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

Obtención de artefactos UML a partir del uso de Procesos de Negocio Seguros y Patrones de Seguridad

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN CIENCIAS DE LA COMPUTACIÓN

AUTOR

Matías Alexis A. Zapata Barra.

PROFESOR GUIA

Dr. Alfonso Enrique Rodríguez Ríos.

CHILLÁN, 2016

Agradecimientos

Me gustaría que estas líneas sirvieran para expresar mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización del presente trabajo, en especial al Dr. Alfonso Rodríguez Ríos, director de esta investigación, por la orientación, el seguimiento y la supervisión continúa de la misma, pero sobre todo por la motivación y el apoyo recibido a lo largo de estos años.

Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibidos de las personas más cercanas a mí.

A todos ellos, muchas gracias.

Resumen

La incorporación de conceptos de seguridad dentro de los modelos de procesos de negocio, ha resultado ser una contribución al ciclo de desarrollo de software, pues permite capturar tempranamente aspectos de seguridad que serán implementados en etapas posteriores. Una manera de complementar la información en lo que respecta a la seguridad incorporada en un proceso de negocio, es vincular dichos requisitos con patrones de seguridad, teniendo en cuenta la importancia de estos últimos en el proceso de desarrollo de software. En esta Tesis de Magister se aborda la transformación de requisitos de seguridad expresados en Procesos de Negocio usando BPMN-BPSec, hacia clases UML, proponiendo un método para generar Clases de Análisis utilizando Patrones de Seguridad, considerando como punto de inicio la especificación de un Proceso de Negocio Seguro.

Summary

The incorporation of security concepts within the business process models has proven to be a contribution for the software development. It allows early captures of security aspects that will be introduced in later stages. One way of complementing the information concerning the built-in security in a business process is to link these requirements with security standards. This Master´s degree thesis addresses the transformation of security requirements expressed in business process using BPM-BPsec, to types of UML classes, suggesting a method to generate types of analysis using security patterns, considering as a starting point the specification of a safe business process.

Índice General

Índice Tablas

Índice Figuras

Capítulo 1

Introducción

1 INTRODUCCIÓN

La ausencia de tecnología, ya sea de herramientas o mecanismos necesarios para brindar soporte al desarrollo de software, es uno de los principales factores de vulnerabilidad y debilidades de los sistemas en general (Solinas *et al.,* 2009). Por otro lado, el desarrollo de las organizaciones trae consigo un incremento de la vulnerabilidad, pues aumenta el número de intentos de ataque, y lo más probable, es que tarde o temprano uno de los ataques realizados tenga éxito (Quirchmayr, 2004). Consecuentemente, la seguridad no puede ser considerada como un objetivo independiente, motivo por el cual, las organizaciones deben coordinar, desplegar y orientar muchas de sus capacidades esenciales para alcanzar soluciones que brinden soporte a la seguridad desde una perspectiva deseada. Una manera de tratar el problema de la seguridad, es incluirla tempranamente en los modelos de Proceso de Negocio (Basin *et al.,* 2006; Herrmann & Herrmann, 2006; Jürjens, 2002; Mülle *et al.,* 2011; Rodríguez *et al.,* 2006, 2007; Wolter *et al.*, 2008). Específicamente, se trata de incluir requisitos de seguridad en las especificaciones de procesos de negocio, dando origen al concepto de Proceso de Negocio Seguro (SBP por sus siglas en ingles Secure Business Process). La descripción de un SBP puede ser utilizada dentro de un proceso de construcción de software seguro y una perspectiva interesante es vincular aspectos de seguridad del software, con Patrones de Seguridad, ya que estos representan las mejores prácticas y experiencia de los expertos a fin de detener o limitar ataques. Materializan mecanismos a fin de brindar soporte para proteger la confidencialidad, integridad y disponibilidad de los datos dentro de un sistema (Schumacher *et al.,* 2013).

Las transformaciones desde un Proceso de Negocio Seguro especificado con BPMN-BPSec (Rodríguez *et al.*, 2007), hacia un Diagrama de Clases UML han sido tratadas por Rodríguez *et al.* (2010). Siguiendo con la idea de evolucionar modelos (Mellor *et al.,* 2002), en esta Tesis de Magister se busca vincular la especificación temprana de requisitos de seguridad con Patrones de Seguridad, tomando como punto de partida la descripción de un Proceso de Negocio con especificaciones de seguridad, para luego generar artefactos útiles para el desarrollo de software que incluyan dichas especificaciones, a partir de la selección y adecuación de Patrones de Seguridad.

1.1 HIPÓTESIS Y OBJETIVOS

Partiendo de la premisa de que a nivel de Proceso de Negocio (BP) los principales involucrados (clientes, usuarios finales o analistas de negocios) son capaces de expresar necesidades/requisitos de seguridad existentes dentro del proceso (Lopez

et al., 2005), se cree que es factible que, a partir de estos requisitos se puedan seleccionar Patrones de Seguridad, los que consideran las mejores prácticas, que permitan traducir estas especificaciones en diagramas de clases UML. Así, la hipótesis fundamental detrás de esta propuesta de investigación, es la siguiente:

> Es factible, considerando como punto de partida la descripción de un Proceso de Negocio con especificaciones de seguridad, generar artefactos que puedan ser utilizados dentro del proceso de desarrollo de software, los cuales incluyan seguridad, a partir de la selección y adaptación de Patrones de Seguridad.

Se considerarán las especificaciones de seguridad realizadas a través de *BPMN-BPSec* (Rodríguez *et al.*, 2007), con la cual es posible especificar requisitos de seguridad dentro de BPMN, los cuales serán analizados con el objeto de generar diagramas de clases UML utilizando para ello patrones de seguridad de arquitectura, diseño e interfaz. En la Figura 1.1 se muestra a grandes rasgos lo que se plantea como propuesta de investigación.

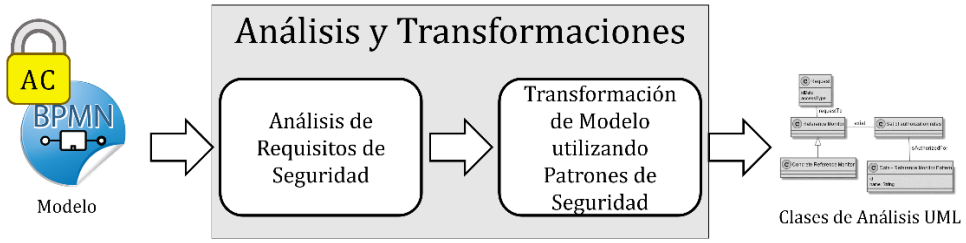


Figura 1.1 - Propuesta - Transformación a través de ATL.

El objetivo que se busca con esto queda expresado como:

> Definir un método que permita generar artefactos, Diagramas de Clases UML, que puedan ser utilizados dentro del proceso de creación de software, a partir de una especificación de Proceso de Negocio Seguro y la selección de Patrones de Seguridad para generar dichas clases.

Como se verá en la Sección 4, se ha creado un método con el cual es posible interpretar los Requisitos de Seguridad dentro de los Procesos de Negocio, seleccionando en primera instancia, Patrones de Seguridad que cumplan con los requisitos especificados. Con lo anterior, se crea un artefacto que brinda soporte en las primeras fases del ciclo de

desarrollo de software, específicamente en las fases de Inicio y Elaboración con respecto al Modelado del Negocio sobre el Proceso Racional Unificado (Kruchten, 2004) (RUP, Rational Unified Proccess)

1.2 ORGANIZACIÓN DE LA TESIS DE MAGISTER

Esta Tesis de Magister se organiza de la siguiente manera:

Capítulo 2. Conceptos Relacionados. Se presentan las definiciones y elementos que se relacionan con esta tesis.

Capítulo 3. Estado del Arte. Se muestran detalle de los principales trabajos que se relacionan con el uso de Patrones de Seguridad en procesos de negocio, considerando especificaciones de seguridad en sus modelos. También se abarcaron trabajos que utilicen patrones de cualquier otro tipo dentro de los procesos de negocio, con el objeto de extraer ideas que puedan ser utilizadas en este trabajo.

Capítulo 4. **Transformación de Modelos utilizando Patrones de Seguridad**. Se muestra la metodología propuesta para la selección y adaptación de Patrones de Seguridad a partir de un modelo de Procesos de Negocio Seguro, proponiendo directrices para la selección de manera automatizada.

Capítulo 5. **Prototipo SecBP&P – Tool**. Se describen los detalles del prototipo que soporta la metodología propuesta.

Capítulo 6. Validación. Se muestran los resultados de una encuesta realizada, con el objeto de comprobar si un modelo generado por nuestra propuesta mejora el nivel de entendimiento percibido por los usuarios.

Capítulo 7. Conclusiones. Se da a conocer el cumplimiento de los objetivos propuestos en esta tesis.

Capítulo 2

Conceptos Relacionados

2 CONCEPTOS RELACIONADOS

En este capítulo se darán a conocer los principales conceptos utilizados en esta tesis. Para lo anterior, se ha definido la siguiente estructura; en la sección 2.1 se describen los Procesos de Negocio, la sección 2.2 corresponde a los Procesos de Negocio Seguro, en la sección 2.3 se describen los Patrones de Seguridad y finalmente, en la sección 2.4 se presenta el lenguaje de trasformación de modelos llamado Atlas Transformation Language (ATL).

2.1 PROCESOS DE NEGOCIO

Un Proceso de Negocio (BP, *Business Process*) es un conjunto de tareas y/o actividades que se relacionan lógicamente para lograr como resultado, la representación de un negocio definido (Muehlen, 2002). Cada Proceso de Negocio tiene sus entradas, funciones y salidas. Las entradas son requisitos que se deben tener antes de que una función pueda ser aplicada y cuando una función es aplicada, se obtienen las salidas o resultados. Champy y Hammer (1994), definen un BP como "*una colección de actividades que toma uno o más tipos de entrada y crea una salida, la cual es de gran valor para el cliente*". Por otro lado, Davenport (2013) define los BP como "*un proceso estructurado y un conjunto de actividades diseñadas, produciendo una salida determinada para un cliente o mercado específico".*

Actualmente dentro de las organizaciones, un objetivo importante es el modelado de la información de sus BP, el monitoreo y mejora continua de los mismos (Delgado, 2007). Junto con esto aparece la necesidad de contar con lenguajes y herramientas para crear este tipo de modelos, además de diseñar e implementar dichos procesos, con el objeto de cubrir las necesidades de la empresa. Para satisfacer dichas necesidades, existe Business Process Model and Notation (BPMN) (OMG, 2015), la cual es una notación gráfica que describe la lógica de los pasos de un BP, la que permite que cualquier persona con cierto conocimiento mínimo del negocio, pueda interpretar los diagramas BPMN con facilidad.

Por otra parte la propuesta de Gestión de Procesos de Negocio (BPM, *Business Process Management*) está orientada a optimizar los Procesos de Negocio a través de la automatización, integración, monitoreo y optimización de forma continua de dichos procesos (Van Der Aalst *et al.,* 2003).

Desde el punto de vista de la Ingeniería de Software, se han presentado varias iniciativas para incluir el modelado de los BP dentro de un ciclo de desarrollo de software. Particularmente, RUP (Kruchten, 2004), propone desarrollar actividades

para obtener entregables relacionados con el modelado de los BP. También se plantea utilizar dicho modelado, para comprender la estructura y dinámica de la organización que requiere el desarrollo de algún sistema, con el objeto de que tanto clientes, usuarios finales y desarrolladores posean un entendimiento común sobre el objetivo de la empresa, comprendiendo así, los problemas para finalmente obtener los requisitos del sistema (Delgado, 2007).

2.2 SEGURIDAD EN PROCESOS DE NEGOCIO

Las organizaciones poseen diferentes perspectivas en cuanto a la seguridad que subyace en los sistemas de información y cada una de estas vistas posee diferentes requisitos. No obstante, al considerar un alto grado de abstracción, todos los sistemas tienden a poseer los mismos tipos básicos de activos valiosos y potenciales vulnerabilidades de los mismos (Firesmith, 2004).

En la literatura existe una propuesta que permite identificar estos requisitos de seguridad, descompuestos como sub factores de calidad, donde se incluyen conceptos de seguridad en forma genérica (Firesmith, 2004). Dichos factores y sub factores de seguridad son mostrados en la Figura 2.1.

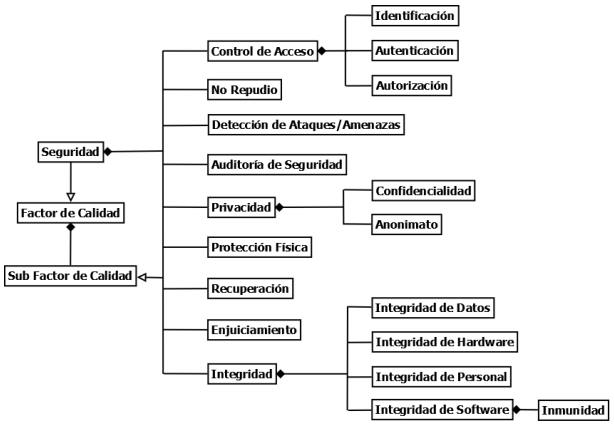


Figura 2.1 - Factores y sub factores de calidad de la seguridad (Firesmith, 2004).

Aunque incorporación de la seguridad en procesos de negocio ha sido tratada por diferentes autores (Basin *et al.*, 2006; Herrmann & Herrmann, 2006; Jürjens, 2002; Mülle *et al.*, 2011; Rodríguez *et al.*, 2006, 2007; Wolter *et al.*, 2008), en esta Tesis de Magister utilizaremos la propuesta presentada por Rodríguez *et al.* (2007) en que se considera una extensión del Diagrama de Procesos de Negocio de BPMN (OMG, 2015) que permitan representar aspectos de seguridad. En esta extensión se incorporan estereotipos asociados a requisitos de seguridad posibles de representar en la descripción de un BP transformando dicho proceso en un Proceso de Negocio Seguro

(SBP, Secure Business Process). También se ha elegido esta propuesta debido a que en trabajos posteriores, han obtenido desde diagramas de Clases UML a partir de un SBP (Rodríguez *et al.*, 2010). En la Figura 2.2 se muestra el metamodelo de BPSec en que se individualizan los requisitos de seguridad posibles de representar a través de BPMN-BPSec (Rodríguez *et al.*, 2007).

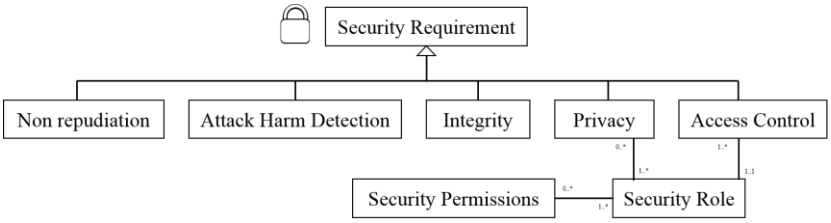


Figura 2.2 – Requisitos de Seguridad y su notación asociada (Rodríguez *et al.*, 2007).

En la extensión, los requisitos de seguridad se relacionan con los elementos de BPMN de acuerdo a lo que se muestra en la Tabla 2.1.

	Pool	Lane	Group	Activity	Message Flow	Data Object
No Repudiación					***X***	***X***
Detección de Ataques/Amenazas	***X***	***X***	***X***	***X***	***X***	***X***
Integridad					***X***	***X***
Privacidad	***X***	***X***	***X***			
Control de Acceso	***X***	***X***	***X***	***X***		
Roles de Seguridad	***X***	***X***	***X***			
Permisos de Seguridad				***X***	***X***	***X***

Tabla 2.1 – Requisitos de Seguridad y elementos de BPD (Rodríguez *et al.*, 2007).

A continuación se muestra una descripción más detallada de los requisitos de seguridad, acompañada de su representación gráfica.

- No Repudiación 

: establece la necesidad de evitar la denegación de cualquier aspecto de la interacción del diagrama. Desde la perspectiva del analista de negocios, el requisito No Repudiación representa la necesidad de proteger una determinada interacción, de manera que minimice los potenciales problemas. Desde la perspectiva de seguridad, esta especificación implica la generación de roles de seguridad.

- Detección de Ataques/Amenazas 

: se define como la detección, registro y notificación de una acción de ataque y/o amenaza, ya sea que tenga éxito o fracase. Desde la perspectiva del analista de negocios, este requisito representa una señal de atención sobre los elementos en que se indica. Desde el punto de vista de la seguridad, esta especificación implica mantener un registro de los eventos (ataques y/o amenazas) ocurridos sobre elementos potencialmente vulnerables.

- Integridad 

: establece el grado de protección de una corrupción. Esto quiere decir que el elemento en el que se especifica tiene que estar protegido de los ataques mal intencionados y no autorizados. La integridad se especifica en los objetos de datos y flujos de mensajes, y la letra *x* representa el grado de protección, el cual puede ser ***l*** (low), ***m*** (médium) y ***h*** (high).

- Privacidad 

: está relacionada con condiciones de protección de la información acerca de un determinado individuo o entidad, limitando el acceso a partes no autorizadas para obtener información sensible. Desde el punto de vista del analista de negocios, la especificación de privacidad implica la no revelación (confidencialidad) y no almacenaje (anonimato) de la información acerca de un determinado rol. Desde el punto de vista de la seguridad, la especificación de privacidad con confidencialidad implica proteger la información acerca de un rol para que no sea develada a terceros. Cabe destacar, que la letra *x* representa el tipo de privacidad, la cual puede tomar el valor ***a*** (anonimato) y ***c*** (confidencialidad).

- Control de Acceso 

: corresponde a la limitación de acceso a recursos sólo a usuarios autorizados. La especificación de este requisito por parte del analista de negocios implica la limitación de acceso a un conjunto de recursos que son valorados como importantes de ser protegidos de manera especial. Desde la perspectiva de la seguridad, esta especificación supone la definición de roles que pueden ser asignados a personas, entidades, programas, dispositivos u otros sistemas, y la definición de permisos para acceder a los objetos que se encuentran en el ámbito de la especificación de control de acceso.

- Roles de Seguridad: contiene la especificación de un rol de seguridad. Se relaciona con todos los requisitos de seguridad y con el registro de auditoría.

- Permisos de Seguridad: contiene las especificaciones de permisos relacionadas con especificaciones de control de acceso. Un permiso debe contener el nombre del objeto y las operaciones permitidas.

Con BPMN-BPSec, el analista de negocios podrá expresar requisitos de seguridad desde su propio punto de vista, considerando el contexto del proceso de negocio.

2.3 PATRONES DE SEGURIDAD

Aunque existe alguna discrepancia entre los investigadores a la hora de definir qué es un patrón, es posible coincidir en que un patrón es una idea que ha sido utilizada en un contexto práctico y que probablemente será útil en otros (Fowler, 1997). Dentro de la ingeniería de software, los patrones comenzaron siendo planteados de forma general para todas las disciplinas, por lo que inicialmente se le conoció sólo como patrón de diseño. No obstante, los patrones constituyen un concepto más general, representando estructuras conceptuales aplicables durante todas las fases del proceso de desarrollo (Bonillo, 2006).

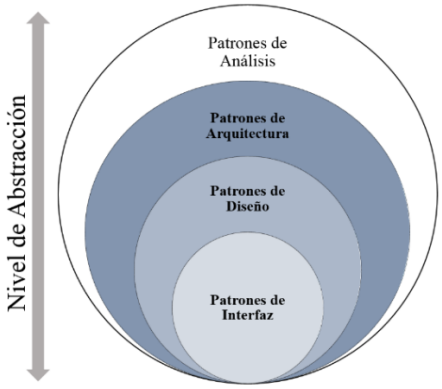


Figura 2.3 - Taxonomía de Patrones (Bonillo, 2006).

Una taxonomía de los patrones, en general, se muestra en la Figura 2.3. En ella es posible distinguir los siguientes niveles de patrones (Bonillo, 2006), a saber:

- **Patrones de análisis:** grupos de conceptos que forman parte de una construcción común en el mundo del modelado conceptual, son relevantes a un dominio o pueden ser adaptados a otros. Visión más conceptual y estructural, identificando la naturaleza de las situaciones.
- **Patrones de arquitectura**: esquemas fundamentales de la organización de un sistema, identificando una serie de subsistemas y sus respectivas responsabilidades.

- **Patrones de diseño:** nivel de abstracción menor que los de arquitectura, es decir, más próximos al código. Su uso no refleja la estructura global del sistema como tal.
- **Patrones de interacción/interfaz**: soluciones exitosas a problemas relacionados con la interfaz de usuario. Forman un medio de comunicación expresado en notación sencilla, para ser entendida por el equipo de diseño.

En esta tesis nos centraremos en los patrones de seguridad. La definición de patrones de seguridad no varía notablemente de la definición de patrón y corresponde a "*la descripción de un problema de seguridad recurrente y particular, el cual surge en contextos específicos y presentar una solución de forma genérica que ha sido probada para dicho problema*" (Schumacher *et al.,* 2013). Los patrones de seguridad también puede ser definidos como un paquete de información valiosa y reutilizable que incorpora conocimiento de expertos en el área, brindando ayuda a personas con menos experiencia (Yoshioka *et al.,* 2008).

En la literatura, existe una amplia gama de Patrones de Seguridad dependiendo del contexto del problema. En esta Tesis de Magister nos centraremos en primera instancia sobre los Patrones de Seguridad recopilados por Schumacher *et al.* (2013), enfocándonos en los niveles de diseño, arquitectura e interfaz, teniendo sólo en cuenta los Patrones de Seguridad orientados al Control de Acceso.

A continuación se muestra una descripción general de los diferentes Patrones de Seguridad orientados al Control de Acceso.

2.3.1 PATRONES DE SEGURIDAD ORIENTADOS A MODELOS DE CONTROL DE ACCESO

- **Autorización**: este patrón describe quién está autorizado para ingresar a ciertos recursos de un sistema, indicando para cada entidad activa (generalmente representada por usuarios o procesos), a qué recursos puede acceder y cómo le es posible acceder a ellos.
- **Control de Acceso Basado en Roles:** describe cómo se asignan los derechos de acceso, en base a las funciones o tareas que debe realizar cada entidad dentro del sistema.
- **Seguridad Multinivel:** este patrón describe como se diferencia la información en categorías, dependiendo de *sensibilidad* de la misma y para evitar la *divulgación* de esta. También describe como asignar autorización a los usuarios sobre los datos.

- **Monitor de Referencia:** este patrón hace cumplir las políticas de acceso a los datos y/o recursos cuando una entidad activa realiza una petición para acceder a dicho recurso.

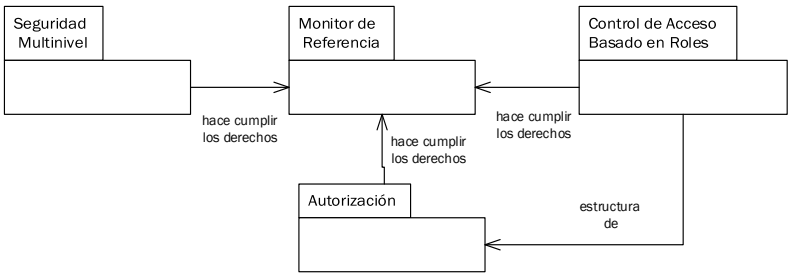


Figura 2.4 - Patrones de Seguridad - Modelo de Control de Acceso (Schumacher *et al.*, 2013).

La Figura 2.4 muestra la relación existente entre los Patrones de Seguridad descritos anteriormente. A pesar de que no se puede apreciar la estructura interna de cada patrón, se puede ver claramente que los patrones no son de uso exclusivo, es decir, pueden ser utilizados de manera conjunta con el objeto de que se complementen entre sí.

2.3.2 PATRONES DE SEGURIDAD ORIENTADOS A ARQUITECTURAS DE CONTROL DE ACCESO

- **Único Punto de Acceso:** este patrón describe la necesidad de proveer un acceso a un sistema, un usuario, un proceso, etc., que sea externo al sistema, además se requiere proteger al mismo sistema, de daños o usos indebidos de información y/o recursos. Para lo anterior se define un único punto de acceso que garantice o prohíba la entrada al sistema cuando se requiera.
- **Punto de Control:** este patrón implementa un mecanismo eficaz de identificación y autorización de los agentes entrantes.
- **Sesión de Seguridad**: este patrón propone establecer una única referencia hacia un objeto de sesión, en lugar de pasar todos los derechos de acceso o volver a autenticar a un usuario en varias ocasiones.
- **Acceso Total con Errores:** este patrón ofrece una vista de la máxima funcionalidad del sistema, pero arroja un error cuando un usuario intenta utilizar una función a la que no está autorizado.
- **Acceso Limitado:** este patrón guía a los desarrolladores a mostrar sólo las funciones que actualmente están disponibles para los derechos de un usuario, ocultando todas las funcionalidades a las cuales no tiene acceso.

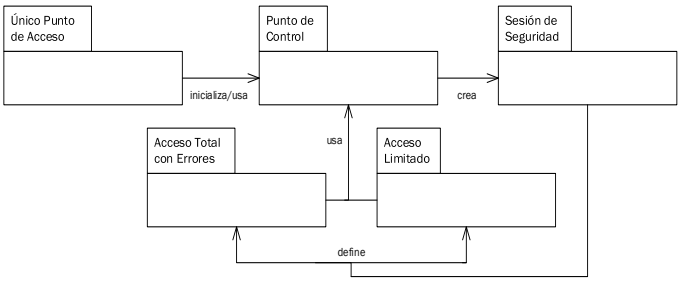


Figura 2.5 Patrones de Seguridad – Arq. de Control de Acceso (Schumacher *et al.*, 2013).

La Figura 2.5, al igual que la figura anterior, muestra sólo la relación existente entre los Patrones de Seguridad descritos anteriormente.

2.4 ATLAS TRANSFORMATION LANGUAGE (ATL)

Atlas Transformation Language es un lenguaje de transformación de modelos. Fue desarrollado como parte de la plataforma AMMA (ATLAS Model Management Architecture) y es clasificado como un lenguaje de transformación híbrido, que combina constructores tanto declarativos como imperativos (López *et al.*, 2009).

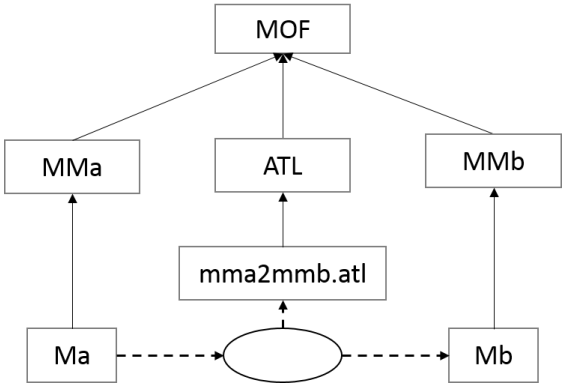


Figura 2.6 - Esquema de enfoque de ATL (López *et al.*, 2009).

La Figura 2.6 muestra la metodología utilizada para realizar las transformaciones de modelos en ATL. Básicamente la definición de la transformación está escrita en ATL (representada por mma2mmb.atl), donde la misma, puede ser vista como un modelo. Por otro lado, los modelos tanto de origen, destino y su transformación, están basados en sus metamodelos MMa, MMb y ATL, respectivamente.

Capítulo 3

Estado del Arte

3 ESTADO DEL ARTE

En este capítulo se mostrarán los trabajos relacionados al contexto de esta tesis. El estado del arte descrito a continuación, está basado en una revisión sistemática de la literatura, la cual se realizó bajo las directrices que propone Kitchenham y Charters (2007), las que son apropiadas para temas relacionados con la investigación dentro del área de la Ingeniería de Software, pero dicha propuesta está enfocada en un grupo de investigación, motivo por el cual se utilizará la adaptación propuesta por Caro *et al,* (2005), la que considera a un investigador que es supervisado en el desarrollo de la revisión. Como se puede apreciar en la Figura 3.1, la estructura de la revisión de la literatura utilizada, posee etapas y sub-etapas.

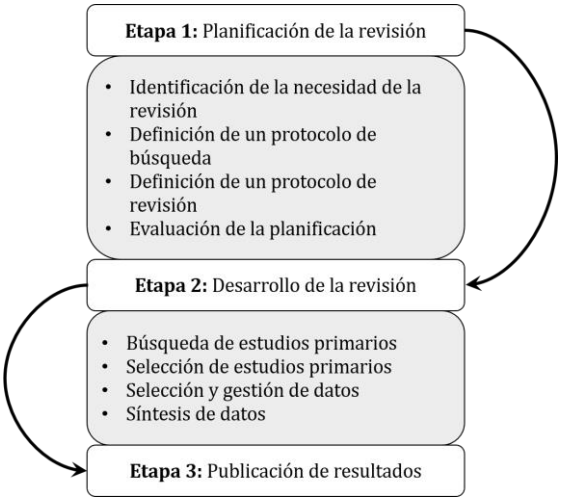


Figura 3.1 - Método de revisión adaptado por Caro *et al.* (2005).

A continuación se mostrará cómo se abarcaron las etapas presentadas en la revisión de la literatura.

3.1 ETAPA 1 – PLANIFICACIÓN DE LA REVISIÓN

Esta etapa tiene como propósito específico establecer los parámetros base, los cuales serán considerados al momento de que se lleve a cabo la revisión. Aquí se deben establecer las razones que justifican llevar a cabo la revisión, la forma en que se hará la búsqueda de trabajos y la manera en que éstos serán revisados, finalmente, se evaluará la planificación realizada.

Los estudios científicos publicados fueron identificados mediante búsquedas bibliográficas en Google Académico, SciELO, SpringerLink, Annualreviews, utilizando

las palabras claves; “security patterns”, “business process”, “secure business process”, “transformation”. El límite establecido será artículos publicados después del año 1990, por otro lado, se tomarán en cuenta solo los estudios realizados en español e inglés. También se complementará la búsqueda consultando las referencias de los artículos seleccionados. En la sección siguiente no se mostrarán los detalles de la búsqueda bibliográfica realizada, ya que como proceso se considera conocido y sólo se ha puesto atención en los resultados obtenidos.

3.2 ETAPA 2 – DESARROLLO DE LA REVISIÓN

En esta etapa se lleva a cabo la revisión propiamente dicha, el desarrollo de la misma viene guiado por la planificación previamente establecida.

Una vez que se lleva a cabo la revisión sistemática de la literatura, se obtienen estudios primarios, que luego pasarán por un proceso de refinamiento, el cual consiste en la lectura completa de los trabajos, con el objeto de extraer toda la información relevante a la propuesta de esta tesis. A pesar de que el objetivo es dar a conocer los trabajos relacionados, también se abarcaron trabajos relacionados con patrones dentro de los Procesos de Negocios, no necesariamente de seguridad, con el propósito de realizar un catastro de las principales contribuciones y dar a conocer una posible relación y/o equivalencia con Patrones de Seguridad. En las siguientes sub-secciones se mostrarán los resultados obtenidos a través de la revisión.

En la Tabla 3.1 se muestra el resumen de los resultados obtenidos al momento de realizar la búsqueda de la información, la cual se llevó a cabo entre Febrero y Agosto del 2015. Como se puede apreciar, los resultados de la base de datos SciELO y Annual Reviews no fueron significativos. Cabe destacar que sólo se seleccionaron estudios en los cuales se abordan los temas de interés desde una perspectiva genérica, es decir, no se seleccionaron trabajos en los cuales se hacía referencia a un contexto específico, como por ejemplo, patrones de seguridad en sistemas ya creados, en telecomunicaciones, etc.

Base de Datos	Combinación	Resultados	Seleccionados
Google Schoolar	"Business Process" "Security Patterns"	674	8
	"Secure Business Process" "Security Patterns"	42	1
SpringerLink	"Business Process" "Security Patterns"	328	4
	"Secure Business Process" "Security Patterns"	6	2
Scielo	"Business Process" "Security Patterns"	243	1
	"Secure Business Process" "Security Patterns"	0	0
Annualreviews	"Business Process" "Security Patterns"	0	0
	"Secure Business Process" "Security Patterns"	1	0

Tabla 3.1 – Resumen Resultados Revisión de la Literatura.

A continuación se detalla el análisis realizado para cada uno de los trabajos seleccionados.

PATRONES EN PROCESOS DE NEGOCIO CON ESPECIFICACIONES DE SEGURIDAD

Ahmed y Matulevičius (2014), proponen un método que introduce requisitos de seguridad en los procesos de negocio a través de la colaboración entre los analistas empresariales y de seguridad. Para apoyar dicha colaboración, utilizan un conjunto de patrones orientados a los riesgos de seguridad (propuestos por Khan (2012)), pero no identifica dichos patrones en el modelo, si no que los presenta explícitamente. Posterior a ello Samarütel *et al.* (2016), realizan un caso de estudio donde utilizan el método antes descrito dentro de cinco procesos de negocio provenientes de un sistema de respuesta de aviación.

PATRONES PROPUESTOS EN PROCESOS DE NEGOCIO

Bonillo (2006) propone un marco teórico referencial integral y una metodología que abarca desde el análisis de los requisitos hasta el monitoreo de los procesos, apoyando las etapas de análisis, diseño, modelado y configuración, a través del uso de patrones. La propuesta metodológica está conformada por dos macro-procesos: uno relacionado con la creación del proceso en sí mismo y otro que corresponde a la administración y comprende: el mantenimiento, administración del proceso y el monitoreo a través de indicadores de gestión. Esta propuesta sólo es un marco

teórico referencial para la inclusión de patrones a nivel de arquitectura, incluyendo conceptos de calidad, pero no muestra cómo evaluar dichos conceptos de calidad.

Forster *et al.* (2007), describen un lenguaje de patrones visuales para la representación y ejecución de las restricciones de calidad en los modelos de procesos de negocio. Las restricciones se describen formalmente a través de patrones de procesos basados en Actividades UML.

Gschwind *et al.* (2008), describen una extensión de herramienta de modelado de procesos de negocio, que permite integrar patrones, advirtiendo sobre el contexto y sus consecuencias de uso.

Schumm *et al*. (2010), presentan un meta modelo para las vistas de procesos (process views) y a su vez muestran los patrones de vistas de proceso, los cuales especifican transformaciones elementales para alterar un proceso existente. En un trabajo posterior (Schumm, Anstett, Leymann, & Schleicher, 2010), muestran cómo se pueden combinar patrones de vistas para brindar ayuda en las fases de diseño, despliegue, monitoreo y análisis de los procesos de negocio.

Schmidt y Jürjens (2011), presentan un enfoque orientado a patrones para conectar el análisis de los requisitos de seguridad con el diseño de arquitecturas seguras utilizando UMLsec. Lo que proponen es dividir el problema del desarrollo de software seguro en sub problemas más sencillos, basados en los patrones de análisis de los requisitos de seguridad.

Brambilla *et al.* (2012), presentan una metodología de diseño de procesos, con el apoyo de un conjunto de herramientas, para incluir características sociales dentro de los procesos de negocio. Básicamente se presenta un enfoque para apoyar el diseño e implementación de soluciones "Social BPMN", extendiendo el lenguaje visual de BPMN para el diseño de procesos con interacciones sociales, recogiendo los escenarios típicos de procesos de socialización en forma de patrones de diseño reutilizables.

Elgammal *et al.* (2014), presentan un framework integral para la gestión del cumplimiento de los procesos de negocio, con un enfoque de este mismo, en tiempos de diseño como un primer paso hacia el soporte preventivo del cumplimiento de los procesos de negocio. Dicho framework posee un lenguaje de especificación de cumplimiento basado en patrones, lo que facilita la especificación formal de los requisitos para el cumplimiento de los procesos de negocio, generando automáticamente las reglas de cumplimiento.

Awad *et al.* (2015), presentan un framework para el monitoreo proactivo en tiempo de ejecución de los procesos de negocio, llamado BP-MaaS, el cual incorpora una

amplia gama de patrones de cumplimiento para la especificación abstracta de las restricciones en tiempo de ejecución.

Lohrmann y Reichert (2015), describen un enfoque para la evaluación de patrones de mejora de procesos en escenarios específicos, considerando limitaciones del mundo real, tales como el papel de las partes interesadas de alto nivel o el costo de adaptación de los sistemas.

3.3 ETAPA 3 – PUBLICACIÓN DE RESULTADOS

En esta etapa se realizan las publicaciones de los resultados en donde se muestra lo obtenido por la investigación. La propuesta de esta Tesis de Magister ha sido publicada en una conferencia iberoamericana (Zapata *et al.,* 2015), en donde se han mostrado parte de los resultados obtenidos en primera instancia.

3.4 CONCLUSIÓN ESTADO DEL ARTE

En la revisión de la literatura se abarcaron trabajos en los cuales se utilizaba patrones de cualquier tipo dentro de los Procesos de Negocios, con el objeto de establecer cierto vínculo y/o extraer ideas relevantes. Por otro lado, existen pocos trabajos relacionados directamente con Procesos de Negocio Seguro, en el cual utilicen Patrones de Seguridad. Particularmente Ahmed y Matulevičius (2014), proponen una buena aproximación al uso de patrones (orientados a riesgos de seguridad) dentro del modelado de Procesos de Negocio Seguro. Pero este trabajo sólo se limita al uso explícito de los patrones (5 patrones, propuestos por Khan (2012)) dentro de BPMN.

En forma resumida, en la Tabla 3.2 se muestran las propuestas antes mencionadas. Para cada una de ellas se indica el lenguaje utilizado para construir el modelo de origen y de destino, se indica además si la manera de generar el modelo se encuentra automatizada y, finalmente el o los tipos de patrones que utilizan. Se puede concluir que no hay trabajos cuyo modelo de origen esté construido con BPMN-BPSec o con alguna extensión que permita representar requisitos de seguridad, que utilicen Patrones de Seguridad para la generación de los modelos de destino y, finalmente, ninguno de los modelos de destino es un diagrama de clases descrito con UML. En el trabajo de Ahmed y Matulevičius (2014) se utiliza una descripción de seguridad en procesos de negocio, basada en el aspecto visual propuesto en BPMN-BPSec, no obstante, ellos no trasforman estas especificaciones en clase UML y utilizan patrones orientados a riesgos de seguridad.

Propuestas	Origen	Destino	Automa-tizado	Tipo de Patrones
(Bonillo, 2006)	BPMN	UML (no especifica tipo de modelo)	No	Patrones en General
(Forster *et al*., 2007)	UML - Activity Diagram	UML - Activity Diagram	Si	Patrones de Vista de Procesos
(Gschwind *et al*., 2008)	BPMN	BPMN	Si	Patrones de Flujo de Trabajo
(Schumm *et al*., 2010)	BPMN	BPMN	Si	Patrones de Vista de Procesos
(Brambilla *et al*., 2012)	BPMN	WebML	Si	Patrones de Socialización
(Khan, 2012)	BPMN	BPMN	No	Patrones orientados a Riesgos de Seguridad
(Ahmed & Matulevičius, 2014)	BPMN	BPMN	Si	Patrones orientados a Riesgos de Seguridad
(Elgammal *et al.*, 2014)	BPMN	BPMN	Si	Patrones de Cumplimiento
(Awad *et al*., 2015)	BPMN	BPMN	Si	Patrones de Cumplimiento
(Lohrmann & Reichert, 2015)	BPMN	BPMN	No	Patrones de mejora de Procesos

Tabla 3.2 – Resumen Trabajos Relacionados.

Finalmente, podemos decir que en la literatura no existen trabajos en que obtengan Clases UML desde Procesos de Negocio Seguros, usando Patrones de Seguridad para la generación de dichas clases. Por lo tanto y como conclusión de esta sección, se puede decir que la transformación de un Proceso de Negocio Seguro hacia un Diagrama de Clases utilizando Patrones de Seguridad de forma automática, no ha sido suficientemente abordado.

Capítulo 4

Selección de Patrones de Seguridad

4 TRANSFORMACIÓN DE MODELOS UTILIZANDO PATRONES DE SEGURIDAD

En este capítulo, se da a conocer en detalle, la propuesta que permite seleccionar Patrones de Seguridad a través del análisis de los requisitos de seguridad representados en un modelo de Proceso de Negocio Seguro.

4.1 MÉTODO PARA LA SELECCIÓN DE PATRONES DE SEGURIDAD

El método M-SecBP&P (Method - Secure Business Process and Patterns) tiene como objetivo, permitir la selección y adaptación de Patrones de Seguridad a través del uso de la información obtenida de un Proceso de Negocio Seguro. El resultado es un artefacto UML que se obtiene desde patrones de seguridad, los que son seleccionados y adaptados a partir de la información obtenida desde un Proceso de Negocio Seguro.

M-SecBP&P, cuya vista completa puede verse en la Figura 4.1, está compuesto por un conjunto de etapas, roles, herramientas y artefactos, los cuales permiten crear clases de análisis, para las que se tiene en cuenta la información obtenida de un Proceso de Negocio Seguro y los Patrones de Seguridad.

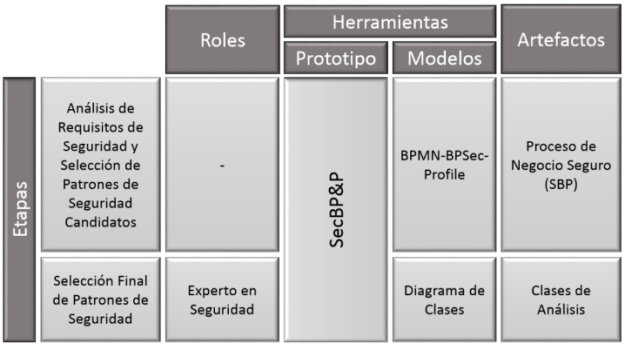


Figura 4.1 – Vista Completa de M-SecBP&P.

ETAPA-1: ANÁLISIS DE REQUISITOS DE SEGURIDAD Y SELECCIÓN DE PATRONES DE SEGURIDAD CANDIDATOS

El objetivo de esta etapa es realizar un análisis de los requisitos de seguridad especificados en el Proceso de Negocio Seguro, el cual es utilizado como modelo de entrada y ha sido especificado con BPMN-BPSec.

En la Figura 4.2, se pueden apreciar las tareas que se realizan en esta etapa. Esta etapa no tiene un rol asociado, debido a que se lleva a cabo de manera automática y

se realiza utilizando el prototipo SecBP&P-Tool (más detalles en la Sección 5), el cual ha sido diseñado para apoyar el método M-SecBP&P.

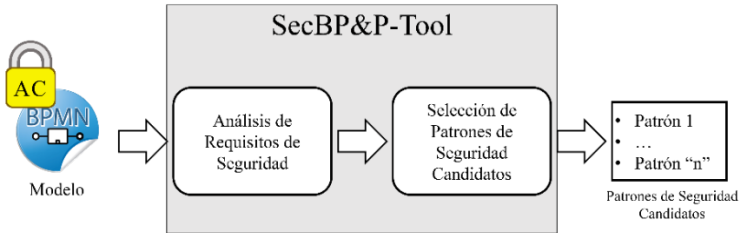


Figura 4.2 – Esquema Análisis de Requisitos de Seguridad.

Como modelo de entrada se considera un Proceso de Negocio Seguro, del cual se procede a analizar los requisitos de seguridad que se encuentran especificados y a partir de esos requisitos se procede a realizar una selección de los Patrones de seguridad candidatos. Para realizar este análisis se ha utilizado el lenguaje ATL (Lopez *et al.*, 2009), el cual permite analizar el código que genera el SBP y determinar el tipo de requisito de seguridad (Control de Acceso, Privacidad, etc.) y los elementos del BP sobre los cuales han sido especificados. El análisis se realiza para cada POOL dentro del proceso de negocio, considerando también los elementos que este mismo posee y los mensajes que recibe, es decir, son considerados los requisitos de seguridad de cada elemento y mensajes recibidos como si fueran parte del POOL en su totalidad y no de forma independiente. Con esto se genera una lista de Patrones de Seguridad candidatos por cada POOL, debido a que, en la mayoría de los casos, este último representa una entidad de negocio mínima e independiente que interactúa con el o los sistemas de forma autónoma a otro POOL.

Una vez obtenida la información de los requisitos de seguridad dentro de cada POOL, se compara dicha información con la relación existente entre los requisitos de seguridad y los Patrones de Seguridad (ver Sección 4.2, Tabla 4.3), generando una lista con los Patrones de Seguridad que cumplen con los requisitos de seguridad especificados en el BP.

En esta etapa la lista de Patrones de Seguridad se genera de forma automática y los criterios para la elegibilidad de dichos patrones son: (i) selección de aquellos patrones que cumplan con la totalidad de los requisitos de seguridad y (ii) presentación de estos patrones en forma ordenada considerando como filtro la cantidad de requisitos de seguridad excedentes, es decir, aquellos requisitos que el Patrón de Seguridad satisface, pero que no están expresados dentro del Proceso de Negocio Seguro.

ETAPA-2: SELECCIÓN FINAL DE PATRONES DE SEGURIDAD

En esta etapa, como se muestra en la Figura 4.3, interviene el experto de seguridad quien tiene la responsabilidad de seleccionar el patrón que evalúe como más conveniente de acuerdo a los requisitos planteados, a partir de un conjunto previo de Patrones de Seguridad.

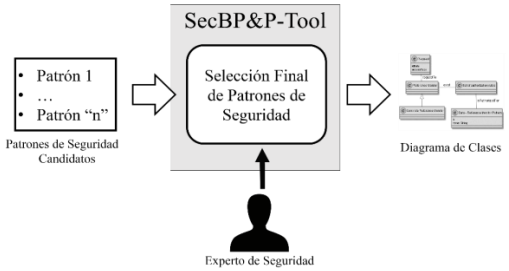


Figura 4.3 – Esquema Selección de Patrones de Seguridad.

Esta etapa tiene como salida un Diagrama de Clases UML que considera el o los Patrones de Seguridad seleccionados. La transformación desde un proceso de negocio hacia un diagrama de clases, se realiza a través de reglas de transformaciones propuestas por Rodríguez *et al.* (2010), las cuales se resumen en la Tabla 4.1.

Con estas reglas es posible obtener un diagrama de clases, que es utilizado como base para adoptar el o los Patrones de Seguridad seleccionados.

Elemento BPMN	Elemento Diagrama de Clases
Pool	Clase
Lane	Clase
Objeto de Dato, Mensaje	Clase
Actividad	Operación
Requisito de Seguridad	Clase

Tabla 4.1 –Equivalencia de Elementos BPMN – Diagrama de Clases (Rodríguez *et al.*, 2010).

4.2 RELACIÓN PATRONES DE SEGURIDAD CON REQUISITOS DE SEGURIDAD

Un requisito de seguridad puede ser interpretado de diferente manera dependiendo de dónde sea especificado. Por ejemplo, el requisito de seguridad *DETECCIÓN DE ATAQUES/AMENAZAS* especificado sobre un POOL, implica contar con un registro sobre todas las actividades que realiza dicha entidad. En el contexto de desarrollo de software, esto implicaría llevar un registro de los usuarios que acceden al sistema y las funcionalidades que estos mismos utilizan. En caso de especificar el mismo

requisito de seguridad sobre un DATA OBJECT, sólo implicaría llevar un registro de las actividades que interactúan con el mismo DATA OBJECT.

Debido a lo anterior, se puede hablar de Monitoreo de Control de Acceso, cuando un requisito de seguridad es especificado en un POOL, LANE o GROUP, ya que estos representan una entidad y/o participante dentro de BPMN. Por otro lado, se puede hablar de Monitoreo de Recursos, cuando un requisito de seguridad es especificado sobre un ACTIVITY, MESSAGE FLOW o un DATA OBJECT, ya que estos representan recursos dentro de BPMN, ya sean tareas/funciones, mensajes y datos respectivamente.

En la Tabla 4.2 y en la Tabla 4.3 se presentan las relaciones posibles entre los requisitos de seguridad, los elementos de BPMN, los tipos de monitoreo y los Patrones de Seguridad posibles a utilizar. Específicamente en la Tabla 4.2 se muestran los requisitos de seguridad (BPMN-BPSec) en relación con los elementos de BPMN, agrupados por tipo de monitoreo, en donde pueden ser representados.

	Elementos de BPMN					
	Monitoreo de Control de Acceso			Monitoreo de Recursos		
Requisito de Seguridad	Pool	Lane	Group	Activity	Message Flow	Data Object
No Repudiación					**X**	
Detección de Ataques/Amenazas	**X**	**X**	**X**	**X**	**X**	**X**
Integridad					**X**	**X**
Privacidad	**X**	**X**	**X**			
Control de Acceso	**X**	**X**	**X**	**X**		

Tabla 4.2 – Tipos de Monitoreo BPMN-BPSec adaptado de (Rodríguez *et al.*, 2007).

A partir de esto se ha construido la Tabla 4.3 en que se muestra los requisitos de seguridad de BPMN-BPSec y su relación de los Patrones de Seguridad agrupados por nivel.

A continuación se explica en forma detallada las relaciones presentadas en la Tabla 4.3 teniendo como referencia los patrones posibles de asociar a cada requisito de seguridad.

En el caso de la **INTEGRIDAD**, este requisito se encuentra asociado a todos los patrones a nivel de arquitectura e interfaz, debido a que dichos patrones permiten verificar que sólo los usuarios autorizados puedan acceder y/o modificar los datos que les corresponden de acuerdo con sus necesidades. En cuanto a los patrones a nivel de diseño, este requisito está asociado a los últimos dos patrones de dicho nivel.

		Patrones de Seguridad a Nivel de Arquitectura			Patrones de Seguridad a Nivel de Diseño				Patrones de Seguridad a Nivel de Interfaz	
Requisitos de Seguridad BPMN-BPSec	**TIPO DE MONITOREO**	**Único Punto de Acceso**	**Punto de Control**	**Sesión de Seguridad**	**Autorización**	**RBAC**	**Seguridad Multinivel**	**Monitor de Referencia**	**Acceso Total con Errores**	**Acceso Limitado**
Integridad	M. R.	**X**	**X**	**X**			**X**	**X**	**X**	**X**
No Repudiación	M. R.			**X**			**X**	**X**	**X**	**X**
Auditoría de Seguridad	M. R.	**X**	**X**	**X**			**X**	**X**		
Privacidad – Confidencialidad	M. CA	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Detección de Ataques/Amenazas	M. R.			**X**			**X**	**X**	**X**	
	M. CA	**X**	**X**	**X**						
Control de Acceso Identificación	M. CA	**X**	**X**	**X**						
Control de Acceso Autenticación	M. CA	**X**	**X**	**X**						
Control de Acceso Autorización	M. CA	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
	M. R	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

M. CA: Monitoreo de Control de Acceso **M. R**: Monitoreo de Recursos

Tabla 4.3 - Relación Patrones de Seguridad - Requisitos de Seguridad.

El requisito **NO REPUDIACIÓN** está vinculado directamente con el monitoreo de recursos y no está explícitamente relacionado con algún patrón en particular. Pero debido a que hay patrones que verifican los derechos de acceso a los recursos, se puede agregar un *Log* con el objetivo de almacenar información referente a quién accede a los datos del sistema, para luego ser analizada. Al implementar esta estrategia, en cuanto a los patrones de arquitectura, sólo *Sesión de Seguridad* permite un monitoreo de recurso, debido a que posee los datos de seguridad del usuario en cada momento y pueden ser obtenidos en el momento que este acceda a algún recurso. Por otro lado, a nivel de diseño, los patrones *Seguridad Multinivel* y *Monitor de Referencia*, están encargados de la asignación de los recursos y de interceptar las solicitudes hacia los mismos. Finalmente, en cuanto a los patrones de interfaz, todos poseen no repudiación de los recursos, debido a que *Acceso Total con Errores* cada vez que un usuario accede a algún recurso del sistema, verifica los derechos de acceso, por lo que se puede aplicar la misma estrategia del *Log*. Por otro lado, *Acceso Limitado*, si bien se enfoca sólo en mostrar las funcionalidades que posee cada usuario, al momento en el que accede a un recurso, es el sistema el que le da acceso a los recursos, por lo que se puede aplicar la misma estrategia del *Log.*

Para el requisito **AUDITORÍA DE SEGURIDAD**, al igual que en el requisito anterior, se puede incorporar un *Log* para auditar al sistema con respecto al acceso de la información. En cuanto a los patrones a nivel de arquitectura, *Único Punto de Acceso* y *Punto de Control*, se pueden auditar a nivel de control de acceso solamente, debido a que dichos Patrones de Seguridad están enfocados en verificar y validar la forma en que un usuario accede al sistema. Por otro lado, *Sesión de Seguridad* permite auditoría a nivel de control de recursos. En cuanto a los patrones a nivel de diseño, *Seguridad Multinivel* y *Monitor de Referencia*, estos permiten saber quién está accediendo a los recursos. Por último, los patrones de interfaz *Acceso Total con Errores* y *Acceso Limitado*, ambos permiten realizar auditoría, pero solo a nivel de recursos, debido a que consideran que el usuario ya está dentro del sistema y no validan su acceso a él.

Con respecto al requisito **PRIVACIDAD**, este se encuentra asociado a la confidencialidad y se da para todos los patrones debido a que todos ellos velan para que la información esté disponible sólo a personas autorizadas.

Para el requisito de **DETECCIÓN DE ATAQUES/AMENAZAS**, se puede utilizar la misma estrategia de contar con un *Log*. Al aplicar dicha estrategia los patrones arquitecturales, *Único Punto de Acceso* y *Punto de Control*, pueden implementar sólo detección a nivel de control de acceso. Por otro lado, el patrón *Sesión de Seguridad* permite implementar una detección a nivel de control de acceso y de recursos. En cuanto a los patrones a nivel de diseño, los patrones a los cuales se puede aplicar dicho *Log* son *Seguridad Multinivel* y *Monitor de Referencia* y sólo se da para el monitoreo de recursos. De esta manera, a nivel de interfaz, el patrón *Acceso Total con Errores* puede implementar detección de ataques a nivel de recursos.

Finalmente, para el requisito de **CONTROL DE ACCESO**, los patrones a nivel de arquitectura cumplen con identificación, autenticación y autorización. En cuanto al nivel de diseño, todos los patrones de dicho nivel coinciden sólo con autorización, y se puede realizar tanto para monitoreo de control de acceso, como para el de recursos. En cuanto a los patrones a nivel de diseño, sólo coincide autorización debido a que estos patrones validan que un usuario posea acceso a los recursos, a un módulo o sistema en particular. Por otro lado, los patrones a nivel de interfaz, cumplen sólo con autorización debido a que consideran a un usuario dentro del sistema para comenzar a realizar validaciones.

Como se puede apreciar, diferentes Patrones satisfacen un mismo requisito de seguridad y no existe uno que posea el mismo funcionamiento que otro, debido a que son específicos para cierto tipo de contexto, como por ejemplo, control de acceso a un

sistema, a recursos, la construcción de interfaz dependiendo del tipo de rol que posea el usuario, etc. Sin embargo, algunos patrones se complementan entre sí, esto los hace flexibles y aumenta la escalabilidad de utilizar estos mismos, mejorando así, características de seguridad del sistema final.

Capítulo 5

Prototipo SecBP&P

5 PROTOTIPO SECBP&P – TOOL

En este capítulo se describe el prototipo que da soporte al método que permite obtener un diagrama de clases, por medio de la combinación de un Proceso de Negocio Seguro y Patrones de Seguridad.

El prototipo SecBP&P-Tool apoya las tareas relacionadas con el análisis de los requisitos de seguridad, generación de Patrones de Seguridad candidatos y selección final de un Patrón de Seguridad, generando así, un diagrama de clases con la adaptación del patrón.

Para la construcción del prototipo se utilizó el lenguaje Java (Oracle, 2015), ATL (Eclipse, 2015) y el plugin PlantUML (PlantUML, 2015). El hecho de utilizar el lenguaje de programación Java, específicamente con la versión estándar 1.8, se justifica ya que era preciso hacer uso de un lenguaje flexible y adaptativo, pues se requería que el producto creado permitiera la facilidad de ser instalado en el entorno del usuario sin complicaciones. Para el análisis del modelo de Procesos de Negocio Seguro, las transformaciones entre modelos (Proceso de Negocio Seguro a Diagrama de Clases) y la inclusión de los Patrones de Seguridad se utilizó ATL (Eclipse, 2015), ya que este lenguaje nos permitió obtener los metadatos del Proceso de Negocio Seguro para su procesamiento. Cabe destacar que con ATL, el modelo generado queda en un archivo UML serializado, el cual es un formato estándar que puede ser reconocido por otras aplicaciones que manipulen modelos del mismo tipo. Finalmente, se utilizó el plugin PlantUML para generar el Diagrama de Clases UML obtenido a través de las reglas de transformaciones. A continuación, en la Sección 5.1 se describe la arquitectura utilizada para la creación del prototipo SecBP&P, en la Sección 5.2 se muestra un extracto del código fuente utilizado para el análisis de los Requisitos de Seguridad en ATL, en la Sección 5.3 se presenta la interfaz del prototipo propiamente tal, para posteriormente, mostrar un ejemplo ilustrativo en la Sección 5.4.

5.1 ARQUITECTURA

La arquitectura escogida para la construcción del prototipo SecBP&P, fue la arquitectura Modelo Vista Controlador (MVC), debido a su simplicidad al momento de separar la lógica interna de la vista.

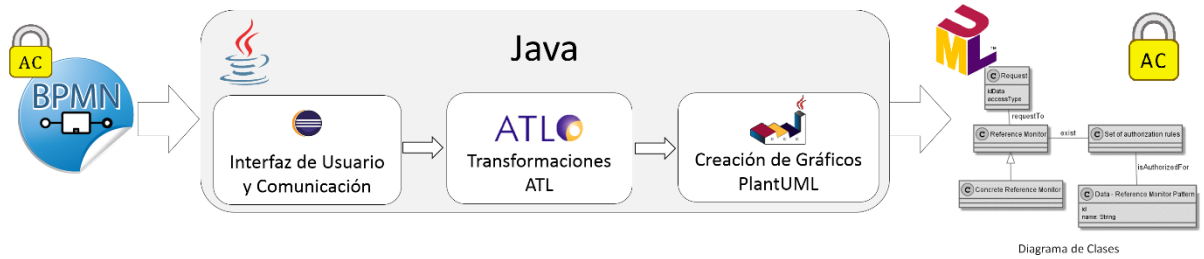


Figura 5.1 – Funcionamiento Interno Prototipo SecBP&P.

En la Figura 5.1 se puede ver, *grosso modo*, las principales funcionalidades que posee la estructura del prototipo SecBP&P, donde se pueden apreciar las siguientes funcionalidades:

1. INTERFAZ DE USUARIO Y COMUNICACIÓN: representa toda la interfaz que se mostrará hacia el usuario, en conjunto con canales de comunicación internos entre ATL y el plugin PlantUML.
2. TRANSFORMACIONES ATL: transformaciones en el lenguaje ATL, las que reciben como entrada, un Proceso de Negocio Seguro, analizando su estructura y reconociendo cada tipo de requisitos de seguridad (ver Algoritmo 1), con el objeto de generar una lista de Patrones de Seguridad candidatos.
3. CREACIÓN DE GRÁFICOS PLANTUML: módulo en el cual, una vez que el usuario realiza la selección final de los Patrones de Seguridad, se generan dos archivos; (i) archivo serializado en formato estándar (.uml) con la inclusión de el o los Patrones de Seguridad seleccionados y (ii) Diagrama de Clases final en formato de imagen (.png).

5.2 RECONOCIMIENTO DE REQUISITOS DE SEGURIDAD MEDIANTE ATL

A continuación se muestra un extracto del código fuente utilizado para el reconocimiento de los Requisitos de Seguridad dependiendo del Tipo de Monitoreo (ver Tabla 4.2).

```
rule CreateAllSRClassAndSelectSP() {
using {}
do {
   for(pool in BPMN!Participant.allInstances()){
      if(pool.haveSR()){
         thisModule.IncrementSRCount(pool.getSR(), thisModule.MCA);
      }
      for(art in pool.processRef.artifacts -> select(ar | ar.oclType() =
            BPMN!Group)){
         if(art.haveSR()){
            thisModule.IncrementSRCount(art.getSR(), thisModule.MCA);
         }
      }
      if(pool.getAllLanes() <> OclUndefined){
         for(ln in pool.getAllLanes()){
            if(ln.haveSR()){
               thisModule.IncrementSRCount(ln.getSR(), thisModule.MCA);
            }
         }
         for(act in ln.getAllActivity()){
            if(act.haveSR()){
               thisModule.IncrementSRCount(act.getSR(), thisModule.MR);
            }
         }
         for(msf in BPMN!getAllMessageFlow() -> select(msg | msg.
            messageRef <> OclUndefined)){
               if(msf.targetRef.oclType() = BPMN!Activity){
                     if(msf.sourceRef.oclIsTypeOf(BPMN!Participant)){}else{
                        if(msf.sourceRef.getLane() = ln){
                           if(msf.messageRef.haveSR()){
                              thisModule.IncrementSRCount(msf.messageRef.
                                    getSR(), thisModule.MR);
                           }
                        }
                     }
                  if(msf.targetRef.oclIsTypeOf(BPMN!Participant)){}else{
                     if(msf.targetRef.getLane() = ln){
                        if(msf.messageRef.haveSR()){
                           thisModule.IncrementSRCount(msf.messageRef.getSR(),
                                 thisModule.MR);
                        }
                     }
                  }
               }
            }
              for(dat in BPMN!DataObject.allInstances() -> select(d | d.
                  getDataAssociation() <> OclUndefined)) {
               for(act in BPMN!Activity.allInstances() -> select(act | act.
                     dataInputAssociations.includes(dat.getDataAssociation()) and
                     act.getLane() = ln)){
                  if(dat.haveSR()){
                     thisModule.IncrementSRCount(dat.getSR(), thisModule.MR);
                  }
               }
            }
         }
      }
   }
}
```

Algoritmo 1 – Extracto código ATL.

Como se mencionó anteriormente, el Algoritmo 1 es sólo un extracto del código ATL, específicamente dicho código o *Regla ATL*, recorre el Proceso de Negocio Seguro recibido como entrada, contando los Requisitos de Seguridad y Tipos de Monitoreo que este posee, con el objeto de generar una lista de Patrones que cumplan con los requisitos encontrados dentro de dicho proceso, ordenados según el criterio mostrado en la ETAPA 1 del método propuesto.

5.3 INTERFAZ GRÁFICA

La interfaz gráfica del prototipo SecBP&P fue diseñada lo más intuitiva posible, con el objeto de que el usuario no requiera de mayor conocimiento para poder utilizarla.

La interfaz del prototipo consta de dos módulos, los cuales se pueden apreciar en la Figura 5.2. Al lado izquierdo se muestra el módulo de **INICIO**, en el cual se deben indicar dos rutas, la primera corresponde al lugar donde se encuentra el Proceso de Negocio Seguro y la segunda ruta corresponde al directorio donde se almacenará el artefacto UML generado.

Figura 5.2– Prototipo SecBP&P.

Al lado derecho de la Figura 5.2, se puede ver el módulo de **ANÁLISIS** del prototipo, donde para cada POOL dentro del Proceso de Negocio Seguro, se le asigna una lista de Patrones de Seguridad candidatos, ordenados según el criterio mostrado en la Etapa 1 del método propuesto.

Finalmente, una vez seleccionado el o los Patrones de Seguridad, se procede a generar el artefacto UML, el que es almacenado como un archivo estándar (.uml) para que cualquier software pueda leerlo y también se almacena el Diagrama de Clases de dicho artefacto en su formato imagen (.png).

5.4 EJEMPLO ILUSTRATIVO

Para el ejemplo ilustrativo se utilizó el Proceso de Negocio Seguro que trata el Registro de un Usuario en una página Web (ver Figura 5.3). El POOL BPI-Member contempla las actividades de llenar el formulario de registro, confirmación de la recepción de correo electrónico e ingresar a la página Web. Por su parte, el POOL BPI-Web contempla las actividades de crear un perfil de usuario, enviar correo de confirmación y habilitar acceso total a los servicios.

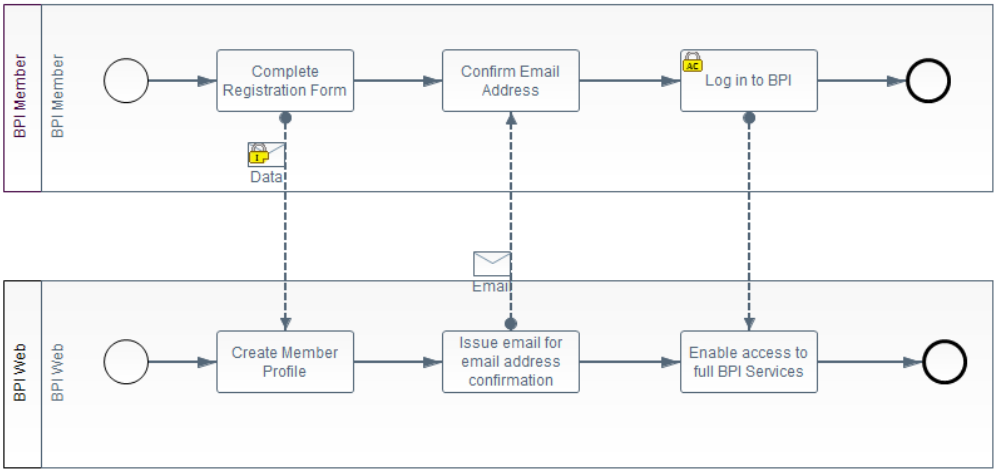


Figura 5.3 – Ejemplo Registro de Usuario adaptado de OMG (2015).

Los requisitos de seguridad dentro del Proceso de Negocio Seguro son:

- **INTEGRIDAD** con registro de auditoría, en el mensaje "Data", esto es para el POOL BPI Web y BPI Member.
- **CONTROL DE ACCESO**, en la tarea "Log in to BPI", esto es para el POOL BPI Member.

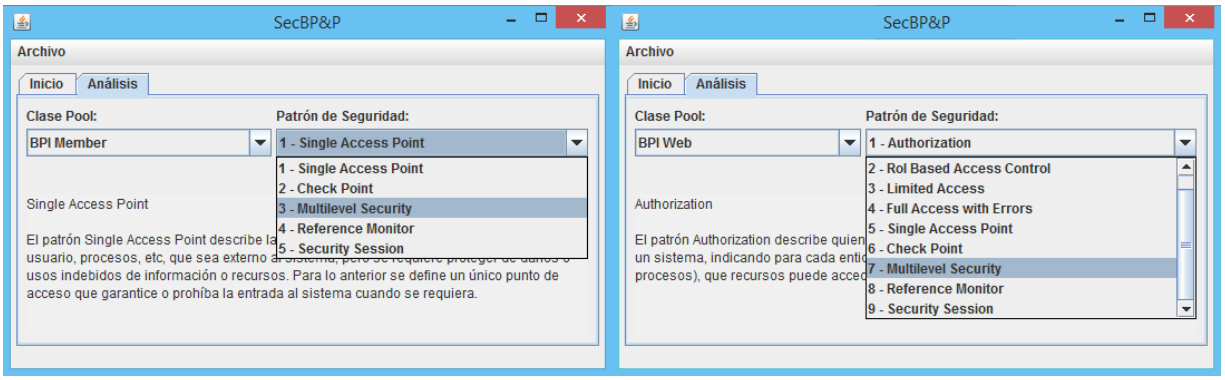


Figura 5.4 – SecBP&P – Patrones Candidatos.

En la Figura 5.4 se pueden ver los Patrones de Seguridad candidatos para cada POOL, los cuales fueron obtenidos contrastando la información de los requisitos de seguridad dentro de cada uno de ellos. Los Patrones de Seguridad candidatos para este ejemplo son:

- **BPI-MEMBER:** Único Punto de Acceso, Punto de Control, Seguridad Multinivel, Monitor de Referencia y Sesión de Seguridad (Figura 5.4, sector izquierdo).

- **BPI-WEB:** Autorización, Control de Acceso basado en Roles, Acceso Limitado, Acceso Total con Errores, Único Punto de Acceso, Punto de Control, Seguridad Multinivel, Monitor de Referencia y Sesión de Seguridad (Figura 5.4, sector derecho).

La información que fluye entre los Pools se puede clasificar en diferentes niveles de seguridad, específicamente, la información que envía BPI Member hacia BPI Web claramente posee un mayor grado de sensibilidad que el correo que se le envía devuelta para confirmar su creación como usuario, además, el tipo o categoría de información que ambos mensajes poseen, es diferente, puesto que la información enviada desde BPI Web, es un simple correo automático confirmando la creación del usuario, no así, el mensaje/información que envía BPI Member. Para este ejemplo en particular, se seleccionó el patrón "Seguridad Multinivel" para ambos POOLS puesto que ambos están dentro del mismo sistema, en el cual se clasificará la información como se mencionó anteriormente.

En la Figura 5.5, se puede ver el resultado de utilizar el patrón Seguridad Multinivel. Las clases de color gris pertenecen al Patrón de Seguridad y las clases con fondo blanco corresponden las clases del Proceso de Negocio Seguro que no están relacionadas con la seguridad.

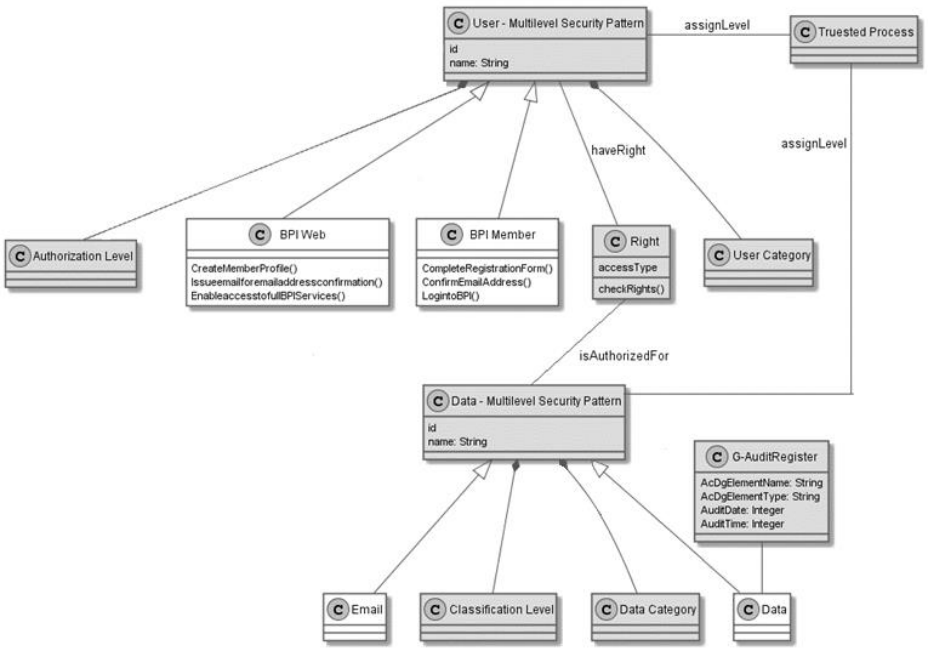


Figura 5.5 – Patrón de Seguridad – Ejemplo Ilustrativo.

En la Figura anterior, la clase *"Data–Multilevel Security Pattern"* representa la información a la que pueden acceder los usuarios (representados por la clase *"User–Multilevel Security Pattern"*). Cabe destacar que las clases obtenidas como usuario o datos desde el SBP, se relacionan directamente con sus clases respectivas (mencionadas anteriormente), a través de herencia y cada una de ellas se agrupan por Categorías ("User Category" y "Data Category" respectivamente). Por su parte, los usuarios poseen un nivel de autorización (representado por la clase *"Authorization Level"*) y derechos de acceso hacia los datos (representado por la clase *"Right"*). Por otro lado, los datos poseen un nivel de clasificación (representada por la clase *"Classification Level"*). Finalmente, existe una clase encargada de realizar cambios sobre las clasificaciones y categorías tanto de los usuarios como los datos (representada por la clase *"Trusted Process"*), la cual, además tiene permitido realizar alguna violación de seguridad, sólo en el caso de ser necesario dichos cambios, ya sea por algún error al momento de asignación de categorías, etc.

Finalmente, la clase *"G-AuditRegister"* es obtenida directamente de BPMN-BPSec, debido a que el Patrón Seguridad Multinivel, al igual que los demás Patrones de Seguridad, no posee una clase específica que lleve un control sobre los registros de auditoría.

Capítulo 6

Validación

6 VALIDACIÓN

Para la validación del método propuesto en esta Tesis de Magister se ha contrastado con una propuesta existente (Rodríguez *et al*., 2010), en que se transforman las especificaciones de seguridad del Proceso de Negocio Seguro, generando un modelo de clases sin usar patrones. Ambos modelos generados son comparados en cuanto a su completitud, entendibilidad y el nivel de claridad que el modelo aporta para comenzar a desarrollar un sistema. Los modelos son presentados primero en forma individual, para luego, a través de encuestas aplicadas a desarrolladores la comparación de los modelos.

La encuesta fue aplicada en un muestreo "por conveniencia" sobre un total de 26 sujetos, que en promedio tenían de 3 a 6 años de experiencia utilizando Diagramas de Clases. Se realizaron dos tipos de encuestas diferentes (ver Anexo 1 y Anexos 2) las que fueron respondidas por la misma cantidad de sujetos (13 encuestados cada una). Cabe destacar que las encuestas median los mismos conceptos, la única diferencia eran los modelos de Proceso de Negocio Seguro por tanto los Diagramas de Clases generados no eran los mismos.

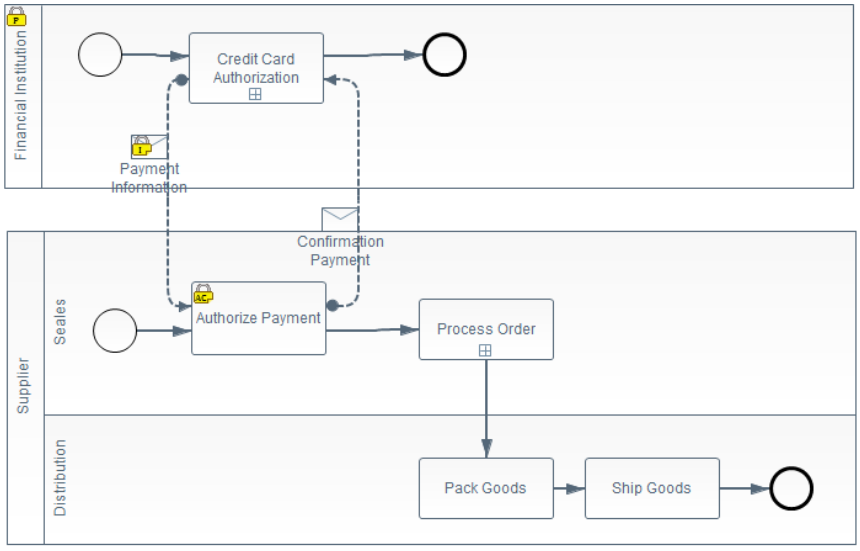


Figura 6.1 - BPMN Procesamiento de Compra adaptado de OMG (2015).

En la Figura 6.1, se muestra el Proceso de Negocio Seguro en el contexto de procesamiento de Orden de Compra por parte de un proveedor, el cual recibe la información del pago desde una institución financiera, posterior a ello, envía la confirmación del pago hacia la misma entidad financiera, para luego procesar la Orden de Compra y enviar los productos.

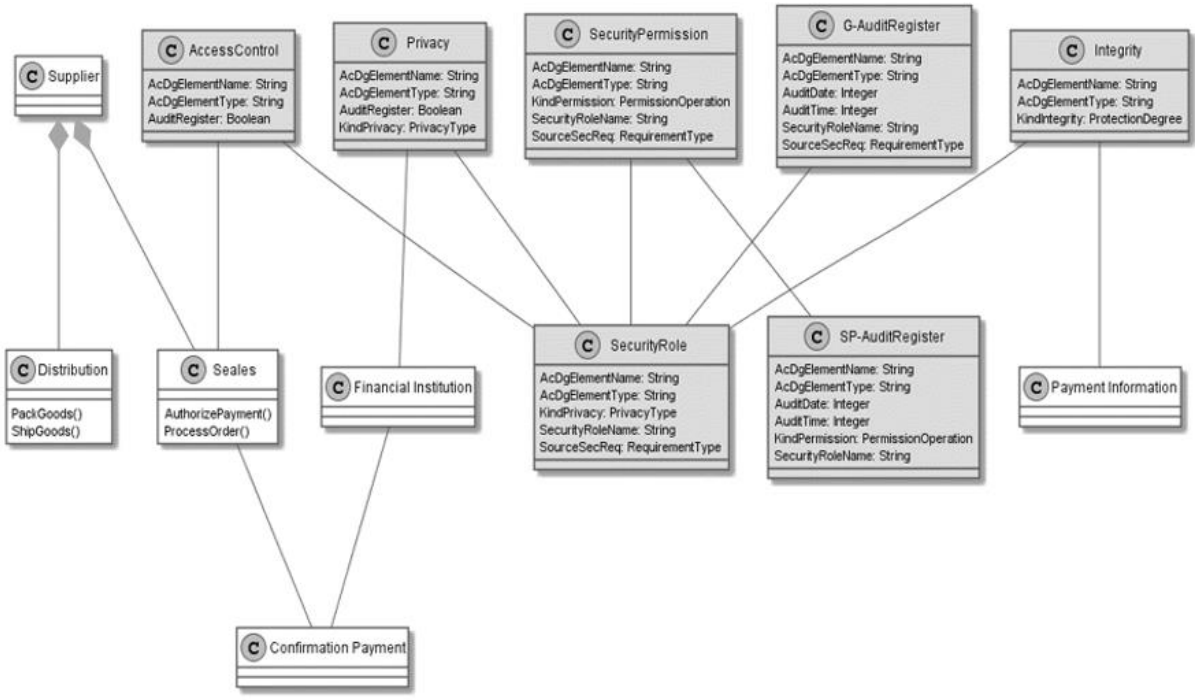


Figura 6.2 – Modelo A – Procesamiento de Compra propuesta (Rodríguez *et al.*, 2010)

En la Figura 6.2, se puede ver el modelo generado con BPMN-BPSec a partir del Proceso de Negocio Seguro antes descrito, utilizando las reglas de transformaciones de Rodríguez *et al.* (2010).

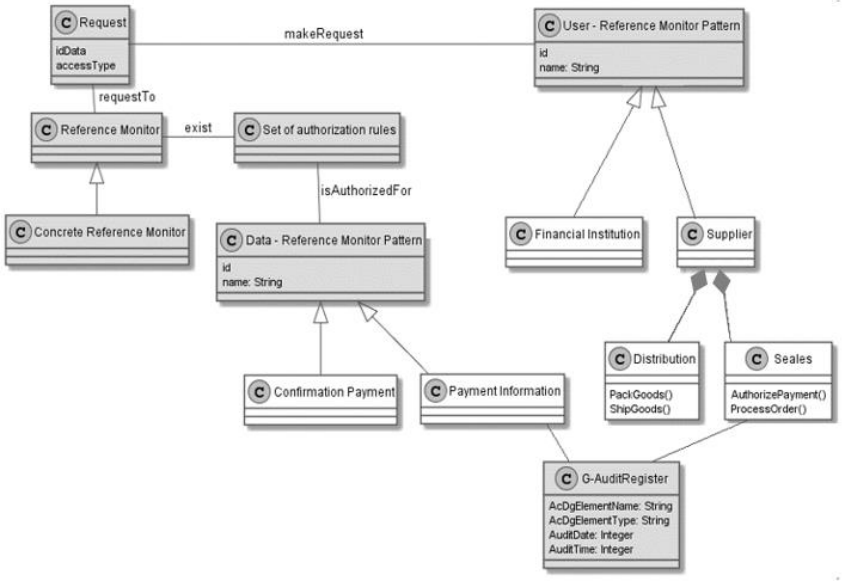


Figura 6.3 – Modelo B – Procesamiento de Compra usando M-SecBP&P.

En la Figura 6.3, se puede ver el modelo generado con M-SecBP&P, que es el método que se está proponiendo. Cabe destacar que ambos modelos fueron objeto de comparación para la encuesta.

6.1 SELECCIÓN DE VARIABLES

La variable independiente, también denominada factor principal, es el origen de los Diagramas de Clase, la cual es una variable nominal que toma dos valores:

1. **Modelo A:** Diagrama UML obtenido automáticamente a través de la propuesta (Rodríguez *et al.*, 2010) (ver Figura 6.2).
2. **Modelo B:** Diagrama UML obtenido automáticamente a través de **M-SecBP&P** (ver Figura 6.3).

Las variables dependientes son la completitud, entendibilidad, y si el nivel de detalle forma la base para crear un sistema, todo esto enfocándonos en los aspectos de seguridad.

Al momento de analizar ambos modelos de forma individual, se ha podido comprobar que ambos poseen un nivel aceptable con respecto a las variables analizadas (completitud de aspectos de seguridad, entendibilidad de aspectos de seguridad y nivel de detalle de seguridad apto para crear un sistema). Sin embargo al momento de comparar ambos modelos generados, se puede apreciar una clara tendencia del *Modelo B,* asociado a M-SecBP&P, por sobre el *Modelo A,* asociado a la propuesta de Rodríguez *et al.* (2010), con respecto a la completitud, es decir, los conceptos de seguridad dentro del Proceso de Negocio Seguro, según los encuestados, se ven reflejados con mayor claridad en el Diagrama de Clases generado (*Modelo B)*. En referencia al nivel de entendibilidad de dichos aspectos, los encuestados perciben un nivel similar tanto para el *Modelo B* como el *Modelo A*. Finalmente, en cuanto a si el nivel de detalle de los aspectos de seguridad forma la base para desarrollar un sistema, existe una gran diferencia con respecto a los modelos, donde el 70% de los encuestados coinciden en que dicho nivel en el *Modelo B* es más apto para comenzar a desarrollar un sistema.

Cabe destacar que el *Modelo B*, hacía uso de Patrones de Seguridad, los cuales están diseñados para que cualquier desarrollador pueda entender el funcionamiento de su estructura, debido a que representan soluciones conceptuales a problemas de seguridad. No pasa lo mismo con el *Modelo A*, el cual extrae directamente los aspectos de seguridad desde el Proceso de Negocio Seguro, se cree que este es el factor principal para que el *Modelo B* sobresaliera por sobre el *Modelo A* según la percepción de los encuestados.

6.2 IMPACTO CONOCIMIENTOS RELEVANTES

La encuesta también permitió analizar el impacto que tienen los conocimientos relevantes sobre los Patrones de Seguridad, en otras palabras, si poseer conocimiento sobre ellos puede influir en el nivel de entendimiento que poseen los sujetos sobre el Modelo B, el cual es generado utilizando Patrones de Seguridad. Para lo anterior, se plantearon las siguientes hipótesis:

- **H0:** No existe una relación significativa con respecto al nivel de conocimiento sobre Patrones de Seguridad, y el nivel de Entendimiento sobre el *Modelo B.*
- **H1:** Existe una relación significativa con respecto al nivel de conocimiento sobre Patrones de Seguridad, y el nivel de Entendimiento sobre el *Modelo B.*

Debido a que las puntuaciones obtenidas en la encuesta no siguen una distribución normal, se decide realizar el análisis no paramétrico U de Mann Whitney, en el cual se obtuvo que "*poseer conocimientos sobre patrones de seguridad no posee una relación significativa con el nivel de entendimiento percibido por los encuestados*", todo esto enfocado solo en el *Modelo B*, que es el que interesa por motivos de investigación.

En la Tabla 6.1, se muestra el resultado de la ejecución del análisis estadístico U Mann Whitney.

Estadísticos de prueba[a]

	¿Se puede comprender fácilmente la relación entre los requisitos de seguridad (dentro del proceso de negocio) y las clases de seguridad (clases en gris dentro del diagrama de clases)?
U de Mann-Whitney	12,000
W de Wilcoxon	48,000
Z	-1,317
Sig. asintótica (bilateral)	,188

a. Variable de agrupación: Posee conocimientos sobre "Patrones de Seguridad"

Tabla 6.1 – U de Mann Withney - Conocimiento – Entendimiento – Encuesta A.

Como se puede apreciar, no se observa una relación estadísticamente significativa (p = 0,188) entre poseer conocimientos sobre Patrones de Seguridad y el nivel de entendimiento del modelo B, resultando en la aceptación de la hipótesis nula.

Lo anterior lleva a la siguiente conclusión: no es estrictamente necesario poseer conocimientos sobre Patrones de Seguridad para poder entender el Modelo B, el cual se propone como una alternativa a la traducción del Proceso de Negocio Seguro hacia Diagrama de Clases, reforzando la idea de utilizar Patrones de Seguridad en etapas tempranas del ciclo de desarrollo de software.

Por otro lado, también pudimos comprobar si el poseer conocimientos de Patrones de Seguridad influencia significativamente la selección de los modelos generados, para lo cual planteamos las siguientes hipótesis:

- **H_0:** No existe una relación significativa entre los sujetos que poseen conocimientos sobre Patrones de Seguridad, y la selección del modelo (*Modelo A* y *Modelo B)* con mejor nivel de entendimiento posee.
- **H_1:** Existe una relación significativa entre los sujetos que poseen conocimientos sobre Patrones de Seguridad, y la selección del modelo (*Modelo A* y *Modelo B)* con mejor nivel de entendimiento posee.

Se utilizó la misma agrupación antes descrita para el nivel de conocimientos de Patrones de Seguridad, con lo cual se obtuvo que *"No existe una relación significativa entre los sujetos que poseen conocimientos sobre Patrones de Seguridad, y la selección del modelo (Modelo A y Modelo B) con mejor nivel de entendimiento posee".*

En la Tabla 6.2 se muestra el resultado de la ejecución del análisis estadístico U Mann Whitney.

Estadísticos de prueba[a]

	¿Cuál de los dos modelos permite comprender con mayor facilidad la relación entre los requisitos de seguridad dentro del Proceso de Negocio Seguro y las clases de seguridad dentro del diagrama de clases?
U de Mann-Whitney	10,500
W de Wilcoxon	25,500
Z	-1,734
Sig. asintótica (bilateral)	,083

a. Variable de agrupación: Posee conocimientos sobre "Patrones de Seguridad"

Tabla 6.2 - U de Mann Withney – Conocimiento - Selección de Modelos – Encuesta A.

Como se puede apreciar, no se observa una relación estadísticamente significativa (p=0,083) entre poseer conocimientos sobre Patrones de Seguridad y la selección del modelo que cuenta con mejor nivel de entendimiento, resultando en la aceptación de la hipótesis nula.

Lo anterior induce a pensar que no es necesario poseer conocimientos sobre Patrones de Seguridad para que los sujetos entiendan mejor el *Modelo B* por sobre el *Modelo A*. Esto también se puede apreciar en la Figura 6.4, donde se observa claramente que a pesar que los sujetos no poseen conocimientos sobre Patrones de Seguridad, esto no fue un impedimento para poder entender mejor el modelo que utilizaba dichos patrones.

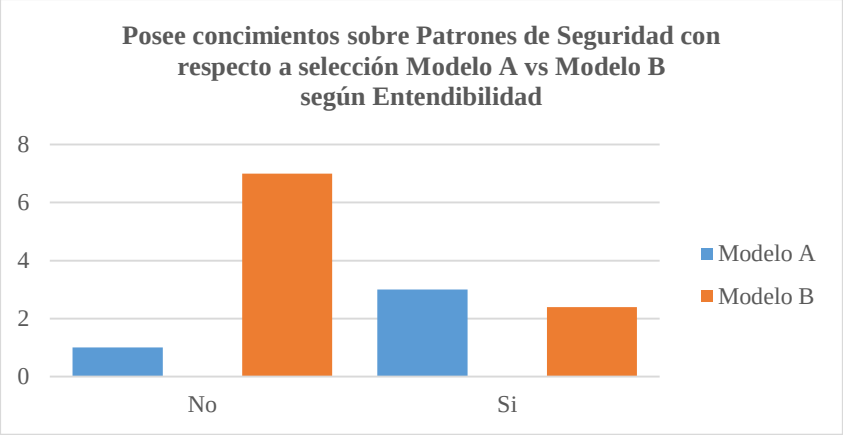


Figura 6.4 – Tabla cruzada - Conocimientos Patrones de Seguridad vs Selección de Modelo.

Con este experimento podemos observar que no existe una relación estadísticamente significativa, entre poseer conocimientos sobre Patrones de Seguridad, y el nivel de entendibilidad que los sujetos percibían sobre el *Modelo B*, el cual hacía uso de dichos patrones, llegando a la misma conclusión antes mencionada, en que es posible utilizar Patrones de Seguridad en etapas tempranas del ciclo de desarrollo de software, a pesar de que no exista un experto en el área de seguridad que brinde soporte en su uso.

Para mayor detalle sobre el análisis de las encuestas, revisar Anexo 3 y Anexo 4, donde se muestran las variables descriptivas y todo el análisis de la segunda encuesta realizada.

Capítulo 7

Conclusiones

7 CONCLUSIONES

Como resultado de la revisión de la literatura, se ha podido comprobar que no hay trabajos directamente relacionados con la obtención de Diagramas de Clase UML, considerando como punto de partido un Proceso de Negocio con alguna extensión de seguridad, en particular con BPMN-BPSec, en que se utilicen Patrones de Seguridad. Aunque Ahmed y Matulevičius (2014) utilizan patrones orientados a los riesgos de seguridad de forma explícita, esta propuesta sólo se limita a un conjunto de patrones establecidos previamente por Khan (2012).

La especificación de requisitos de seguridad en procesos de negocio, en este caso usando BPMN-BPSec, ha demostrado ser un aporte para la definición de la seguridad en tempranas etapas del desarrollo de software. También se ha mostrado, que la relación con Patrones de Seguridad propuesta, permitirá aprovechar al máximo dicha especificación de seguridad. Además, como se ha comprobado a través de la validación del modelo, en general, el uso de Patrones de Seguridad posee una buena aceptación por parte de los usuarios, en cuanto a la percepción de su completitud, entendimiento y la manera en que sirve de base para comenzar a desarrollar un sistema. Otro de los resultados del experimento, es que se ha demostrado que no existe una relación estadísticamente significativa, en cuanto a poseer conocimientos sobre Patrones de Seguridad y el nivel de entendibilidad que los sujetos percibían sobre los mismos. Esto refuerza la idea de utilizar Patrones de Seguridad en etapas tempranas del ciclo de desarrollo de software, independiente del hecho de que exista o no un experto de seguridad, debido a que no es exclusivamente necesario poseer altos niveles de conocimientos sobre patrones para poder entenderlos, puesto que estos representan una idea conceptual de cómo resolver un problema en específico relacionado a la seguridad y la implementación de un Patrón de Seguridad, dependerá netamente del lenguaje de programación, arquitectura de software escogida, marco de trabajo utilizado, etc.

Por otro lado, se ha contribuido con método, M-SecBP&P, mediante el cual es posible utilizar la especificación de un Proceso de Negocio Seguro, para generar un Diagrama de Clases UML. En este caso se utilizan Patrones de Seguridad los que son contrastados con los requisitos de seguridad especificados en el proceso de negocio seguro, generando así, un artefacto que puede ser utilizado dentro del ciclo de desarrollo de software, específicamente, en la fase del Modelado de Negocio. También construimos un prototipo capaz de dar soporte a dicho método (M-SecBP&P), con el cual se puede analizar el modelo de proceso de negocio y seleccionar los Patrones de

Seguridad aptos al contexto del mismo, para finalmente generar un Diagrama de Clases UML en formato de imagen y formato estándar (archivo serializado).

Finalmente, se cumplió con todos los objetivos propuestos para esta Tesis de Magister, se demostró que es factible tomar como punto de partida la descripción de un Proceso de Negocio Seguro y generar artefactos que puedan ser utilizados dentro del proceso de desarrollo de software, específicamente se creó un Diagrama de Clases utilizando Patrones de Seguridad para satisfacer los requisitos de seguridad dentro del Proceso de Negocio Seguro. Por otro lado, como se mencionó anteriormente, se creó un método con la cual se puede obtener el artefacto antes descrito, desarrollando un prototipo para brindar soporte a dicho método, haciendo el proceso de forma automática, recibiendo como entrada la descripción de un Proceso de Negocio Seguro y posterior selección de el o los patrones candidatos más aptos al contexto deseado.

Referencias

REFERENCIAS

Ahmed, N., & Matulevičius, R. (2014). Securing business processes using security risk-oriented patterns. *Computer Standards & Interfaces*, *36*(4), 723–733. article.

Awad, A., Barnawi, A., Elgammal, A., Elshawi, R., Almalaise, A., & Sakr, S. (2015). Runtime Detection of Business Process Compliance Violations: An Approach based on Anti Patterns. In *Proceedings of the 30th ACM/SIGAPP Symposium On Applied Computing - Enterprise Engineering Track (SAC 2015), Salamanca, Spain*. article.

Basin, D., Doser, J., & Lodderstedt, T. (2006). Model driven security: From UML models to access control infrastructures. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, *15*(1), 39–91. article.

Bonillo, P. (2006). Metodología para la gerencia de los procesos del negocio sustenda en el uso de patrones. *Journal of Information Systems and Technology Management*, *3*(2), 143–162. article.

Brambilla, M., Fraternali, P., & Vaca, C. (2012). BPMN and design patterns for engineering social BPM solutions. In *Business Process Management Workshops* (pp. 219–230). inproceedings.

Champy, J., & Hammer, M. (1994). *Reengineering the corporation*. book, GW National Satellite Network.

Davenport, T. H. (2013). *Process innovation: reengineering work through information technology*. book, Harvard Business Press.

Delgado, A. (2007). Desarrollo de Software con enfoque en el Negocio. In *Conference Proceeding JISBD: I Taller sobre Procesos de Negocio e Ingeniería del Software (PNIS'07), September, Zaragoza, España*. inproceedings.

Eclipse. (2015). ATL - a model transformation technology. Retrieved from https://eclipse.org/atl/

Elgammal, A., Turetken, O., van den Heuvel, W.-J., & Papazoglou, M. (2014). Formalizing and appling compliance patterns for business process compliance. *Software & Systems Modeling*, 1–28. article.

Firesmith, D. (2004). Specifying Reusable Security Requirements. *Journal of Object Technology*, *3*, 61–75. article.

Forster, A., Engels, G., Schattkowsky, T., & Van Der Straeten, R. (2007). Verification of business process quality constraints based on visual process patterns. In *Theoretical Aspects of Software Engineering. First Joint IEEE/IFIP Symposium* (pp. 197–208). inproceedings.

Fowler, M. (1997). *Analysis patterns: reusable object models*. book, Addison-Wesley Professional.

Gschwind, T., Koehler, J., & Wong, J. (2008). Applying patterns during business process modeling. In *Business process management* (pp. 4–19). incollection, Springer.

Gutiérrez, M. A. C., Ríos, A. R., Calero, C., Fernández-Medina, E., & Piattini, M. (2005). Análisis y revisión de la literatura en el contexto de proyectos de fin de carrera: Una propuesta.

Revista Sociedad Chilena de Ciencia de La Computación, *6*(1). article.

Herrmann, P., & Herrmann, G. (2006). Security requirement analysis of business processes. *Electronic Commerce Research*, *6*(3–4), 305–335. article.

Jürjens, J. (2002). UMLsec: Extending UML for secure systems development. In *UML 2002 — The Unified Modeling Language* (pp. 412–425). incollection, Springer.

Khan, N. H. (2012). *APattern-Based Development of Secure Business Processes* (phdthesis). Master's Thesis, University of Tartu.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *EBSE Technical Report EBSE-2007-01*. techreport.

Kruchten, P. (2004). *The rational unified process: an introduction*. Addison-Wesley Professional.

Lohrmann, M., & Reichert, M. (2015). Effective application of process improvement patterns to business processes. *Software & Systems Modeling*, 1–23. article.

López, H., Veresi, F., Viñolo, M., Calegari, D., & Luna, C. (2009). *Reporte Técnico RT 09-19 Estado del Arte de Lenguajes y Herramientas de Transformación de Modelos*.

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

Lopez, J., Montenegro, J. A., Vivas, J. L., Okamoto, E., & Dawson, E. (2005). Specification and design of advanced authentication and authorization services. *Computer Standards & Interfaces*, *27*(5), 467–478. article.

Mellor, S. J., Scott, K., Uhl, A., & Weise, D. (2002). Model-driven architecture. In *Advances in Object-Oriented Information Systems* (pp. 290–297). incollection, Springer.

Muehlen, M. zur. (2002). Workflow-based Process Controlling. *Advances in Information Systems and Management Science*. article.

Mülle, J., von Stackelberg, S., & Böhm, K. (2011). *A security language for BPMN process models*. book, KIT, University of the State of Baden-Wuerttemberg and National Research Center of the Helmholtz Association.

OMG. (2015). Business Process Model and Notation. Retrieved from http://www.bpmn.org

Oracle. (2015). Java Developer Center. Retrieved from http://www.oracle.com/technetwork/es/java/index.html

PlantUML. (2015). PlantUML : Open-source tool that uses simple textual descriptions to draw UML diagrams. Retrieved from http://plantuml.com/

Quirchmayr, G. (2004). Survivability and business continuity management. In *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32* (pp. 3–6). inproceedings.

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*(9), 945–971. article.

Rodríguez, A., Fernández-Medina, E., & Piattini, M. (2006). Towards a UML 2.0 extension for the modeling of security requirements in business processes. In *Trust and Privacy in*

Digital Business (pp. 51–61). incollection, Springer.

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*(4), 745–752. article.

Samarütel, S., Matulevičius, R., Norta, A., & Noukas, R. (2016). Securing Airline Turnaround Processes using Security-Risk Oriented Patterns. *University of Tartu*.

Schmidt, H., & Jürjens, J. (2011). Connecting security requirements analysis and secure design using patterns and UMLsec. In *Advanced Information Systems Engineering* (pp. 367–382). inproceedings.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2013). *Security Patterns: Integrating security and systems engineering*. book, John Wiley & Sons.

Schumm, D., Anstett, T., Leymann, F., & Schleicher, D. (2010). Applicability of Process Viewing Patterns in Business Process Management. In *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2010 14th IEEE International* (pp. 79–88). inproceedings.

Schumm, D., Leymann, F., & Streule, A. (2010). Process viewing patterns. In *Enterprise Distributed Object Computing Conference (EDOC), 2010 14th IEEE International* (pp. 89–98). inproceedings.

Solinas, M., Fernandez, E. B., & Antonelli, L. (2009). Embedding security patterns into a domain model. In *Database and Expert Systems Application, 2009. DEXA'09. 20th International Workshop* (pp. 176–180). inproceedings.

Van Der Aalst, W. M. P., Ter Hofstede, A. H. M., & Weske, M. (2003). Business process management: A survey. In *Business process management* (pp. 1–12). incollection, Springer.

Wolter, C., Menzel, M., & Meinel, C. (2008). Modeling Security Goals in Business Processes. In *Modellierung* (Vol. 127, pp. 201–216). inproceedings.

Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). A survey on security patterns. *Progress in Informatics*, *5*(5), 35–47. article.

Zapata, M., Rodríguez, A., & Caro, A. (2015). SecBP&P: Hacia la obtención de Artefactos UML a partir de Procesos de Negocio Seguros y Patrones de Seguridad. *VIII Congreso Iberoamericano de Seguridad Informática CIBSI Y Taller Educativo TIBETS*. article.

Anexos

8 ANEXOS

ANEXO 1 – ENCUESTA REGISTRO DE USUARIOS

A continuación, se presenta la encuesta realizada utilizando un Proceso de Negocio Seguro bajo el contexto del Registro de un Usuario.

PARTE I: CUESTIONARIO DEMOGRAFICO

Lea detenidamente las instrucciones a seguir.

A continuación, se realizan una serie de preguntas relacionadas con sus conocimientos y experiencia. Esta información no influenciará el resultado de ninguna de las partes que siguen en el cuestionario. Por favor, responda lo más preciso posible, marcando con una X en el interior del recuadro que corresponda.

1. Indique el nivel de conocimiento que posee sobre **Procesos de Negocio**, específicamente sobre la notación **BPMN.**

Conocimiento muy bajo	Conocimiento bajo	Conocimiento regular	Conocimiento Alto	Conocimiento muy alto
☐	☐	☐	☐	☐

2. Indique el nivel de conocimiento que posee sobre "**Requisitos de Seguridad**"

Conocimiento muy bajo	Conocimiento bajo	Conocimiento regular	Conocimiento Alto	Conocimiento muy alto
☐	☐	☐	☐	☐

3. Indique el nivel de conocimiento que posee sobre "**Patrones de Seguridad**"

Conocimiento muy bajo	Conocimiento bajo	Conocimiento regular	Conocimiento Alto	Conocimiento muy alto
☐	☐	☐	☐	☐

4. Indique el nivel de utilización que posee con **Diagrama de Clases**

Nunca utilizado	Muy poco utilizado	Poco utilizado	Regularmente utilizado	Muy frecuentemente utilizado
☐	☐	☐	☐	☐

5. Indique el número de años de experiencia que posee utilizando diagramas de clases:

☐☐

DESCRIPCIÓN PARTE II

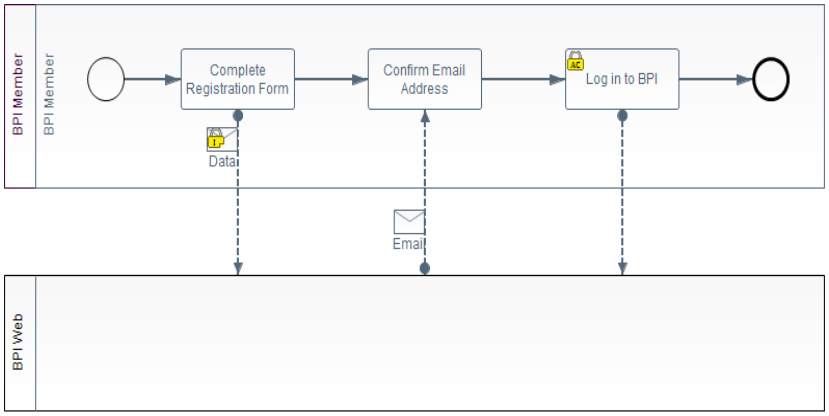
En las siguientes páginas, se le presenta un modelo de Proceso de Negocio Seguro (ver Figura 8.1), bajo el contexto del Registro de un Usuario en una página web. Se utiliza un enfoque de caja negra sobre la página web, es decir, no se muestran los procesos realizados por la misma. Por otra parte, las actividades del usuario contemplan las tareas de llenar el formulario de registros, confirmación de email y log in dentro de la página web.

Además, bajo el modelo de Proceso de Negocio, se presenta un Diagrama de Clases (ver Figura 8.2), el cual es obtenido utilizando BPMN-BPSec y se incluyen clases que dan cuenta de la seguridad especificada en el Proceso de Negocio Seguro.

A continuación se realiza una serie de preguntas relacionadas con el diagrama generado, al cual se le ha dado el nombre de Modelo A.

PROCESO DE NEGOCIO SEGURO: REGISTRO DE USUARIO

MODELO A



En el proceso de negocio seguro, se pueden apreciar los siguientes requisitos de seguridad:

- **Integridad** con registro de auditoría, en el mensaje "Data".
- **Control de Acceso**, en la tarea "Log in to BPI".

Figura 8.1 - Registro de Usuario adaptado de OMG (2015).

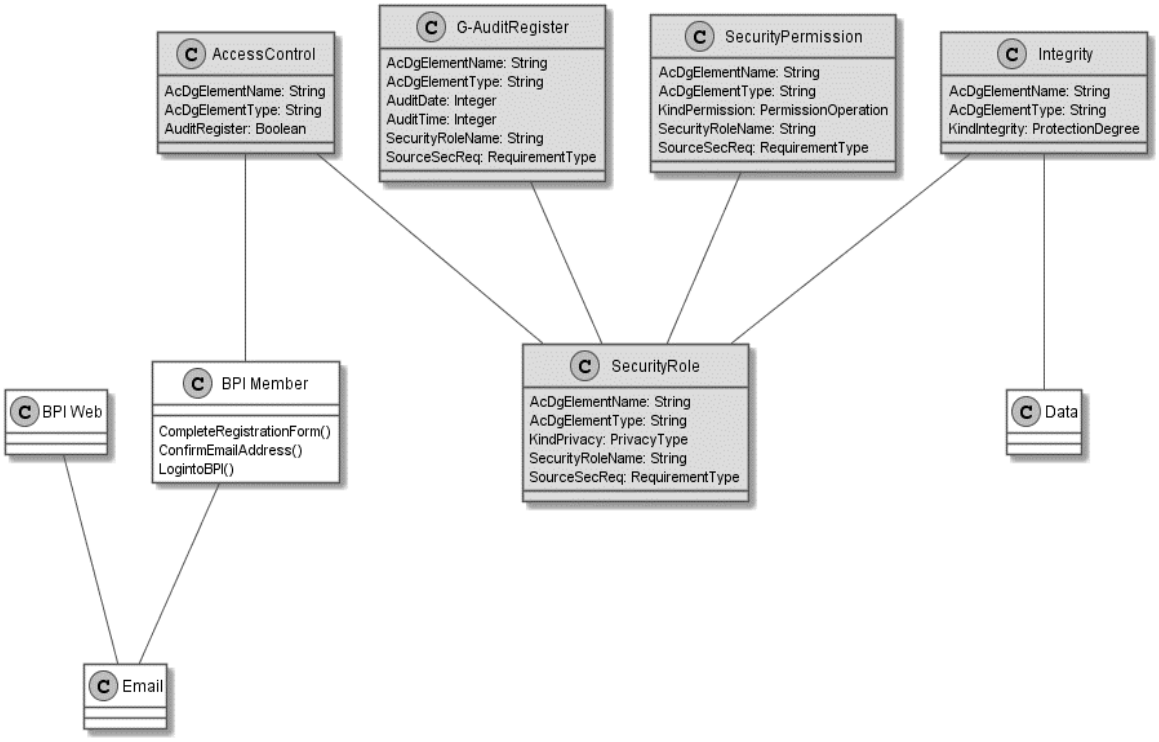


Figura 8.2 – Transformación BPMN-BPSec – Registro de Usuarios.

PARTE II – REGISTRO DE USUARIO - MODELO A

De acuerdo a su criterio, responda cada una de las siguientes preguntas referentes al **Modelo A**:

1. Dentro del Proceso de Negocio Seguro, los conceptos de seguridad ahí presentes ¿se ven reflejados en su totalidad en el diagrama de clases generado?

Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Muy de acuerdo
☐	☐	☐	☐	☐

2. ¿Se puede comprender fácilmente la relación entre los requisitos de seguridad (dentro del proceso de negocio) y las clases de seguridad (clases en gris dentro del diagrama de clases)?

Muy difícil de entender	Algo difícil de entender	Ni difícil ni fácil de entender	Algo fácil de entender	Muy fácil de entender
☐	☐	☐	☐	☐

3. El concepto de **Integridad** hace referencia a que los mensajes y/o datos deben estar protegidos frente a la corrupción intencional y no autorizada.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.3:

- La clase **Integrity**, almacena el tipo de integridad y los elementos que poseen integridad.
- La clase **SecurityRole**, almacena el nombre del rol de seguridad, y el del elemento que posee integridad.
- La clase **G-AuditRegister**, almacena el nombre y tipo de elemento que posee registro de auditoría, también se registran la hora y fecha de los eventos realizados.

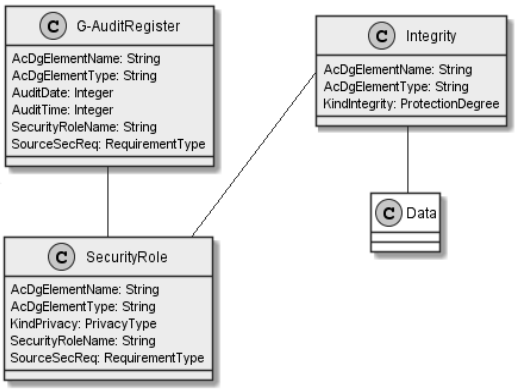


Figura 8.3 – BPMN-BPSec - Integridad - Modelo A

Considerando el diagrama de clases presentado en la Figura 8.3, indique si el concepto **Integridad** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

4. El concepto de **Control de Acceso**, hace referencia a la limitación de acceso a los recursos, permitiendo acceso sólo a usuarios autorizados.

A continuación, se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.4:

- La clase **AccessControl**, almacena el nombre y tipo de elementos que poseen control de acceso, también si posee o no registro de auditoría.
- La clase **SecurityPermission**, almacena el nombre y tipo de elementos que poseen control de acceso, además del tipo de permiso asociado a cada elemento del diagrama.
- La clase **SecurityRole**, almacena el nombre del rol de seguridad, y el del elemento que posee integridad.

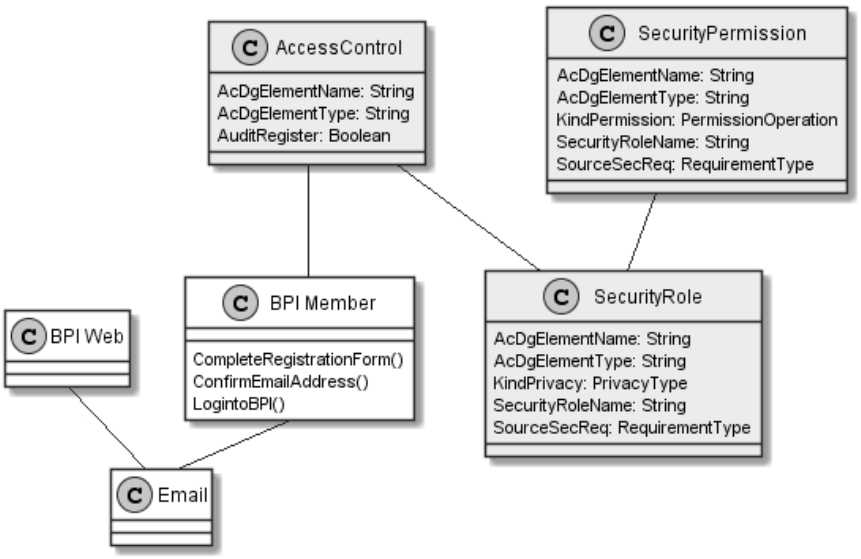


Figura 8.4 - BPMN-BPSec - Control de Acceso – Modelo A.

Considerando el diagrama de clases presentado en la Figura 8.4, indique si el concepto **Control de Acceso** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

5. ¿El nivel de detalle del diagrama de clases generado, que incluye aspectos de seguridad, puede servir de base para comenzar a desarrollar un sistema?

Muy en desacuerdo	**En desacuerdo**	**Neutral**	**De acuerdo**	**Muy de acuerdo**
☐	☐	☐	☐	☐

6. Agregue algún comentario en el recuadro si lo desea:

DESCRIPCIÓN PARTE III

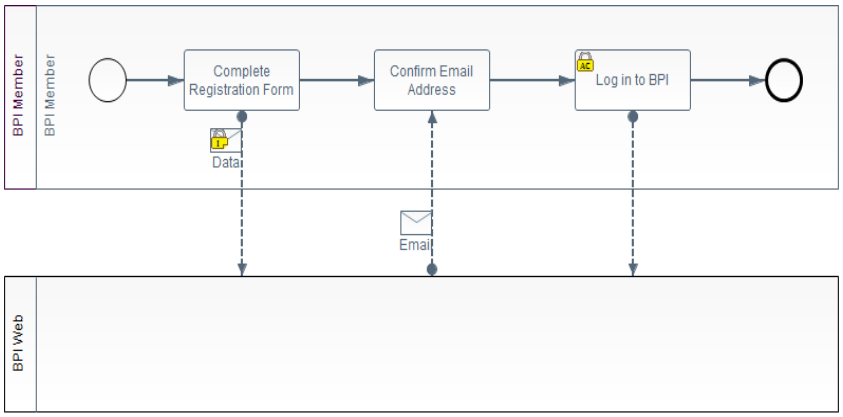
En las siguientes páginas se le presenta un modelo de Proceso de Negocio Seguro (ver Figura 8.5), bajo el contexto del Registro de un Usuario en una página web. Se utiliza un enfoque de caja negra sobre la página web, es decir, no se muestran los procesos realizados por la misma. Por otra parte, las actividades del usuario contemplan las tareas de llenar el formulario de registros, confirmación de email y log in dentro de la página web.

Además, bajo el modelo de Proceso de Negocio, se presenta un Diagrama de Clases (ver Figura 8.6), el que es obtenido M-SecBP&P y se incluyen Patrones de Seguridad, los cuales satisfacen los requisitos de seguridad especificados dentro del Proceso de Negocio Seguro.

A continuación se harán una serie de preguntas relacionadas con el diagrama generado, al cual se le ha dado el nombre de Modelo B.

PROCESO DE NEGOCIO SEGURO: REGISTRO DE USUARIO

MODELO B



En el proceso de negocio seguro, se pueden apreciar los siguientes requisitos de seguridad:

- **Integridad** con registro de auditoría, en el mensaje "Data".
- **Control de Acceso**, en la tarea "Log in to BPI".

Figura 8.5 - Registro de Usuario adaptado de OMG (2015).

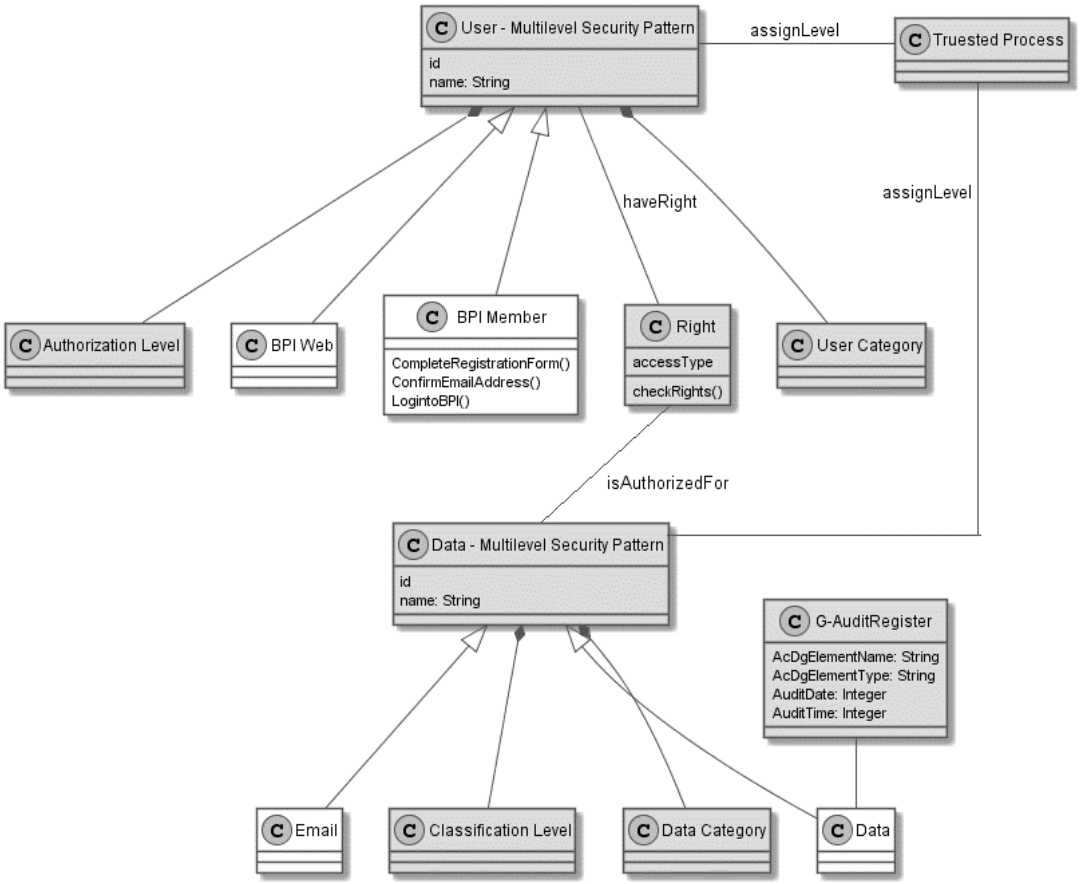


Figura 8.6 - Transformación M-SecBP&P – Registro de Usuarios.

PARTE III – REGISTRO DE USUARIO - MODELO B

De acuerdo a su criterio, responda cada una de las siguientes preguntas:

1. Dentro del Proceso de Negocio Seguro, los conceptos de seguridad ahí presentes ¿se ven reflejados en su totalidad en el diagrama de clases generado?

Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Muy de acuerdo
☐	☐	☐	☐	☐

2. ¿Se puede comprender fácilmente la relación entre los requisitos de seguridad (dentro del proceso de negocio) y las clases de seguridad (dentro del diagrama de clases)?

Muy difícil de entender	Algo difícil de entender	Ni difícil ni fácil de entender	Algo fácil de entender	Muy fácil de entender
☐	☐	☐	☐	☐

3. El concepto de **Integridad** hace referencia a que los mensajes y/o datos deben estar protegidos frente a la corrupción intencional y no autorizada.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.7:

- La clase **User – Multilevel Security Pattern**, es una clase abstracta para representar los usuarios del sistema
- La clase **Authorization Level**, almacena los diferentes niveles de autorización que posee un usuario dentro del sistema.
- La clase **User Category**, almacena las diferentes categorías que poseen los usuarios dentro del sistema.
- La clase **Right**, almacena los derechos de acceso que posee un usuario dentro del sistema.
- La clase **Data – Multilevel Security Pattern**, es una clase abstracta para representar los recursos del sistema.
- La clase **Classification Level**, almacena los diferentes niveles que poseen los datos dentro del sistema.
- La clase **Data Category**, almacena las diferentes categorías que poseen los datos dentro del sistema.
- La clase **G-AuditRegister**, almacena el nombre y tipo de elemento que posee registro de auditoría, también se registran la hora y fecha de los eventos realizados.
- La clase **Trusted Proccess**, es la clase encargada de asignar los diferentes niveles de autorización y categoría a los usuarios. También asigna los diferentes niveles de clasificación y categorías de los datos.

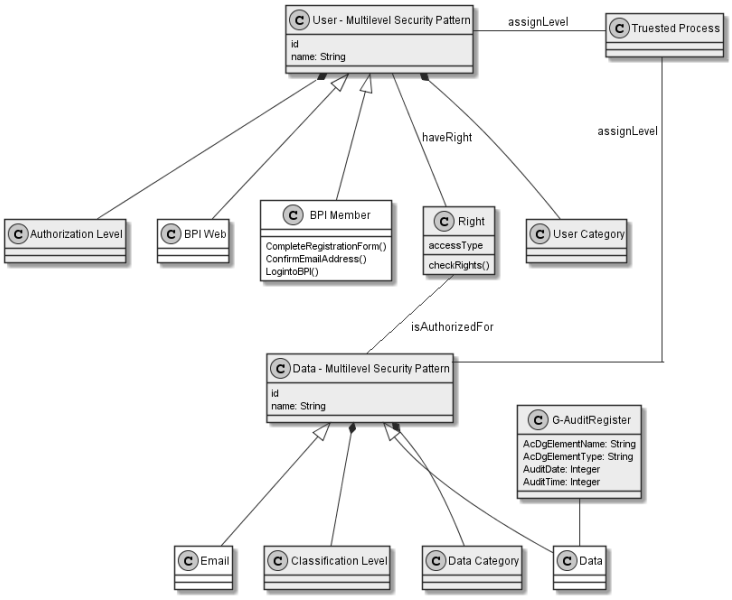


Figura 8.7 – M-SecBP&P - Integridad – Modelo B.

Considerando el diagrama de clases presentado en la Figura 8.7, indique si el concepto de **Integridad** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

4. El concepto de **Control de Acceso** hace referencia a la limitación de acceso a los recursos, permitiendo acceso sólo a usuarios autorizados.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.8:

- La clase **User – Multilevel Security Pattern**, es una clase abstracta para representar los usuarios del sistema
- La clase **Authorization Level**, almacena los diferentes niveles de autorización que posee un usuario dentro del sistema.
- La clase **User Category**, almacena las diferentes categorías que poseen los usuarios dentro del sistema.
- La clase **Right**, almacena los derechos de acceso que posee un usuario dentro del sistema.

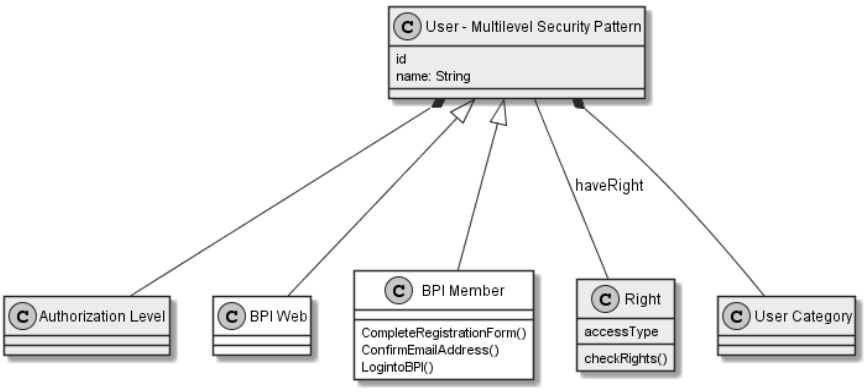


Figura 8.8 – M-SecBP&P - Control de Acceso – Modelo B.

Considerando el diagrama de clases presentado en la Figura 8.8, indique si el concepto de **Control de Acceso** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

5. ¿El nivel de detalle del diagrama de clases generado, que incluye aspectos de seguridad, puede servir de base para comenzar a desarrollar un sistema?

Muy en desacuerdo	**En desacuerdo**	**Neutral**	**De acuerdo**	**Muy de acuerdo**
☐	☐	☐	☐	☐

6. Agregue algún comentario en el recuadro si lo desea:

PARTE IV - ANÁLISIS MODELO A VS MODELO B

De acuerdo a su criterio, responda cada una de las siguientes preguntas:

1. Con respecto a la seguridad dentro del Proceso de Negocio Seguro ¿Cuál de los modelos vistos representa mejor dichos conceptos?

Modelo A ☐

Modelo B ☐

2. ¿Cuál de los dos modelos permite comprender con mayor facilidad la relación entre los requisitos de seguridad dentro del proceso de negocio seguro y las clases de seguridad dentro del diagrama de clases?

Modelo A ☐

Modelo B ☐

3. Dentro de los diagramas de clases mostrados ¿Cuál de los dos modelos posee mayor facilidad para implementar la **Integridad**?

Modelo A ☐

Modelo B ☐

4. Dentro de los diagramas de clases mostrados ¿Cuál de los dos modelos posee mayor facilidad para implementar un **Control de Acceso**?

Modelo A ☐

Modelo B ☐

5. ¿Qué modelo visto posee un mayor nivel de detalle referente a la seguridad, teniendo en cuenta que sería la base para comenzar a desarrollar un sistema?

Modelo A ☐

Modelo B ☐

ANEXO 2 – ENCUESTA PROCESAMIENTO ORDEN DE COMPRA

A continuación, se presenta la encuesta realizada utilizando un Proceso de Negocio Seguro bajo el contexto de una Orden de Compra.

PARTE I: CUESTIONARIO DEMOGRAFICO

Lea detenidamente las instrucciones a seguir.

A continuación, se realizan una serie de preguntas relacionadas con sus conocimientos y experiencia. Esta información no influenciará el resultado de ninguna de las partes que siguen en el cuestionario. Por favor, responda lo más precisamente que sea posible, marcando con una **X** en el interior del recuadro que corresponda.

1. Indique el nivel de conocimiento que posee sobre **Procesos de Negocio**, específicamente sobre la notación **BPMN.**

Conocimiento muy bajo	Conocimiento bajo	Conocimiento regular	Conocimiento Alto	Conocimiento muy alto
☐	☐	☐	☐	☐

2. Indique el nivel de conocimiento que posee sobre "**Requisitos de Seguridad**"

Conocimiento muy bajo	Conocimiento bajo	Conocimiento regular	Conocimiento Alto	Conocimiento muy alto
☐	☐	☐	☐	☐

3. Indique el nivel de conocimiento que posee sobre "**Patrones de Seguridad**"

Conocimiento muy bajo	Conocimiento bajo	Conocimiento regular	Conocimiento Alto	Conocimiento muy alto
☐	☐	☐	☐	☐

4. Indique el nivel de utilización que posee con **Diagrama de Clases**

Nunca utilizado	Muy poco utilizado	Poco utilizado	Regularmente utilizado	Muy frecuentemente utilizado
☐	☐	☐	☐	☐

5. Indique el número de años de experiencia que posee utilizando diagramas de clases:

☐☐

DESCRIPCIÓN PARTE II

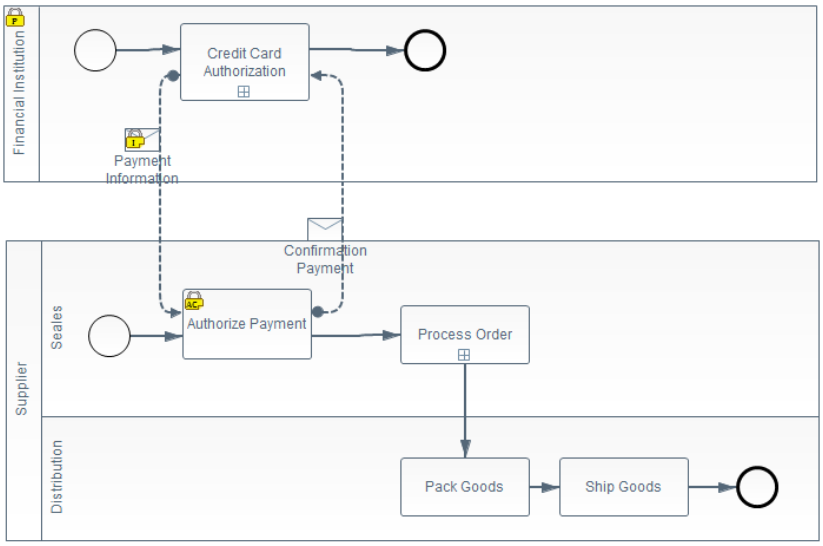
En las siguientes páginas se presenta un modelo de Proceso de Negocio Seguro (ver Figura 8.9), bajo el contexto de un procesamiento de Orden de Compra por parte de un proveedor, el cual recibe la información del pago desde una institución financiera, posterior a ello, envía la confirmación del pago hacia la misma entidad financiera, para luego procesar la Orden de Compra y enviar los productos.

Por otro lado, bajo el modelo de Proceso de Negocio se presenta un Diagrama de Clases (ver Figura 8.10), el cual es obtenido utilizando BPMN-BPSec y se incluyen clases que dan cuenta de la seguridad especificada en el proceso de negocio seguro.

A continuación, se realizan una serie de preguntas relacionadas con el diagrama generado, al cual se le ha dado el nombre de Modelo A.

PROCESO DE NEGOCIO SEGURO: PROCESAMIENTO DE COMPRA

MODELO A



En el proceso de negocio seguro, se pueden apreciar los siguientes requisitos de seguridad:

- **Privacidad**, en el pool "Financial Institution".
- **Integridad**, en el mensaje "Payment Information".
- **Control de Acceso** con registro de auditoría, en la tarea "Authorize Payment".

Figura 8.9 – Procesamiento Orden de Compra adaptado de OMG (2015).

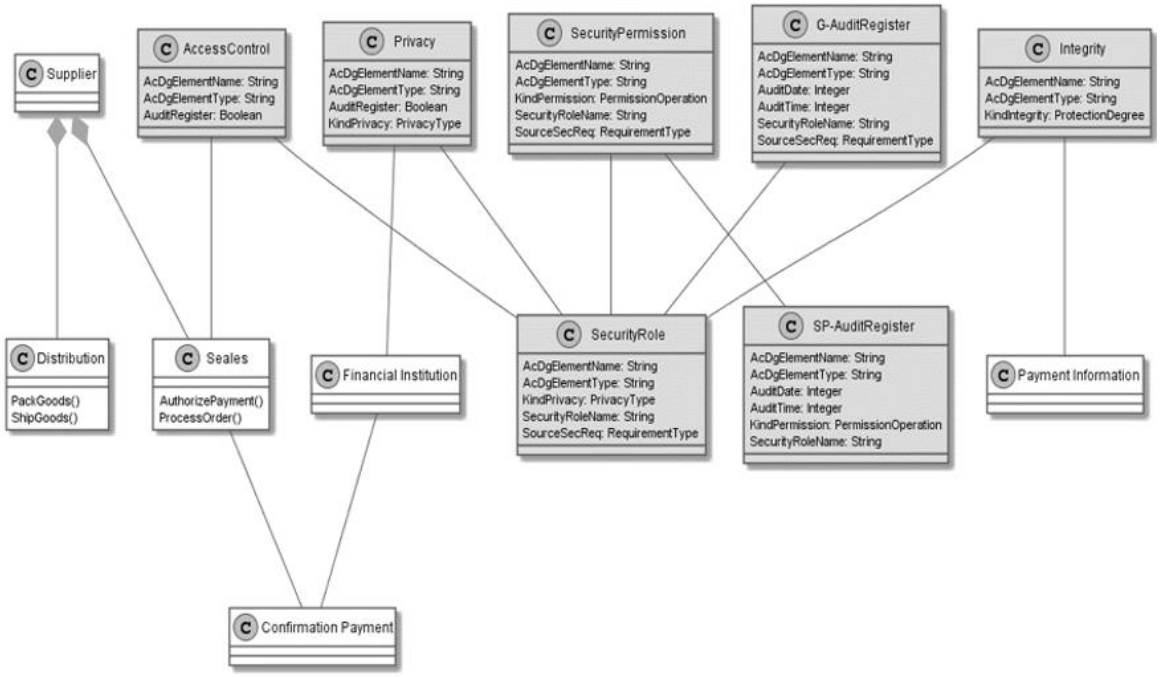


Figura 8.10 - Transformación BPMN-BPSec – Registro de Usuarios.

PARTE II – PROCESAMIENTO DE COMPRA - MODELO A

De acuerdo a su criterio, responda cada una de las siguientes preguntas referentes al **Modelo A**:

1. Dentro del Proceso de Negocio Seguro, los conceptos de seguridad ahí presentes ¿se ven reflejados en su totalidad en el diagrama de clases generado?

Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Muy de acuerdo
☐	☐	☐	☐	☐

2. ¿Se puede comprender fácilmente la relación entre los requisitos de seguridad (dentro del proceso de negocio) y las clases de seguridad (clases en gris dentro del diagrama de clases)?

Muy difícil de entender	Algo difícil de entender	Ni difícil ni fácil de entender	Algo fácil de entender	Muy fácil de entender
☐	☐	☐	☐	☐

3. La **Privacidad** hace referencia a que la información, datos y/o mensajes no puedan ser divulgados a personas no autorizadas.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.11:

- La clase **Privacy**, almacena el tipo de privacidad y qué elementos poseen privacidad.
- La clase **SecurityRole**, almacena el nombre del rol de seguridad y el del elemento que posee privacidad, además del tipo de privacidad.

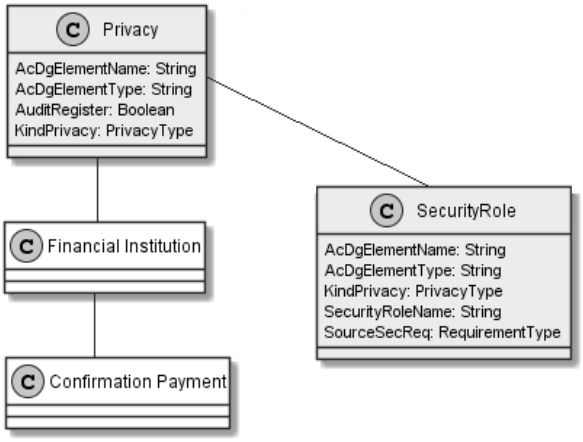


Figura 8.11 – BPMN-BPSec - Privacidad – Modelo A.

Considerando el diagrama de clases presentado en la Figura 8.11, indique si el concepto **Privacidad** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

4. La **Integridad** hace referencia a que los mensajes y/o datos deben estar protegidos frente a la corrupción intencional y no autorizada.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.12:

- La clase **Integrity**, almacena el tipo de integridad y los elementos que poseen integridad.
- La clase **SecurityRole**, almacena el nombre del rol de seguridad, y el del elemento que posee integridad.
- La clase **G-AuditRegister**, almacena el nombre y tipo de elemento que posee registro de auditoría, también se registran la hora y fecha de los eventos realizados.

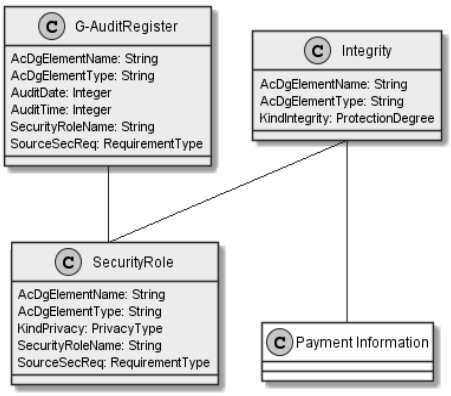


Figura 8.12 - BPMN-BPSec - Integridad - Modelo A

Considerando el diagrama de clases presentado en la Figura 8.12**,** indique si el concepto **Integridad** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

5. El **Control de Acceso** hace referencia a la limitación de acceso a los recursos, permitiendo acceso sólo a usuarios autorizados.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.13:

- La clase **AccessControl**, almacena el nombre y tipo de elementos que poseen control de acceso, también si posee o no registro de auditoría.
- La clase **G-AuditRegister**, almacena el nombre y tipo de elementos que poseen registro de auditoría, además de la fecha y hora en que ocurren eventos asociados.
- La clase **SP-Auditegister**, almacena el nombre y tipo de elementos que poseen registro de auditoría, además de la fecha y hora en que ocurren eventos asociados.
- La clase **SecurityPermission**, almacena el nombre y tipo de elementos que poseen control de acceso, además del tipo de permiso asociado a cada elemento del diagrama.
- La clase **SecurityRole**, almacena el nombre del rol de seguridad, y el del elemento que posee integridad.

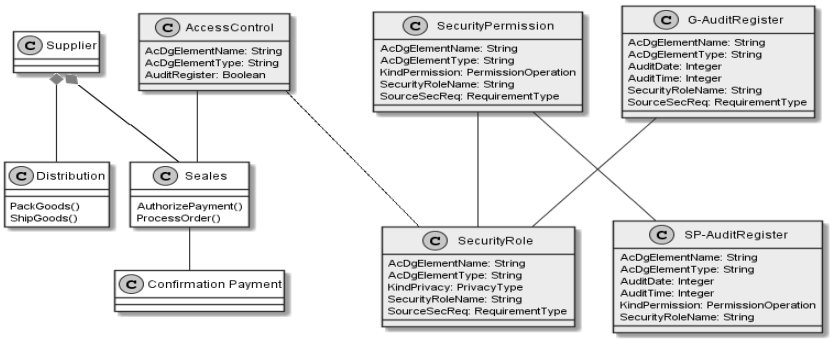


Figura 8.13 – BPMN-BPSec - Control de Acceso – Modelo A.

Considerando el diagrama de clases presentado en la Figura 8.13, indique si el concepto **Control de Acceso** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

6. ¿El nivel de detalle del diagrama de clases generado, que incluye aspectos de seguridad, puede servir de base para comenzar a desarrollar un sistema?

Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Muy de acuerdo
☐	☐	☐	☐	☐

7. Agregue algún comentario en el recuadro si lo desea:

DESCRIPCIÓN PARTE III

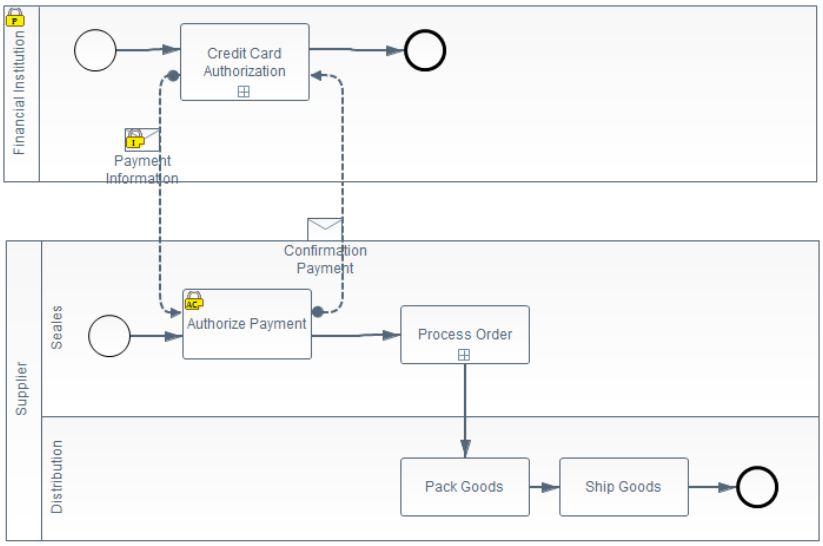
En las siguientes páginas se presenta un modelo de Proceso de Negocio Seguro (ver Figura 8.14), bajo el contexto de un procesamiento de Orden de Compra por parte de un proveedor, el cual recibe la información del pago desde una institución financiera, posterior a ello, envía la confirmación del pago hacia la misma entidad financiera, para luego procesar la Orden de Compra y enviar los productos.

Por otro lado, bajo el modelo de Proceso de Negocio, se presenta un Diagrama de Clases (ver Figura 8.15), el que es obtenido automáticamente y se incluyen Patrones de Seguridad, los cuales satisfacen los requisitos de seguridad especificados en el Proceso de Negocio Seguro.

A continuación se realizan una serie de preguntas relacionadas con el diagrama generado, al cual se le ha dado el nombre de Modelo B.

PROCESO DE NEGOCIO SEGURO: PROCESAMIENTO DE COMPRA

MODELO B



En el proceso de negocio seguro, se pueden apreciar los siguientes requisitos de seguridad:

- **Privacidad**, en el pool "Financial Institution".
- **Integridad**, en el mensaje "Payment Information".
- **Control de Acceso** con registro de auditoría, en la tarea "Authorize Payment".

Figura 8.14 – Procesamiento Orden de Compra adaptado de OM (2015).

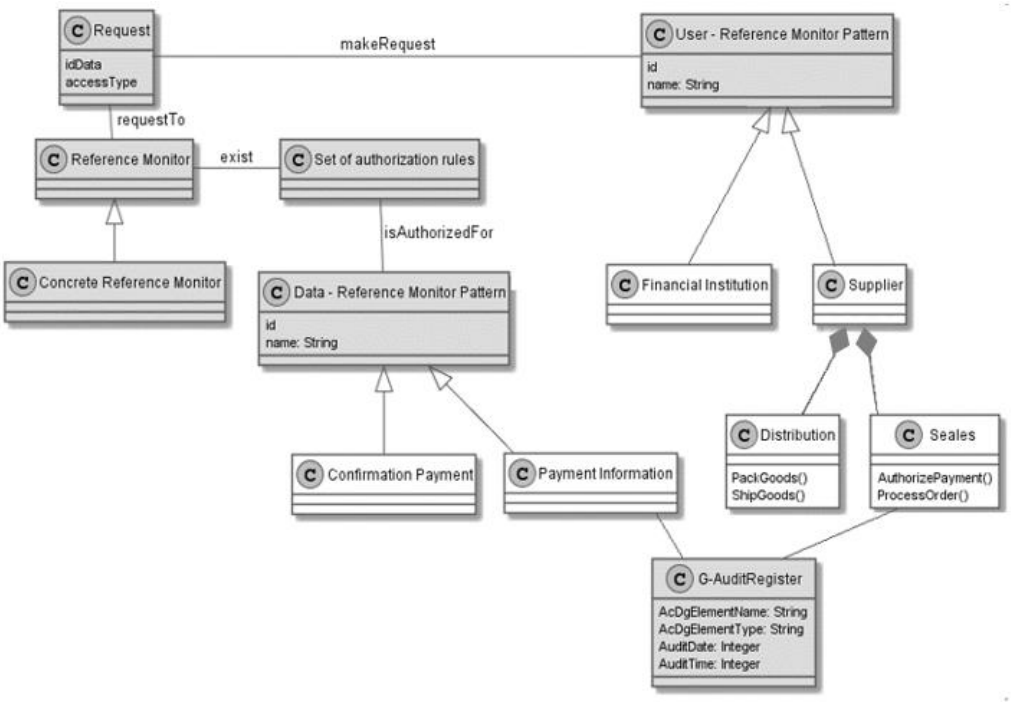


Figura 8.15 - Transformación M-SecBP&P – Procesamiento Orden de Compra.

PARTE III - PROCESAMIENTO DE COMPRA - MODELO B

De acuerdo a su criterio, responda cada una de las siguientes preguntas:

1. Dentro del Proceso de Negocio Seguro, los conceptos de seguridad ahí presentes ¿se ven reflejados en su totalidad en el diagrama de clases generado?

Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Muy de acuerdo
☐	☐	☐	☐	☐

2. ¿Se puede comprender fácilmente la relación entre los requisitos de seguridad (dentro del proceso de negocio) y las clases de seguridad (dentro del diagrama de clases)?

Muy difícil de entender	Algo difícil de entender	Ni difícil ni fácil de entender	Algo fácil de entender	Muy fácil de entender
☐	☐	☐	☐	☐

3. La **Privacidad** hace referencia a que la información, datos y/o mensajes no puedan ser divulgados a personas no autorizadas.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.16:

- La clase **User – Reference Monitor Pattern**, es una clase abstracta para representar los usuarios del sistema
- La clase **Request**, representa las peticiones de acceso hacia recursos realizadas por los usuarios.
- La clase **Reference Monitor**, es la clase encargada de capturar las peticiones de los usuarios y validar si dicho usuario posee acceso al recurso solicitado.
- La clase **Set of authorization rules**, representa las reglas de acceso que posee cada recurso dentro del sistema.
- La clase **Data – Reference Monitor Pattern**, es una clase abstracta para representar los recursos del sistema.

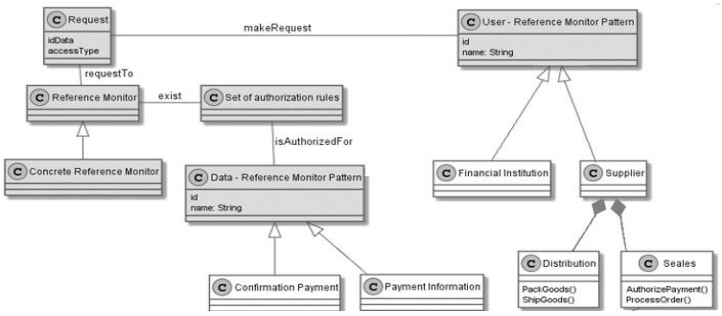


Figura 8.16 –M-SecBP&P - Privacidad – Modelo B.

Considerando el diagrama de clases presentado en la Figura 8.16, indique si el concepto **Privacidad** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

4. La **Integridad** hace referencia a que los mensajes y/o datos deben estar protegidos frente a la corrupción intencional y no autorizada.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.17:

- La clase **User – Reference Monitor Pattern**, es una clase abstracta para representar los usuarios del sistema
- La clase **Request**, representa las peticiones de acceso hacia recursos realizadas por los usuarios.
- La clase **Reference Monitor**, es la clase encargada de capturar las peticiones de los usuarios y validar si dicho usuario posee acceso al recurso solicitado.
- La clase **Set of authorization rules**, representa las reglas de acceso que posee cada recurso dentro del sistema.
- La clase **Data – Reference Monitor Pattern**, es una clase abstracta para representar los recursos del sistema.
- La clase **G-AuditRegister**, almacena información relacionada sobre quién accede la información del sistema.

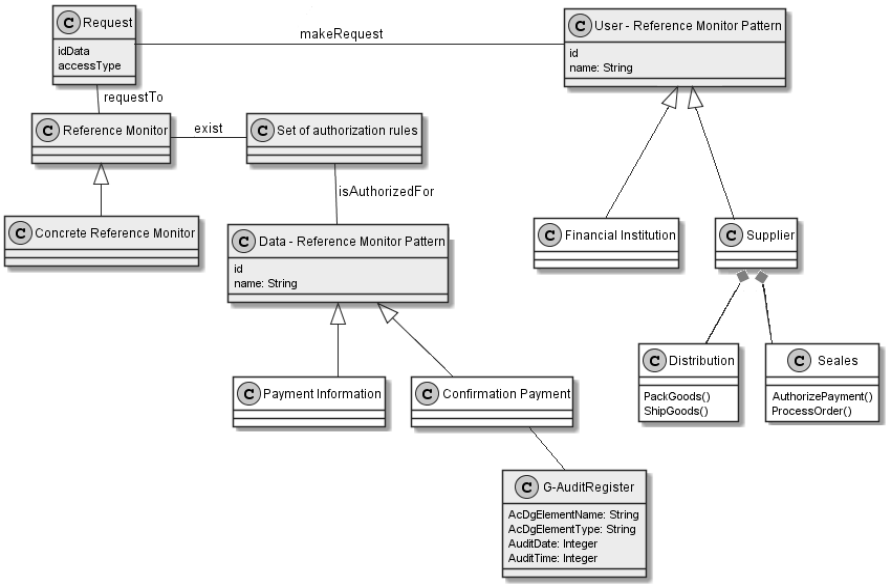


Figura 8.17 – M-SecBP&P - Integridad – Modelo B.

Considerando el diagrama de clases presentado en la Figura 8.17, indique si el concepto de **Integridad** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

5. El **Control de Acceso** hace referencia a la limitación de acceso a los recursos, permitiendo acceso sólo a usuarios autorizados.

A continuación se presenta la definición de las clases que representan seguridad (clases en gris) referentes al diagrama de clases presentado en la Figura 8.18:

- La clase **User – Reference Monitor Pattern**, es una clase abstracta para representar los usuarios del sistema
- La clase **G-AuditRegister**, almacena el nombre y tipo de elementos que poseen registro de auditoría, además de la fecha y hora en que ocurren eventos asociados.

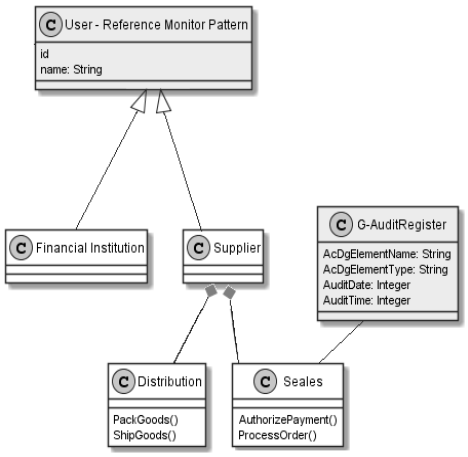


Figura 8.18 – M-SeBP&P - Control de Acceso – Modelo B.

Considerando el diagrama de clases presentado en la Figura 8.18, indique si el concepto de **Control de Acceso** se puede entender en dichas clases:

Muy difícil de entender	**Algo difícil de entender**	**Ni difícil ni fácil de entender**	**Algo fácil de entender**	**Muy fácil de entender**
☐	☐	☐	☐	☐

6. ¿El nivel de detalle del diagrama de clases generado, que incluye aspectos de seguridad, puede servir de base para comenzar a desarrollar un sistema?

Muy en desacuerdo	**En desacuerdo**	**Neutral**	**De acuerdo**	**Muy de acuerdo**
☐	☐	☐	☐	☐

7. Agregue algún comentario en el recuadro si lo desea:

PARTE IV - ANÁLISIS MODELO A VS MODELO B

De acuerdo a su criterio, responda cada una de las siguientes preguntas:

1. Con respecto a la seguridad dentro del proceso de negocio seguro ¿Cuál de los modelos vistos representa mejor dichos conceptos?

Modelo A ☐

Modelo B ☐

2. ¿Cuál de los dos modelos permite comprender con mayor facilidad la relación entre los requisitos de seguridad dentro del proceso de negocio seguro y las clases de seguridad dentro del diagrama de clases?

Modelo A ☐

Modelo B ☐

3. Dentro de los diagramas de clases mostrados ¿Cuál de los dos modelos posee mayor facilidad para implementar la **Privacidad**?

Modelo A ☐

Modelo B ☐

4. Dentro de los diagramas de clases mostrados ¿Cuál de los dos modelos posee mayor facilidad para implementar la **Integridad**?

Modelo A ☐

Modelo B ☐

5. Dentro de los diagramas de clases mostrados ¿Cuál de los dos modelos posee mayor facilidad para implementar un **Control de Acceso**?

Modelo A ☐

Modelo B ☐

6. ¿Qué modelo visto posee un mayor nivel de detalle referente a la seguridad, teniendo en cuenta que sería la base para comenzar a desarrollar un sistema?

Modelo A ☐

Modelo B ☐

ANEXO 3 - ANÁLISIS DE ESTADÍSTICOS DESCRIPTIVOS ENCUESTA REGISTRO DE USUARIOS

A continuación se detallan los resultados obtenidos de la encuesta relacionada con el Proceso de Negocio Seguro de Registro de Usuarios. El contexto de dicho proceso, es sobre el registro de un usuario en una página Web. Se utiliza un enfoque de caja negra sobre la página Web, es decir, no se muestran los procesos realizados por la misma. Por otra parte, las actividades del usuario contemplan las actividades de llenar el formulario de registros, confirmación de email y log in dentro de la página Web. El Proceso de Negocio Seguro descrito anteriormente, corresponde al que se muestra en la Figura 8.19.

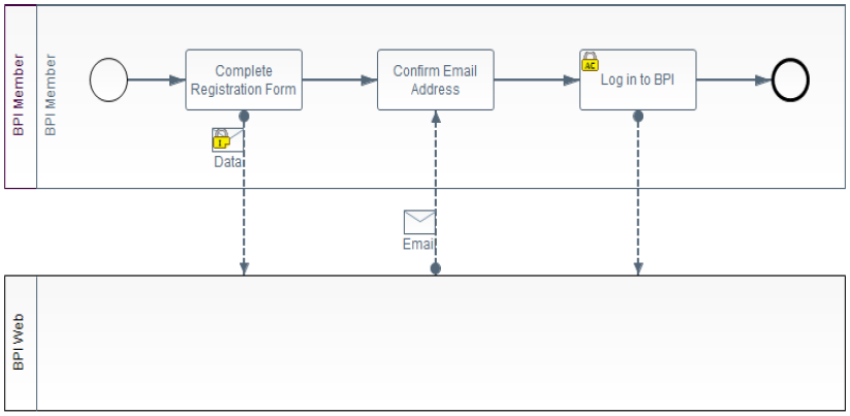


Figura 8.19 – BPMN Registro de Usuario.

SELECCIÓN DE VARIABLES

La variable independiente (también denominada factor principal) es el origen de los Diagramas de Clase, la cual es una variable nominal que toma dos valores:

1. **Modelo A:** Diagrama UML obtenido automáticamente a través de **BPMN-BPSec**.
2. **Modelo B:** Diagrama UML obtenido automáticamente a través de **M-SecBP&P**.

Las variables dependientes son la completitud, entendibilidad, y si el nivel de detalle forma la base para crear un sistema, todo esto enfocándonos en los aspectos de seguridad.

El Diagrama de Clases correspondiente al *Modelo A*, corresponde al mostrado en la Figura 8.20, el cual es realizado con BPMN-BPSec.

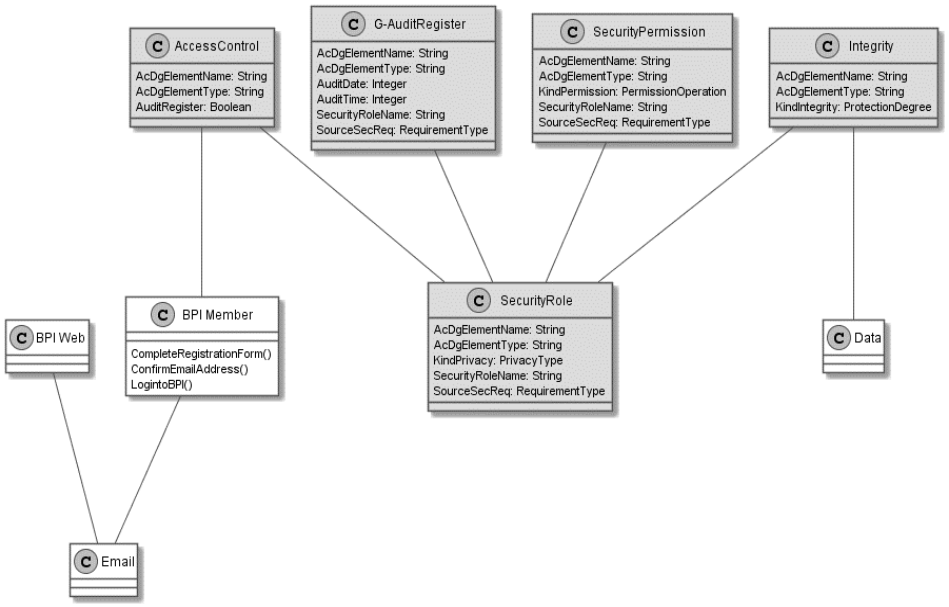


Figura 8.20 – Modelo A – Registro de Usuario – BPMN-BPSec.

Por otro lado, la traducción realizada con el método que se está proponiendo se muestra en la Figura 8.21.

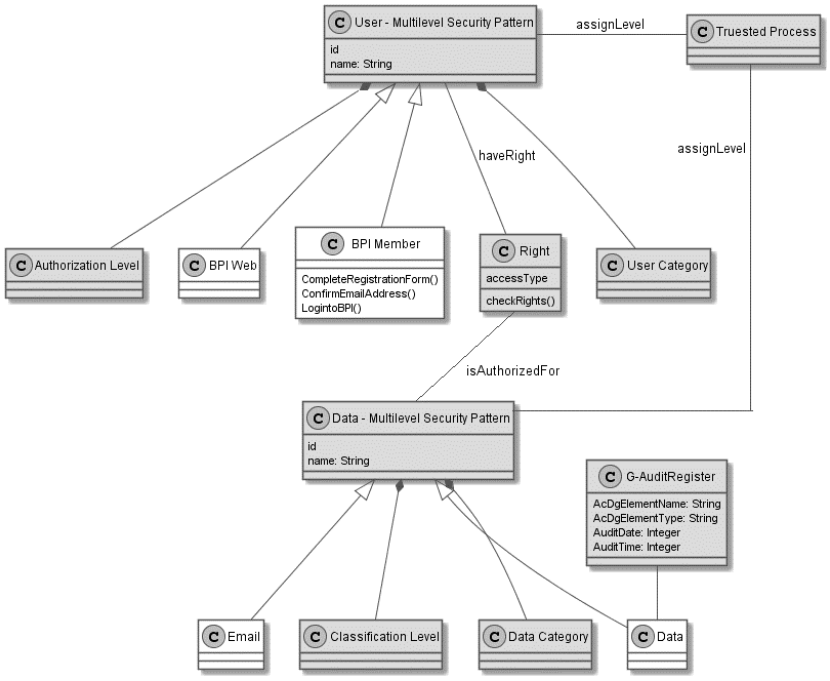


Figura 8.21 – Modelo B – Registro de Usuario – M-SecBP&P.

COMPLETITUD ASPECTOS DE SEGURIDAD

Con respecto a la completitud de los aspectos de seguridad percibida por los sujetos, primero se analizó de forma individual para cada modelo, y luego de forma comparativa.

De forma individual, según los usuarios encuestados, ambos modelos poseen un nivel aceptable y similar sobre la completitud de los aspectos de seguridad, es decir, se ve claramente reflejada la totalidad de dichos aspectos en los modelos generados.

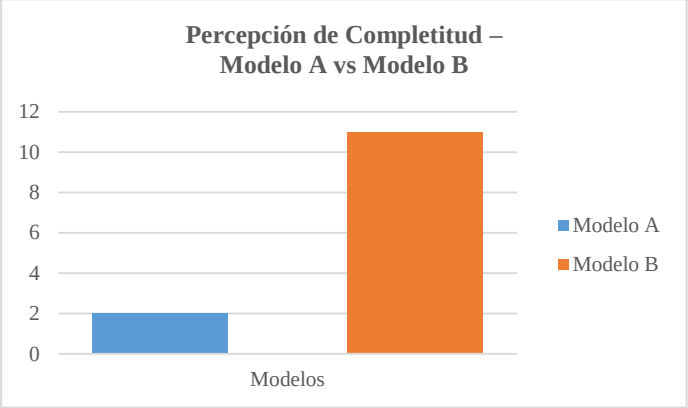


Figura 8.22 - Percepción de Completitud Modelo A vs Modelo B.

Al momento de comparar ambos modelos, en la Figura 8.22 se puede ver claramente una tendencia con respecto al *Modelo B* por sobre el *Modelo A*, donde el 84% de los sujetos encuestados perciben que el *Modelo B*, posee una mejor completitud con respecto a los aspectos de seguridad extraídos desde el Proceso de Negocio Seguro.

ENTENDIBILIDAD ASPECTOS DE SEGURIDAD

Al momento de preguntar a priori, sobre si se comprende fácilmente la relación entre los requisitos de seguridad dentro del Proceso de Negocio, y las clases de seguridad generadas, el *Modelo B* posee un nivel de comprensión un tanto mejor que el *Modelo A*. Sin embargo, al momento de hacer la comparación, se puede apreciar en la Figura 8.23, que la mayoría de los sujetos encuestados prefieren el *Modelo B* por sobre el *Modelo A*, lo que indica que sin tener conocimientos sobre la funcionalidad de las clases generadas, el *Modelo B* posee un mayor nivel de entendimiento sobre los aspectos de seguridad allí representados.

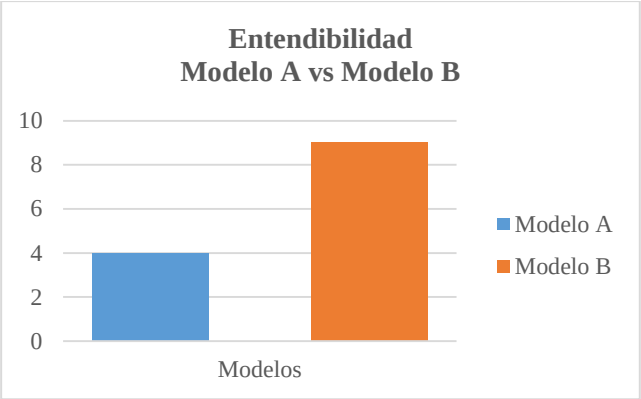


Figura 8.23 – Entendibilidad Modelo A vs Modelo B.

Por otro lado, como muestra la Figura 8.24, al momento de preguntar en qué modelo se ve mejor reflejado cada uno de los aspectos de seguridad presentes en el Proceso de Negocio Seguro, existe una clara tendencia a elegir el *Modelo B*.

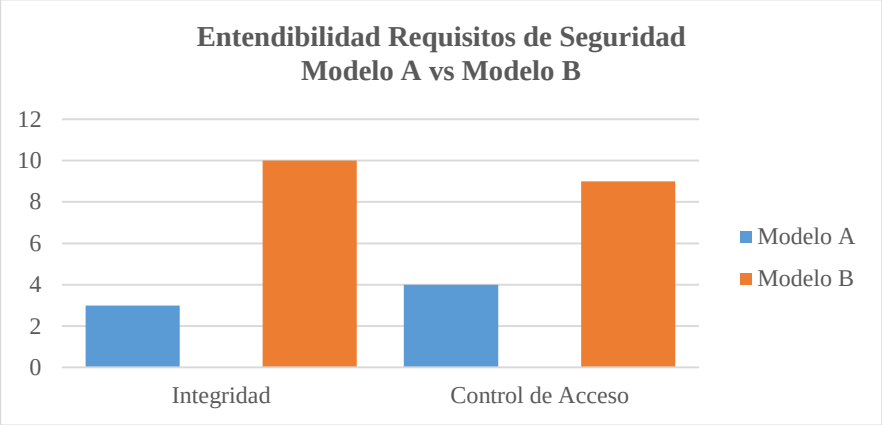


Figura 8.24 – Entendibilidad Requisitos de Seguridad Modelo A vs Modelo B.

La tendencia a elegir el *Modelo B* sobre el *Modelo A*, se debe a que en el segundo modelo, los encuestados perciben un nivel menor de entendibilidad sobre cada aspecto de seguridad por separado, no así con respecto al *Modelo B*, donde todos los encuestados tuvieron un nivel aceptable de entendimiento de cada aspecto de seguridad. Cabe destacar que para esta parte de la encuesta, a los sujetos se le entregó información acerca del funcionamiento de las clases de seguridad.

NIVEL DE DETALLE APTO PARA CREAR UN SISTEMA

Cuando se le preguntó a los encuestados sobre si el modelo generado posee un nivel de detalle sobre los aspectos de seguridad que fuese apto para crear un sistema, el *Modelo B* posee un mejor nivel que el *Modelo A*.

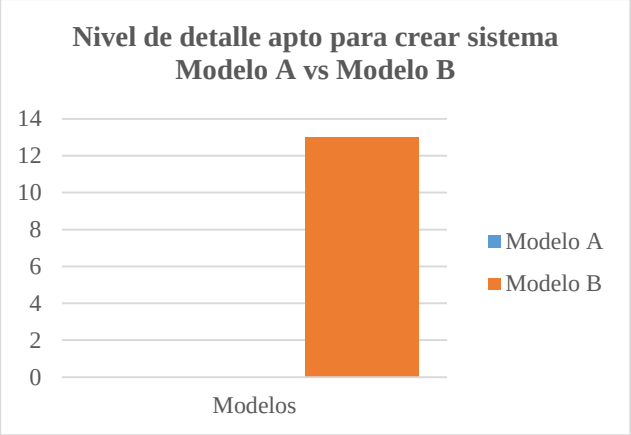


Figura 8.25 – Percepción Nivel de Detalle Modelo A vs Modelo B.

Cuando comparan ambos modelos (*Modelo A y Modelo B)*, el 100% de los encuestados coincide en la idea de que los aspectos de seguridad dentro del *Modelo B*, forman una mejor base para el desarrollo de un sistema. Dichos resultados se ven reflejados en la Figura 8.25.

CONCLUSIÓN ANÁLISIS ESTADÍSTICOS DESCRIPTIVOS

Se puede concluir que al momento de analizar ambos modelos de forma individual, estos poseen un nivel aceptable con respecto a las variables analizadas (completitud de aspectos de seguridad, entendibilidad de aspectos de seguridad y nivel de detalle de seguridad apto para crear un sistema). Sin embargo cuando comparamos ambos modelos generados, se puede apreciar una clara tendencia del *Modelo B* por sobre el *Modelo A* con respecto a la completitud, es decir, los conceptos de seguridad dentro del Proceso de Negocio Seguro se ven reflejados en el Diagrama de Clases generado. Referente al nivel de entendibilidad, los encuestados perciben que el *Modelo B* posee un mejor nivel de entendibilidad con respecto a la seguridad, en comparación con el *Modelo A*. Finalmente, en cuanto a si el nivel de detalle de seguridad forma la base para desarrollar un sistema, existe una gran diferencia en cuanto a los modelos, donde el 100% de los encuestados coinciden en que el nivel de detalle de seguridad del *Modelo B* es el más apto para comenzar a desarrollar un sistema.

Cabe destacar que el *Modelo B* hacía uso de Patrones de Seguridad, los cuales están diseñados para que cualquier desarrollador pueda entender el funcionamiento de su estructura, debido a que representan soluciones conceptuales a problemas de seguridad, no pasa lo mismo con el *Modelo A*, el cual extrae directamente los aspectos de seguridad desde el Proceso de Negocio Seguro, se cree que este es el factor principal para que el *Modelo B* sobresaliera sobre el *Modelo A.*

ANEXO 4 - ANÁLISIS DE ESTADÍSTICOS DESCRIPTIVOS ENCUESTA PROCESAMIENTO DE COMPRA

A continuación se detallan los resultados obtenidos de la encuesta relacionada con el Proceso de Negocio Seguro de Procesamiento de Compra. El contexto de este proceso es sobre un procesamiento de Orden de Compra por parte de un proveedor, el cual recibe la información del pago desde una institución financiera, posterior a ello, envía la confirmación del pago hacia la misma entidad financiera, para luego procesar la Orden de Compra y enviar los productos. El Proceso de Negocio Seguro descrito anteriormente, corresponde al que se muestra en la Figura 8.26.

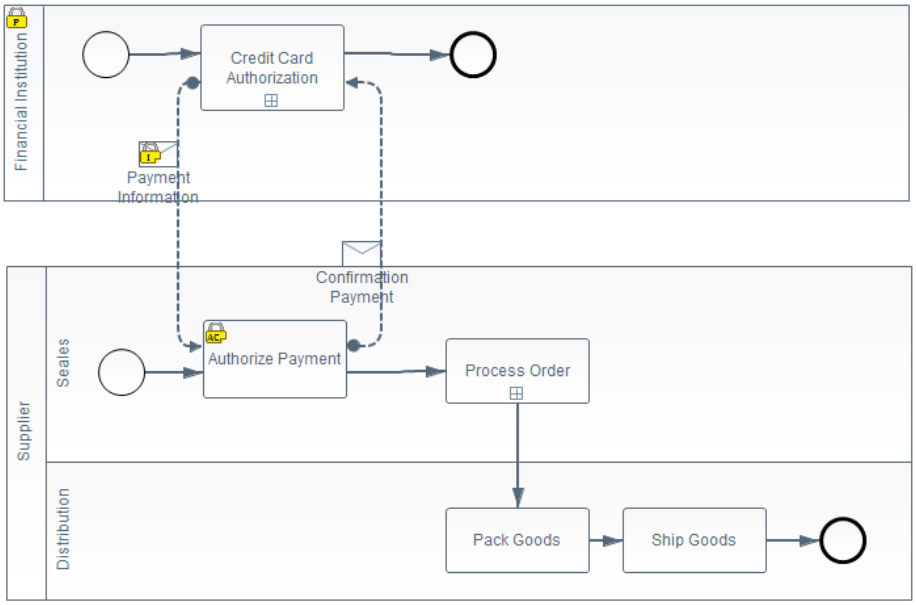


Figura 8.26 – Ejemplo Procesamiento de Compra adaptado de OMG (2015).

SELECCIÓN DE VARIABLES

La variable independiente (también denominada factor principal) es el origen de los Diagramas de Clase, la cual es una variable nominal que toma dos valores:

3. **Modelo A:** Diagrama UML obtenido automáticamente a través de la extensión **BPMN-BPSec.**
4. **Modelo B:** Diagrama UML obtenido automáticamente a través de **M-SecBP&P.**

Las variables dependientes son la completitud, entendibilidad, y si el nivel de detalle forma la base para crear un sistema, todo esto enfocándonos en los aspectos de seguridad.

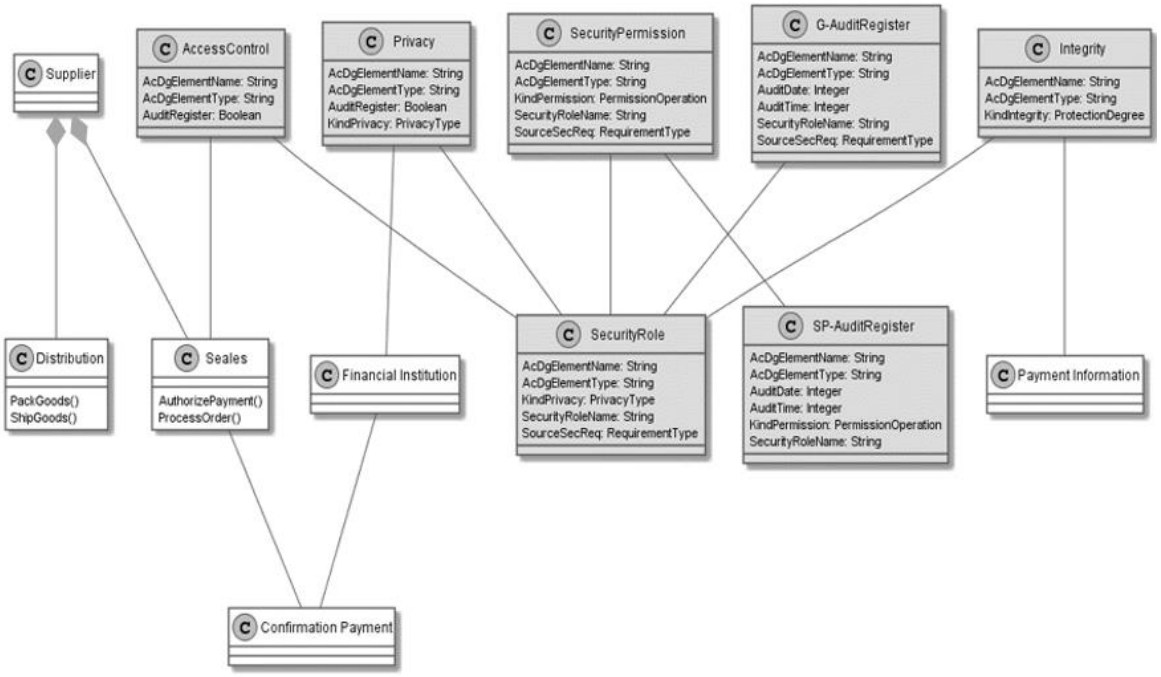


Figura 8.27 – Modelo A – Procesamiento de Compra – BPMN-BPSec.

El Diagrama de Clases correspondiente al *Modelo A*, es el que se muestra en la Figura 8.27, el cual es realizado con la extensión BPMN-BPSec.

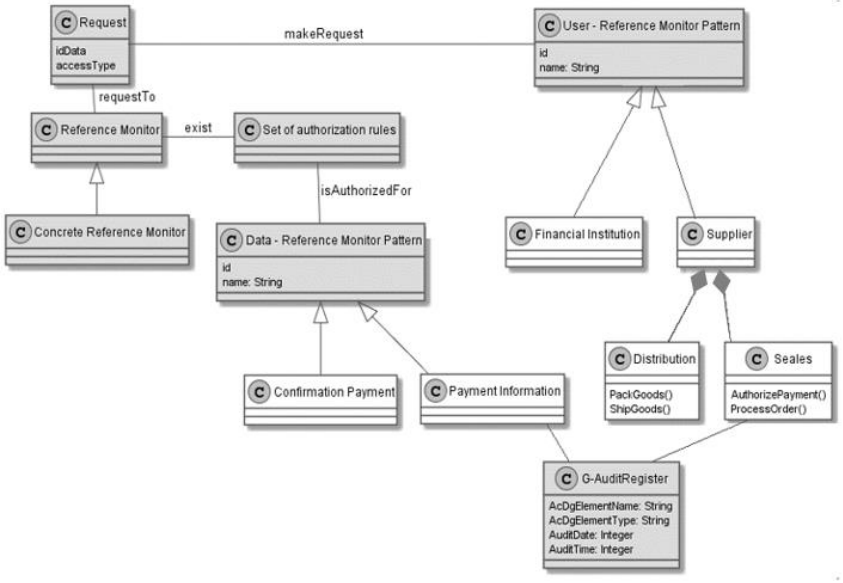


Figura 8.28 – Modelo B – Procesamiento de Compra – M-SecBP&P.

Por otro lado, la traducción realizada con el método que se está proponiendo, se muestra en la Figura 8.28.

COMPLETITUD ASPECTOS DE SEGURIDAD

Con respecto a la completitud de los aspectos de seguridad percibida por los sujetos, primero se analizó de forma individual para cada modelo, y luego de forma comparativa.

De forma individual, ambos modelos poseen un nivel aceptable y similar según los usuarios encuestados, resaltando una leve mejoría con respecto al *Modelo A*.

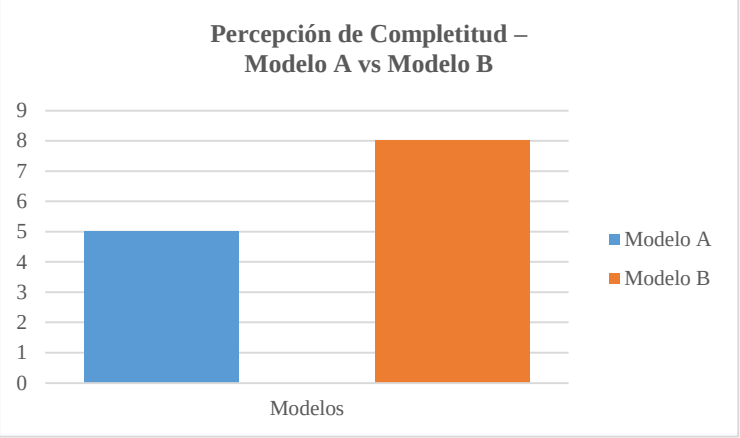


Figura 8.29 - Percepción de Completitud Modelo A vs Modelo B.

Sin embargo, al momento de comparar ambos modelos, en la Figura 8.29 se puede ver claramente una tendencia con respecto al *Modelo B* sobre el *Modelo A*, donde el 62% de los sujetos encuestados perciben que el *Modelo B*, posee una mejor completitud con respecto a los aspectos de seguridad extraídos desde el Proceso de Negocio Seguro.

ENTENDIBILIDAD ASPECTOS DE SEGURIDAD

Al momento de preguntar a priori, sobre si es posible comprender fácilmente la relación entre los requisitos de seguridad dentro del Proceso de Negocio, y las clases de seguridad generadas, el *Modelo A* posee un nivel un tanto mejor que el *Modelo B*. Por otro lado, al momento de hacer la comparación de los modelos, se puede apreciar en la Figura 8.30, que ambos modelos poseen un nivel similar con respecto a la entendibilidad de los aspectos de seguridad.

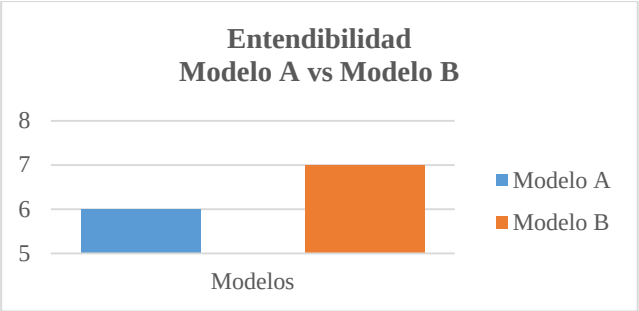


Figura 8.30 – Entendibilidad Modelo A vs Modelo B.

Por otro lado, como muestra la Figura 8.31, al momento de preguntar sobre qué modelo refleja mejor cada uno de los aspectos de seguridad presentes en el Proceso de Negocio Seguro, existe una clara tendencia a elegir el *Modelo B*.

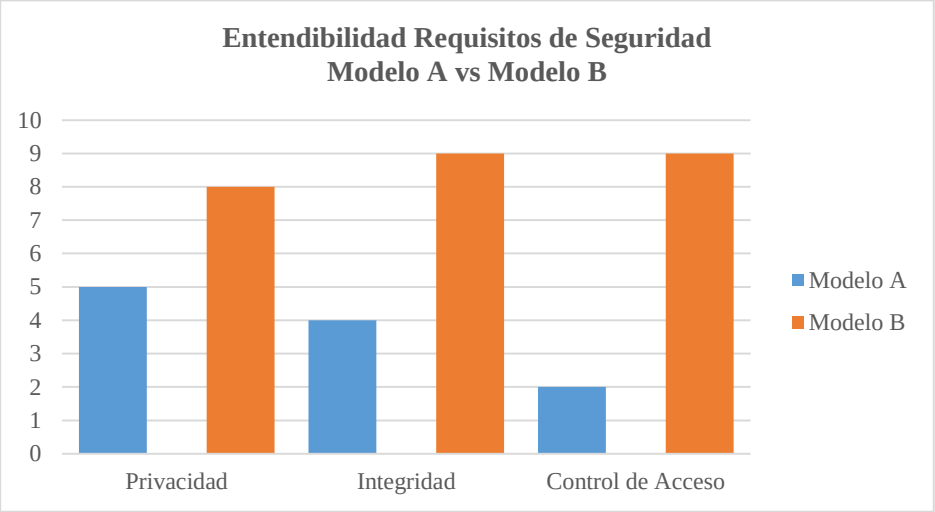


Figura 8.31 – Entendibilidad Requisitos de Seguridad Modelo A vs Modelo B.

La tendencia a elegir el *Modelo B* sobre el *Modelo A*, se debe a que en el segundo modelo mencionado, los encuestados perciben un nivel más bajo de entendibilidad sobre cada aspecto de seguridad por separado, no así con respecto al *Modelo B*, donde todos los encuestados tuvieron un nivel aceptable de entendimiento de cada aspecto de seguridad. Cabe destacar que para esta parte de la encuesta, a los sujetos se le entregó información acerca del funcionamiento de las clases relacionadas a la seguridad.

NIVEL DE DETALLE APTO PARA CREAR UN SISTEMA

Cuando se le preguntó a los encuestados sobre si el modelo generado posee un nivel de detalle sobre los aspectos de seguridad que fuese apto para crear un sistema, el *Modelo B* posee un mejor nivel que el *Modelo A*.

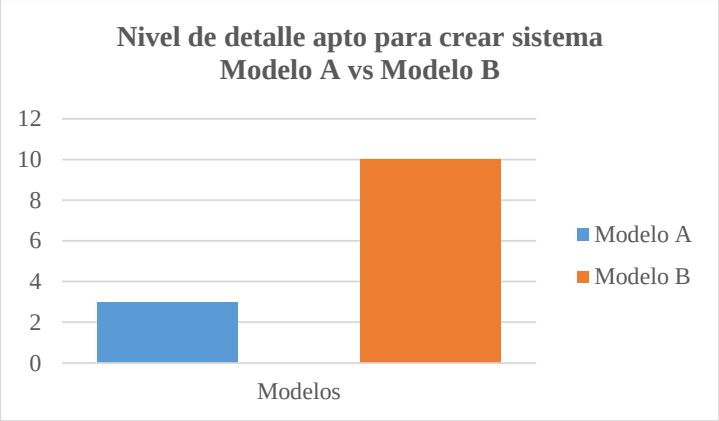


Figura 8.32 – Percepción Nivel de Detalle Modelo A vs Modelo B.

Cuando comparan ambos modelos (*Modelo A y Modelo B)*, el 70% de los encuestados coincide en la idea de que los aspectos de seguridad del *Modelo B* forman un mejor base para el desarrollo de un sistema. Dichos resultados se ven reflejados en la Figura 8.32.

CONCLUSIÓN ANÁLISIS ESTADÍSTICOS DESCRIPTIVOS

Se puede concluir que al momento de analizar ambos modelos de forma individual, estos poseen un nivel aceptable con respecto a las variables analizadas (completitud de aspectos de seguridad, entendibilidad de aspectos de seguridad y nivel de detalle de seguridad apto para crear un sistema). Sin embargo al momento de comparar los modelos generados, se puede apreciar una clara tendencia del *Modelo B* por sobre el *Modelo A* con respecto a la completitud, es decir, los conceptos de seguridad dentro del Proceso de Negocio Seguro se ven reflejados en el Diagrama de Clases generado. En cuanto al nivel de entendibilidad de los aspectos de seguridad, los encuestados perciben un nivel similar tanto para el *Modelo B* como el *Modelo A*.

Finalmente, en cuanto a si el nivel de detalle de seguridad es apto para crear un sistema, existe una gran diferencia entre los modelos, donde el 70% de los encuestados coinciden en que el nivel de detalle de los aspectos de seguridad del *Modelo B* es el más apto para comenzar a desarrollar un sistema.

Cabe destacar que el *Modelo B* hacía uso de Patrones de Seguridad, los cuales están diseñados para que cualquier desarrollador pueda entender el funcionamiento de su estructura, debido a que representan soluciones conceptuales a problemas de seguridad, no así mismo con el *Modelo A*, el cual extrae directamente los aspectos de seguridad desde el Proceso de Negocio Seguro, se cree que este es el factor principal para que el *Modelo B* sobresaliera por sobre el *Modelo A.*

IMPACTO CONOCIMIENTOS RELEVANTES SOBRE PATRONES DE SEGURIDAD

La encuesta también permitió para analizar el impacto que tienen los conocimientos relevantes sobre los Patrones de Seguridad, en otras palabras, si poseer conocimiento sobre estos puede influir en el nivel de entendimiento que poseen los sujetos sobre el *Modelo B*, el cual es generado utilizando Patrones de Seguridad.

Para el análisis, se plantearon las siguientes hipótesis de investigación:

- H_0: No existe una relación significativa con respecto al nivel de conocimiento sobre Patrones de Seguridad, y el nivel de Entendimiento sobre el *Modelo B.*
- H_1: Existe una relación significativa con respecto al nivel de conocimiento sobre Patrones de Seguridad, y el nivel de Entendimiento sobre el *Modelo B.*

Debido a que las puntuaciones obtenidas por el cuestionario no siguen una distribución normal, se decide realizar el análisis no paramétrico U de Mann Whitney, lo cual se obtuvo que *"Poseer conocimientos sobre patrones de seguridad no posee una relación significativa con el nivel de entendimiento percibido por los encuestados"*, todo esto enfocado solo en el *Modelo B*, que es el que interesa por motivos de investigación.

En la Tabla 8.1 se muestra el resultado de la ejecución del análisis estadístico U Mann Whitney.

Estadísticos de prueba[a]

	¿Se puede comprender fácilmente la relación entre los requisitos de seguridad (dentro del proceso de negocio) y las clases de seguridad (clases en gris dentro del diagrama de clases)?
U de Mann-Whitney	14,500
W de Wilcoxon	20,500
Z	-,092
Sig. asintótica (bilateral)	,927

Tabla 8.1 – U de Mann Withney – Conocimiento – Entendimiento – Encuesta B.

Como se puede apreciar, no se observa una relación estadísticamente significativa (p = 0,927) entre poseer conocimientos sobre Patrones de Seguridad y el nivel de entendimiento del *Modelo B*, resultando en la aceptación de la hipótesis nula.

Lo anterior lleva a la conclusión de que no es estrictamente necesario poseer conocimientos sobre Patrones de Seguridad para poder entender el *Modelo B*, que es

el que se está proponiendo como una alternativa a la traducción del Proceso de Negocio Seguro hacia Diagrama de Clases.

Por otro lado, también quisimos ver si el poseer conocimientos de Patrones de Seguridad influencia significativamente la selección de los modelos generados, para lo cual planteamos las siguientes hipótesis:

- **H_0:** No existe una relación significativa entre los sujetos que poseen conocimientos sobre Patrones de Seguridad, y la selección del modelo (*Modelo A* y *Modelo B)* con mejor nivel de entendimiento posee.
- **H_1:** Existe una relación significativa entre los sujetos que poseen conocimientos sobre Patrones de Seguridad, y la selección del modelo (*Modelo A* y *Modelo B)* con mejor nivel de entendimiento posee.

Se utilizó la misma agrupación antes descrita para el nivel de conocimientos de Patrones de Seguridad, con lo cual se obtuvo que *"No existe una relación significativa entre los sujetos que poseen conocimientos sobre Patrones de Seguridad, y la selección del modelo (Modelo A y Modelo B) con mejor nivel de entendimiento posee".*

En la Tabla 8.2 se muestra el resultado de la ejecución del análisis estadístico U Mann Whitney.

Estadísticos de prueba[a]

	¿Cuál de los dos modelos permite comprender con mayor facilidad la relación entre los requisitos de seguridad dentro del Proceso de Negocio Seguro y las clases de seguridad dentro del diagrama de clases?
U de Mann-Whitney	11,000
W de Wilcoxon	17,000
Z	-,781
Sig. asintótica (bilateral)	,435

a. Variable de agrupación: ¿Posee conocimientos sobre Patrones de Seguridad?

Tabla 8.2 - U de Mann Withney – Conocimiento - Selección de Modelos – Encuesta B.

Como se puede apreciar, no se observa una relación estadísticamente significativa (p = 0,435) entre poseer conocimientos sobre Patrones de Seguridad y la selección del modelo que mejor nivel de entendimiento posee, resultando en la aceptación de la hipótesis nula.

Lo anterior induce a pensar de que no es necesario poseer conocimientos sobre Patrones de Seguridad para que los sujetos entiendan mejor el *Modelo B* por sobre el *Modelo A*. Esto se puede apreciar igual en la Figura 8.33, donde se puede ver claramente que a pesar de que los sujetos no poseen conocimientos sobre Patrones

de Seguridad, no fue un impedimento para poder entender mejor el modelo que utilizaba dichos patrones.

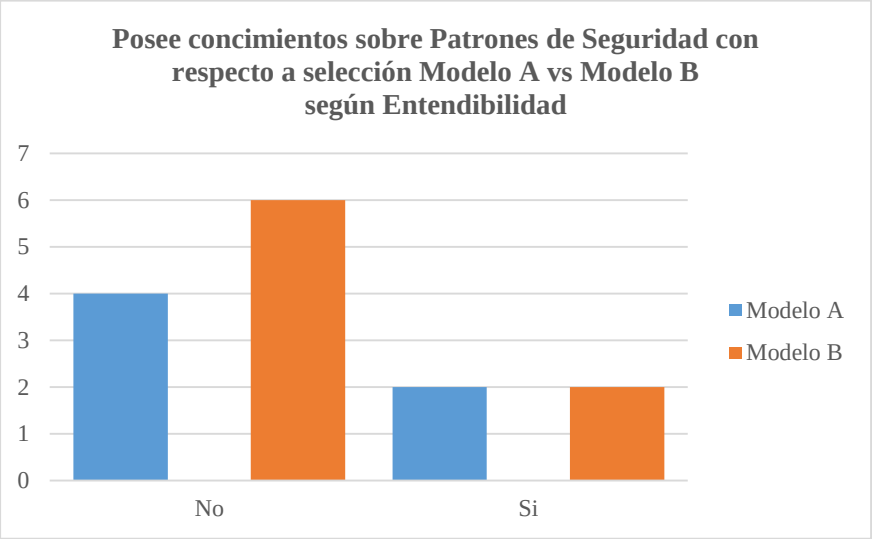


Figura 8.33 – Tabla cruzada – Conocimientos Patrones de Seguridad vs Selección de Modelo.

Con este experimento podemos observar que no existe una relación estadísticamente significativa entre poseer conocimientos sobre Patrones de Seguridad, y el nivel de entendibilidad que los sujetos percibían sobre el *Modelo B*, el cual hacía uso de dichos patrones.

Lo anterior refuerza la idea de utilizar Patrones de Seguridad en etapas tempranas del ciclo de desarrollo de software a pesar de que no exista un experto en el área de seguridad que brinde soporte en su uso.