitoAC <- a.requisitoControlAc(a)

                )
    }
```

Gráficamente:

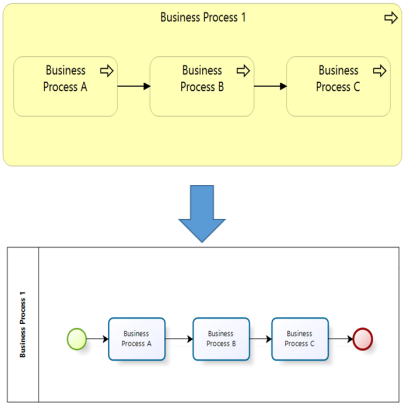


Figura 44: Proceso de negocio que contiene otros procesos

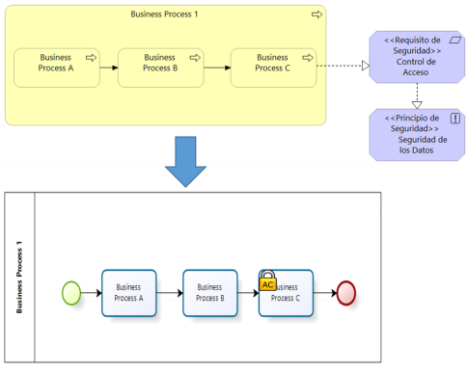


Figura 45: Proceso de negocio que contiene otros procesos (Con Control de Acceso)

Regla 3.- Cuando se aplica la Regla 2, si existen relaciones de *<Triggering>* (relación dinámica, que describe dependencias temporales) en ArchiMate, entonces las *<líneas de secuencia>* en las *<actividades>* correspondientes en BPMN van en el mismo sentido que como se modelan las relaciones *<Triggering>* en ArchiMate.

N° de Regla: 3

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Agregación relationship>, <Composición relationship>, <Triggering relationship>	*<Actividad>, <Pool>, <Linea de secuencia>*

Regla en ATL:

```
rule TriggeringToSecuenceFlow {
        from
                a : ARC!Relacion (a.isTriggering(a.Tipo)
                        and (not a.fuenteO.oclIsUndefined()
                        and not a.objetivoO.oclIsUndefined())
                        and a.fuenteRelacionIsBusinessP(a) and a.objetivoRelacionIsBusinessP(a)
                        and not a.fuenteRelacionPIsPool(a) and not
                        a.objetivoRelacionPIsPool(a))
        to
                b : BPS!SecuenceFlow (
                        FuenteA <- a.fuenteO,
                        ObjetivoA <- a.objetivoO
                )
    }
```

Gráficamente:

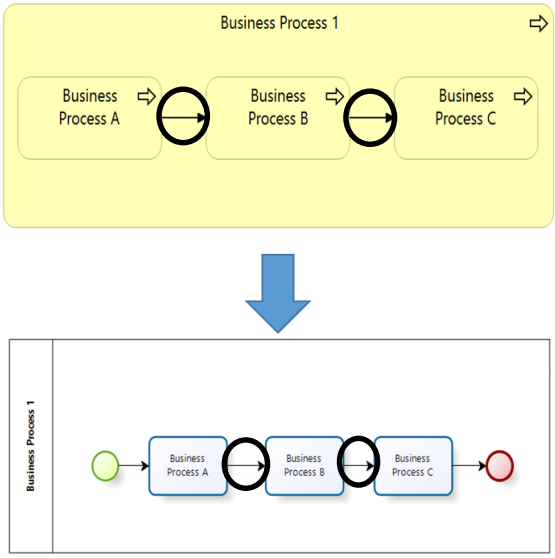


Figura 46: Proceso de negocio que contiene otros procesos y relación Triggering

Regla 4.- Cuando ocurre lo mismo que en la Regla 2, pero se trata de una relación de *<Flow>* en ArchiMate, se procede de igual forma que en la Regla 2, con la diferencia de que se interpreta como que existe un flujo de datos entre ambos elementos de la relación por lo tanto en BPMN debe existir una *<asociación>* con un *<Data Object>* entre ambos elementos.

N° de Regla: 4

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Agregación relationship>, <Composición relationship>, <Flow relationship>	*<Actividad>, <Pool>, <Linea de secuencia>, <Asociación>, <Data Object>*

Regla en ATL:

```
rule FlowToMessageFlow {
        from
                a : ARC!Relacion (a.isFlow(a.Tipo)
                        and (not a.fuenteO.oclIsUndefined() and not
                        a.objetivoO.oclIsUndefined())
                        and a.fuenteRelacionIsBusinessP(a) and a.objetivoRelacionIsBusinessP(a)
                        and not a.fuenteRelacionPIsPool(a) and not a.objetivoRelacionPIsPool(a)
                        and a.compararPools(a.buscaElementoPoolInFuente(a),
                        a.buscaElementoPoolInObjetivo(a)))
        to
                c : BPS!DataObject (
                        Name <- 'DataObject'
                ),
                b : BPS!Association (
                        AsociationF <- a.fuenteO,
                        AsociationO <- c
                ),
                d : BPS!Association(
                        AsociationF <- c,
                        AsociationO <- a.objetivoO
                ),
                e : BPS!SecuenceFlow (
                        FuenteA <- a.fuenteO,
                        ObjetivoA <- a.objetivoO
                )
   }
```

Gráficamente:

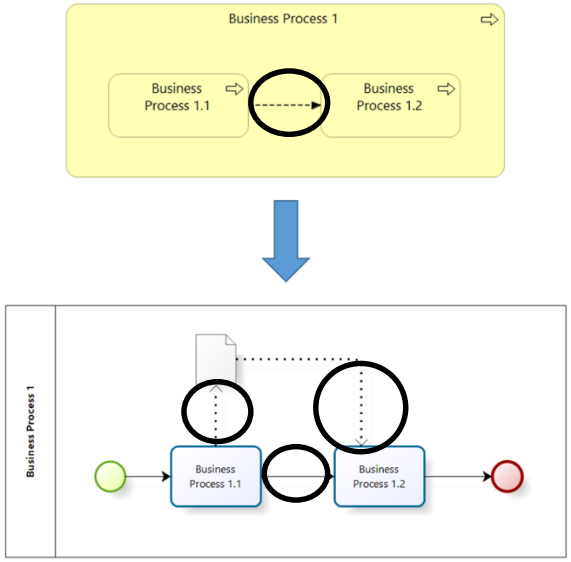


Figura 47: Proceso de negocio que contiene otros procesos y relación Flow

Escenario 2.- El servicio representa el contacto con el entorno: Un *<servicio de negocio>* expone una funcionalidad o comportamiento del negocio hacia el entorno. Cuando un elemento de estructura activa como un *<rol de negocio>*, un *<actor de negocio>* o una *<colaboración de negocio>* (elementos internos de estructura activa) y un *<proceso de negocio>* tienen una relación de *<servicio>* en ArchiMate (relación de servicio es el nombre de la relación que antiguamente se llamaba relación de *<<uso>>* hasta la versión 2.1) con un *<servicio de negocio>*, significa que el *<rol de negocio>*, el *<actor de negocio>*, la *<colaboración de negocio>* o el *<proceso de negocio>* tiene una relación con el comportamiento a través del *<servicio de negocio>*, o dicho de otra manera, el elemento hace uso del servicio para interactuar con el comportamiento.

Regla 5.- En este caso el *<rol de negocio>*, *<actor de negocio>*, *<colaboración de negocio>* o *<proceso de negocio>* se puede clasificar como un participante externo al comportamiento (interactúa pero no realiza el comportamiento, tiene su propio comportamiento), por ello cuando ocurre esto, este participante tiene una correspondencia con un *<Pool>* en BPMN. Ya que es un participante que interactúa con el comportamiento, tiene que haber un *<flujo de mensaje>* bidireccional entre el <Pool> del participante externo y el *<Pool>* del proceso. El requisito de seguridad realizado por el elemento en ArchiMate es también especificado en el elemento correspondiente en BPMN.

N° de Regla: 5

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business role>, <Business actor>, <Business interation>, <Business process>, <Business service>, <realization relationship>, <serving relationship>	*<Pool>, <Flujo de mensaje>*

Regla en ATL:

```
rule ServiceAndARCToPool {
        from
                a : ARC!Elemento(a.arcConService(a))
        to
                b : BPS!Pool (
                        Name <- a.Name,
                        --Requisitos de Seguridad--
                        RequisitoAC <- a.requisitoControlAc(a),
                        RequisitoAD <- a.requisitoDetecAtacAm(a),
                        RequisitoP <- a.requisitoPrivacidad(a)
                )
}

rule ServiceAndARCToMensageFlowPools {
        from
                a : ARC!Elemento(a.isBusinessService(a.Tipo)
                    and not a.servicioNServiceToARC(a).oclIsUndefined()
                    and not a.realisationPIFToService(a).oclIsUndefined() )
        to
                c : BPS!MessageFlow(
                        FuenteP <- a.servicioNServiceToARC(a),
                        ObjetivoP <- a.realisationPIFToService(a)
                ),
                d : BPS!MessageFlow(
                        FuenteP <- a.realisationPIFToService(a),
                        ObjetivoP <- a.servicioNServiceToARC(a)
                )
}
```

Gráficamente:

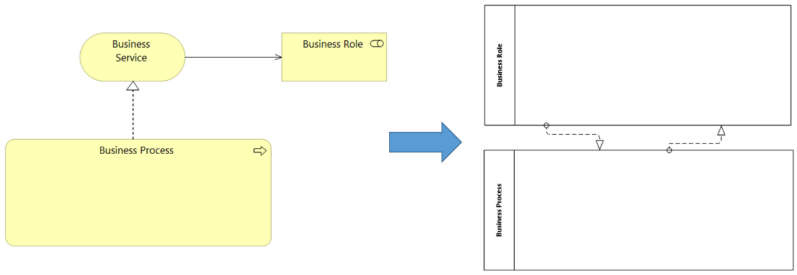


Figura 48: Servicio de negocio en la correspondencia

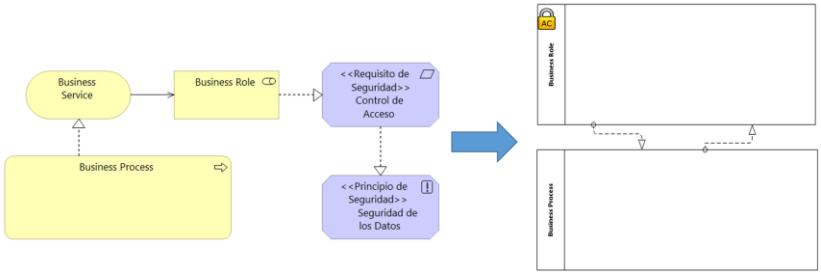


Figura 49: Servicio de negocio en la correspondencia (Con Control de Acceso)

Escenario 3.- Un actor de negocio, rol de negocio o una colaboración de negocio que está asignado a un proceso de negocio: Cuando un *<actor de negocio>*, *<rol de negocio>* o *<colaboración de negocio>* está *<asignado>* a un *<proceso de negocio>* en ArchiMate significa que es un participante. Un *<proceso de negocio>* solo puede estar asignado a un *<actor de negocio>* o varios a través de un *<rol de negocio>* o *<colaboración de negocio>* que se representan en un solo elemento que tiene relación directa, de otra forma no es posible cumplir las reglas asociadas a este escenario.

Regla 6.- Cuando un *<rol de negocio>*, *<actor de negocio>* o *<colaboración de negocio>* está *<asignado>* a un *<proceso de negocio>* en ArchiMate, significa que es un participante interno del *<proceso de negocio>* por lo cual tiene una correspondencia con un *<Lane>* dentro del *<Pool>* que representa el *<proceso de negocio>* en BPMN. El requisito de seguridad realizado por el elemento en ArchiMate es también especificado en el elemento correspondiente en BPMN.

N° de Regla: 6	
Elementos y relaciones de ArchiMate: *<Business process>, <Business actor>, <Business role>, <Business colaboration>, <Assignment relationship>*	**Elementos BPMN:** *<Pool>, <Lane>*

Regla en ATL:

```
--Regla 5--
rule AssignmentARCToLane {
        from
                a : ARC!Relacion(a.objetivoRelacionIsBusinessP(a)
                        and a.objetivoRelacionPIsPool(a)
                        and a.assignmentRel(a.Tipo)
                        and a.fuenteRelacionisARC(a))
        to
                b : BPS!Lane (
                        Name <- a.fuenteO.Name,
                        --Requisitos de Seguridad--
                        RequisitoAC <- a.requisitoControlAc(a),
                        RequisitoAD <- a.requisitoDetecAtacAm(a),
                        RequisitoP <- a.requisitoPrivacidad(a)

                )
    }
--Regla 1--
rule BusinessPToPool {
        from
                a : ARC!Elemento (a.isBusinessP(a.Tipo) and
                        a.BusinessPIsPool(a.Id))
        to
                b : BPS!Pool (
                        Name <- a.Name,
                        --Regla 5--
                        Lanes <- a.buscarLanes(a)
                )
    }
```

Gráficamente:

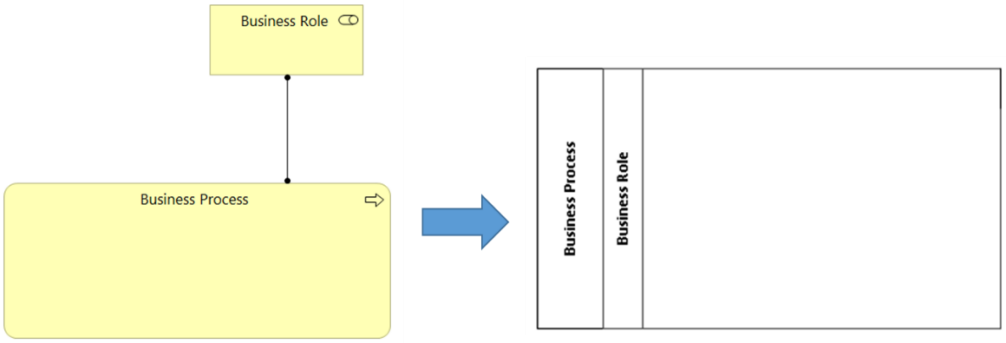


Figura 50: Proceso de negocio asignado a un Actor, Rol o Colaboración

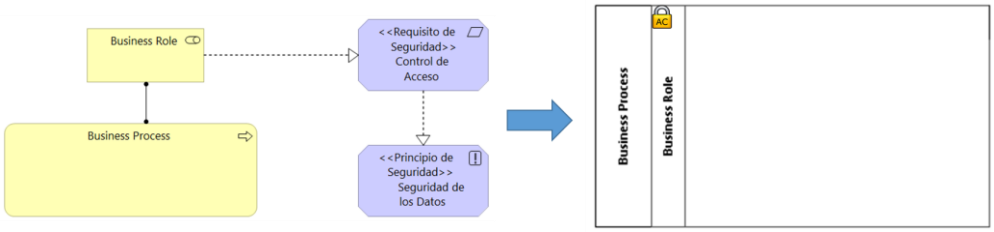


Figura 51: Proceso de negocio asignado a un Actor, Rol o Colaboración (Con Control de Acceso)

Regla 7.- Si el *<rol de negocio>*, *<actor de negocio>* o *<colaboración de negocio>* está *<asignado>* a un *<proceso de negocio>* que está conteniendo otros *<procesos de negocio>* en ArchiMate, entonces las *<actividades>* que corresponden con los elementos contenidos, deben estar en el *<Lane>* de BPMN que corresponde con el *<rol de negocio>*, *<actor de negocio>* o *<colaboración de negocio> <asignado>*, considerando que solo existe uno de estos *<asignado>*.

N° de Regla: 7

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Business actor>, <Business role>, <Business colaboration>, <assignment relationship>, <agregación relationship>, <composición relationship>	*<Pool>, <Lane>, <Actividad>, <Linea de secuencia>, <Evento>*

Regla en ATL:

```
rule BusinessPToActividad {
        from
                a : ARC!Elemento (a.isBusinessP(a.Tipo) and not a.businessPIsPool(a.Id))
        to
                b : BPS!Activity (
                        Name <- a.Name,
                        PoolO <- a.buscaElementoPool(a.Id),
                        --Regla 6--
                        LaneO <- a.laneDeActividad(a.buscarLanes(a.buscaElementoPool(a.Id)))

                )
```

Gráficamente:

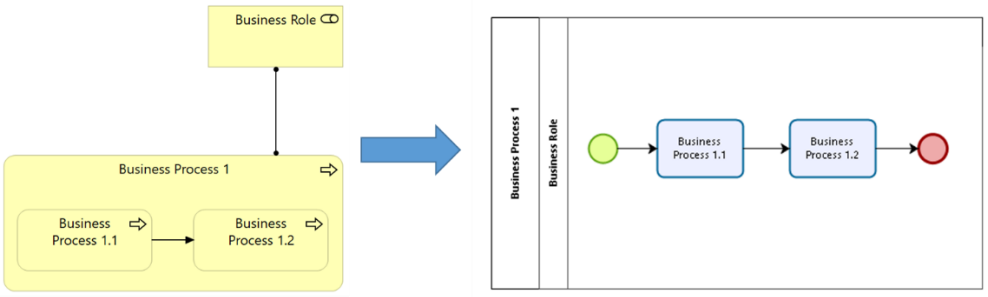


Figura 52: Propiedad de las actividades en un Pool

Escenario 4.- Relación de flojo entre procesos de negocio de ArchiMate: Una *<relación de flujo>* en ArchiMate describe el intercambio o transferencia de información o valor entre *<procesos de negocio>* (tiene relación con el flujo de datos).

Regla 8.- Cuando dos *<procesos de negocio>* de ArchiMate que tienen una correspondencia con un *<Pool>* en BPMN se relacionan a través de una *<relación de flujo>* significa que los *<Pool's>* en BPMN tienen un *<flujo de mensaje>* en el mismo sentido de la *<relación de flujo>* en ArchiMate. En BPMN siempre la comunicación entre *<Pool's>* es a través de *<flujos de mensaje>* así que esto es consistente con lo anterior.

N° de Regla: 8

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process,<Flow relationship>	*<Pool>,<Flujo de mensaje>*

Regla en ATL:

```
rule FlujoDeMensajeInPools {
        from
                a : ARC!Relacion(a.fuenteRelacionIsBusinessP(a)
                        and a.fuenteRelacionPIsPool(a)
                        and a.objetivoRelacionIsBusinessP(a)
                        and a.objetivoRelacionPIsPool(a)
                        and a.isFlow(a.Tipo)
                        and not a.fuenteO.oclIsUndefined() and not a.objetivoO.oclIsUndefined())
        to
                b : BPS!MessageFlow (
                        FuenteP <- a.fuenteO,
                        ObjetivoP <- a.objetivoO
                )
    }
```

Gráficamente:

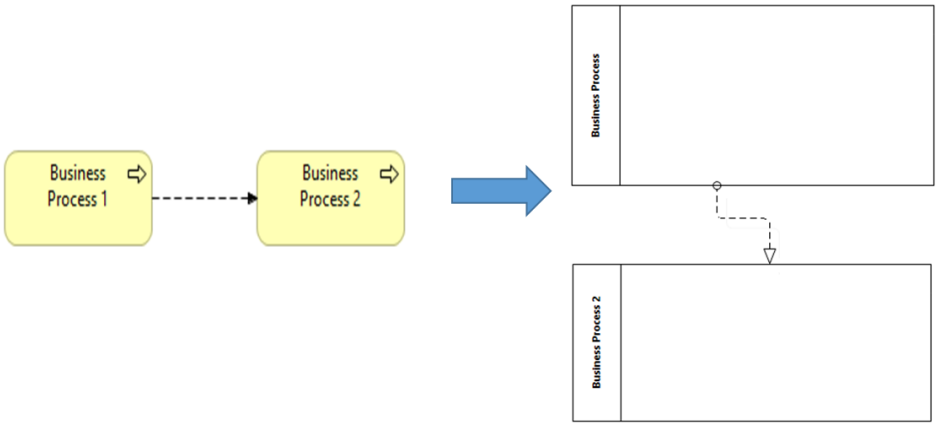


Figura 53: Flow entre dos Business Process Caso 1

Regla 9.- Cuando uno de dos *<procesos de negocio>* de ArchiMate contiene otros *<procesos de negocio>* que tienen una correspondencia con *<actividades>* en BPMN (relación de *<composición>* o *<agregación>* entre procesos de negocio en ArchiMate) y de uno de ellos surge un *<flujo>* al otro *<proceso de negocio>* que no está formado por otros *<procesos de negocio>*, entonces en BPMN la *<actividad>* que es la correspondencia del elemento que inicia el flujo corresponde al inicio del *<flujo de mensaje>* y el final va a dar al *<Pool>* en BPMN.

N° de Regla: 9

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Business function>, <Business interaction>,<Flow relationship>	*<Pool>, <actividad>, <Flujo de mensaje>, <Linea de secuencia>, <Evento>*

Regla en ATL:

```
rule FlujoDeMensajeDeActToPool {
        from
                a : ARC!Relacion(a.fuenteRelacionIsBusinessP(a)
                        and not a.fuenteRelacionPIsPool(a)
                        and a.objetivoRelacionIsBusinessP(a)
                        and a.objetivoRelacionPIsPool(a)
                        and a.isFlow(a.Tipo)
                        and not a.fuenteO.oclIsUndefined() and not a.objetivoO.oclIsUndefined())
        to
                b : BPS!MessageFlow (
                        FuenteA <- a.fuenteO,
                        ObjetivoP <- a.objetivoO
                )
    }
```

Gráficamente:

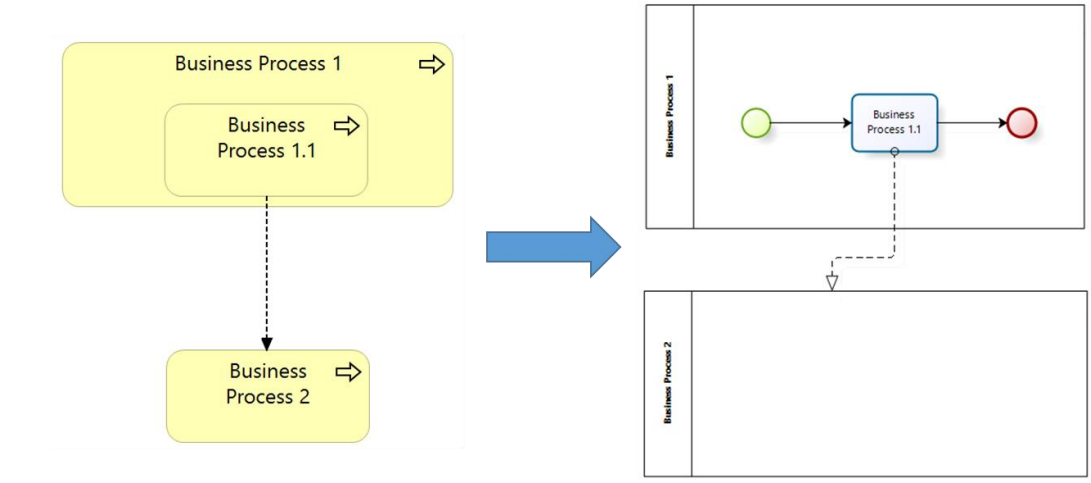


Figura 54: Flow entre dos Business process Caso 2

Regla 10.-Cuando dos *<procesos de negocio>* de ArchiMate contiene otros *<procesos de negocio>* que tienen una correspondencia con *<actividades>* en BPMN (relación de *<composición>* o *<agregación>* entre procesos de negocio en ArchiMate) y de uno de ellos surge un *<flujo>* hacia otro *<proceso de negocio>* que también está formando parte de otro *<proceso de negocio>*, entonces en BPMN existe un *<flujo de mensaje>* desde una *<actividad>* a otra en el mismo sentido que se modela la *<relación de flujo>* en ArchiMate.

N° de Regla: 10

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Business function>, <Business interaction>,<Flow relationship>	*<Pool>, <actividad>, <Flujo de mensaje>, <Linea de secuencia>, <Evento>*

Regla en ATL:

```
rule FlujoDeMensajeDeActToActPD {
        from
                a : ARC!Relacion(a.fuenteRelacionIsBusinessP(a)
                        and not a.fuenteRelacionPIsPool(a)
                        and a.objetivoRelacionIsBusinessP(a)
                        and not a.objetivoRelacionPIsPool(a)
                        and a.isFlow(a.Tipo)
                        and not a.fuenteO.oclIsUndefined() and not a.objetivoO.oclIsUndefined()
                        and not a.compararPools(a.buscaElementoPoolInFuente(a),
                        a.buscaElementoPoolInObjetivo(a)))

        to
                b : BPS!MessageFlow (
                        FuenteA <- a.fuenteO,
                        ObjetivoA <- a.objetivoO
                )
   }
```

Gráficamente:

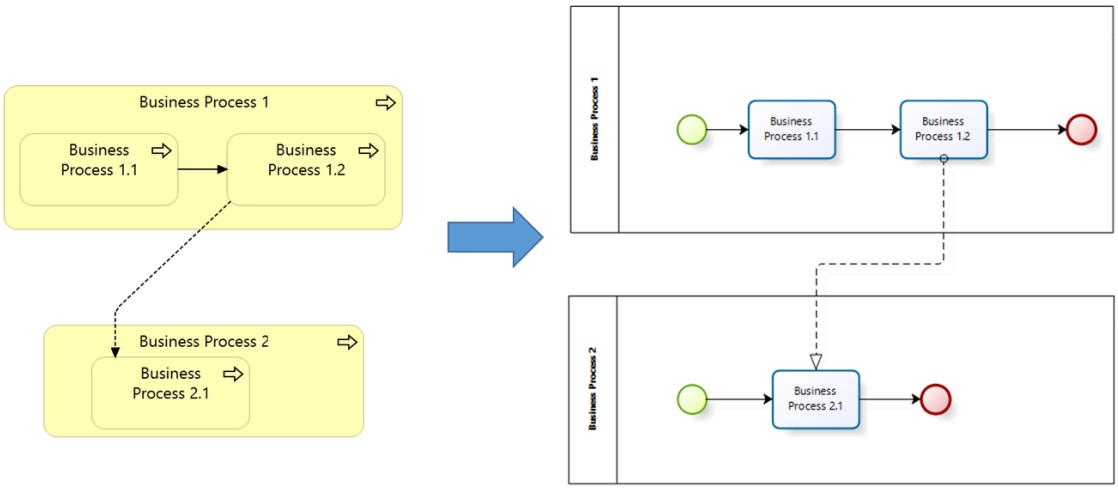


Figura 55: Flow entre dos Business process Caso 3

Escenario 5.- Eventos de negocio en ArchiMate como eventos en BPMN: En ArchiMate, un *<evento de negocio>* que se relaciona a un *<proceso de negocio>*, significa que es él quien gatilla el proceso de negocio (causa-efecto) (relación de *<Triggering>*) o que interrumpe el flujo. Un *<evento de negocio>* de ArchiMate se transforma en un *<evento simple>* en BPMN.

Cuando el *<proceso de negocio>* no se encuentra compuesto por otros en ArchiMate, no es necesario transformar los *<eventos de negocio>* ya que no habrá actividades dentro del *<Pool>* en BPMN y no tendría sentido tener solo *<eventos>*.

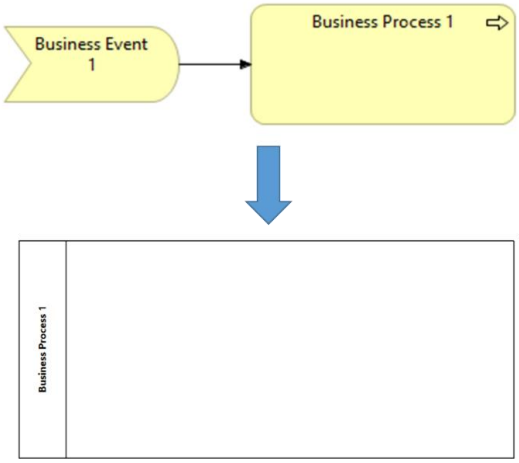


Figura 56: Caso evento de negocio sin correspondencia

Regla 11.- Cuando un *<evento de negocio>* gatilla un *<proceso de negocio>* en ArchiMate al inicio del flujo de las relaciones significa que es un *<evento de inicio simple>* en BPMN. No se realiza una distinción de un posible evento de inicio por mensaje, tiempo, etc, eso no es posible de identificar, y en BPMN puede hacerse el cambio una vez que el modelador enriquezca el modelo. Considerando que i) en BPMN a los eventos de inicio no se les asigna un nombre, ii) que solo existen cuando el proceso es descrito (hay actividades y otros elementos de por medio) y iii) que la Regla 1.2.3 establece que siempre que el proceso es descrito, deben haber eventos de inicio y de fin; entonces si existe un evento de negocio en ArchiMate de la forma descrita anteriormente, este no tiene impacto en el modelo correspondiente en BPMN.

N° de Regla: 11

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business event>, <Business process>, <Business function>, <Business interaction>, <Triggering relationship>	*<Pool>, <Actividad>, <Evento de inicio>, <Linea de secuencia>, <Evento>*

Regla en ATL:

```
rule BusinessEventToEventoInicio {
        from
                a : ARC!Elemento(a.isBusinessEvent(a.Tipo) and a.isEventoInicio(a))
        to
                b : BPS!Event (
                        Name <- 'Evento Inicio'

                ),
                c : BPS!SecuenceFlow(
                        FuenteE <- b,
                        ObjetivoA <- a.traeElementoObjetivoEvento(a)
                )
    }
```

Gráficamente:

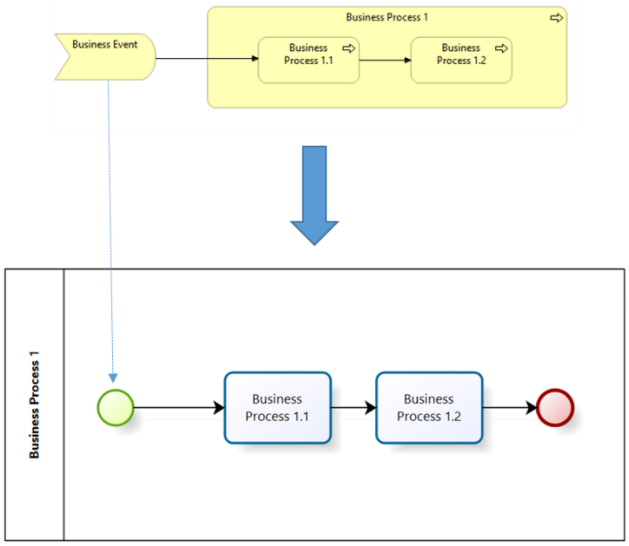


Figura 57: Evento de negocio como evento de inicio en BPMN

Regla 12.- Cuando un *<evento de negocio>* se encuentra en medio de *<procesos de negocio>* en ArchiMate que componen otro de estos mismos elementos, significa que tienen una correspondencia con *<eventos intermedio simple>* en BPMN. Al igual que en el caso anterior, no se realiza una distinción entre un tipo de evento intermedio de mensaje, múltiple, etc, eso no es posible de identificar, aunque muy probablemente sea temporal.

N° de Regla: 12

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business event>, <Business process>, <Business function>, <Business interaction>, <Triggering relationship>	*<Pool>, <Actividad>, <Evento intermedio>, <Linea de secuencia>*

Regla en ATL:

```
rule BusinessEventToEventoIntermedio {
        from
                a : ARC!Elemento(a.isBusinessEvent(a.Tipo) and a.isEventoIntermedio(a))
        to
                b : BPS!Event (
                        Name <- 'Evento Intermedio'
                ),
                c : BPS!SecuenceFlow(
                        FuenteA <- a.traeElementoFuenteEvento(a),
                        ObjetivoE <- b
                ),
                d : BPS!SecuenceFlow(
                        FuenteE <- b,
                        ObjetivoA <- a.traeElementoObjetivoEvento(a)
                )
    }
```

Gráficamente:

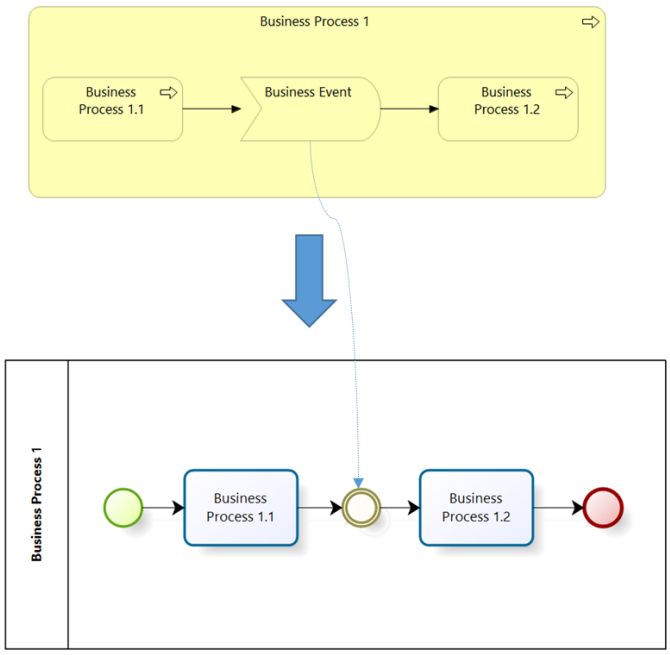


Figura 58: Evento de negocio como evento intermedio en BPMN

Regla 13.- Cuando un *<evento de negocio>* se encuentra al final del flujo de los *<procesos de negocio>* que componen otro de estos elementos en ArchiMate, significa que son *<eventos de fin simple>* en BPMN. No se puede realizar una diferenciación entre los distintos tipos de fin como mensaje, error, etc. Por las mismas razones que la correspondencia del evento de inicio, el evento de fin no tiene impacto en la correspondencia en BPMN.

N° de Regla: 13

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business event>, <Business process>, <Business function>, <Business interaction>, <Triggering relationship>	*<Pool>, <Actividad>, <Evento de fin>, <Linea de secuencia>*

Regla en ATL:

```
rule BusinessEventToEventoFin {
        from
                a : ARC!Elemento(a.isBusinessEvent(a.Tipo) and a.isEventoFin(a))
        to
                b : BPS!Event (
                        Name <- 'Evento Fin'

                ),
                c : BPS!SecuenceFlow(
                        FuenteA <- a.traeElementoFuenteEvento(a),
                        ObjetivoE <- b
                )
    }
```

Gráficamente:

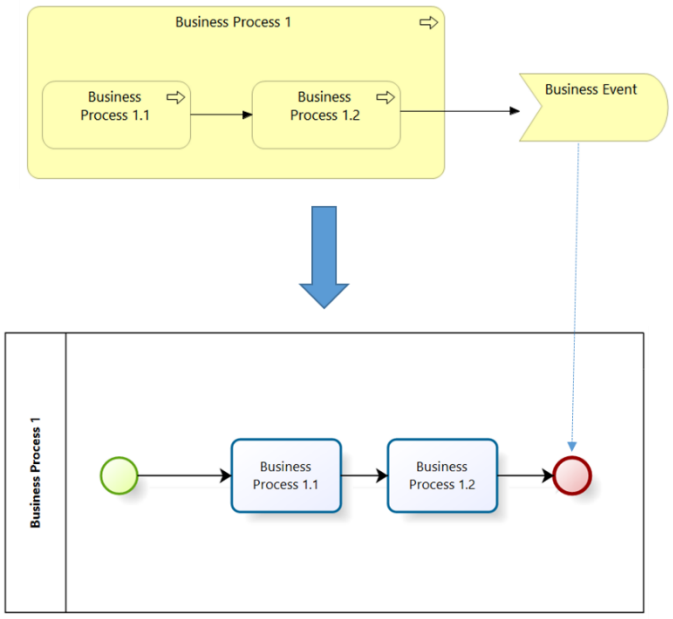


Figura 59: Evento de negocio como un evento de fin en BPMN

Escenario 6.- Objetos de negocio de ArchiMate como DataObject en BPMN: En ArchiMate existen varios elementos de estructura pasiva que tienen una correspondencia con un DataObject de BPMN.

Cuando un *<objeto de negocio>* u otro elemento de estructura pasiva de ArchiMate que tiene una correspondencia con un *<DataObject>* de BPMN se relaciona con un *<proceso de negocio>* en ArchiMate que tiene *<acceso>* a él y que no está compuesto por otros de estos elementos, entonces no es posible de representar dicha relación en BPMN por lo tanto el elemento no se transforma. Lo mismo sucede si el *<proceso de negocio>*, en ArchiMate está compuesto por estos elementos pero la relación entre el *<objeto de negocio>* no es con los *<procesos de negocio>* que lo componen sino que al elemento contenedor.

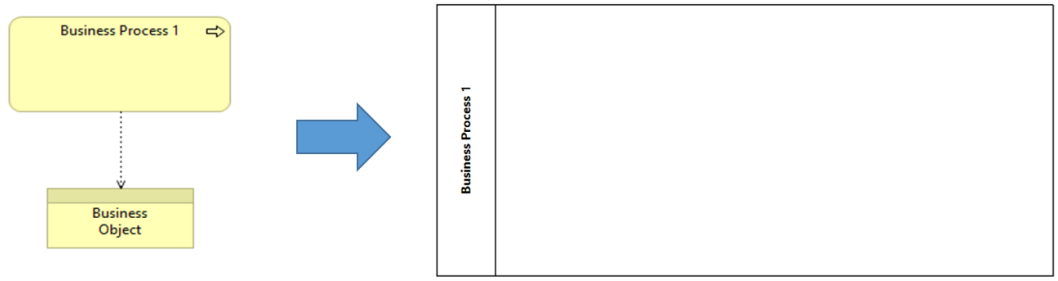


Figura 60: Objeto de negocio sin correspondencia Caso 1

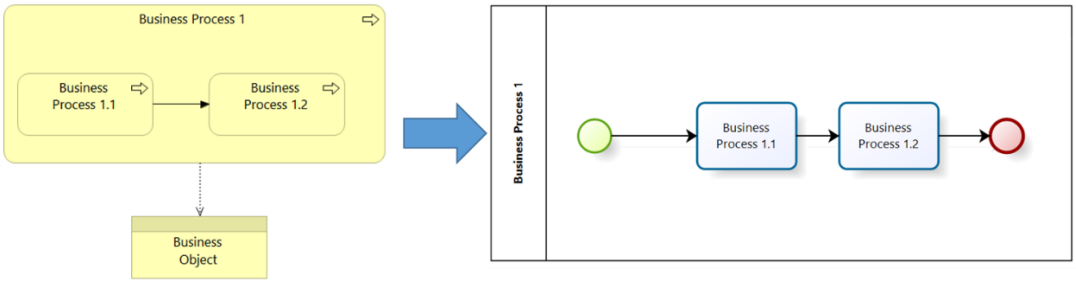


Figura 61: Objeto de negocio sin correspondencia Caso 2

Regla 14.- Si existe un elemento que tiene una correspondencia con un *<DataObject>* en BPMN y este está relacionado con un *<proceso de negocio>* (relación de *<acceso>*) que es parte de otro en ArchiMate, entonces el elemento tiene efectivamente una correspondencia con un *<Data Object>* en BPMN y está *<asociado>* con la *<actividad>* que representa al *<proceso de negocio>* al que está relacionado en ArchiMate. El requisito de seguridad realizado por el elemento en ArchiMate es también especificado en el elemento correspondiente en BPMN.

N° de Regla: 14	
Elementos y relaciones de ArchiMate: *<Business Object>, <Business process>, <Access relationship >*	**Elementos BPMN:** *<Pool>, <Actividad>, <DataObject>,<Linea de secuencia>, <Asociación>, <Evento>*

Regla en ATL:

```
rule BusinessObjectToDataObject {
        from
                a : ARC!Elemento(a.isOCR(a.Tipo) and not a.accessToORC(a.Id).oclIsUndefined())
        to
                b : BPS!DataObject (
                        Name <- a.Name,
                        --Requisitos de Seguridad--
                        RequisitoI <- a.requisitoIntegridad(a),
                        RequisitoAC <- a.requisitoControlAc(a),
                        RequisitoAD <- a.requisitoDetecAtacAm(a)
                ),
                c : BPS!Association(
                        AsociationF <- a.accessToORC(a.Id),
                        AsociationO <- b
                )
   }
```

Gráficamente:

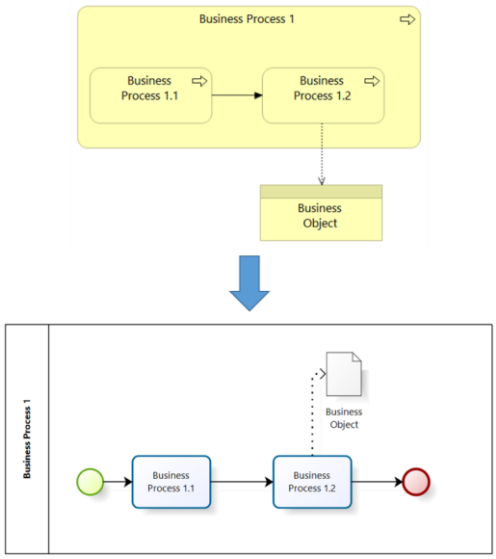


Figura 62: Proceso de negocio con acceso a un Business Object

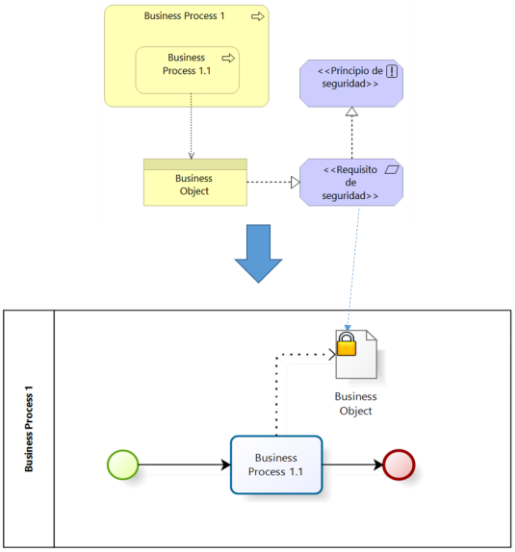


Figura 63: Proceso de negocio con acceso a un Business Object (Con Requisito de Seguridad)

Escenario 7.- La proximidad en la relación en los elementos: Al realizar una correspondencia a BPMN no todos los elementos de ArchiMate tienen cabida. Uno de estos casos son los *<actores de negocio>* relacionados a un *<rol de negocio>* y otro caso son las *<representaciones de negocio>* y *<contract's>* relacionados a un *<objeto de negocio>* en ArchiMate.

Uno de estos casos ocurre cuando por ejemplo se modela un *<rol de negocio>* relacionado a un *<proceso de negocio>* en ArchiMate, este *<rol de negocio>* se considera un participante en el proceso por lo cual tiene una relación con un *<Lane>* y el proceso es el *<Pool>* en BPMN. Además del *<rol de negocio>* que es el que tiene una relación directa con el proceso de negocio es posible que existan *<actores de negocio>* asignados a ese *<rol de negocio>*, lo cual ya no pueden tener una correspondencia con BPMN de ninguna forma ya que un *<Lane>* no pude volver a dividirse en otros contenedores. En este caso el *<rol de negocio>* es el *<Lane>* y los *<actores de negocio>* que están asignados al rol de negocio se pierden en la correspondencia.
Solo se realiza la transformación de los elementos hasta que sea posible, comenzando desde el elemento con la relación directa que es quien tiene prioridad absoluta.

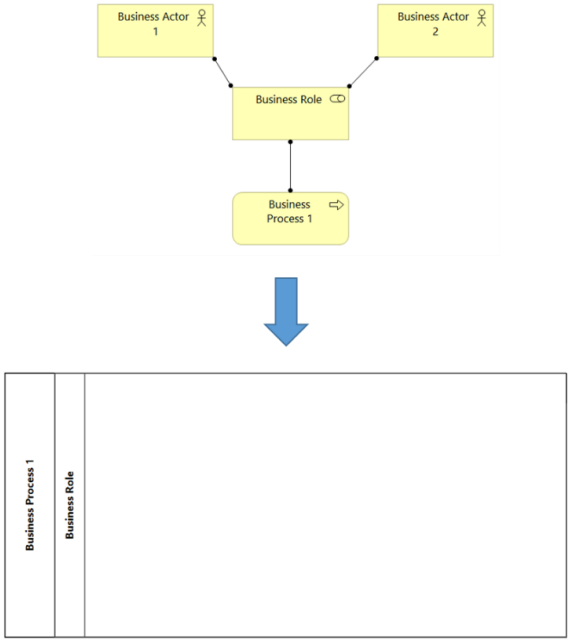


Figura 64: Modelo donde dos actores de negocio están asignados a un rol

Regla 15.- El segundo caso ocurre cuando por ejemplo un *<objeto de negocio>* es *<accedido>* por un *<proceso de negocio>* que compone un *<proceso de negocio>* mayor en ArchiMate. En este caso el *<proceso de negocio>* de ArchiMate es un *<Pool>* en BPMN, el *<proceso de negocio>* que lo compone es una *<actividad>* y esta tiene una *<asociación>* con un *<DataObject>*. Si el *<objeto de negocio>* es *<realizado>* por algunas *<representaciones de negocio>* ocurre algo similar que el caso de los roles y actores pero con la diferencia de que estas *<representaciones de negocio>* u otro elemento de estructura pasiva que se relacione con el *<objeto de negocio>* pueden tener una correspondencia con una *<anotación>* *<asociada>* al *<DataObject>* o varias si es más de una *<representación de negocio>*.

N° de Regla: 15

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Business Object>, <Representation>, <Access relationship>	*<Pool>, <Actividad>, <DataObject>, <Asociación>, <Anotación>, <Linea de secuencia>, <Evento>*

Regla en ATL:

```
rule RepresentationRealizationToAnotacion {
        from
                a : ARC!Relacion(a.fuenteRelacionIsRepresentation(a)
                        and a.objetivoRelacionIsBusinessObject(a)
                        and not a.objetivoRelacionAccessToORC(a).oclIsUndefined()
                        and not a.fuenteO.oclIsUndefined()
                        and not a.objetivoO.oclIsUndefined())
        to
                b : BPS!TextAnnotation (
                        Name <- a.fuenteO.Name

                ),
                c : BPS!Association(
                        AsociationT <-b,
                        AsociationO <-a.objetivoO
                )
    }
```

Gráficamente:

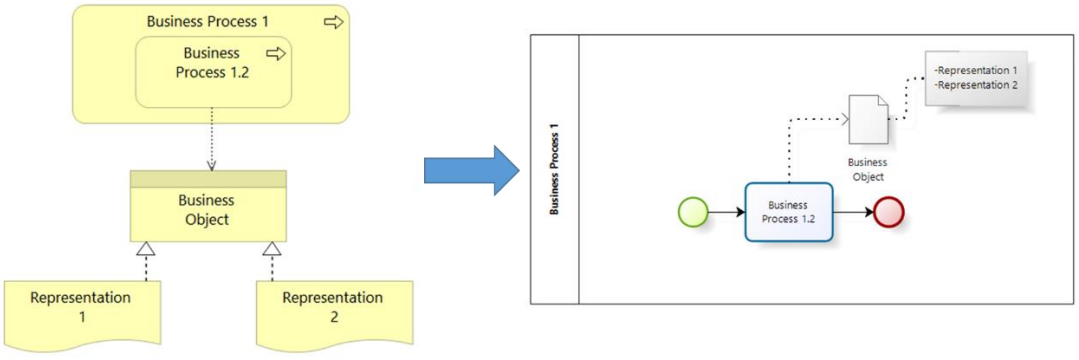


Figura 65: Business Object con representaciones

Escenario 8.- La unión de ArchiMate como compuertas en BPMN: En ArchiMate las *<uniones>* se utilizan para conectar las relaciones del mismo tipo. Una *<unión>* puede tener múltiples relaciones entrantes y una relación de salida, una relación de entrada y múltiples relaciones salientes, o múltiples relaciones de entrada y salida. Las relaciones que se pueden utilizar en combinación con una *<unión>* son todas las relaciones dinámicas (*<Flow>* y *<Triggering>*), así como la *<asignación>*, *<realización>*, y *<asociación>*. Existen dos tipos, la *<Unión And>* y la *<Unión Or>*. La *<Unión And>* se utiliza para expresar que varios elementos juntos participan en la relación y la *<Unión Or>* se utiliza para expresar que uno de los elementos participa en la relación. Pueden ser utilizados para modelar el flujo de proceso de alto nivel. Las *<uniones>* utilizadas en las relaciones *<Triggering>* son similares a las *<compuertas>* en BPMN (The Open Group, 2016).

Las *<compuertas>* son los elementos para controlar los puntos de divergencia y convergencia del flujo en BPMN. La divergencia o bifurcación consiste en la separación del flujo y la convergencia consiste en la unión del flujo.

Las *<compuertas>* siempre consisten en un flujo que se separa en varios otros en una bifurcación o varios flujos se unen en un punto en una convergencia.

En una bifurcación de las relaciones de *<Triggering>* en ArchiMate, el uso de la *<Unión And>* significa que todos los caminos son activados en el flujo y el uso de la *<Unión Or>* significa que uno de los caminos es activado.

En una convergencia de relaciones de *<Triggering>* en ArchiMate, el uso de la *<Unión And>* significa que todos los caminos son activados para seguir el flujo y el uso de la *<Unión Or>* significa que uno de los caminos es activado para seguir el flujo.

Regla 16.- Cuando existe una bifurcación de relaciones *<Triggering>* en ArchiMate y se usa la *<Unión And>*, significa que dicha *<Unión And>* tiene una correspondencia con una *<compuerta de decisión paralela>* en BPMN. En una *<compuerta paralela>* la bifurcación significa que todos los caminos son activados simultáneamente.

N° de Regla: 16

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Triggering relationship>, <And junction>	*<Pool>, <Actividad>, <Linea de secuencia>, <Compuerta paralela>, <Evento>*

Regla en ATL:

```
rule BifurcacionAndToGataway {
        from
                a : ARC!ConectorRelacion(a.isJunctionAnd(a.Tipo)
                        and a.unaEntradaAlConec(a)
                        and a.variasSalidasAlConec(a))
        to
                b : BPS!Gataway (
                        Name <- 'Compuerta Paralela'

                )
   }
```

Gráficamente:

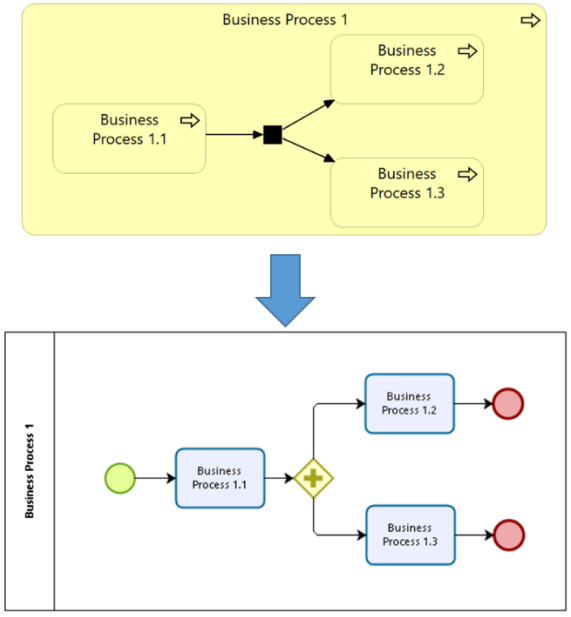


Figura 66: Modelo con divergencia de Unión And

Regla 17.- Cuando existe una bifurcación de relaciones *<Triggering>* en ArchiMate y se usa la *<Unión Or>*, significa que dicha *<Unión Or>* tiene una correspondencia con una *<compuerta de decisión exclusiva>* en BPMN. En una *<compuerta de decisión exclusiva>* en con bifurcación se selecciona exactamente un flujo de secuencia de entre las alternativas existentes.

N° de Regla: 17

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Triggering relationship>, <Or junction>	*<Pool>, <Actividad>, <Asociación>, <Compuerta exclusiva>, <Evento>, <Linea de secuencia>*

Regla en ATL:

```
rule BifurcacionOrToGataway {
        from
                a : ARC!ConectorRelacion(a.isJunctionOR(a.Tipo)
                        and a.unaEntradaAlConec(a)
                        and a.variasSalidasAlConec(a))
        to
                b : BPS!Gataway (
                        Name <- 'Compuerta Exclusiva'
                )
    }
```

Gráficamente:

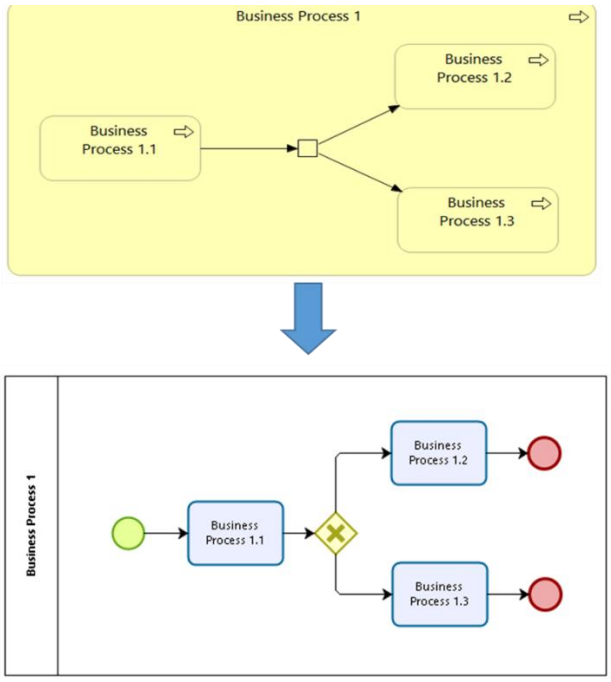


Figura 67: Modelo con divergencia de Unión Or

Regla 18.- Cuando existe una convergencia de relaciones *<Triggering>* en ArchiMate y se usa la *<Unión And>*, significa que dicha *<Unión And>* tiene una correspondencia con una *<compuerta paralela>* en BPMN. La *<compuerta paralela>* en una convergencia se utiliza para unir caminos alternativos, las compuertas esperan todos los flujos que concurren en ellas antes de continuar.

N° de Regla: 18

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Triggering relationship>, <And junction>	*<Pool>, <Actividad>, <Asociación>, <Compuerta paralela>, <Evento>, <Linea de secuencia>*

Regla en ATL:

```
rule ConvergenciaAndToGataway {
        from
                a : ARC!ConectorRelacion(a.isJunctionAnd(a.Tipo)
                        and a.variasEntradasAlConec(a)
                        and a.unaSalidaAlConec(a))
        to
                b : BPS!Gataway (
                        Name <- 'Compuerta Paralela'
                )
    }
```

Gráficamente:

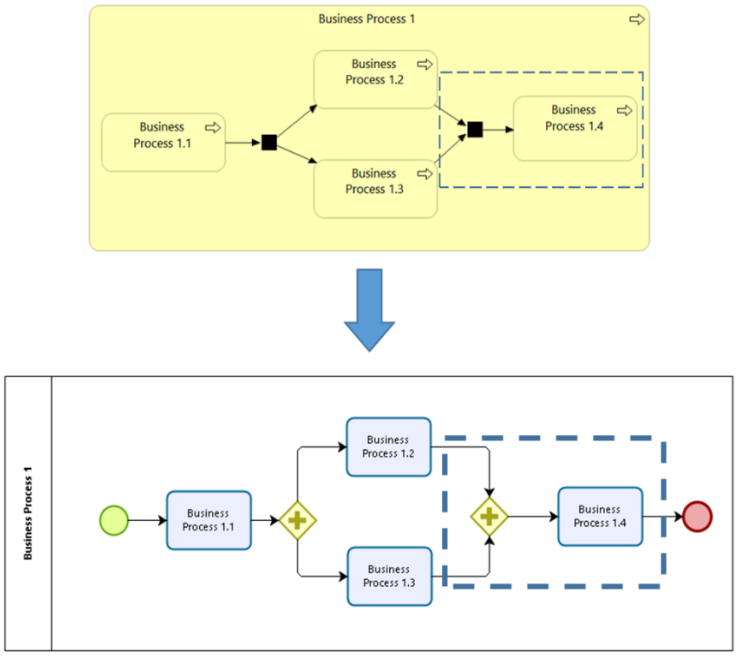


Figura 68: Modelo convergencia de Unión And

Regla 19.- Cuando existe una convergencia de relaciones *<Triggering>* en ArchiMate y se usa la *<Unión Or>*, significa que dicha *<Unión Or>* tiene una correspondencia con una *<compuerta exclusiva>* en BPMN. La *<compuerta exclusiva>* en una convergencia espera a que un flujo incidente complete para activar el flujo saliente.

N° de Regla: 19

Elementos y relaciones de ArchiMate:	**Elementos BPMN:**
<Business process>, <Triggering relationship>, <Or junction>	*<Pool>, <Actividad> <Asociación>, <Compuerta exclusiva>, <Evento>, <Linea de secuencia>*

Regla en ATL:

```
rule ConvergenciaOrToGataway {
        from
                a : ARC!ConectorRelacion(a.isJunctionOR(a.Tipo)
                        and a.variasEntradasAlConec(a)
                        and a.unaSalidaAlConec(a))
        to
                b : BPS!Gataway (
                        Name <- 'Compuerta Exclusiva'

                )
   }
```

Gráficamente:

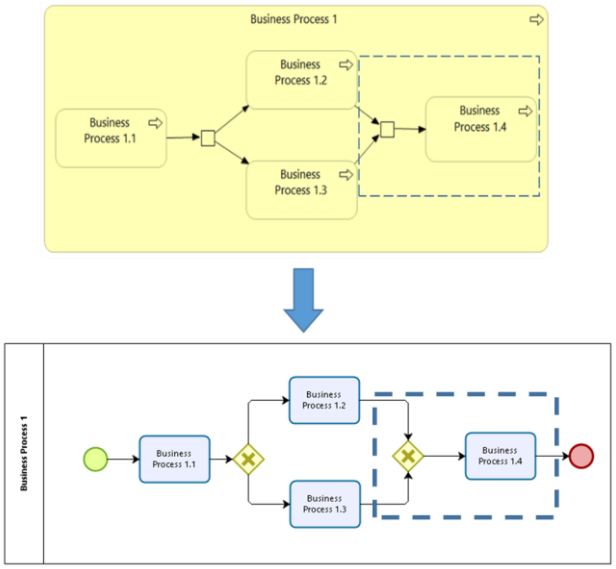


Figura 69: Modelo convergencia de Unión Or

Anexo B. Reglas de Transformación de modelo BPMN-BPSec hacia IFML

En este anexo se presentan reglas la transformación BPMN-BPSec hacia IFML, solo para los requisitos de seguridad involucrados. Son reglas para aquellos requisitos de seguridad que tienen una representatividad y/o relación con el Front End, los cuales son el control de acceso y la privacidad, respectivamente.

a) Correspondencia con Control de acceso

Regla 1.- Actividad con Control de Acceso:

En el caso de una actividad con Control de Acceso, este requisito debe ser implementado antes de realizar la actividad. De los patrones de seguridad que tienen relación con el Control de Acceso, el más adecuado para esta correspondencia es el patrón *IA-SPLOG: Login a un viewContainer específico*. En la Figura 70 se muestra este caso en BPMN-BPSec y en la Figura 71 se muestra su representación en IFML. Se debe tener en cuenta que, en algunos patrones (Como el que se muestra en la Figura 71), se ha integrado el LogOut, que es otro patrón que posee una relación indirecta con el control de acceso, pues representa el término de la autorización que brinda el Login.

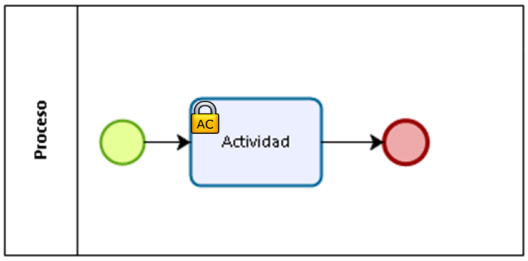


Figura 70: Caso 1 de actividad en BPMN-BPSec

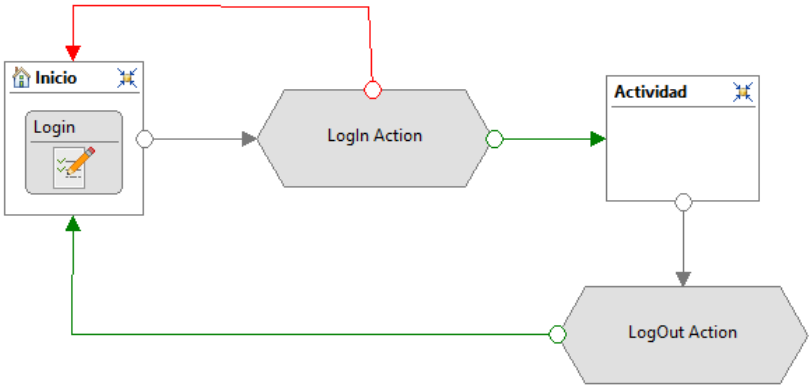


Figura 71: Correspondencia caso 1 de actividad en IFML

Como se aprecia en la Figura 71, se realiza el Login para cumplir con el requisito Control de Acceso especificado en el modelo BPMN-BPSec. Luego el flujo de navegación se dirige al primer

elemento que es parte de la actividad, donde se inicia el flujo o representación de la actividad como tal. Dicha representación, con un ViewContainer para la actividad, puede ser un conjunto de viewContainer, flows, events, actions y/o viewComponent que siguen el flujo después de la acción de Login.
Un ejemplo de esta regla se muestra en la Figura 72 en BPMN-BPSec, mientras que en la Figura 73 se muestra la correspondencia en IFML.

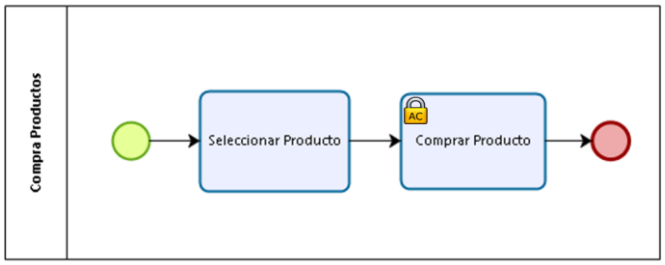


Figura 72: Ejemplo caso 1 de actividad en BPMN-BPSec

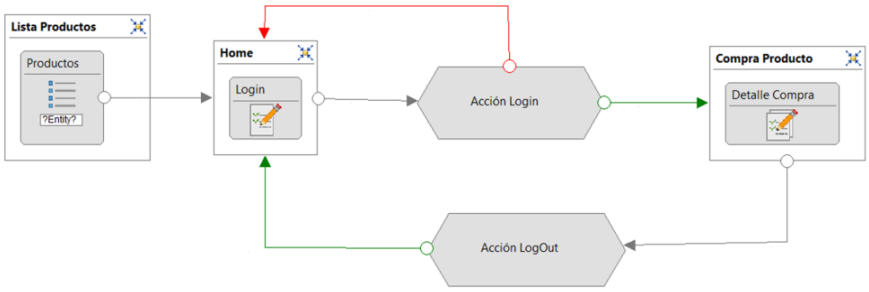


Figura 73: Ejemplo de una actividad con control de acceso en IFML

Para este ejemplo se realizan dos Actividades. La primera no necesita Control de Acceso a través de un Login, pero la segunda actividad lo necesita. Después de realizar el Login el flujo de navegación se divide en un caso donde la acción de Login es correcta y un caso donde ocurre una excepción y el Login es incorrecto, en el primer caso el flujo dirige a la actividad de "Comprar Producto" que se encuentra compuesta por un viewContainer. En el caso de que la acción de Login sea incorrecta, el flujo se dirige a la vista inicial del Login (viewContainer con el Form de Login). El LogOut dirige el flujo a donde el modelador lo defina, puede ser a la actividad anterior a la actividad con Control de Acceso, puede ser a la actividad siguiente sin Control de Acceso o a la vista inicial del Login. La acción de Login no implica la acción de LogOut al finalizar la actividad con Control de Acceso, eso es decidido por el modelador.

Regla 2.- Lane con control de acceso:
Si el control de acceso está en un Lane en específico, este Lane representa un participante y el Pool un proceso, entonces el control de acceso debe estar al inicio de todas las actividades que se realizan en el Lane. De los patrones de seguridad que tienen relación con el control de acceso, el

más adecuado para esta correspondencia es el patrón *IA-SPLOG: Login a un viewContainer específico*. En la Figura 74 se muestra este caso en BPMN-BPSec y en la Figura 75 se muestra su correspondencia en IFML.

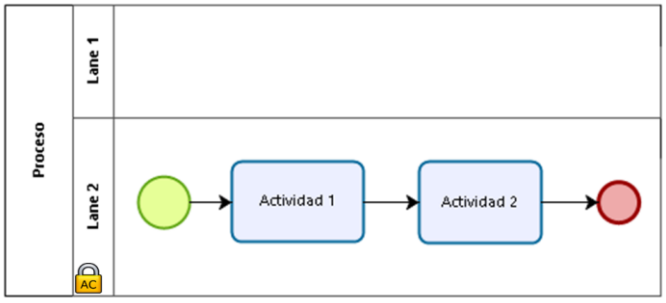


Figura 74: Control de acceso en Lane BPMN

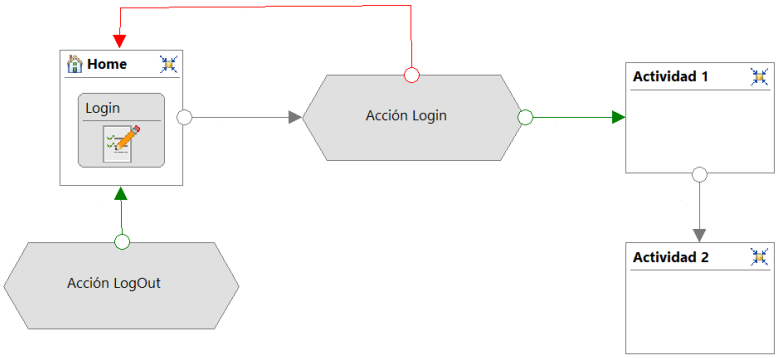


Figura 75: Correspondencia Control de acceso en Lane

Se debe tener en cuenta que, cuando el control de acceso se encuentra en un Lane, entonces se está indicando que todas las actividades y elementos del Lane tienen control de acceso, es decir, el Login se realiza al inicio y se mantiene hasta la realización de la última actividad. En cambio, cuando el control de acceso es sobre una actividad, entonces se está indicando que el control de acceso se aplica al inicio de la actividad y termina cuando ésta finaliza.

Regla 3.- Pool con control de acceso:

Si el control de acceso se aplica sobre el Pool y éste tiene uno o más Lane´s (Ver Figura 76), entonces el control de acceso se aplica a través del patrón *IA-RBP: Permisos basados en roles para elementos de vista*. En este patrón, como se observa en la Figura 77, se realiza el control de acceso al inicio del modelo y luego, a través de la acción de Login, el flujo se divide en la misma cantidad de participantes. Cada una de las bifurcaciones representa un Lane, por lo tanto, después de la bifurcación, se deben representar las actividades correspondientes al participante que representa dicha bifurcación.

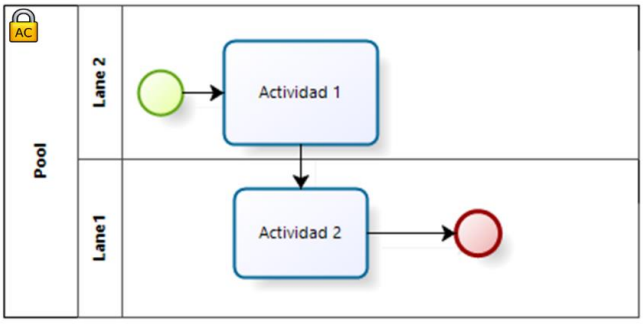


Figura 76: Control de acceso en Pool BPMN

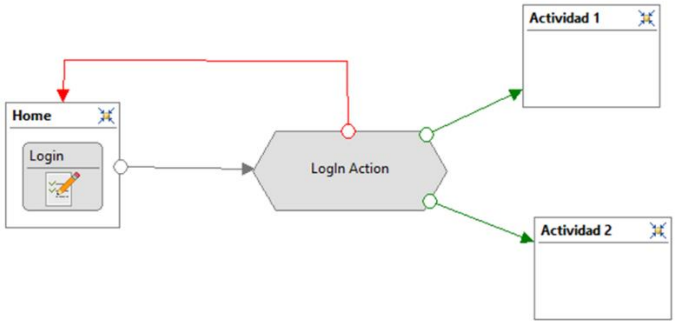


Figura 77: Representación en IFML de control de acceso en Pool

En base a lo anterior, en la Figura 78 se presenta un ejemplo de un diagrama BPMN que presenta un Pool con control de acceso y en la Figura 79 se presenta la representación de dicho modelo en IFML.

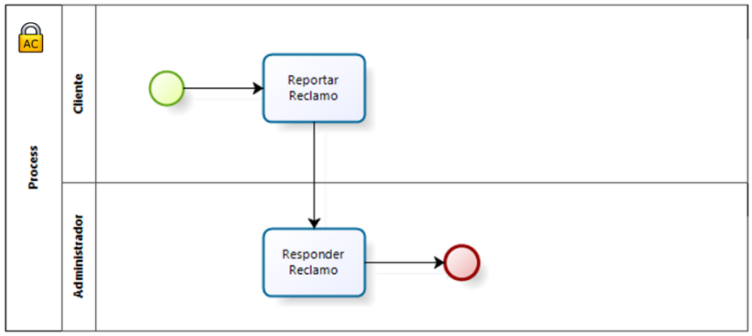


Figura 78: Ejemplo modelo BPMN con un Pool con control de acceso

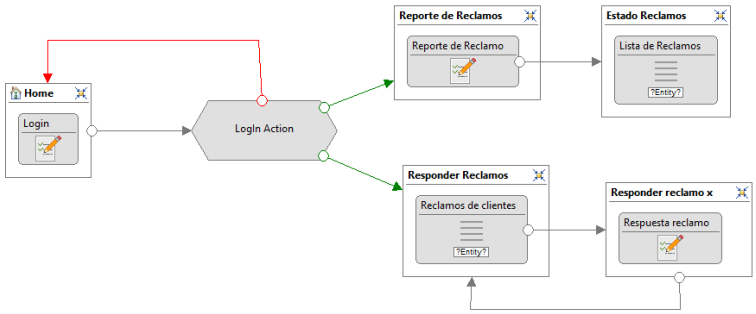


Figura 79: Modelo IFML del proceso modelado en la Figura 78

Regla 4.- Group con Control de acceso:

Si el control de acceso se aplica sobre un Group de la forma que se visualiza en la Figura 80 (el Group solo está afectando actividades de un mismo Lane), entonces el control de acceso se aplica con el patrón *IA-SPLOG: Loggin a un viewContainer específico* al inicio de la primera actividad del Group y se extiende hasta la última actividad del grupo. De esta forma, al realizar la correspondencia de la Figura 80 a IFML, quedaría de la misma forma que como se muestra en la Figura 81.

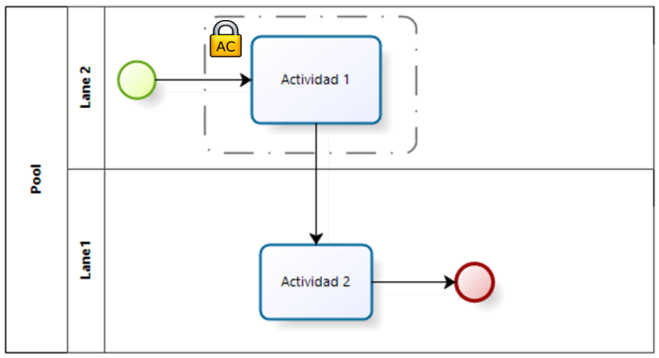


Figura 80: Control de acceso en Group en solo un Lane

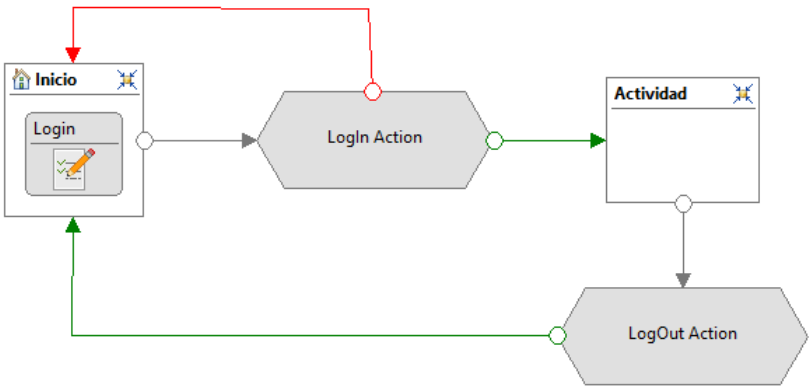


Figura 81: Correspondencia Control de acceso en Group en solo un Lane

Si el Group está agrupando una parte del diagrama BPMN que se encuentra en más de un Lane (Figura 82), entonces el control de acceso se realiza a través del patrón *IA-SPLOG: Login a un viewContainer especifico* al inicio de cada una de las actividades de cada Lane que se encuentran dentro del Group, tal como se muestra en la Figura 83.

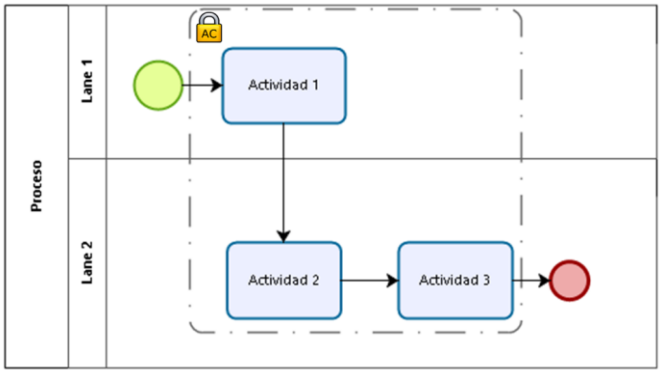


Figura 82: Control de acceso en Group en más de un Lane

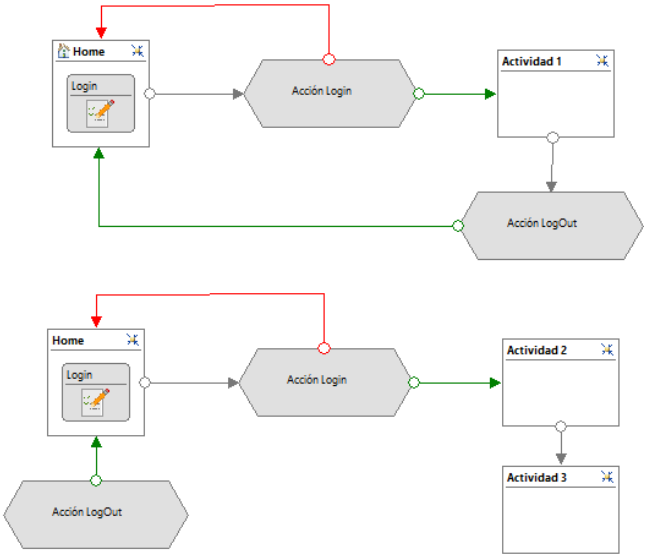


Figura 83: Correspondencia Control de acceso en Group en más de un Lane

Regla 5.- DataObject con control de acceso:

Si el control de acceso se aplica sobre un DataObject (Figura 84), entonces, se debe realizar antes de mostrar el Objeto de Dato (Su contenido) a través del patrón *IA-SPLOG: Login a un ViewContainer especifico* como se muestra en la Figura 85.

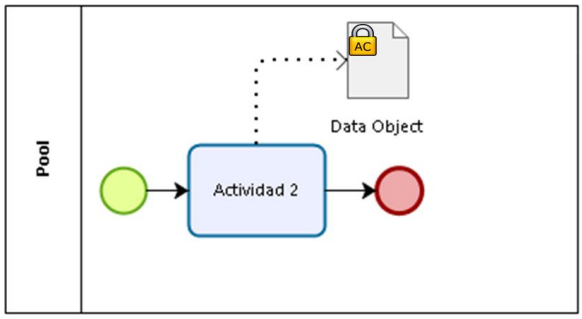


Figura 84: Control de acceso en Objeto de Dato BPMN

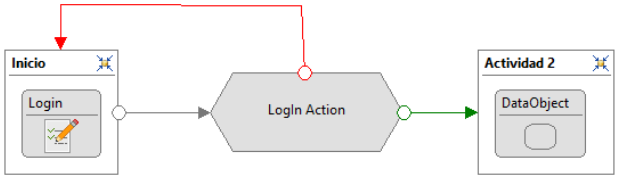


Figura 85: Representación en IFML de Control de acceso en DataObject

En la Figura 86 se muestra un ejemplo de este caso, donde un participante requiere realizar la actividad de "Revisar Ficha Médica". Para la representación de esta actividad en IFML (Figura 87), se requiere acceder al Objeto de Dato que se representa mediante el ViewComponent "Fichas Médicas", para lo que es necesario realizar un Login, cuyo flujo positivo permite la visualización de la ficha médica (El contenido).

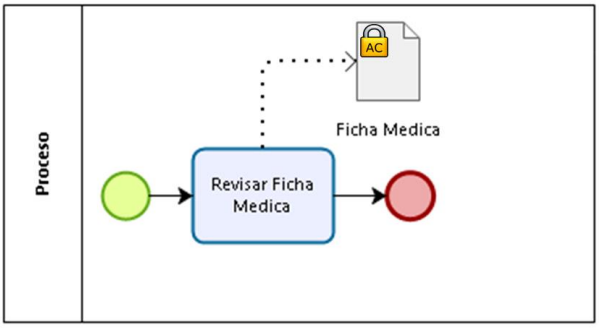


Figura 86: Ejemplo control de acceso en DataObject BPMN

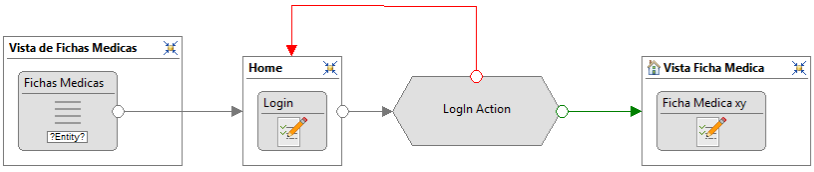


Figura 87: Ejemplo representación de DataObject en IFML

b) Correspondencia con Privacidad

Ya que la privacidad se aplica sobre los Group, Lane y Pool, la única forma de modelar la privacidad a nivel de Front End es a través de las bifurcaciones de un flujo de navegación que se origina de una acción de Login. Con la poca información que presentan los modelos de proceso de negocio con BPMN-BPSec, solo se puede representar la privacidad cuando se usa el Login.

Regla 6.- Privacidad y control de acceso:

Cuando un requisito de privacidad y un requisito de control de acceso están especificados en un elemento, entonces se deben aplicar las reglas relacionadas al control de acceso, pues al realizar el Login ya se está aplicando la privacidad, después de la autorización que provee el control de acceso. En la Figura 88 se muestra un modelo de proceso de negocio seguro donde se presenta este caso y en la Figura 89 se muestra la correspondencia de este caso. Cada una de las bifurcaciones indica que existen vistas diferentes para cada usuario, es decir las bifurcaciones después de la acción representan la privacidad y el alcance del control de acceso solo llega hasta la acción de Login.

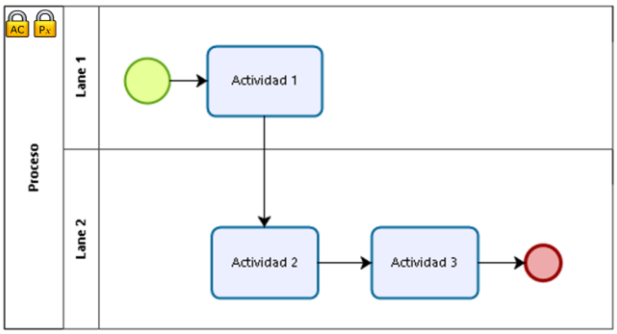


Figura 88: Pool con Control de Acceso y Privacidad

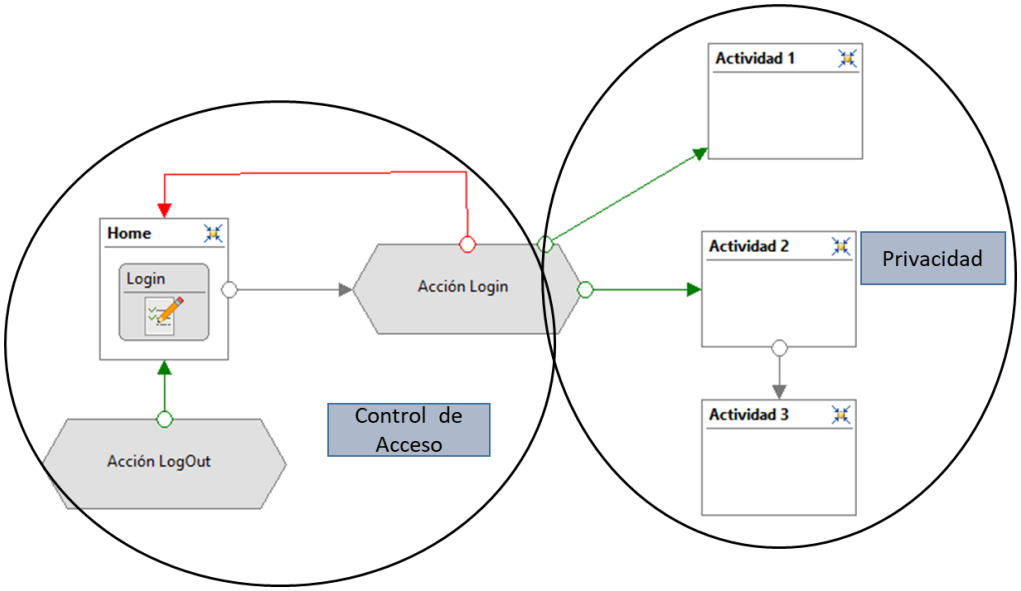


Figura 89: Correspondencia IFML de Pool con Control de Acceso y Privacidad

Anexo C. Instrumento de Medición Sobre Transformación de Modelos de ArchiMate a BPMN-BPSec y de BPMN-BPSec a IFML

El presente instrumento de medición tiene como objetivo validar las reglas de transformación de modelos propuestas en la investigación titulada "Integración de la seguridad en la capa de negocio y la interfaz de usuario a través de ArchiMate, BPMN-BPSec e IFML". Esta investigación tiene como objetivo definir un mecanismo para integrar la seguridad en la capa de negocio y la interfaz de usuario, estableciendo una correspondencia entre los elementos que modelan los requisitos de seguridad ya expresados en BPMN-BPSec y los elementos de ArchiMate e IFML.

Este instrumento está dirigido a personas con conocimientos sobre los estándares de modelado ArchiMate, BPMN e IFML. Siendo no necesariamente obligatorio el conocimiento al respecto del estándar IFML ya que las preguntas se encuentran explicadas de tal forma que no es necesario el conocimiento de esta estándar, solo se deben poseer algunos conocimientos generales relacionados al diseño interfaz de usuario.

El instrumento se encuentra dividido en 3 secciones: Sección de selección múltiple, Sección de construcción de modelos y Sección de preguntas de opinión personal. Siendo las dos primeras secciones relacionadas a propuestas de reglas de transformación de modelos de ArchiMate a BPMN-BPSec y la última sección relacionada a propuestas de reglas de transformación de modelos de BPMN-BPSec a IFML. La primera sección de selección múltiple consiste en la presentación de un escenario (una parte de un modelo de Arquitectura Empresarial modelado con ArchiMate) y diferentes alternativas de posibles transformaciones del escenario. La segunda sección de construcción de modelos consiste en la presentación de un modelo de Arquitectura Empresarial modelado con ArchiMate y se pide modelar un modelo de proceso de negocio seguro con BPMN-BPSec que usted considera es la transformación del modelo de arquitectura. La última sección de preguntas de opinión personal consiste en la presentación de una posible correspondencia entre BPMN-BPSec e IFML o afirmaciones sobre esta transformación de modelos con la finalidad de pedir su opinión con respecto a si está en acuerdo o en desacuerdo con respecto a estas correspondencias propuestas y afirmaciones realizadas.

Este instrumento es confidencial y las respuestas se usaran para validar las reglas de transformación que se han propuesto para esta investigación.

Si desea realizar alguna pregunta sobre el instrumento de medición, envié un correo electrónico a: luasanma@alumnos.ubiobio.cl.

Agradecemos su cooperación y el tiempo dedicado a responder este instrumento de medición.

Nombre Sujeto: ……

I. Selección Múltiple

Para las siguientes preguntas de este instrumento de medición, seleccione la alternativa correcta encerrándola con un círculo o resaltándola de alguna forma. Solo se permite una respuesta por pregunta. Si considera que no está presentada la alternativa correcta, no responda.

1. Si en un Modelo de Arquitectura Empresarial con ArchiMate se encuentra un "Business Process simple" como se muestra en la Figura 90, es decir no es una agregación o composición de otros "Business Process", entonces, según su opinión que elemento de BPMN sería su correspondencia en una transformación de Modelos.

Figura 90: Business Process Simple

Posibles correspondencias:

a) Lane
b) Pool
c) Data Object
d) Activity

2. Si en un Modelo de Arquitectura Empresarial con ArchiMate se encuentra un “Business Process Complejo” como se muestra en la Figura 91, donde el Business Process está compuesto por otros, entonces según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

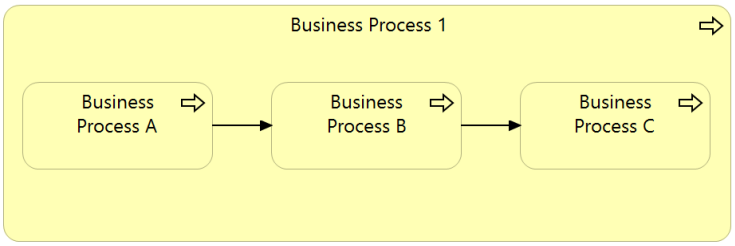
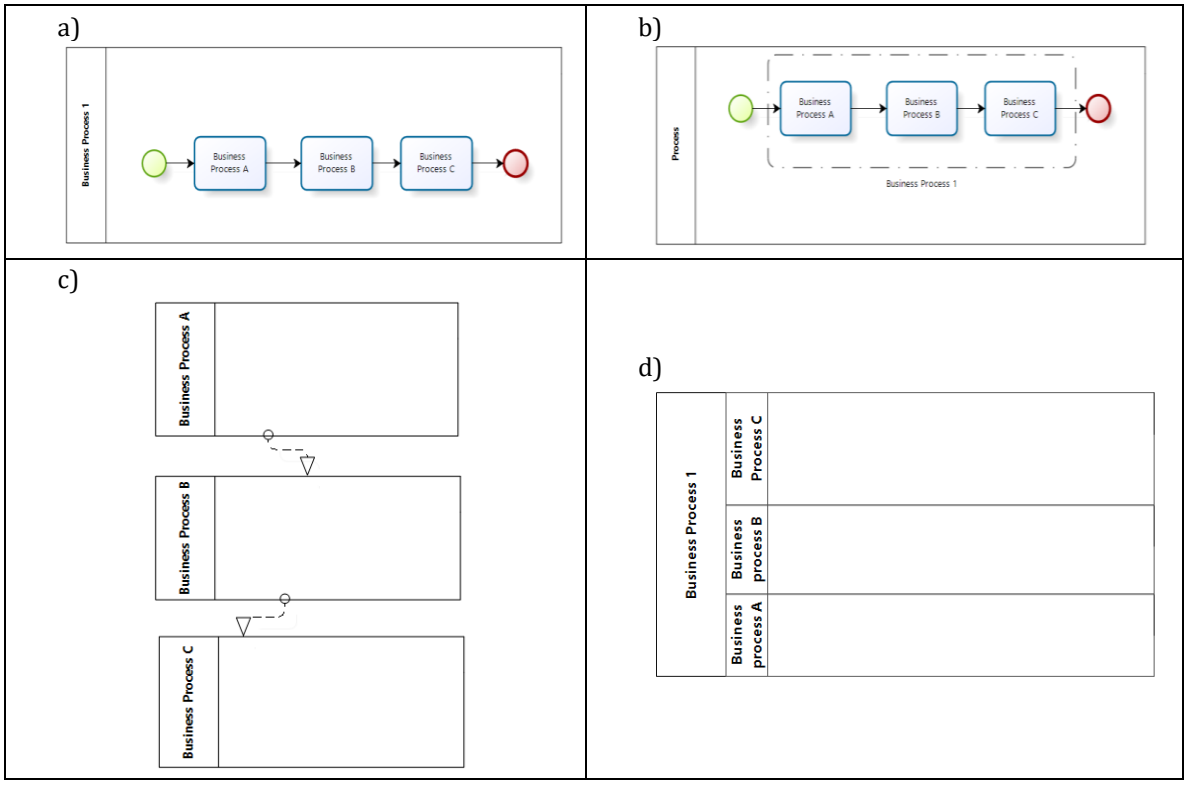


Figura 91: Business Process Complejo

Posibles correspondencias:



3. Considera que las respuestas de 1 y 2 son aplicables si en lugar de un “Business Process” fuera una “Business Function” y una “Business Interaction”
    a) Si
    b) NO
    c) Solo para Business Function
    d) Solo para Business Interaction

4. Considerando la siguiente situación donde un “Business Process Simple” realiza un “Servicio de Negocio” y un “Business Role” usa dicho “Servicio de Negocio” como se muestra en la Figura 92. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

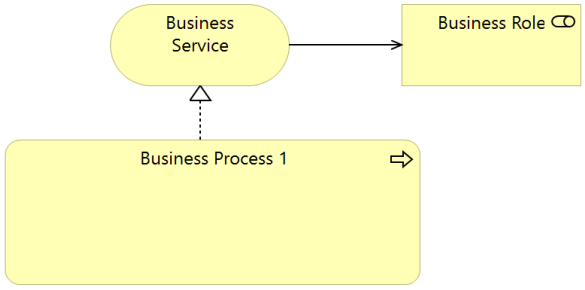
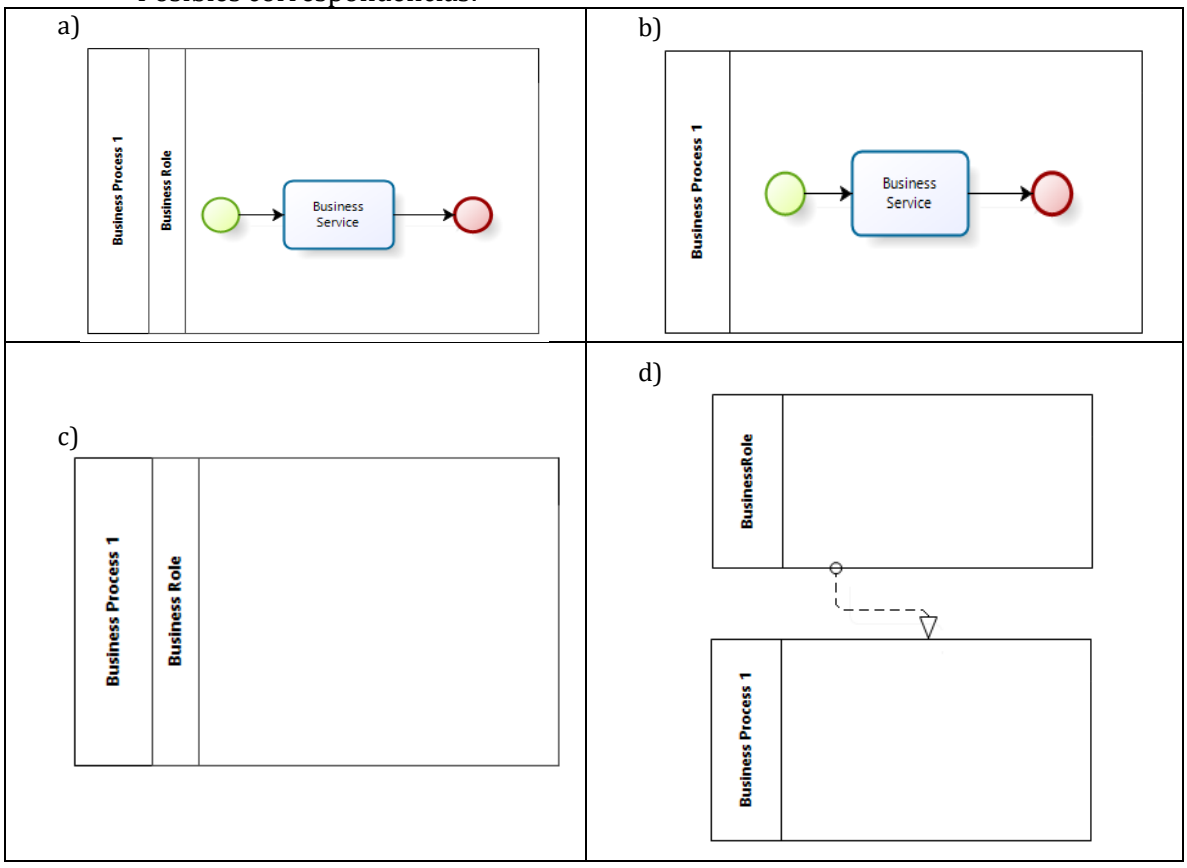


Figura 92: Situación 4

Posibles correspondencias:



5. Considerando la situación mostrada en la Figura 93, donde un “Business Role” está asignado a un “Business Process Simple” y este es usado por un “Business Actor”. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

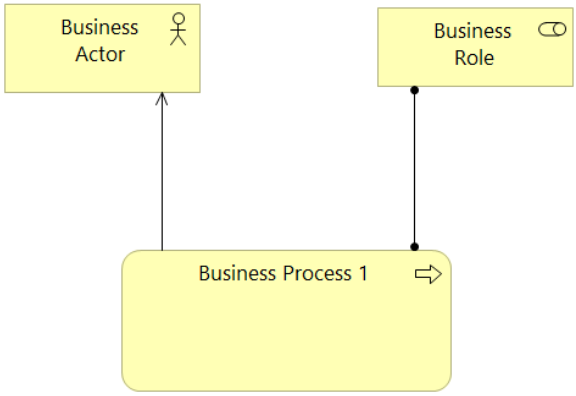
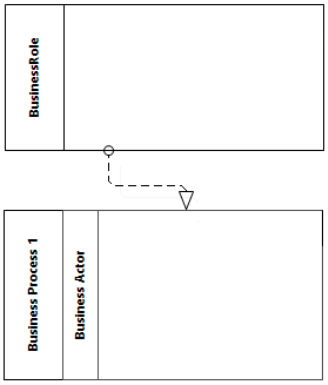


Figura 93: Situación 5

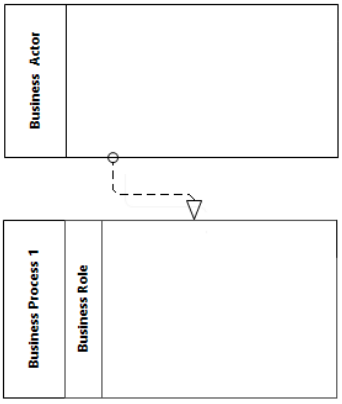
Posibles Correspondencias:

a)

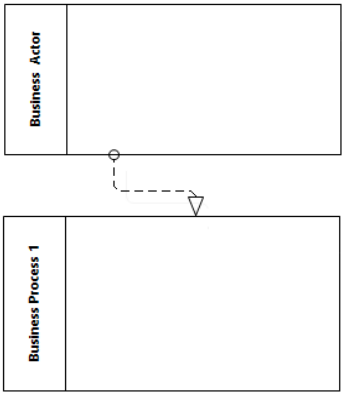
b)



c)



d)



6. Considerando la situación mostrada en la Figura 94, donde un "Business Role" está asignado a un "Business Process Complejo" y este es usado por un "Business Actor". Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

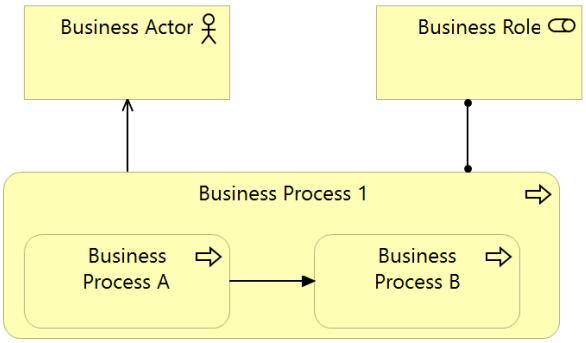
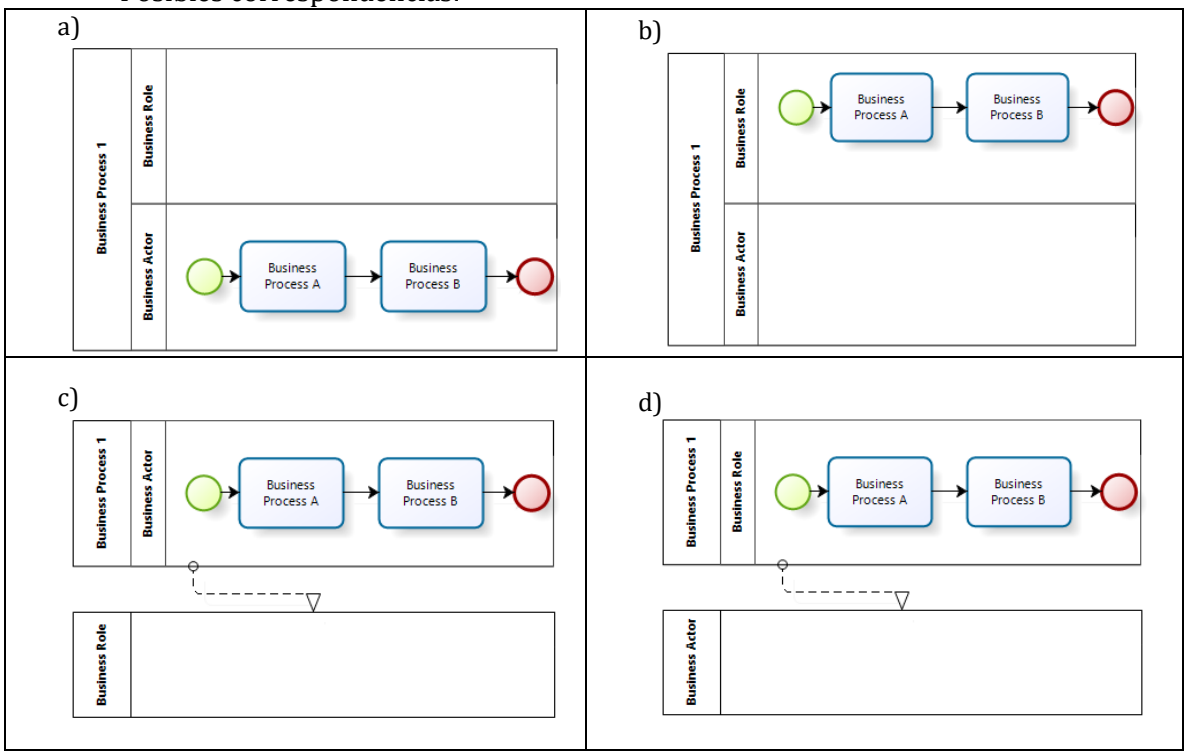


Figura 94: Situación 6

Posibles correspondencias:



7. Considerando la situación mostrada en Figura 95, donde entre dos "Business Process Simples" existe un flujo. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

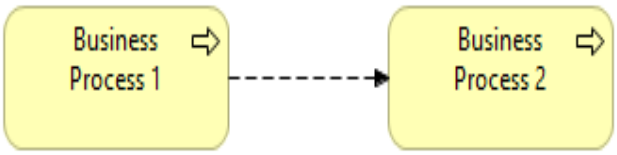
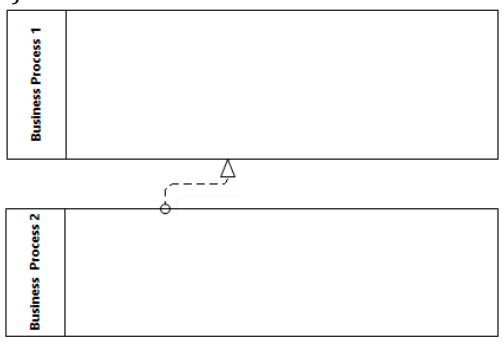


Figura 95: Flujo entre Business Process Simples

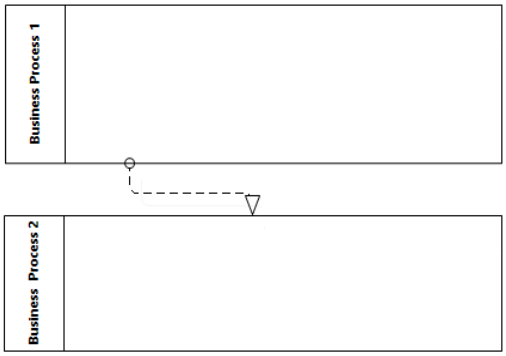
Posibles correspondencias:

a)



b)

c)



d)

8. Considerando la situación mostrada en la Figura 96 , donde existe un flujo entre dos “Business Process” de dos “Business Process Complejos” distintos. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

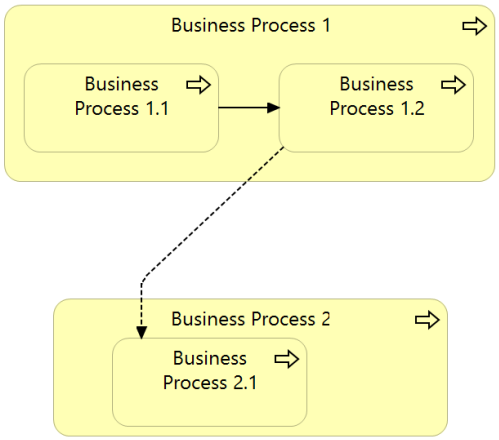
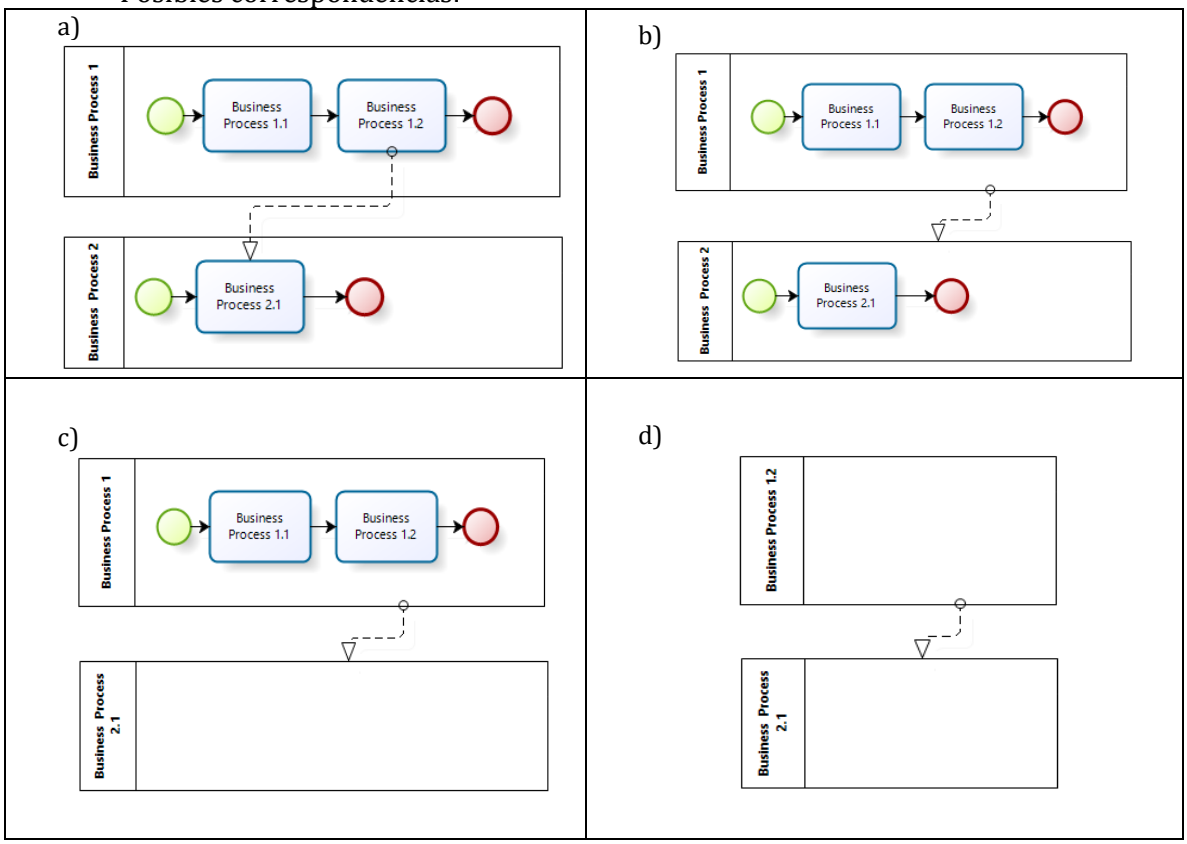


Figura 96: Situación 8

Posibles correspondencias:



9. Considerando la situación mostrada en la Figura 97, donde existe un “Business Event” entre dos “Business Process” pertenecientes a un “Business Process Complejo”. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

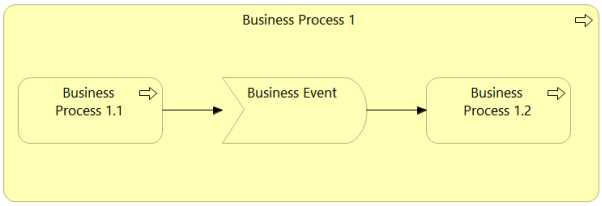
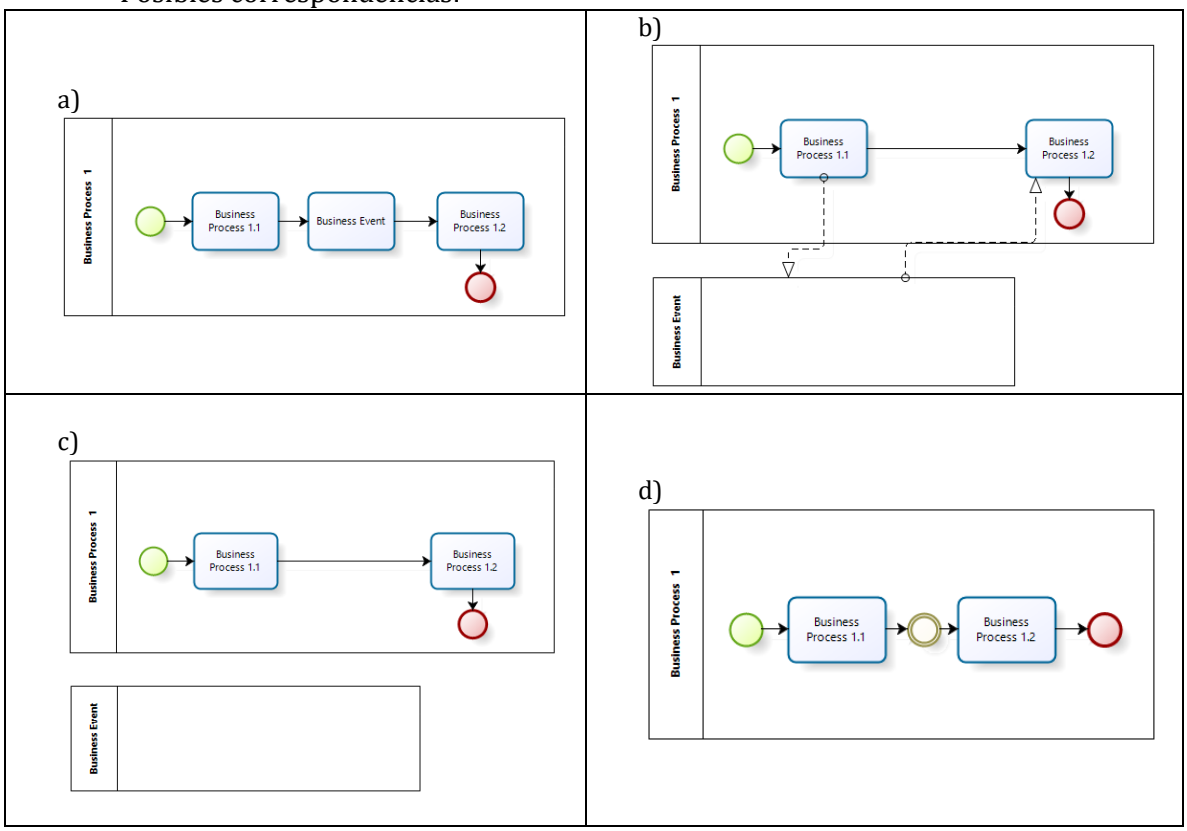


Figura 97: Situación 9

Posibles correspondencias:



10. Considerando la situación mostrada en la Figura 98, donde existe un “Business Process” que es parte de un “Business Process Complejo” y tiene acceso a un “Business Object”. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

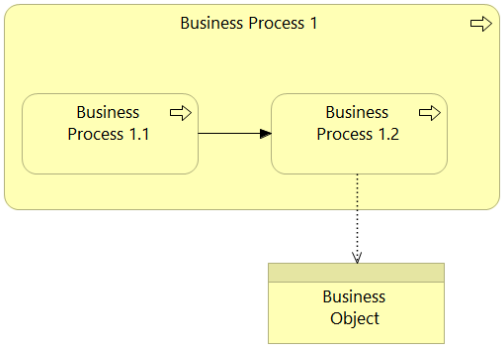
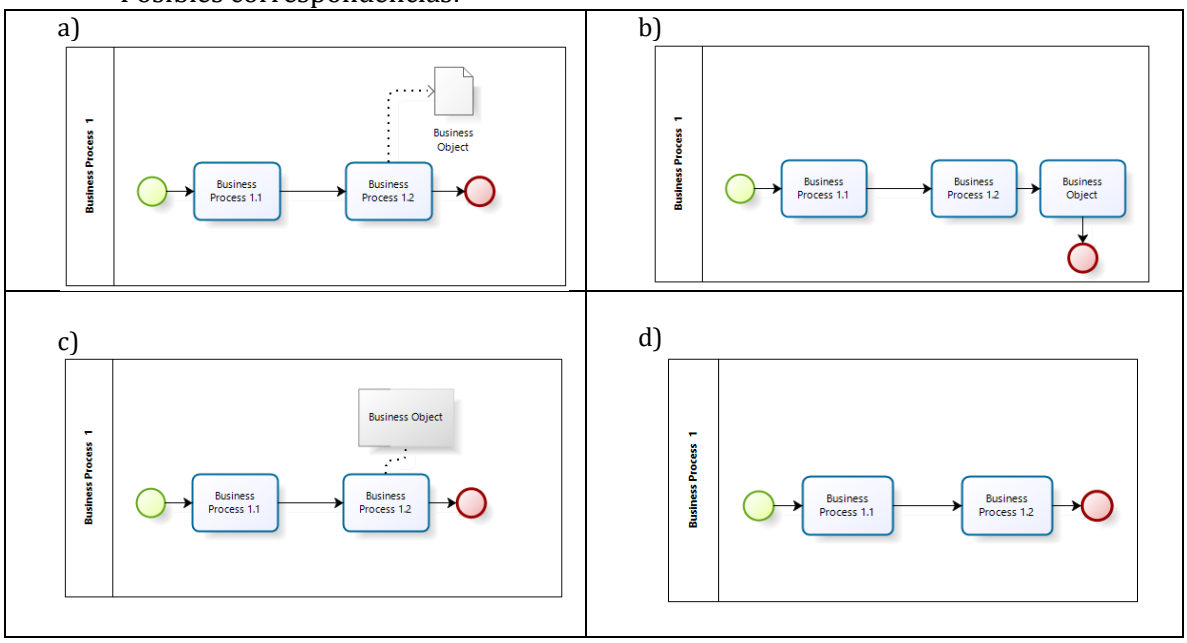


Figura 98: Situación 10

Posibles correspondencias:



11. Considerando la situación mostrada en la Figura 99, donde existe una “Union And” el cual es usado para realizar una Bifurcación. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos.

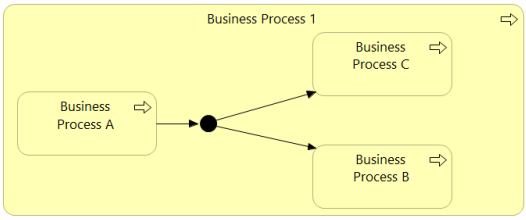
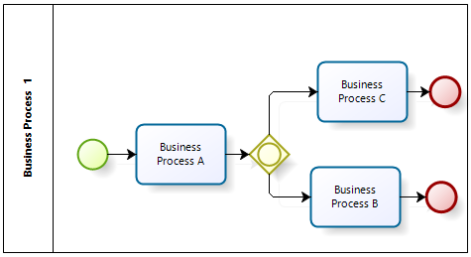


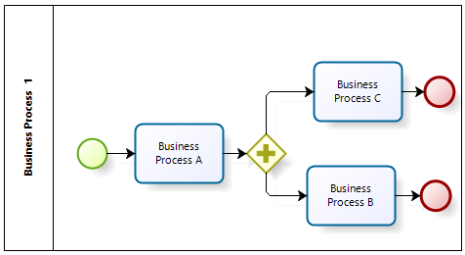
Figura 99: Situación 11

Posibles correspondencias:

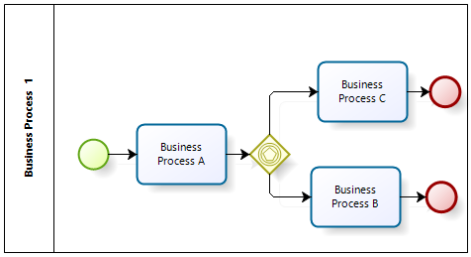
a)



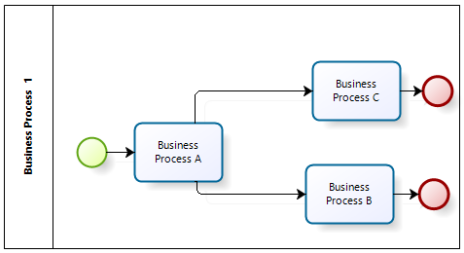
b)



c)



d)



12. Considerando la situación mostrada en la Figura 100 , donde existe un “Business Object” que realiza un “Requisito de Seguridad” y este último realiza un “Principio de Seguridad”. Según su opinión, cuál de los modelos BPMN sería su correspondencia en una transformación de Modelos

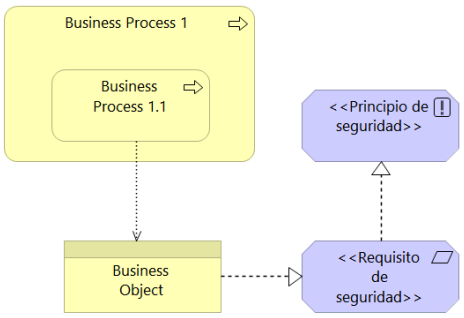
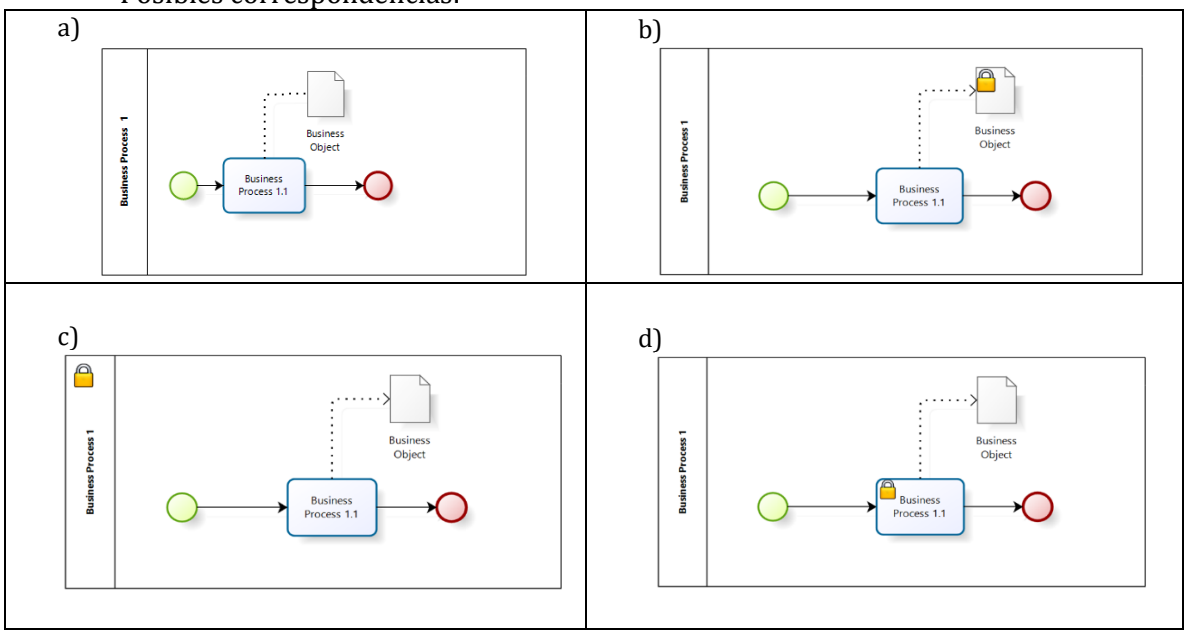


Figura 100: Situación 12

Posibles correspondencias:



II. Construcción de Modelos

1. **Transformación Modelo de Arquitectura Empresarial sin contexto:** Para la siguiente pregunta se le pide crear un "Diagrama de Proceso de Negocio con BPMN-BPSec" que usted considera es la correspondencia del "Modelo de Arquitectura Empresarial con ArchiMate" presentado a continuación en la Figura 101. Considere que existe la posibilidad de que no todo lo modelado en el Modelo con ArchiMate tiene una correspondencia en un modelo con BPMN-BPSec. El Diagrama debe ser dibujado en el área designada después de la Figura 101, si considera que no es suficiente el espacio, puede realizar el modelo en las hojas finales o al reverso indicando de alguna forma de que modelo se trata.

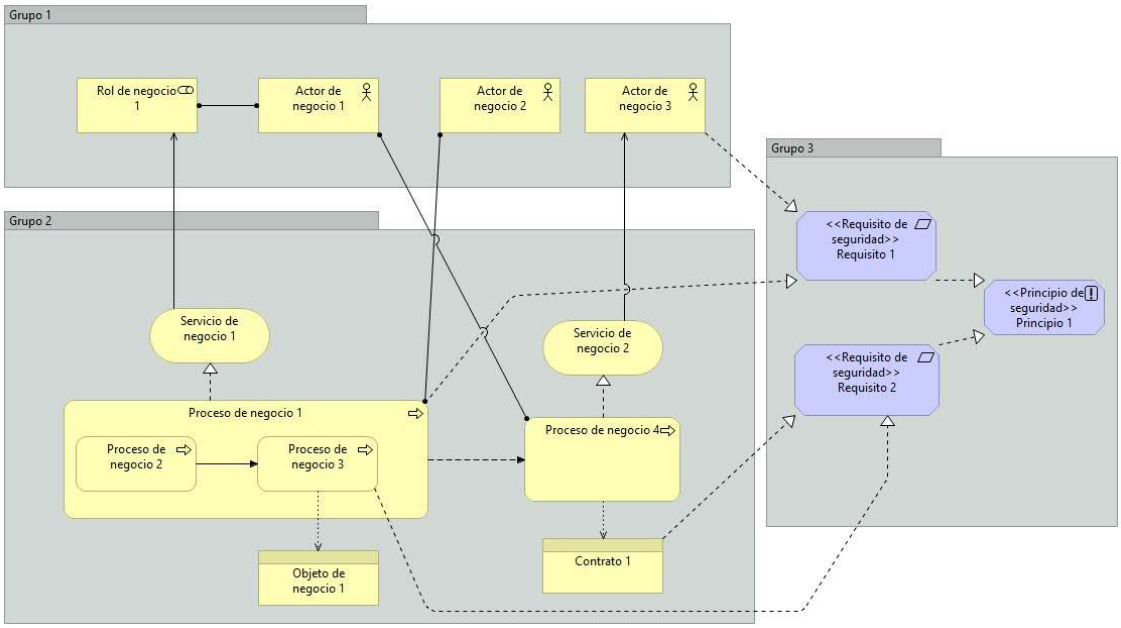


Figura 101: Modelo de AE sin contexto

2. **Transformación Modelo de Arquitectura Empresarial con contexto:** Para esta pregunta se le pide crear un "Diagrama de Proceso de Negocio con BPMN-BPSec" que usted considera es la correspondencia del "Modelo de Arquitectura Empresarial con ArchiMate" presentado a continuación en la Figura 102. Considere que existe la posibilidad de que no todo lo modelado en el Modelo con ArchiMate tiene una correspondencia en un modelo con BPMN-BPSec. El Diagrama debe ser dibujado en el área designada después de la Figura 102, si considera que no es suficiente el espacio, puede realizar el modelo en las hojas finales o al reverso indicando de alguna forma de que modelo se trata.

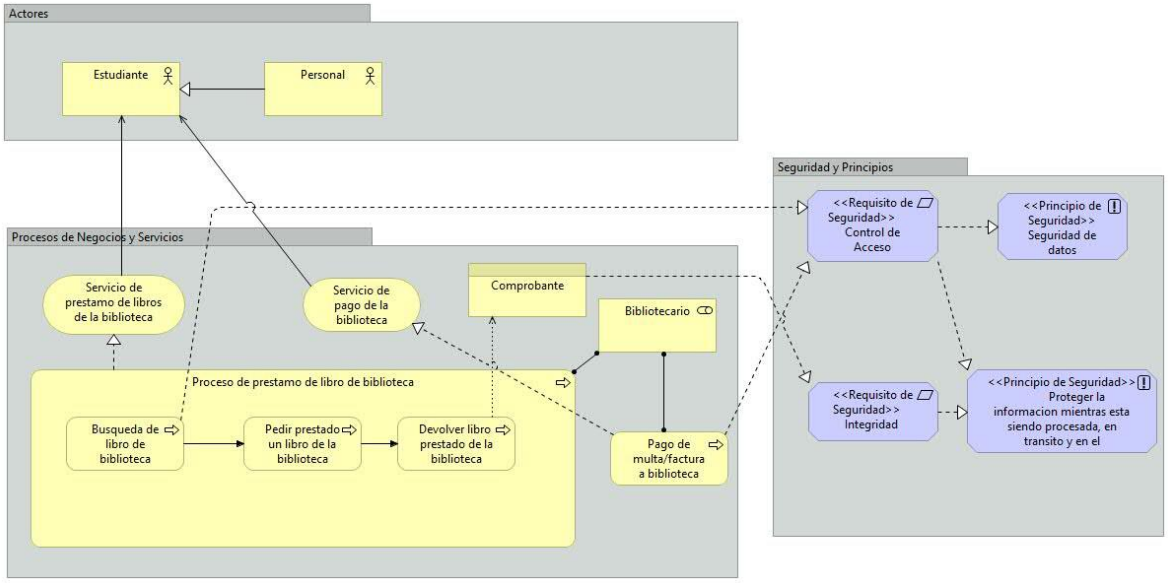


Figura 102: Modelo de AE con Contexto

III. Preguntas de opinión personal

Para las siguientes preguntas se presenta una afirmación simple sobre la correspondencia entre BPMN-BPSec e IFML o se muestra un modelo de proceso de negocio seguro modelado con BPMN-BPSec y a continuación su posible representación en un modelo IFML. También en este último caso, para una mayor comprensión se muestra un modelo de interfaz de usuario usando modelos Mockup que representa lo mismo que el modelo IFML. Se pide que se responda si está de acuerdo o en desacuerdo con las afirmaciones o con las representaciones propuestas. Para responder encierre en un círculo o destaque de alguna forma la alternativa elegida.

1. **Representación:** En la Figura 103 se muestra un modelo BPMN-BPSec donde existe una actividad con un requisito de control de acceso. En la Figura 104 se muestra una posible correspondencia en un modelo IFML para la actividad con control de acceso, donde se indica que se aplica un control de acceso a través de un Login justo antes de la interfaz de usuario correspondiente a la actividad. Y en la Figura 105 se muestra una representación de la interfaz de usuario usando modelos Mockup. Se debe tener en cuenta que se considera un logout solo en este caso y no en los siguientes ya que complica el modelo y no es lo importante.

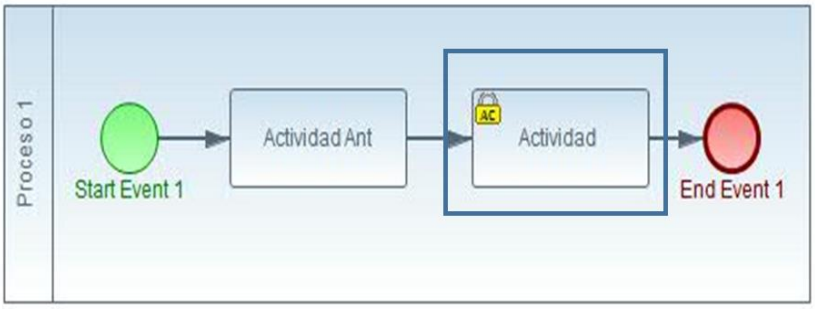


Figura 103: Modelo BPMN-BPSec con una actividad con control de acceso

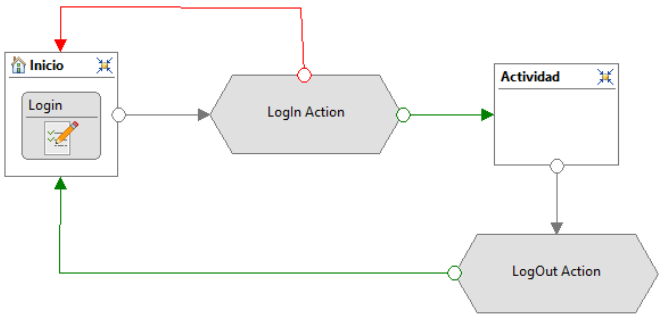


Figura 104: Modelo IFML correspondencia de una actividad con control de acceso

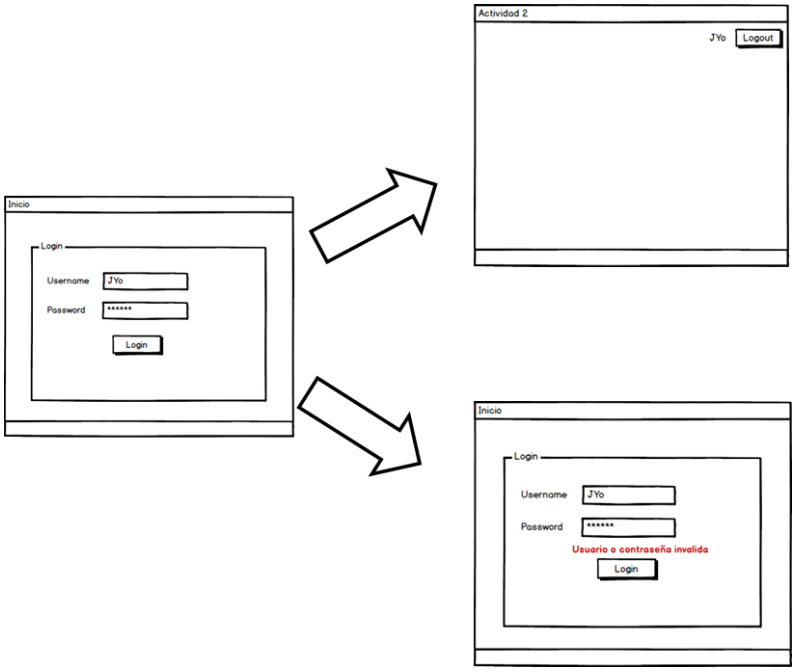


Figura 105: Modelo de una actividad con control de acceso usando Mockup

Alternativas:

a) De acuerdo
b) En desacuerdo

2. **Afirmación:** En la Figura 106 se muestra un modelo con BPMN-BPSec donde un Lane tiene un requisito de control de acceso. Bajo este caso se considera que la correspondencia a un modelo IFML sigue el mismo patrón de la pregunta anterior, con la diferencia que el control de acceso se aplica antes de iniciar la primera actividad perteneciente al Lane.

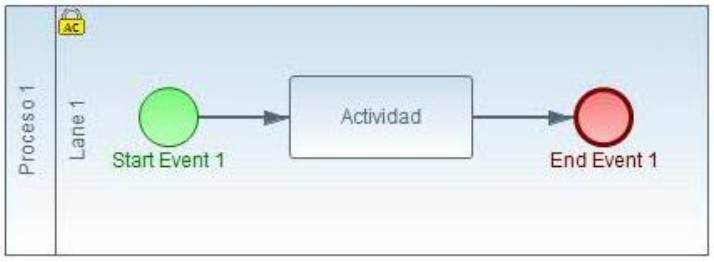


Figura 106: Modelo BPMN-BPSec con un Lane con control de acceso

Alternativas:

a) De acuerdo
b) En desacuerdo

3. **Representación:** En la Figura 107 se muestra un modelo con BPMN-BPSec donde un Pool tiene un requisito de control de acceso y este Pool tiene más de un Lane. En la Figura 108 se muestra una posible correspondencia en IFML del Pool con control de acceso, donde se produce el control de acceso a través de un login al inicio de todo el proceso y producto de la autorización del usuario (participante) representado por los Lane's, el flujo se divide hacia la primera actividad de cada Lane (cada bifurcación en el flujo representa un Lane). Y en la Figura 109 se muestra una representación de la interfaz de usuario usando modelos Mockup.

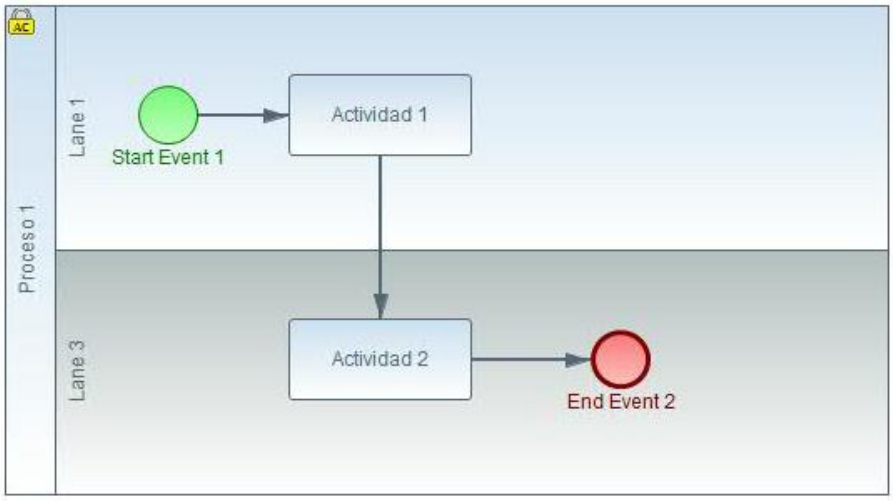


Figura 107: Modelo BPMN-BPSec con un Pool con control de acceso

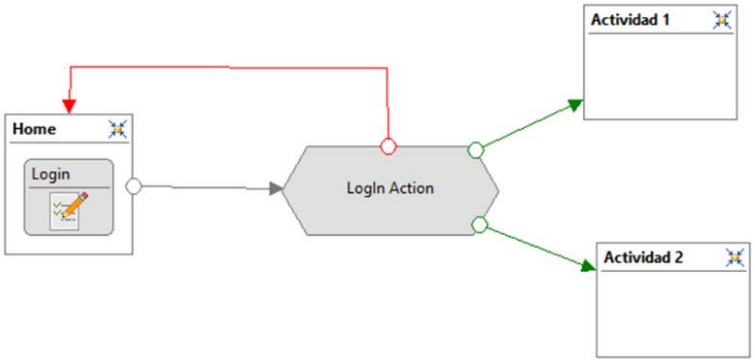


Figura 108: Modelo IFML correspondencia de un Pool con control de acceso

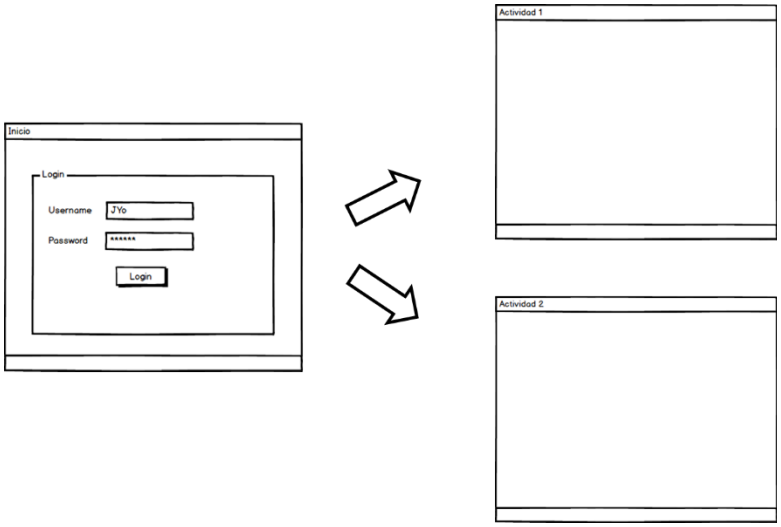


Figura 109: Modelo de interfaz de usuario de Pool con control de acceso usando Mockup

Alternativas:

a) De acuerdo
b) En desacuerdo

4. **Afirmación:** En los casos de las Figura 110 y Figura 111 se presenta un Group con control de acceso en dos situaciones distintas, en la primera el Group afecta solo a un Lane y la segunda afecta a dos Lanes. Se considera que en el primer caso se requiere realizar el control de acceso a través de un login antes de la representación de la primera actividad del Group. Para el segundo caso el control de acceso se debe realizar en por separado antes de la primera actividad del Group en cada Lane.

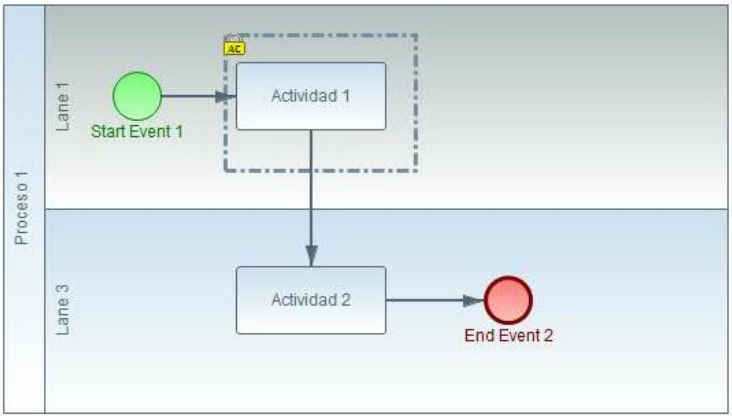


Figura 110: Modelo BPMN-BPSec con un Group con control de acceso en un Lane

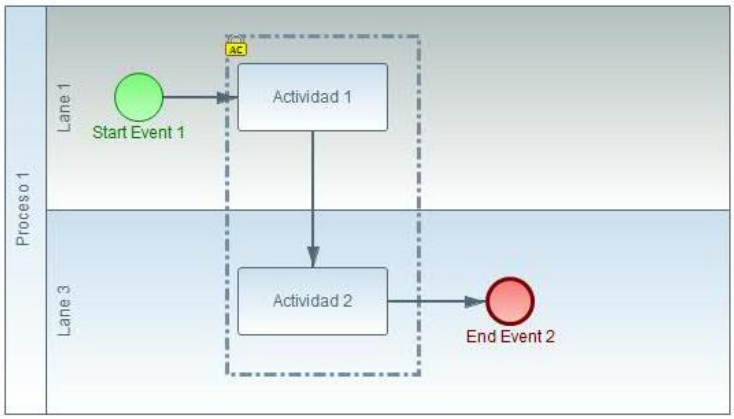


Figura 111: Modelo BPMN-BPSec con un Group con control de acceso en dos Lane's

Alternativas:

a) De acuerdo
b) En desacuerdo

5. **Afirmación:** Considerando que un control de acceso se aplica sobre un Objeto de Dato, se considera que el control de acceso a través de un login se debe realizar antes de visualizar el objeto de dato.

   Alternativas:

   a) De acuerdo
   b) En desacuerdo