IX Congreso iberoamericano
de seguridad informática
Universidad de Buenos Aires
Ciudad Autónoma de Buenos Aires, Argentina
1 al 3 de noviembre de 2017

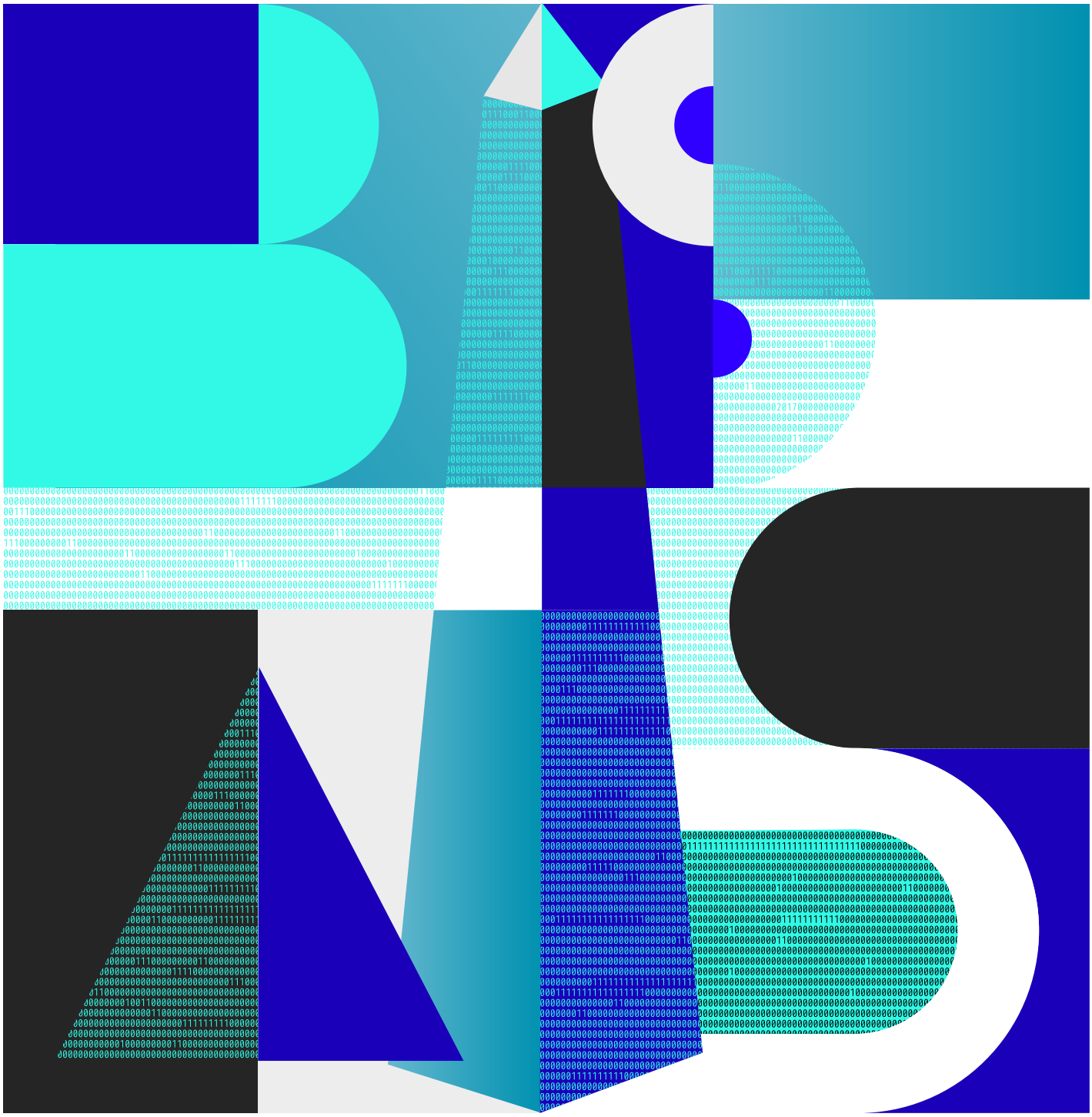
CIBSI

EU DE BA

PSI
POSGRADO EN SEGURIDAD INFORMATICA

CRIPTORED

Libro de Actas



Actas del IX Congreso Iberoamericano de Seguridad Informática
CIBSI2017, Buenos Aires, Argentina, 1 al 3 de Noviembre de 2017

Editores
Alberto E. Dams
Hugo A. Pagola
Luis E. Sánchez Crespo
Jorge Ramió Aguirre

Diseño de Tapas
Federico Dams

ISBN: en trámite

Prefacio

Del 1 al 3 de Noviembre se celebrará en la Universidad de Buenos Aires el IX Congreso Iberoamericano de Seguridad Informática - CIBSI 2017. El congreso está organizado por la Maestría en Seguridad Informática de la UBA en colaboración con la Red Temática Iberoamericana de Criptografía y Seguridad de la Información Criptored.

Este espacio permitirá a las empresas, entidades públicas, entornos militares, de defensa, centros académicos y de investigación exponer sus avances y servicios vinculados con la seguridad, facilitando el intercambio de conocimientos y la formación de redes de colaboración en este ámbito.

El congreso contará con la presencia de especialistas de Latinoamérica y de Europa entre otros de Argentina, Brasil, Colombia, Ecuador, México, Perú, Uruguay, España y Francia. Estamos muy satisfechos por el nivel de los artículos que se presentarán y el de los invitados especiales que tendremos. En esta novena edición del CIBSI, se destacan las presencias de referentes internacionales en la materia como Hugo Scolnik director de la Maestría en seguridad Informática de la UBA y Hugo Krawczyk Distinguished Research Staff Member with the Cryptography Group at the IBM T.J. Watson Research Center.

Organización de la Conferencia

Comité Organizador

Hugo Pagola, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Alberto Dams, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España
Luis E. Sánchez Crespo, Universidad de Castilla La Mancha, España

Comité Local

Facundo Caram, FIUBA, Argentina
Luis Catanzariti, UTNfrba, Argentina
Marcia Maggiore, MUBA, Argentina
Patricia Prandini, MUBA, Argentina

Comisión de Posgrado Maestría en Seguridad Informática UBA

Mg Ing Alberto Dams, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Pedro Hecht, Maestria en Seguridad Informatica UBA, Argentina
Ing Hugo Pagola, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Ricardo Rivas, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Raul Saroka, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Hugo Scolnik, Maestria en Seguridad Informatica UBA, FCEN-UBA Argentina

Comité del Programa

Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp, Brasil
Javier Areitio	Universidad de Deusto, España
Rodolfo Baader	Universidad de Buenos Aires, Argentina
Gustavo Betarte	Facultad de Ingeniería, Universidad de la República, Uruguay
Carlos Blanco Bueno	Universidad de Cantabria, España
Joan Borrell	Universitat Autònoma de Barcelona, España
Pino Caballero-Gil	DEIOC, Universidad de La Laguna, España
Jeimy Cano	Universidad de los Andes, Colombia
Eduardo Carozo	Universidad de Montevideo, Uruguay
Joan-Josep Climent	Universitat d'Alacant, España
Roger Clotet	Universidad Simón Bolívar, Venezuela
Alberto Dams	Universidad de Buenos Aires, Argentina
José María De Fuentes	Universidad Carlos III de Madrid, España
Josep Domingo-Ferrer	Universitat Rovira i Virgili, España
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, España
Angelica Florez Abril	Universidad Pontificia Bolivariana, Colombia
Walter Fuertes	Universidad de las Fuerzas Armadas ESPE, Ecuador
Amparo Fuster-Sabater	Institute of Applied Physics, Madrid, España
Giovana Garrido	Universidad Tecnologica de Panama
Lorena González Manzano	Universidad Carlos III de Madrid, España
Juan Pedro Hecht	Universidad de Buenos Aires, Argentina

Luis Hernandez Encinas	Institute of Physical and Information Tecnologies, España
Emilio Hernández	Universidad Simón Bolívar, Venezuela
Leobardo Hernández	Universidad Nacional Autónoma de México
Jordi Herrera	Universitat Autònoma de Barcelona, España
Monica Karel Huerta	Universidad Politécnica Salesiana, Ecuador
Angel Martin Del Rey	Universidad de Salamanca, España
Maria Vanina Martinez	Universidad Nacional del Sur in Bahia Blanca, Argentina
Vincenzo Mendillo	Universidad Central de Venezuela
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María, Chile
Karel Huerta Monica	Universidad Politécnica Salesiana, Ecuador
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados, Mexico
Alfonso Muñoz	Criptored, España
Hugo Pagola	UBA - Facultad de Ingenieria, Argentina
Graciela Pataro	Universidad de Buenos Aires, Argentina
Alberto Peinado	Universidad de Malaga, España
Jose Pirrone	Universidad Catolica Andres Bello, Venezuela
Gustavo Presman	Universidad de Buenos Aires, Argentina
Jorge Ramio	Universidad Politécnica de Madrid, España
Ricardo Rivas	Universidad de Buenos Aires, Argentina
David Rosado	University of Castilla-La Mancha, España
Luis Enrique Sanchez Crespo	Universidad de Castilla La Mancha, España
Antonio Santos-Olmo Parra	Sicaman Nuevas Tecnologías
Raul Saroka	Universidad de Buenos Aires, Argentina
Hugo Scolnik	Universidad de Buenos Aires, Argentina
Pablo Silberfich	Universidad de Buenos Aires, Argentina
Jenny Torres	Escuela Politécnica Nacional, Ecuador
Urko Zurutuza	Mondragon University, España

SMiLeModel: A Model for the Secure Migration of Legacy Systems to Cloud Computing

Luis Márquez, David G. Rosado, Haralambos Mouratidis, Eduardo Fernández-Medina

***Abstract*— Cloud Computing is gaining importance and receiving growing attention in scientific and industrial communities. The cloud model has motivated industry and academia to adopt Cloud Computing to host a wide spectrum of applications, ranging from high computationally intensive applications to lightweight services. Notwithstanding, the migration of applications to Cloud Computing must be performed in a strategic and methodological manner, considering elements such as application performance and availability, security and privacy requirements, regulatory requirements, among others. Our research is focused on offering a framework (called SMiLe2Cloud) to help migrating legacy systems to Cloud Computing, taking into account the security features. In this paper, we have defined a model with all concepts and elements that are used in our framework, and that allows us to define inputs and outputs in each of the stages of our migration process. A case study has been conducted applicating the model in our framework, which allows us to analyze the results and proposing improvements for our framework.**

***Index Terms*—Cloud Computing, Legacy systems, Migration, Model, Security**

I. INTRODUCCIÓN

El término "Cloud Computing" cubre una amplia variedad de soluciones y entornos técnicos, incluyendo los modelos: software como servicio (SaaS, Software-as-a-service), plataforma como servicio (PaaS, Platform-as-a-service), o infraestructura como servicio (IaaS, infrastructure-as-a-service). Cloud Computing permite el aprovisionamiento de servicios a través de la abstracción de recursos físicos y virtuales. Cloud Computing está ganando popularidad entre las empresas, y cuantos más datos y servicios se muevan a la nube, más atención atrae de los investigadores de seguridad y los ciberdelincuentes [1]. Los proveedores de servicios de Cloud están construyendo confianza y atrayendo clientes. Además, los servicios en la nube continúan multiplicándose, madurando y creciendo a un ritmo acelerado, proporcionando nuevas oportunidades y amenazas a organizaciones, criminales y naciones [2]. Sin embargo, la seguridad se presenta como una de las barreras que este nuevo tipo de servicios tiene que superar para alcanzar su potencial completo [3].

Los sistemas heredados suelen formar la columna vertebral de los sistemas informáticos empresariales, aunque estos sistemas suelen plantear problemas como "fragilidad, inflexibilidad, aislamiento, inexistencia, falta de apertura, etc." [4]. Las aplicaciones y sistemas heredados son un componente importante en casi todas las organizaciones establecidas. En todas las industrias, se está creando el impulso para migrar las aplicaciones a Cloud Computing. A la vez que se ahorran costes, la velocidad de expansión y la escalabilidad encabezan la lista de motivaciones empresariales. Un número creciente de empresas considera Cloud Computing como una herramienta clave de la transformación del negocio que puede ayudar a mejorar el compromiso del cliente, forjar nuevas alianzas y generar ventajas competitivas [5]. Una vez las inversiones ya han sido realizadas, es difícil abandonar los sistemas heredados a pesar de la disponibilidad de nuevas tecnologías como Cloud. Sin embargo, muchos profesionales informáticos todavía están ávidos por empezar a aprovechar los costes, la escala y otros beneficios del almacenamiento de objetos basado en Cloud. No obstante, la seguridad es uno de los obstáculos que presentan desafíos al ejecutar aplicaciones heredadas en la nube [6]. Actualmente, no hemos encontrado trabajos con un enfoque centrado en la seguridad para los procesos de migración de los sistemas heredados [7].

Para solventar esta carencia, hemos propuesto un marco de trabajo (SMiLe2Cloud) para la migración segura de los sistemas heredados a la nube [8, 9]. Este marco de trabajo está apoyado por un conjunto de artefactos que nos permiten obtener y analizar los requisitos del sistema, definir y modelar los requisitos de seguridad con atributos específicos de la nube, seleccionar los proveedores de Cloud más apropiados, definir métricas o alinear los mecanismos de seguridad en los controles de la nube definidos por Cloud Security Alliance (CSA) [10]. Para lograr este objetivo, es necesario proporcionar una definición de nuestro modelo, el cual se basa en el lenguaje de modelado extendido Secure Tropos [11] añadiendo características de la nube.

Este artículo presenta nuestro modelo llamado "SMiLeModel" que guía el proceso de migración a la nube siguiendo las tareas definidas en nuestro marco de trabajo SMiLe2Cloud [9]. Definiremos el modelo utilizado en el marco de trabajo SMiLe2Cloud y explicaremos en detalle cómo se utiliza el modelo en cada una de las actividades y

Luis Márquez, Spanish National Authority for Markets and Competition (CNMC), Madrid, 28004, Spain, luis.marquez@cnmc.es

David G. Rosado, GSyA Research Group, Department of Information Systems and Technologies, University of Castilla-La Mancha, Ciudad Real, 13071, Spain, david.grosado@uclm.es

Haralambos Mouratidis, Secure and Dependable Software Systems (SenSe), University of Brighton, Brighton, BN2 4GJ, UK, H.Mouratidis@brighton.ac.uk

Eduardo Fernández-Medina, GSyA Research Group, Department of Information Systems and Technologies, University of Castilla-La Mancha, Ciudad Real, 13071, Spain, eduardo.fdezmedina@uclm.es

tareas de nuestro marco de trabajo.

El resto de este artículo está estructurado de la siguiente manera: La sección 2 presenta el modelo SMiLeModel donde se explican todos los conceptos, elementos y fundamentos. La sección 3 describe cómo se utiliza el modelo en nuestro marco de trabajo SMiLe2Cloud y qué elementos del modelo se usan en cada una de las actividades y tareas que muestran los resultados obtenidos en estudio de caso. Finalmente, la sección 4 muestra las conclusiones de nuestra investigación.

II. SMILEMODEL

En esta sección se presenta el modelo SMiLeModel. En primer lugar, se explican los fundamentos de esta investigación. A continuación, se describe el marco de trabajo SMiLeModel en detalle explicando los principales conceptos basados en Secure Tropos. Finalmente, se definen los nuevos conceptos de la extensión de Secure Tropos introducidos en el modelo.

A. Fundamentos

Mouratidis y Giorgini [12] proponen Secure Tropos, que es una extensión de la metodología Tropos. El enfoque se basa en el concepto de restricción de seguridad para analizar los requisitos de seguridad desde las primeras etapas del proceso de desarrollo. Similar a ese trabajo, Giorgini et al. [13] han ampliado el marco de trabajo de trabajo de ingeniería de requisitos de i */Tropos para hacer frente a los requisitos de seguridad.

Mouratidis et al. [14] se centra en la integración de las características de seguridad capturadas a través de Secure Tropos en los procesos de negocio. La introducción de la seguridad en los procesos de negocio requiere enfoques estructurados y flexibles, capaces de encapsular la lógica de las opciones de seguridad, alinearla con los objetivos organizativos de alto nivel y facilitar decisiones bien informadas y conscientes del riesgo. También consideran el ecosistema organizacional y los requisitos de seguridad alrededor de los sistemas de software. Sin embargo, para capturar completamente los requisitos de seguridad en el nivel de cloud, las propiedades de la nube deben estar bien definidas en función del contexto.

B. Modelo SMiLe

El modelo que hemos definido es una versión simplificada del modelo definido en Mouratidis et al. [14] eliminando algunos conceptos que no son esenciales para el marco de trabajo SMiLe2Cloud [9] (soft goal, por ejemplo) e incluyendo algunas otras clases que abordan problemas particulares de seguridad en la nube, como controles específicos de la nube, o abordar aspectos particulares del marco de trabajo SMiLe2Cloud, como los controles de cloud, las métricas de seguridad, propiedades o dimensiones. Nuestro modelo simplificado se puede ver en la Fig.1.

C. Conceptos principales de Secure Tropos

Secure Tropos [15] combina conceptos de ingeniería de requisitos, para representar conceptos generales e ingeniería de seguridad, para representar conceptos orientados a la seguridad. Los principales conceptos se muestran en la Fig. 2.

Un *objetivo* representa una condición en el mundo que un actor desea lograr [16]. En otras palabras, los objetivos representan los intereses estratégicos de los actores. Un *actor* representa una entidad que tiene intencionalidad y metas estratégicas dentro del sistema multiagente o dentro de su entorno organizacional [16]. Un actor puede ser un ser humano, un sistema, o una organización. En el contexto de Cloud Computing, también definimos una clase especial de actor; *un actor de la nube*. Un actor de la nube es un actor que demuestra dos características únicas, proporciona un modelo de implementación y apoya un modelo de servicio. Vale la pena afirmar que, como actor, un actor de la nube también hereda todos los atributos y asociaciones del actor, por ejemplo, tiene metas, capacidades y requiere recursos [17]. También diferenciamos una clase especial de actor; un *actor malicioso*. La intención de los actores maliciosos es introducir amenazas al sistema, que explotan las vulnerabilidades [17].

Un *plan* representa, a un nivel abstracto, una forma de hacer algo [18]. El cumplimiento de una tarea puede ser un medio para satisfacer una meta. Un *recurso* presenta una entidad física o de información requerida por uno de los actores [18]. La principal preocupación al tratar con los recursos es la disponibilidad del recurso y quién es responsable de su entrega. Una *restricción* de seguridad es el concepto principal introducido por Secure Tropos. Las *restricciones* de seguridad se utilizan, en la metodología Secure Tropos, para representar los requisitos de seguridad [19]. Una restricción de seguridad es una especialización del concepto de restricción.

Los *objetivos* de seguridad representan un conjunto de principios o reglas que contribuyen al logro de la seguridad del sistema [19]. Estos principios identifican posibles soluciones a los problemas de seguridad y, por lo general, se pueden encontrar en forma de la política de seguridad de la organización. Ejemplos de tales objetivos son la autorización, la integridad y la disponibilidad. Una *vulnerabilidad* se define como una debilidad o defecto, en términos de seguridad y privacidad que existe de un recurso, un actor y/o una meta [17]. Las *vulnerabilidades* son explotadas por amenazas, como un ataque o incidente dentro de un contexto específico. Una *amenaza* representa circunstancias que tienen el potencial de causar pérdida o un problema que puede poner en peligro las características de seguridad del sistema [17]. Las amenazas pueden ser operacionalizadas por diferentes métodos de ataque, cada uno de ellos explotando una serie de vulnerabilidades del sistema. Un *método de ataque* en Secure Tropos es una acción que trata de causar una posible violación de la seguridad en el sistema [19]. Los *mecanismos de seguridad* representan métodos de seguridad estándar para ayudar a satisfacer los objetivos de seguridad [19].

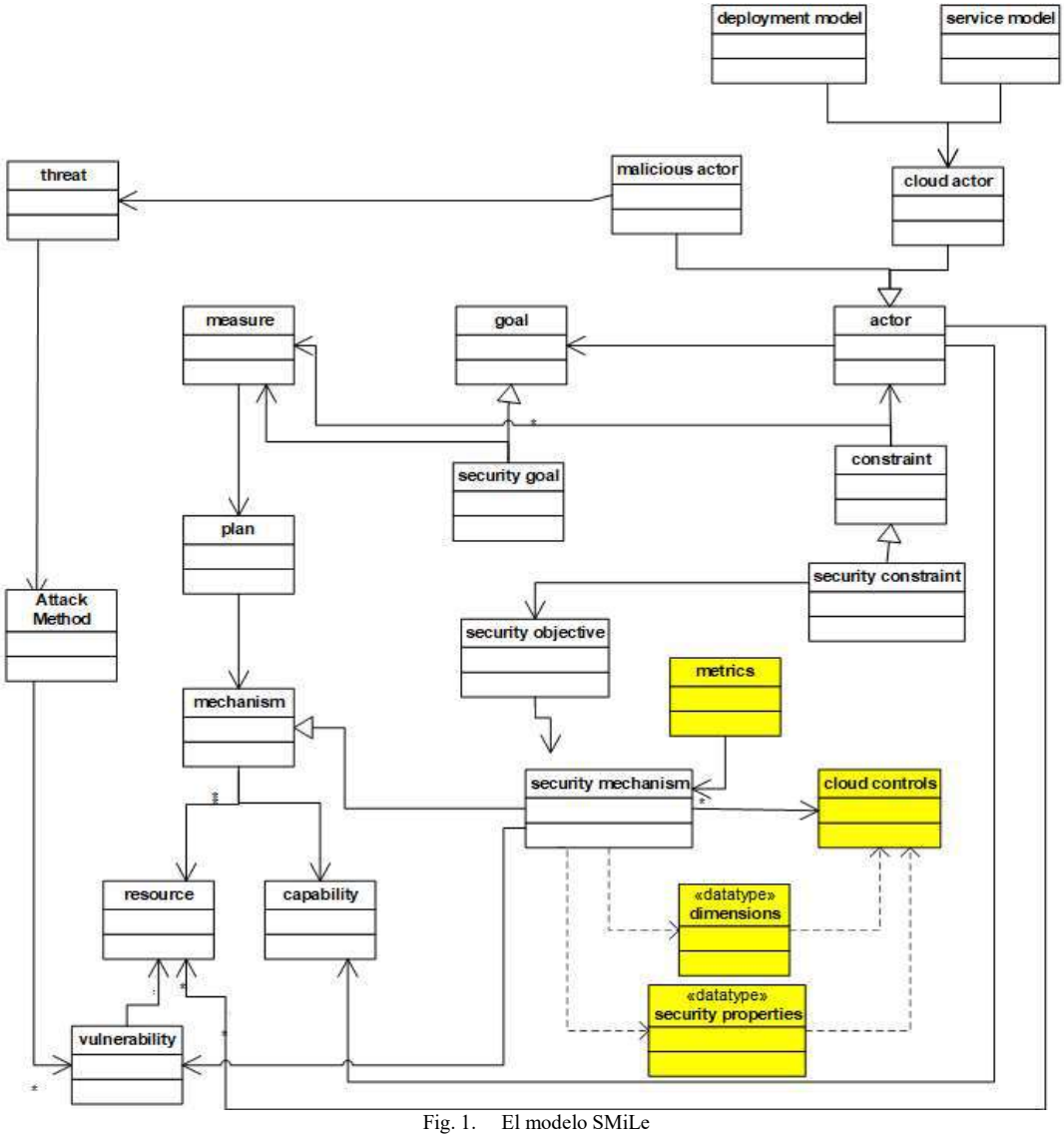


Fig. 1. El modelo SMiLe

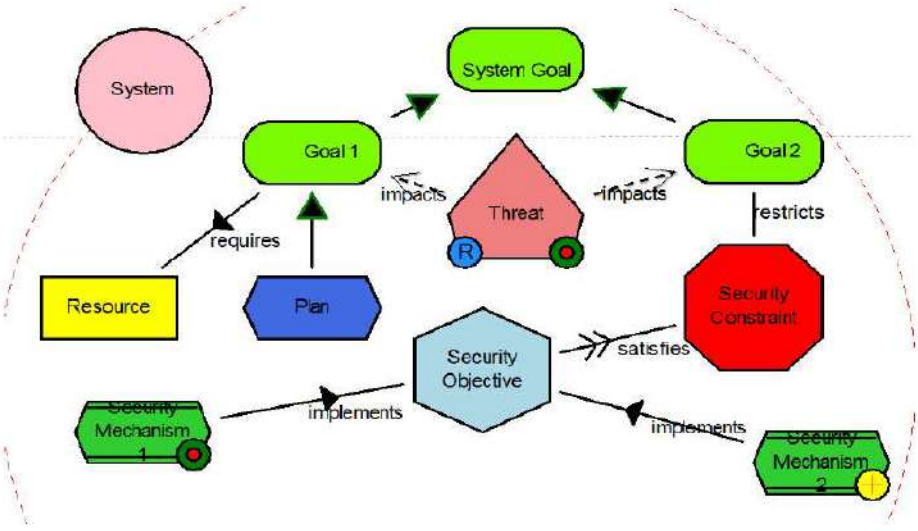


Fig. 2. Conceptos principales de Secure Tropos

D. Conceptos SMiLeModel

El SMiLeModel incluye nuevos conceptos, cuya representación gráfica se muestra en la Fig. 3: controles de la nube, propiedades de seguridad, dimensiones y métricas de migración de la nube.

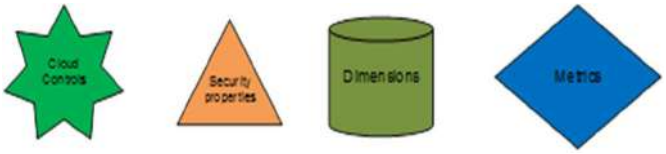


Fig. 3. Conceptos del modelo SMiLe

Asegurar que las normas de seguridad y las directrices se sigan y se certifiquen es crucial para construir y mantener una relación saludable basada en la confianza, la seguridad y la transparencia entre los proveedores de servicios en la nube y los clientes. Si bien es cierto hay muchos organismos de normalización que proporcionan una gran variedad de buenas prácticas, directrices y controles para la seguridad en Cloud Computing, desafortunadamente, no hay estándares de facto que estén universalmente aceptados y adoptados por los proveedores de servicios en la nube. El CSA (*Cloud Security Alliance*) es una organización que tiene como objetivo proporcionar garantía de seguridad dentro de Cloud Computing a través de varias directrices y normas. Una de sus ofertas es Cloud Control Matrix (CCM), que es un marco de trabajo de control de seguridad para proveedores y clientes de la nube. El CCM tiene como objetivo guiar a los proveedores y clientes de la nube en la evaluación de los riesgos de seguridad en las ofertas de la nube. Proporciona un análisis detallado de los principios y conceptos de seguridad basados en la "Orientación de seguridad para el área crítica de interés en Cloud Computing v3.0" [20]. El marco de trabajo de control consta de 16 dominios y 133 controles, los cuales son referencias cruzadas a los estándares y regulaciones de seguridad aceptadas por la industria. Cada dominio de control contiene una especificación que describe las condiciones y políticas del control. La relevancia arquitectónica del control se proporciona a través de varios campos que cubren la infraestructura de la nube; físico, red, computación, almacenamiento, aplicación, y datos. La aplicabilidad del dominio a los modelos de entrega de servicios en la nube se da a través de los modelos estándares SaaS, PaaS, modelo IaaS (SPI), que informa al usuario acerca de qué modelos de servicio se ven afectados para un control dado. Se describe la relación del control con el proveedor de servicios y el cliente. Por último, la aplicabilidad del alcance se da a través de una lista exhaustiva de normas y regulaciones, con el fin de facilitar la transparencia.

Secure Tropos identifica los requisitos de seguridad (modelados como restricciones de seguridad) y para cada uno de ellos identifica un conjunto de objetivos de seguridad y un conjunto de mecanismos de seguridad. Cada *mecanismo de seguridad* está relacionado con una o más propiedades de seguridad definidas en IAS-octave (Confidencialidad, Integridad, Disponibilidad, Responsabilidad, Auditoría, Autenticidad, No Repudio y Privacidad) y con una o más *dimensiones* de la cuarta dimensión del RMIAS (Organizacional, Orientado a las personas, Técnico y Legal). Para cada propiedad de seguridad y dimensiones existen algunos controles relacionados. *Los controles de la nube* están alineados con los mecanismos de seguridad a través de propiedades y dimensiones de seguridad. En otros términos, los controles de nube son implementaciones de los mecanismos de seguridad para la nube.

Por otro lado, una vez que todo el proceso ha sido trasladado a la nube de una manera segura, es el momento de verificar y validar la seguridad del sistema. Esta actividad está basada en un repositorio de *métricas de migración en la nube*. Estas métricas evaluarán la disponibilidad de un mecanismo de seguridad, la corrección de una entidad de seguridad y el nivel de efectividad de un mecanismo de seguridad.

III. SMiLeModel como guía del proceso SMiLe2Cloud

El proceso SMiLe2Cloud [9] consta de cinco actividades dirigidas por 16 dominios de seguridad, descritos en [20] e ilustrados en la Fig. 4.

El modelo SMiLe o SMiLeModel nos guía a través del proceso SMiLe2Cloud. Cada actividad completa el modelo a partir de un modelo simple.

Posteriormente, se muestran las diferentes actividades del proceso SMiLe2Cloud y la aplicación del modelo SMiLe en cada una de ellas. Para ello, se muestra un estudio de caso para explicar mejor el proceso.

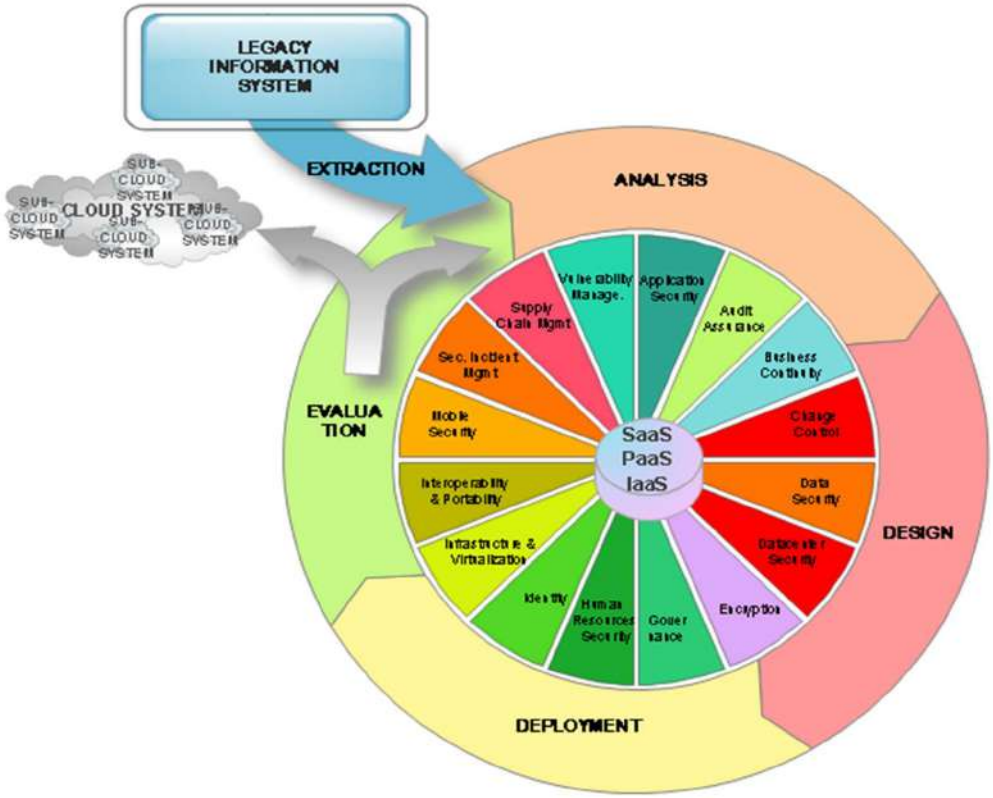


Fig. 4. Las Actividades de SMiLe2Cloud

A. Descripción del estudio de caso

El sistema seleccionado para este estudio de caso es el módulo para Bulk Loads (REM), una aplicación utilizada por la Comisión Nacional de los Mercados y la Competencia (CNMC) para gestionar el intercambio de grandes cantidades de datos entre la organización y sus clientes. Debido al carácter delicado de los datos que se manejan, el sistema debe cumplir con una serie de requisitos de seguridad. Sus usuarios deben tener un certificado criptográfico válido para fines de autenticación, mientras que los datos transmitidos deben ser firmados y transferidos a través de un canal seguro para garantizar su autenticidad, integridad y confidencialidad. Después de la transferencia, los usuarios deben poder descargar un archivo de registro con la información de entrega de datos.

B. Actividad de extracción

La extracción es la actividad (ver detalles en [21]) en la cual los requisitos del sistema para el LIS se derivan del código real y la documentación técnica del LIS. Es un subproceso de ingeniería inversa que es paralelo al subproceso de obtención del modelo arquitectónico general para el LIS. El proceso es asistido por herramientas de ingeniería inversa con el fin de facilitar las tareas y los pasos que el analista debe realizar para establecer los diferentes requisitos y controles en su lugar.

La actividad tiene tres fases: la extracción de modelos de procesos BPMN a partir del código fuente del sistema heredado, la refactorización del modelo de proceso extraído y una transformación de "proceso a objetivo" para crear un modelo de objetivo inicial a partir del modelo de proceso BPMN refactorizado.

El resultado será un modelo de proceso de negocio, alineado con los objetivos de alto nivel de la organización. Este modelo de proceso operacionaliza los requisitos del sistema capturados a nivel del modelo de objetivo.

El SMiLeModel incluye este modelo de objetivos de requisitos del sistema. Esto incluye metas, actores, plan, recursos y restricciones.

Caso de Estudio

El resultado de la aplicación de la actividad de extracción al caso de estudio es la definición del modelo de objetivos de requisitos del sistema REM, como se puede observar en la Fig. 5. Se han identificado los siguientes objetivos: facilitar las transferencias de archivos de gran tamaño, configurar la conexión, finalizar la sesión, enviar parte, reiniciar la sesión, actualizar los registros de transferencia, eliminar la sesión, descargar los registros de transferencia, firmar los registros de transferencia, inicializar la sesión, agregar certificados personalizados y CRL y comprobar los certificados de seguridad. Además, se ha identificado un recurso (registros de transferencia).

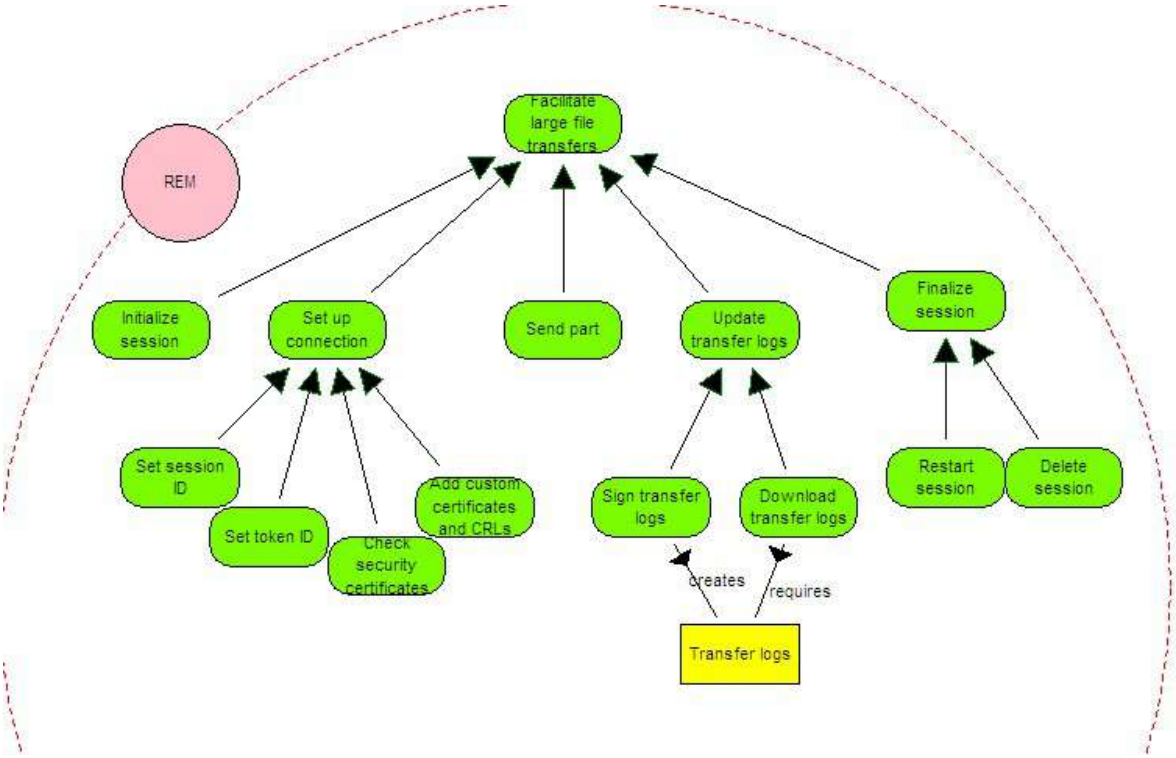


Fig. 5. Modelo de objetivos REM

C. *Actividad de Análisis*

Durante esta actividad (ver detalles en [11]) se define el modelo de requisitos de seguridad, extendiendo la metodología Secure Tropos [12] para la nube. Esta actividad se compone de dos tareas: Análisis de los requisitos de seguridad y la alineación de mecanismos de seguridad.

- Análisis de los requisitos de seguridad.

En la tarea "análisis de requisitos de seguridad" se utiliza SMiLeModel para derivar un conjunto de especificaciones de requisitos de seguridad con el que el sistema debe cumplir con los requisitos en el nuevo entorno. Los requisitos de seguridad se obtienen principalmente analizando la actitud de una organización hacia la seguridad y después de estudiar su política de seguridad. Los requisitos de seguridad se modelan como restricciones de seguridad y para cada uno de ellos se identifica un conjunto de objetivos de seguridad y un conjunto de mecanismos de seguridad.

El análisis de los requisitos de seguridad es una parte fundamental del proceso SMiLe2Cloud, ya que los requisitos de seguridad se extraen y se definen en función de los requisitos del sistema obtenidos de la actividad anterior. La entrada para esta actividad son los requisitos del sistema obtenidos durante la actividad de extracción anterior, que se basa en el modelo BPMN y se convierte al modelo SMiLe2Cloud.

Durante esta tarea, las limitaciones de seguridad, las amenazas, los objetivos de seguridad y los mecanismos de seguridad se identifican y se introducen en los objetivos de SMiLeModel.

Por lo tanto, el SMiLeModel incluye, como salida de esta tarea, los requisitos de seguridad del sistema, que incluye amenazas, restricciones de seguridad, objetivos de seguridad y mecanismos de seguridad.

Caso de Estudio

El resultado de la aplicación del análisis de tareas de los requisitos de seguridad al estudio de caso se muestra en la Fig. 6. Se han identificado dos amenazas (espionaje y suplantación de usuarios). Además, se han detectado cinco restricciones de seguridad: acceso sólo a usuarios autorizados, se debe permitir la personalización de medidas de seguridad, la transferencia de datos debe ser confidencial, no se deben modificar los datos durante la transferencia, y la transferencia de datos no debe ser rechazada. Además, se han identificado los siguientes mecanismos de seguridad: la lista blanca de usuarios (o *whitelist*), inicio de sesión con certificado digital, certificados personalizados, marco de trabajos de firma de certificados avanzados, configuración de red personalizada, canal encriptado, símbolo de verificación y firma digital.

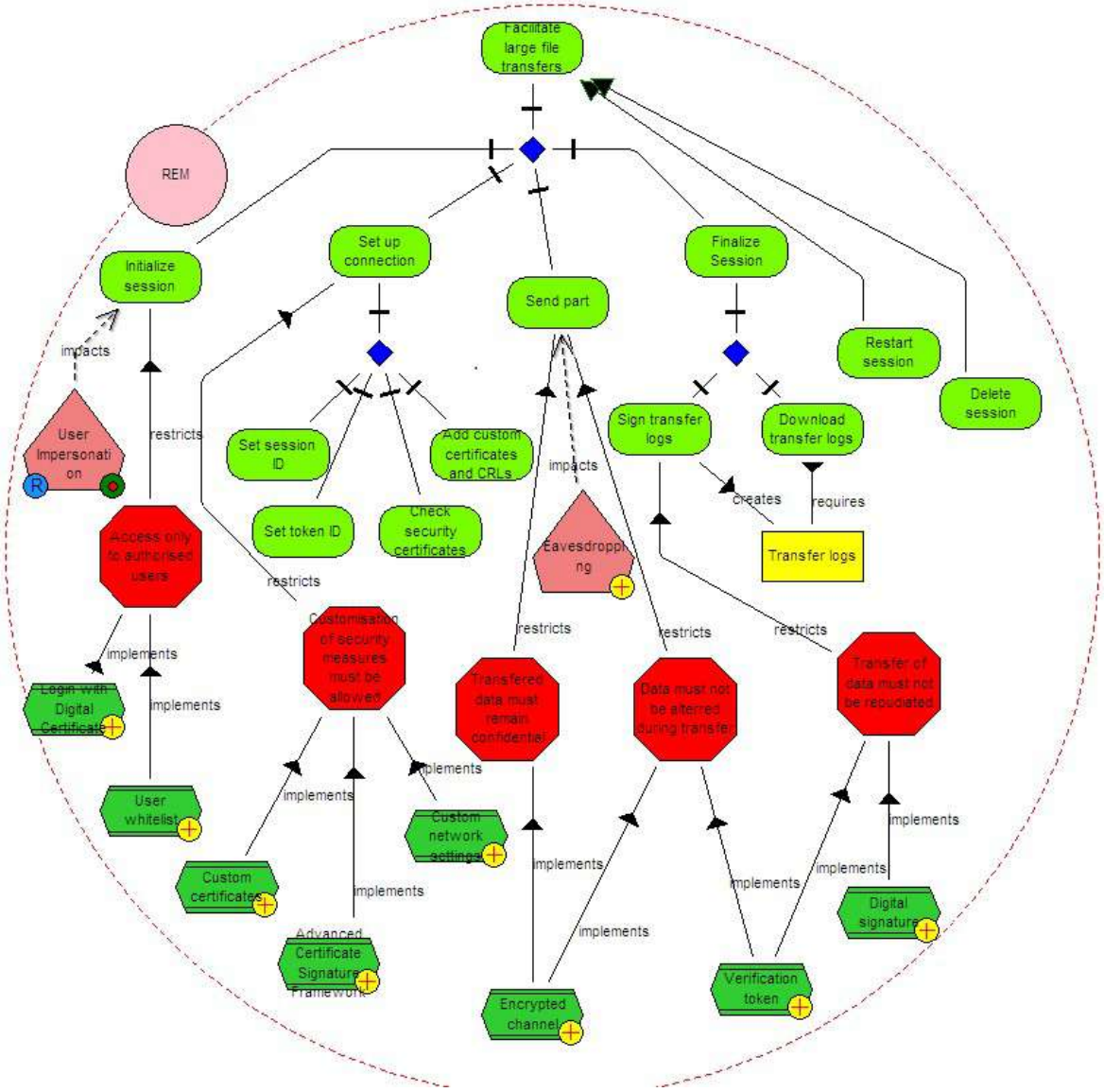


Fig. 6. Requisitos de seguridad del Sistema REM

- Alinear el Mecanismo de Seguridad

El objetivo de esta tarea es mapear el mecanismo de seguridad identificado en el paso anterior con los controles de la nube especificados en el CCM.

Para cada mecanismo de seguridad se identifican las propiedades de seguridad y las dimensiones. Los controles de la nube están alineados con los mecanismos de seguridad a través de propiedades y dimensiones de seguridad. Hay algunos controles relacionados para cada propiedad de seguridad y dimensiones.

El SMiLeModel incluye, como resultado de esta tarea, los requisitos de seguridad del sistema alineados con los Dominios CSA. Esto incluye propiedades de seguridad, dimensiones y controles de la nube.

Caso de Estudio

Por ejemplo, para el mecanismo de seguridad 'canal encriptado' se han identificado las siguientes propiedades de seguridad: confidencialidad, integridad, no repudio. Además, se ha identificado la dimensión técnica.

La lista de controles (nomenclatura utilizada por CCM) que se aplican a las propiedades de seguridad identificadas (confidencialidad, integridad y no repudio) y a la dimensión técnica se muestran en la Fig. 7: AIS-04 - Seguridad de aplicación y de interfaz. Seguridad de los datos, EKM-01 - privilegio, EKM-02 - Generación de claves, EKM-03 - Protección de datos sensibles y MOS-11 - Encriptado.

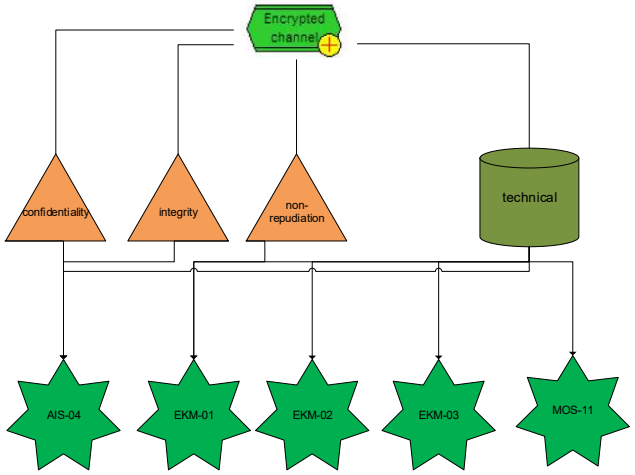


Fig. 7. Controles Cloud del Caso de Estudio

D. Actividad de Diseño

La actividad de diseño (ver detalles en [22]) se centra en seleccionar el modelo de servicio y el modelo de despliegue en función de las necesidades del cliente, cumplimiento con los requisitos, recursos disponibles, etc. Para ello, se basa en la distinción realizada por el NIST (El Instituto Nacional de Normas y Tecnología) [23].

La actividad de diseño consta de dos tareas, "Identificación del modelo de implementación y modelo de servicio" y "Selección del proveedor Cloud". La primera tarea se centra en la identificación del modelo de implementación y de servicio al que se quiere migrar, dependiendo de las necesidades del cliente, del cumplimiento de los requisitos, de los recursos disponibles, etc. Una vez se seleccionan el modelo de implementación y el modelo de servicio, y una vez están disponibles los requisitos de seguridad del sistema alineados con los dominios CSA, se puede seleccionar el proveedor de la nube que mejor se adapte a las necesidades de seguridad basándose en la Cloud Security Alliance: CSA STAR [24] (Security, Trust and Assurance Registry). El estándar STAR proporciona, para cada proveedor de la nube, la lista de controles que implementa. Una vez obtenida la lista de proveedores Cloud que cumplen los requisitos de seguridad se selecciona uno u otro en función de otras variables como pueden ser el coste, las tecnologías a implementar, etc. Para ello se realizará un análisis DAFO.

El SMiLeModel incluye, como salida de esta actividad, el modelo de implementación y el modelo de servicio.

Caso de Estudio

En el estudio de caso (ver ejemplo en [22]) se ha identificado el modelo de despliegue y el modelo de servicio. En el sistema REM, el modelo de despliegue identificado es la nube pública. Además, el modelo de servicio identificado es el IaaS.

E. Actividad de despliegue

Una vez que hayamos seleccionado el modelo de servicio, el modelo de despliegue y el proveedor de la nube, entonces tiene lugar la actividad de despliegue. La actividad de despliegue se centra en el desarrollo de la especificación de despliegue. Esta tarea se centra en el modelado de los servicios de datos.

Finalmente, se lleva a cabo el proceso de la implementación. Durante la tarea de implementación podría ser necesario contratar los servicios y firmar el Acuerdo de Nivel de Servicio (SLA, Service Level Agreement), desarrollar los elementos de seguridad personalizados o establecer todos los controles de seguridad en las condiciones de trabajo.

El SMiLeModel no incluye ni la especificación ni la implementación. Por lo tanto, la salida es el mismo SMiLeModel que en la entrada.

F. Actividad de Evaluación

Una vez que todo el proceso se ha trasladado a la nube de una manera segura, es hora de verificar y validar la seguridad del sistema.

Un repositorio formal de métricas de seguridad en un entorno cambiante como la nube es de gran utilidad. En esta tarea, el repositorio de métricas se aplicará a nuestro sistema.

Es necesario un análisis de los resultados obtenidos en la tarea anterior. Es necesario analizar si se han alcanzado todos los requisitos del sistema, si se cubren todos los requisitos de seguridad y si se completa la arquitectura.

Pero incluso si las especificaciones de seguridad se cumplen como están escritas, basar nuestro proceso en un ciclo Deming significa una reevaluación continua de las posibles mejoras al sistema. Los nuevos requisitos serán la entrada para la actividad de análisis.

El SMiLeModel incluye, como resultado de esta actividad, las diferentes métricas para verificar y validar la seguridad del sistema. Además, incluye los nuevos requisitos expresados como objetivos, actores, planes, recursos y restricciones.

Caso de Estudio

En el estudio de caso, las métricas que se han identificado para el mecanismo de seguridad—canal encriptado—se muestran en la Fig. 8: disponibilidad del canal encriptado, corrección del canal encriptado y la eficacia del canal encriptado.

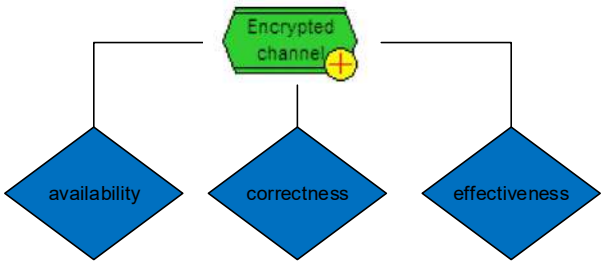


Fig. 8. Métricas del Caso de Estudio

IV. Conclusiones y trabajo futuro

En este artículo hemos presentado SMiLeModel, un modelo que da soporte al marco de trabajo SMiLe2Cloud en el proceso de migración de las características de seguridad de un sistema heredado a un nuevo entorno como Cloud Computing. Este modelo define conceptos extraídos de Secure Tropos, en el que está basado, y nuevos conceptos y elementos ampliados para tener en cuenta las características de seguridad de los sistemas basados en la nube. Este modelo se integra en todas las etapas de nuestro marco de trabajo, y explicamos en detalle cómo se utilizan estos nuevos conceptos y elementos en cada una de las actividades y tareas de nuestro marco de trabajo. Se presenta un estudio de caso que nos ha permitido mostrar los resultados obtenidos en cada tarea del marco de trabajo y qué elementos específicos del modelo se utilizan y cómo se transforman.

Este trabajo nos ha ayudado a validar el modelo en nuestro marco de trabajo y hemos mejorado el modelo añadiendo conceptos y nuevos elementos que hemos considerado necesarios para dar un soporte coherente y completo a nuestro marco de trabajo SMiLe2Cloud.

Agradecimientos

Este trabajo ha sido financiado por el proyecto SEQUOIA (Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER, TIN2015-63502-C3-1-R).

Referencias

[1] Symantec, Internet Securiyt Threat Report. 2016.
[2] McAfee Labs, Predicciones sobre amenazas para 2016. 2016.
[3] Telefónica, F., Ciberseguridad, la protección de la información en un mundo digital, Ariel, Editor. 2016.
[4] Bisbal, J., et al. An overview of legacy information system migration. in Software Engineering Conference, 1997. Asia Pacific... and International Computer Science Conference 1997. APSEC'97 and ICSC'97. Proceedings. 1997. IEEE.
[5] Council, C., Migrating applications to public cloud services: roadmap for success. 2016.
[6] Weaver, G., Migrating Legacy System to the Cloud, in Storage Performance and Cloud Enablement. 2017, AVERE.
[7] Márquez-Alcañiz, L., et al., Security in Legacy Systems Migration to the Cloud: A Systematic Mapping Study, in 11th International Workshop on Security in Information Systems. 2014: Lisbon, Portugal. p. 93-100.
[8] Márquez Alcañiz, L., et al., Hacia un Proceso de Migracion de la Seguridad de Sistemas heredados al Cloud, in XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2014). 2014: Alicante. p. 191-196.
[9] Márquez, L., et al. A Framework for Secure Migration Processes of Legacy Systems to the Cloud. in Fifth International Workshop on Information Systems Security Engineering - Advanced Information Systems Engineering Workshops. 2015. Springer International Publishing.
[10] Cloud Security Alliance. Cloud Controls Matrix V3.0.1. 2014; Available from: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/.
[11] Shei, S., et al. Modelling secure cloud systems based on system requirements. in Evolving Security and Privacy Requirements Engineering (ESPRE), 2015 IEEE 2nd Workshop on. 2015. IEEE.
[12] Mouratidis, H. and P. Giorgini, Secure Tropos: A Security-oriented Extension of the Tropos Methodology. International Journal of Software Engineering and Knowledge Engineering, 2007. 17(2): p. 285-309.
[13] Giorgini, P., F. Massacci, and J. Mylopoulos. Requirement engineering meets security: A case study on modelling secure electronic transactions by VISA and Mastercard. in International Conference on Conceptual Modeling. 2003. Springer.
[14] Mouratidis, H., N. Argyropoulos, and S. Shei, Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach, in Domain-Specific Conceptual Modeling. 2016, Springer. p. 357-380.
[15] Mouratidis, H., A security oriented approach in the development of multiagent systems: applied to the management of the health and social care needs of older people in England. 2004, University of Sheffield;.
[16] Yu, E., Modelling Strategic Relationships for Process Reengineering. PhD thesis, Computer Science Department, University of Toronto, Toronto (Canada). 1995, Phd thesis, also appears as Technical Report DKBS-TR-94-6, December 1994.
[17] Mouratidis, H., et al., A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software, 2013. 86(9): p. 2276-2293.
[18] Bresciani, P., et al., Tropos: An agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems, 2004. 8(3): p. 203-236.
[19] Mouratidis, H., Secure software systems engineering: the Secure Tropos approach. JSW, 2011. 6(3): p. 331-339.
[20] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011.
[21] Argyropoulos, N., et al. Eliciting security requirements for business processes of legacy systems. in IFIP Working Conference on The Practice of Enterprise Modeling. 2015. Springer.
[22] Marquez, L., et al., Design Activity in the Process of Migrating Security Features to Cloud. IEEE Latin America Transactions, 2016. 14(6): p. 2846-2852.
[23] NIST, The NIST Definition of Cloud Computing, P. Mell and T. Grance, Editors. 2009, National Institute of Standards and Technology.
[24] Cloud Security Alliance. CSA Security, Trust & Assurance Registry (STAR). 2014; Available from: https://cloudsecurityalliance.org/star/.

Luis Márquez Alcañiz is civil servant in the Spanish National Authority for Markets and Competition (CNMC). He is leading the group of forensic it experts in the CNMC and participates in the forensic it experts group (FIT) of the Directorate General for Competition in the European Commission. Previously he has been working in different public organisms like Ministry of Foreign Affairs and Spanish Tax Agency. His email is luis.marquez@cnmc.es

David G. Rosado holds a Ph.D. in Computer Science from University of Castilla-La Mancha and has an MSc in Computer Science from the University of Málaga (Spain). He is assistant Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain). His research activities are focused on security architectures, security for Information Systems and security in Cloud Computing and Big Data. He is co-editor of several books and chapter books on these subjects, and has numerous papers in national and international conferences. Author of several manuscripts in national and international journals. He has been acting as a member of many conference program committees and as cochairs of some workshops such as WOSIS and WISSE. He is a member of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain. His email is david.grosado@uclm.es.

Haralambos Mouratidis is Reader in Secure Systems and Software Development at the School of Architecture, Computing and Engineering (ACE) at the University of East London (UEL). He holds a B.Eng. (Hons) from the University of Wales, Swansea (UK), and a M.Sc. and PhD from the University of Sheffield (UK). Haris is co-director of the Distributed Software Engineering Research Group. His research interests lie in the area of secure software systems engineering, requirements engineering, information systems development and agent oriented software engineering. He has published more than 100 papers and he has secured funding as Principal Investigator from national – Engineering and Physical Sciences Research Council, Royal Academy of Engineering, Technology Strategy Board (TSB) - and international – European Unionfunding bodies as well as industrial funding -British Telecom, ELC, Powerchex - towards his research. He is member of the ERCIM Security and Trust Management Working Group and of the IFIP Working Group 8.1: Design and Evaluation of Information Systems. He is editor in Chief of the International Journal of Agent Oriented Software Engineering and on the editorial board of the Requirements Engineering Journal. His email is H.Mouratidis@brighton.ac.uk

Eduardo Fernández-Medina holds a PhD. and an MSc. In Computer Science from the University of Sevilla. He is an Associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain)- his research activity being in the field of security in information systems, and particularly in security in business processes, databases, datawarehouses, and web services. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has published several dozens of papers in national and international conferences (BPM, UML, ER, ESORICS, TRUSTBUS, etc.). He is author of several manuscripts in national and international journals (Decision Support Systems, Information Systems, ACM Sigmod Record, Information Software Technology, Computers & Security, Computer Standards and Interfaces, etc.). He leads the GSyA research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain and belongs to various professional and research associations (ATI, AEC, AENOR, etc.). His email is eduardo.fdezmedina@uclm.es