CIBER

REVISTA HISPÁNICA DE TENDENCIAS EN CIBERSEGURIDAD

Quiénes somos

Con la revista CIBER se pretende abrir la divulgación científica y tecnológica en español sobre diferentes temas de interés sobre ciberseguridad. La revista surge como una iniciativa entre la Universidad de León (España) y el Instituto Nacional de Tecnologías de la Comunicación (INTECO).

La Universidad de León y el INTECO tienen suscrito un convenio marco de colaboración de fecha 28 febrero de 2009, que tiene por objeto establecer el marco adecuado que agilice los futuros proyectos de colaboración entre ambas entidades.

La revista tiene una periodicidad semestral, puedes acceder a nuestro apartado de Información para autores para informarte y enviarnos tu artículo.

La próxima revista también estará disponible a través del repositorio Open Journal Systems de la Universidad de León, llamado Buleria, es el repositorio institucional de la Universidad de León. Se trata de un archivo digital de acceso abierto que alberga el texto completo de los documentos generados por la comunidad científica y tecnológica.

CIBER

REVISTA HISPÁNICA DE TENDENCIAS EN CIBERSEGURIDAD

Último número

En los enlaces que aparecen a continuación te puedes descargar nuestros últimos artículos de la revista CIBER.

Hacia una migración de la seguridad de sistemas heredados a la nube

Luis Marquez Alcañiz[#1], David G. Rosado[*2], Daniel Mellado[&3], Eduardo Fernández-Medina[*4]

[#] *Comision Nacional de la Competencia*

c/Barquillo, Madrid, España

[1]luismarquezalcaniz@yahoo.es

[*]*Universidad de Castilla-La Mancha, Grupo de Investigación GSyA,*

Departamento de Tecnologías y Sistemas de Información,

Ciudad Real, 13071, España

[2]David.GRosado@uclm.es

[4]Eduardo.FdezMedina@uclm.es

[&]*Agencia Tributaria*

Madrid, 28046, España

[3]damefe@esdebian.org

Resumen— **El desarrollo de la computación en la nube es una tendencia fuerte en la industria de las TI que hace que los clientes de este nuevo modelo de prestación de servicios, sobre todo las empresas, se enfrenten a desafíos nuevos en lo que se refiere a la gestión de la seguridad de sus aplicaciones heredadas (las más importantes de sus aplicaciones entre las de uso diario) en el nuevo entorno. La cuestión sobre cómo migrar de forma segura los sistemas de información heredados de estas empresas, que se ejecutan en centros de proceso de datos controlados de forma completa por el departamento de tecnologías de la organización, a entornos donde la infraestructura tiene un control mucho menos definidos y que está controlado al menos parcialmente fuera del ámbito de la empresa propietaria y responsable de los sistemas de información. Este artículo presenta un proceso (SMiLe2Cloud) y un marco de trabajo con el que se puede mirar de forma segura los sistemas corporativos heredados a infraestructuras o entornos en la nube. Proponemos un proceso que se basa en un ciclo de mejora continua que comienza con un conjunto de modelos KDM (Knowledge Discovery Metamodel) a partir del cual derivamos un modelo de seguridad para la migración del sistema heredado. Este modelo es después convertido en una serie de cláusulas a incorporar en los contratos relacionados y controles de seguridad específicos para la nube a implantar.**

***Clave*— nube, seguridad informática, migración de sistemas heredados, KDM, SLA, SecSLA**

I. INTRODUCCIÓN

Desde sus primeros inicios, los directivos de Tecnologías de la Información (TI) se han mostrado muy suspicaces sobre el tema de la seguridad del modelo de computación en la nube. Así fue tras la concepción del modelo [2], y así seguía siendo el año pasado cuando el Open Group realizó su última encuesta [3].

Para algunos expertos, la computación en la nube está "*desalineada con los modelos y controles de seguridad tradicionales*" [4]. Sin embargo, otros ven en este modelo una gran oportunidad para mejorar la seguridad de los sistemas heredados. Por ejemplo, aunque Kinkler indica que "*muchas de las actuales aplicaciones que mueven a las empresas no pueden ser migradas fácilmente a la nube", también afirma que la migración a la nube "nos ofrece una esperanza de que podamos recuperar el control […] debido a la seguridad pobremente integrada o pensada de mala manera.*" [5]. Sin embargo, hay algo en lo que todos coinciden: la nube supone nuevas amenazas y estas amenazas deben ser resueltas antes de que las aplicaciones de las grandes corporaciones entren en juego.

¿Qué tienen en especial esas aplicaciones de las grandes corporaciones? Que la mayoría de ellas se basan en sistemas de información heredados (LIS). El problema de la herencia es importante en volumen. Según una encuesta realizada por MeriTalk [6] a un total de 166 directivos de TI del gobierno federal norteamericano, "*el 47% de las aplicaciones de TI se basan en tecnología heredada que necesita modernización*". El mismo estudio calcula el total del gasto federal aplicable al soporte de aplicaciones heredadas en el entorno de los 35.000 millones de dólares. Y gran parte de la modernización no sólo se beneficiaría de una mejora tecnológica pura, sino que entrarían en juego reducciones de coste importantes a raíz de una migración a la nube de parte de la infraestructura que las soporta. De hecho, el año

pasado el principal responsable de las tecnologías de la información de la casa Blanca, Vivek Kundra, señaló que casi el 20% del gasto total federal de los EEUU (unos 20.000 millones de dólares) podría ser susceptibles de pasar a ser gasto directamente relacionado con la computación en la nube [7].

Y sin embargo, aunque la modernización de los sistemas de información heredados (LIS – Legacy Information Systems) por medio de la migración a la nube podría implicar inmensos ahorros y reducciones de los presupuestos, y a pesar de la preocupación a la que antes nos hemos referido relativa a la seguridad intrínseca del modelo en la nube, hasta la fecha parece que todavía no hay un modelo que permita la migración a la nube de sistemas que de forma explícita incluyan procesos relacionados con la seguridad de dichos sistemas; peor aún si hablamos de integración de estándares de seguridad en dichos procesos de migración. Sí que es cierto que existen propuestas de procesos de migración, pero ninguno de ellos propone una verdadera integración con las cuestiones específicas de seguridad en forma de necesidades y/o de oportunidades que se derivan del modelo en la nube.

Nuestro propósito con este artículo es proponer un marco de trabajo para tal proceso mediante un conjunto de métodos que resuelvan de forma concreta las cuestiones de seguridad y la integración de la seguridad con procesos de otra naturaleza orientados todos ellos a la migración segura a la nube de sistemas de información heredados. Este trabajo ha evolucionado de estudios previos sobre los criterios de seguridad ya publicados en [8] y [9].

El artículo está estructurado en 3 secciones adicionales a esta introducción. En la sección 2 presentamos los trabajos relacionados con el nuestro. En la sección 3 presentamos el marco de trabajo propiamente dicho. Y en la sección 4 ofrecemos unas someras conclusiones y presentamos lo que serán las líneas de actuación futuras.

II. Trabajo Relacionado

La mayor parte del trabajo relacionado con nuestra propuesta tiene que ver con alguno de los dos aspectos principales del problema: ya sea la seguridad en la nube o los procesos de migración de sistemas heredados a la nube.

En lo que se refiere a la seguridad en la nube, las dos referencias esenciales son: [4] y [10]. Ninguna de ellas ofrece un modelo de arquitectura de seguridad para la nube y mucho menos un proceso completo para migrar a la nube de forma segura sistemas de información heredados. De todos modos, ambos son muy importantes en el sentido de que establecen los fundamentos elementales y las recomendaciones básicas en lo que se refiere a los diferentes aspectos de la seguridad en la nube. Son, sin duda alguna, el punto de inicio para el desarrollo de cualquier estrategia que tenga que ver con la migración a la nube de la seguridad de los sistemas.

Otro trabajo directamente relacionado con la seguridad en la nube que hemos encontrado útil en nuestra investigación ha sido el de [1], en el cual los autores presentan un análisis taxonómico que caracteriza los diferentes desafíos a los que se enfrentan lo que pretenden ubicar sus sistemas en la nube. Algunos de estos desafíos son comunes a la mayoría de los sistemas heredados (véase Fig. 1).

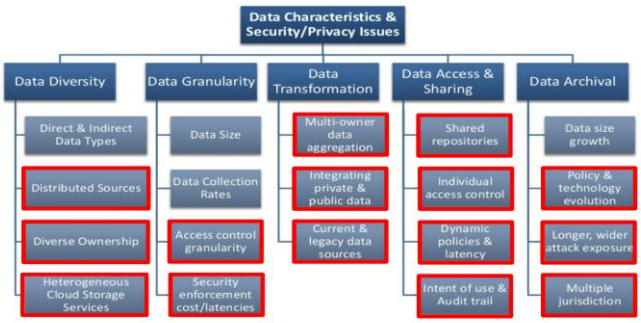

Fig. 1 Principales desafíos identificados en [1]. En rojo, los temas que consideramos que son comunes a la mayoría de proyectos de migración a la nube.

Por otro lado, también hay diversos trabajos relacionados con procesos de migración de sistemas heredados a la nube. Algunos ofrecen estrategias de migración, mientras que otros presentan modelos específicos. En alguno de ellos hay alguna referencia inespecífica a la seguridad; sin embargo ninguno de estos trabajos profundiza en la cuestión, ni define una verdadera integración con los modelos de seguridad existentes o define actividades relacionadas con la seguridad.

La primera referencia que debemos señalar es la de [11]. Su trabajo presenta una metodología para migrar sistemas heredados a la nube mediante una serie de transformaciones de arquitectura dirigida por el modelo (MDA – Model Driven Architecture) que están acopladas al modelo de herradura del SEI (Software Engineering Institute) presentado en [12] (véase Fig. 2). Como se ha indicado antes, la propuesta de Zhang trata las cuestiones de seguridad de manera inespecífica y no detallada. Su principal relación con nuestro trabajo es el hecho de que nosotros también utilizamos el modelo de herradura, aunque nuestro proceso se enfoca de manera específica en la parte del modelo de herradura que se desarrolla una vez que la fase de ingeniería inversa ya ha sido realizada y existe una arquitectura definida para el LIS original; es decir, empezamos justo antes de que la verdadera transformación comience.

Por otro lado, nuestra aproximación utiliza el estándar ISO/IEC 19506 [13] como metamodelo de descubrimiento de conocimiento (KDM - Knowledge Discovery Metamodel) de la estructura básica de la arquitectura del sistema objetivo. No es extraño que otro trabajo relacionado que debemos mencionar es el de [14]. La propuesta de Frey y Hasselbring en realidad comienza en un estadio anterior al de la nuestra y de hecho presenta una aproximación semiautomática que extrae parte de la arquitectura objetivo mediante herramientas. Como nosotros, ellos proponen el metamodelo de descubrimiento de conocimiento del OMG (KDM) para documentar la arquitectura básica. Sin embargo, de nuevo, dejan completamente de lado cualquier referencia a la seguridad de los sistemas migrados. En contraste con esta propuesta, y en el estado actual de nuestro propio trabajo, nosotros todavía no hemos desarrollado un proceso automático del que pueda derivar un modelo de seguridad desde la arquitectura básica; de hecho nuestro foco principal es el proceso en sí y no las herramientas automáticas que vendrían en un estado de madurez de la propuesta mucho más avanzado.

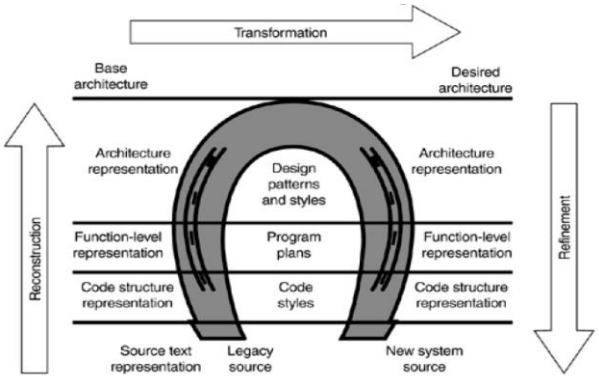

Fig. 2 Horseshoe model for legacy software migration (Software Engineering Institute, CMU).

En [15] podemos ver una aproximación diferente. Su propuesta se basa en la creación de una ontología del software de la empresa que facilite la comprensión y la exploración de todos los elementos relacionados con el sistema heredado. El trabajo de Zhou et al se concreta en una propuesta muy elaborada para un marco de trabajo con un proceso en cinco pasos que incluso tiene el soporte de herramientas para la visualización de UML (Unified Modeling Language), la construcción de la ontología y la transformación del modelo. Y de nuevo, la carencia es la misma que las anteriores: ni ofrece actividades relacionadas con la seguridad, ni ofrece ninguna pista de cómo pueden concebirse o integrarse tales actividades: en el método propuesto, la seguridad es asunto de otros.

El último trabajo que mencionaremos en esta sección es el presentado por [16]. En este caso, más que una propuesta general, dedican su análisis a la cuestión de cuándo es factible realmente migrar un sistema heredado a la nube (en cualquiera de los diferentes modelos de servicio). Un aspecto que nos atrajo particularmente de su aproximación fue el sesgo económico debido al análisis de costes; algo que queríamos introducir en nuestra propia aproximación. Una vez más, sin embargo, la seguridad sólo es mencionada para indicar que *"aunque es un tema importante que debe ser resuelto si hay que plantear la migración a la nube de sistemas de bases de datos … queda fuera de nuestro alcance."*

III. SMiLe2Cloud: Proceso para la migración a la nube de la seguridad de los sistemas heredados.

En esta sección proponemos un proceso (denominado SMiLe2Cloud - Security MIgration of LEgacy systems TO Cloud computing) que pretende resolver el problema de la migración con seguridad a la nube de sistemas de información heredados. Este proceso está basado, como ya hemos indicado antes, en el modelo de herradura del SEI; pero también tiene una vocación de proceso de mejora continua al estilo de Deming. Dado que estamos interesados en los aspectos propiamente relacionados con la seguridad (y no en los esfuerzos generales de ingeniería inversa necesarios para obtener la especificación funcional) hemos partido de la base de que los ingenieros a cargo de la migración ya han desarrollado un modelo del sistema heredado que define las especificaciones funcionales y los elementos arquitectónicos de sistema (con exclusión de las especificaciones relacionadas con la seguridad y la arquitectura de seguridad) y que han documentado dichas especificaciones y elementos en un entorno que puede exportar dicha especificación en formato KDM. Es en este punto en el que nosotros entramos y empezamos a desarrollar los aspectos de seguridad a partir del diseño obtenido mediante ingeniería inversa y luego continuamos con el resto del proceso de segurización del sistema migrado. Definiremos el proceso intentando seguir la notación SPEM (Software Process Engineering Metamodel) en la medida de lo posible.

A. Visión general

Como se ha indicado antes, nuestro proceso comienza en el punto más alto del modelo de herradura del SEI, una vez que la arquitectura básica ha sido obtenida, y justo antes de que comience la transformación. Desde este punto, continuará transformando y refinando el sistema objetivo, ya desde una perspectiva puramente enfocada en los temas relacionados específicamente con la nube.

El proceso SMiLe2Cloud consta de siete actividades dirigidas por 14 dominios de seguridad [10] que son mostradas en Fig. 3. La actividad de "extracción" está enfocada al uso de la reingeniería inversa para extraer aspectos de seguridad desde el LIS a un modelo de

seguridad (SMiLe model) definido para nuestro proceso de migración. La segunda actividad es la "valoración" durante la cual se estudian las principales características del cloud, los principales proveedores y diferentes modelos cloud. La tercera actividad es el "análisis" de los requisitos de seguridad (SecR), las cláusulas en los acuerdos a nivel de servicio de seguridad y los servicios ofrecidos por los proveedores de seguridad del cloud. La actividad de "diseño" está enfocada en el diseño de la arquitectura de seguridad y en la definición de una estrategia de migración que será aplicada en la siguiente actividad del proceso de migración, que es la actividad de "migración" donde los elementos de seguridad son desarrollados, configurados y contratados siguiente la estrategia previamente definida. La sexta actividad es la "evaluación" donde se verifica y valida el modelo de seguridad migrado. Finalmente, la actividad de "mejora" captura los nuevos aspectos de seguridad que se quieren incorporar dentro de un nuevo ciclo del proceso y se analizan las mejoras y cambios propuestos para nuestro sistema cloud.

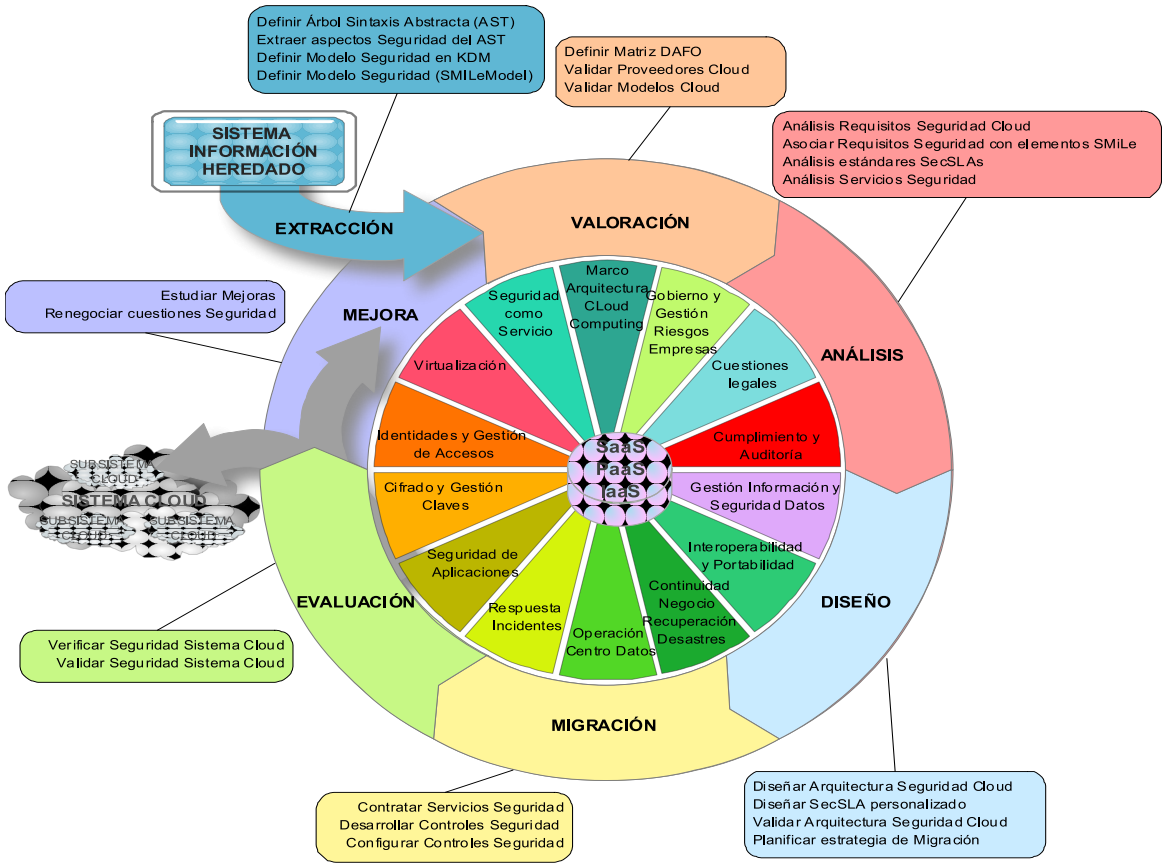

Fig. 3 El proceso SMiLe2Cloud: un proceso para migrar a la nube la seguridad de sistemas de información heredados.

Dado que KDM carece de elementos específicos para modelizar aspectos de seguridad de un sistema heredado, en realidad parte de nuestro proceso debe realizarse antes de que exista una especificación completa del sistema obtenida por ingeniería inversa. La actividad de extracción, específicamente definida en nuestro proceso, precisamente trata con esta última parte de la fase de reingeniería del modelo de herradura. Sin embargo, esta fase no es específica de un proceso de migración a la nube. Podría ser utilizada de forma separada en cualquier proceso que pretendiera migrar un sistema heredado de forma segura a cualquier tipo de arquitectura objetivo.

Lo que sí es necesario entender de antemano, cuando estamos pensando en migrar a la nube, es el papel central que tienen para la seguridad y para la arquitectura del sistema completo los acuerdos de nivel de servicio (SLA - Service Level Agreement) específicos de seguridad (comúnmente denominados SecSLA). Los SecSLA son el núcleo de la seguridad en la nube y la mayoría de controles específicos que se pueden implantar se instancian como cláusulas en el SecSLA siempre que es posible. Por supuesto, esto depende en gran media del modelo de despliegue elegido (véase la Fig. 4); con un modelo de infraestructura como servicio (IaaS – Infrastructure as a

Service) como el que ofrece Amazon EC2, la organización que está migrando el sistema heredado tiene que trabajar a un nivel más bajo y diseñar e implementar controles tradicionales por sí misma; sin embargo, con modelos de software como servicio puros (SaaS - Software as a Service), casi todos los controles de seguridad deben ser implementados como SecSLA ya sean acordados con el proveedor funcional del servicio o con un proveedor específico de seguridad como servicio (SecaaS - Security as a Service); finalmente con un modelo de plataforma como servicio (PaaS - Platform as a Service) como el que ofrece Google App Engine una solución intermedia que balancee controles de ambos tipos será la aproximación adecuada (la seguridad de la plataforma recae en el proveedor y la seguridad de las aplicaciones y la seguridad del propio proceso de desarrollo y despliegue es responsabilidad del cliente).

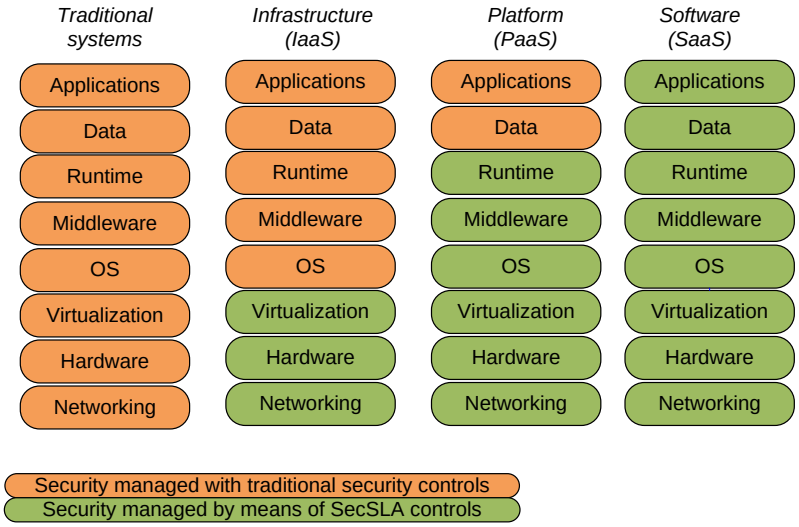

Fig. 4 Modelos de despliegue y tipo de gestión necesaria de los controles de seguridad relacionados.

Todo esto es importante para la definición de la arquitectura de seguridad, puesto que algunas actividades en un proceso tradicional de aseguramiento de sistemas (ya sea en migración de sistemas o en desarrollo de sistemas desde cero) implican el diseño de controles, mientras que en un proceso orientado a la nube, la mayoría del proceso tiene que ver con el aspecto nuclear de seleccionar qué controles diseñados por los proveedores son aplicables y asegurar que las cláusulas del SLA cubren dichos controles. De esa manera, las cláusulas se convierten, de facto, en los propios controles que salvaguardan a la organización cliente (normalmente mediante la aplicación de obligaciones contractuales o penalizaciones en caso de que el proveedor no pueda cumplir dichas obligaciones). El problema, pues, se convierte en una mezcla de diseño de sistemas, selección de proveedores de servicio y técnicas de negociación de contratos.

En nuestro caso, el objetivo es orientar nuestra aproximación lo más posible hacia la ingeniería de sistemas de información. Por ello excluiremos inicialmente las soluciones puramente SaaS que tienden a estar orientadas principalmente hacia la reingeniería de procesos que a la de sistemas. Esto es, una propuesta SaaS supone normalmente un diseño de cómo el proceso de negocio debe ser migrado (es decir cómo podemos seleccionar el mejor proveedor SaaS que pueda cumplir con el proceso de negocio y/o en qué manera debe cambiar dicho proceso de negocio para acomodarse al nuevo sistema) pero tiene poco que ver con cuestiones relacionadas con la ingeniería de sistemas. En cierto sentido, una solución puramente SaaS no sería una migración pura de un sistema heredado, sino que sería un cambio completo del sistema que trataría con cuestiones como la migración de los datos del sistema heredado original más que la migración de funcionalidades.

B. Modelo de Seguridad propuesto

El modelo de seguridad SMiLe2Cloud está basado en el metamodelo de la OSA (Open Security Architecture) [17] y lo extiende con diversas clases que hacen de interfaz con otros metamodelos de KDM, así como con algunos conceptos de Secure Tropos [18] tales como el de “actor”, y con requisitos de seguridad específicos de la nube, controles específicos para la nube y cuestiones relacionadas con los proveedores del servicio en la nube y la contratación con éstos (véase Fig. 5).

Como en otros metamodelos de seguridad existentes, el núcleo del modelo son los activos que es necesario proteger (de los que deriva una clase que representa de forma concreta a los activos que serán específicamente migrados a la nube). Estos activos están relacionados con los controles de seguridad que mitigan los riesgos derivados de las vulnerabilidades que los primeros tienen.

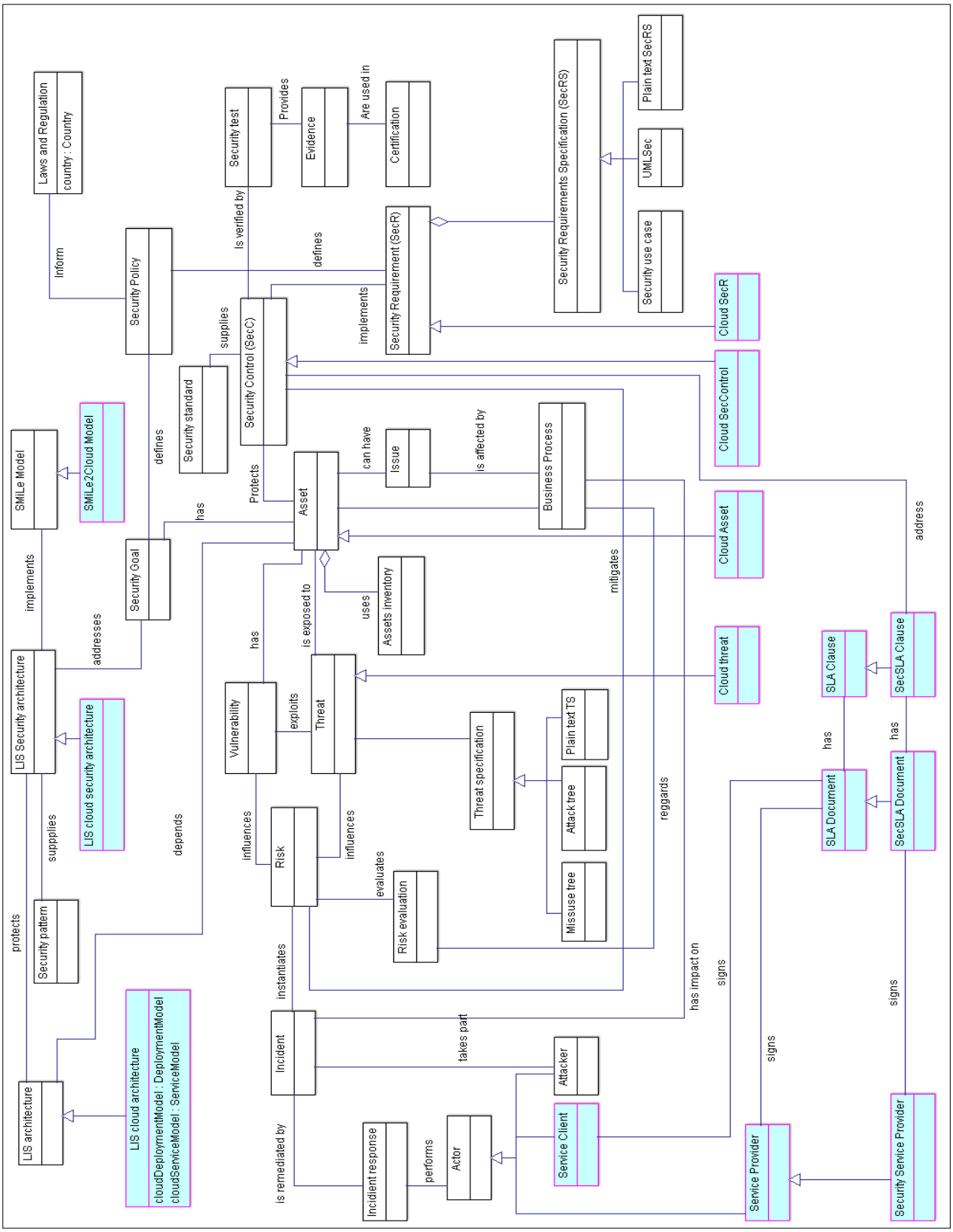

Fig. 5 Modelo SMiLe y modelo SMiLe2Cloud

Un modelo SMiLe2Cloud implementa una arquitectura de seguridad implícita o explícitamente definida en el sistema heredado. La arquitectura de seguridad responde a la existencia de una serie de objetivos de seguridad (que también pueden ser implícitos o explícitos en el sistema heredado) que a su vez se definen como políticas de seguridad que se instancian en requisitos de seguridad para los diferentes activos definidos en el inventario. Los requisitos de seguridad se definen en forma de especificaciones (SecRS – Security Requirements Specification) que pueden realizarse mediante diferentes técnicas: casos de uso de seguridad, la extensión UMLSec presentada por [19], o incluso texto plano. Algunas políticas pueden aparecer al elegir la nube o un modelo de servicio o de despliegue concreto; otras pueden venir forzadas por la legislación local o regulaciones específicas del sector. También hemos recogido una serie de estándares de seguridad que pueden haber sido definidos (ya sea para el entorno de la nube o para otros entornos no tan concretos).

Como se ve en la figura, también hemos recogido en el metamodelo una clase específica para modelizar la evaluación de riesgos. Esto nos permite incluir de forma estándar las matrices de riesgo y su relación con los impactos en los activos del sistema y en los procesos de negocio (que se recogen también de forma separada).

Nuestro modelo permite que el sistema heredado sea derivado incluso antes de decidir qué partes del mismo van a ser migradas a la nube; ya sea si se va a migrar todo el sistema al nuevo entorno de forma global o se considera un modelo híbrido.

Para cada activo en nuestro inventario, se debe realizar un análisis de amenazas y se debe derivar una matriz de evaluación de riesgo. Los riesgos que son específicos de la nube deben aislarse y ser tratados de forma separada.

Como ya hemos indicado, los activos están organizados en un inventario así como los requisitos de seguridad están organizados en una especificación.

También hemos incluido el concepto de actor como forma de definir y realizar un seguimiento de los diferentes perfiles (clientes, proveedores, atacantes, usuarios, etc.) que afectan al sistema migrado de diferentes maneras. Algunos de estos actores tienen papeles que son específicos al metamodelos SMiLe2Cloud, por ejemplo, los clientes pueden firmar contratos y acuerdos de nivel de servicio con cláusulas específicas que afectan a los requisitos y a los controles de seguridad. De hecho, algunos aspectos del modelo pueden ser vistos de forma diferente por los diferentes actores; por ejemplo, para un proveedor de servicios en la nube una cláusula de un SLA puede ser considerada un requisito de seguridad a satisfacer, mientras que la misma cláusula es considerada un control desde el punto de vista del cliente del servicio.

Hemos separado de forma explícita los elementos relacionados con la nube, pero todos se derivan de elementos que no son específicos a este modelo. De esta manera es fácil utilizar el modelo en una actividad de ingeniería inversa de la seguridad de un sistema heredado en cualquier tipo de proceso (sea el sistema objetivo final un sistema en la nube o no) así como en las actividades de ingeniería directa (cuando el modelo de seguridad del sistema heredado ha sido transformado, al menos parcialmente, en un modelo de seguridad en la nube). La fig. 5 señala en azul los elementos del modelo que son específicos al metamodelo SMiLe2Cloud.

C. *Actividades de SMiLe2Cloud*

En esta sección presentaremos una descripción en profundidad del conjunto de actividades en nuestro proceso SMiLeCloud las cuales son mostradas en Fig. 3. El proceso SMiLe2Cloud tiene 7 actividades: Extracción, Valoración, Análisis, Diseño, Migración, Evaluación y Mejora, y un amplio conjunto de artefactos de entrada y salida para cada una de las actividades y que son descritas a continuación.

Actividad 1: Extracción

La extracción es la actividad en la que el modelo de seguridad del sistema heredado es obtenido a partir del propio código del sistema y de la documentación del mismo. Se trata de un subproceso de ingeniería inversa que se puede realizar en paralelo al subproceso de obtención del modelo de arquitectura general del sistema heredado. Normalmente ambos procesos se supone que son realizados con la ayuda parcial de herramientas de ingeniería inversa que faciliten las tareas y pasos que el analista debe realizar para identificar los diferentes requisitos y controles de seguridad existentes en el sistema origen.

Se trata de una actividad orientada por los datos y parte de la especificación formal de los programas y subprogramas del sistema heredado, así como de los datos gestionados por cada unidad de programa. Esta especificación formal tiene la forma de árbol de sintaxis abstracta (AST - Abstract Syntax Tree) que modeliza cada unidad de programa y los datos manejados.

Esta actividad produce artefactos internos que son las salidas de algunas tareas y las entradas de otras. Fig. 6 muestra una representación gráfica de las tareas de la actividad de extracción usando diagramas SPEM 2.0.

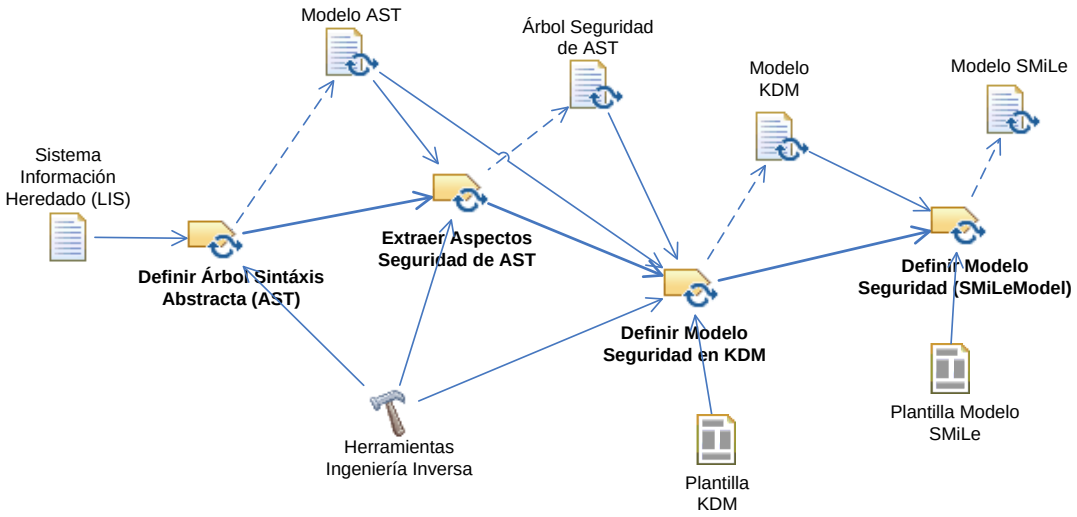

Fig. 6 Actividad de Extracción

Como ejemplo, ofrecemos una descripción detallada de las actividades que hemos considerado en nuestro proceso usando la notación textual SPEM 2.0. Para ello, definimos: tareas, roles, pasos, productos de trabajo y guías, las cuales serán caracterizadas de acuerdo a la disciplina a la que pertenecen. Respecto a SPEM, se describe la actividad de extracción del proceso SMiLeCloud usando la estructura mostrada en Fig. 7.

```
Activity {kind = Iteration}: Name of the iterative Activity
    TaskUse: Name of the Task
        ProcessPerformer {kind: primary}
            RoleUse: Role Name {kind: in}
        WorkDefinitionParameter {kind: in}
            WorkProductUse: Name
        WorkDefinitionParameter {kind: out}
            WorkProductUse: Name {state: state}
        Steps
            Step: Name of the step
        Guidance
            Guidance {kind: type}: Name
```

Fig. 7 Estructura del proceso SMiLe2Cloud usando SPEM 2.0

Cada actividad especifica un WorkProductUse tanto de entrada como de salida (respectivamente), los roles que llevan a cabo o participan en esta actividad (RoleUse), y la colección de pasos (Steps) definidas para una definición de tarea la cual representa todo el trabajo que debe ser llevado a cabo para alcanzar el desarrollo completo de la definición de la tarea. Esta es la estructura seguida en todas las actividades siguientes, pero por restricciones de espacio solo mostraremos una de las tareas, la tarea A1.1 de la actividad de extracción que es mostrada en la Fig. 8.

- A1.1 Definir el árbol de sintaxis abstracta (AST – abstract syntax tree)

Un árbol de sintaxis abstracta es una representación en forma de árbol de la estructura del programa y de los elementos de datos del sistema heredado y ofrece una equivalencia 1-a-1 entre todos los elementos incluidos en el código en forma de estructura arbórea. El AST es usado para derivar los requisitos de seguridad del sistema.

La tarea tiene dos pasos, como se muestra en la fig. 8: el primer paso implica la extracción de toda la información del sistema heredado mediante técnicas de ingeniería inversa tradicionales (análisis estático/dinámico, segmentación, etc.) y se realiza con la ayuda parcial de herramientas; el segundo paso implica la definición del AST con la información extraída.

- A1.2 Extraer aspectos de seguridad del AST

Para cada elemento de datos y de subprograma que ha sido representado en el AST, el analista de sistemas debe extraer los parámetros de seguridad concretos para cada uno de los perfiles de usuarios definidos en su operación habitual normal (acceso, creación, modificación, borrado, administración, auditoría).

Esta tarea tiene tres pasos: el primer paso es identificar los patrones de búsqueda de elementos de seguridad en el modelo AST; el segundo paso es traducir los aspectos de seguridad que se definen en las hojas del árbol AST; el tercer paso es definir el modelo de seguridad derivado del AST en términos de permisos.

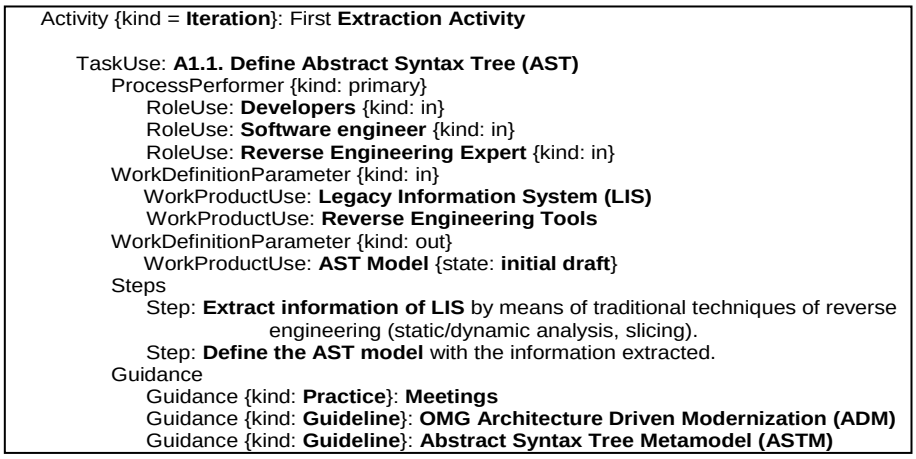

Fig. 8 Descripción detallada de la tarea A1.1 perteneciente a la actividad de Extracción usando SPEM 2.0

- A1.3 Definir el modelo de seguridad en KDM (Knowledge Discovery Metamodel)

Como se indicaba antes, el metamodelo KDM de reingeniería está enfocado en las especificaciones funcionales y no un área de de interés específica en la seguridad integrado en al propio estándar. El trabajo en [20] indica que hay algunas herramientas que utilizan KDM para formalizar contenidos que puedan ser automáticamente importado en otras herramientas; estas herramientas se utilizarían antes de buscar patrones de vulnerabilidad y de realizar el análisis estático de la representación del código, pero el estándar en sí no se refiere a la formalización de los aspectos de seguridad del sistema heredado. Sin embargo, algunos dominios, paquetes y modelos definidos en KDM sí pueden incluir referencias de seguridad (por ejemplo, el dominio de las reglas de negocio, el dominio de datos, el dominio de la plataforma, o el dominio del código fuente). Así, las referencias de seguridad no tienen un único dominio, paquete o modelo en el que se relacionen los aspectos de seguridad y por ello es fácil que los aspectos de seguridad del sistema heredado terminen dispersos entre los distintos modelos y especificaciones de KDM.

Nuestra aproximación propone evitar esta situación haciendo que cada artefacto y control e seguridad del sistema heredado sea instanciado en una regla de seguridad de negocio y se incluye en el modelo conceptual durante la fase de análisis. Para ofrecer apoyo en esta tarea, estamos desarrollando una serie de plantillas con las que identificar y extraer los elementos de seguridad del modelo (por ejemplo, las reglas de negocio relacionadas con los objetivos y requisitos de seguridad y los activos a proteger) desde los diferentes modelos definidos en KDM (fuentes, código, acción, interfaz de usuario, datos), y definir un conjunto de reglas de negocio que recogen los objetivos de seguridad, las políticas y los requisitos del sistema heredado. También intentamos derivar una serie de elementos de la mayoría de los restantes dominios de KDM (fuente, datos, plataforma, interfaz de usuario) que también formarán parte del modelo de seguridad (por ejemplo, los activos).

Esta tarea tiene cuatro pasos: asociación de los permisos de seguridad con las reglas concretas de seguridad, generalizar las reglas concretas de seguridad para obtener objetivos de seguridad del negocio, derivar las políticas de seguridad a partir de los objetivos de seguridad del negocio, y asociar elementos desde los dominios de las fuentes, datos, plataformas e interfaz de usuario del sistema con los activos a asegurar definidos en el inventario.

- A1.4 Definir el modelo de seguridad (modelo SMiLe)

El modelo SMiLe (Security MIgration of LEgacy systems) es un modelo de seguridad de un sistema heredado que ha sido derivado desde las reglas de negocio de seguridad definidos mediante KDM y los activos identificados en el paso A1.3. Ahora es necesario incluir las políticas y controles de seguridad que fueron predefinidos para el sistema heredado (con independencia de si el sistema debe ser migrado a la nube o no).

En este punto es bastante improbable que hayamos identificado los estándares y regulaciones que el sistema heredado original seguía. Para identificar este tipo de elementos en el modelo sería necesario que el sistema heredado tuviera un modelo explícito de especificación de la seguridad con identificación de activos, evaluación de riesgos, análisis de amenazas y otros elementos similares. Si este fuera el caso, completar el resto del modelo SMiLe es sólo una tarea de asociación simple entre el modelo explícitamente definido y los conceptos equivalentes en el modelo SMiLe. Pero, como hemos ya indicado, la disponibilidad de este tipo de modelo de seguridad explícitamente

definido y documentado para un sistema heredado es poco probable (no en vano, un sistema heredado precisamente se caracteriza por estar pobremente documentado de forma explícita y ser resistente al cambio).

Por ello, esta tarea es probablemente la parte más laboriosa de toda la actividad de extracción y cubre la mayor parte del análisis de seguridad que es común a la mayoría de los métodos de definición de requisitos de seguridad. Por ejemplo, será necesario definir árboles de amenazas, evaluar riesgos e identificar vulnerabilidades. Estas tareas no son de naturaleza diferente de la de sus contrapartes en otros procesos de ingeniería de la seguridad en su modalidad de ingeniería directa, y por ello lo que proponemos es utilizar cualquiera de estos métodos de ingeniería directa (por ejemplo, SREP presentado en [21]) para obtener el modelo base SMiLe del sistema heredado. Por supuesto que el analista no utilizará el proceso completo de ingeniería directa de la seguridad, sino sólo aquellas partes del mismo que están relacionadas con el desarrollo básico del modelo de seguridad del sistema, sin preocuparse de desarrollar realmente los controles de seguridad. La decisión de quién será el responsable de desarrollar la mayoría de los controles necesarios para minimizar los riesgos será realizada una vez que otros aspectos de la solución en la nube objetivo hayan sido decididos.

Tal y como se indicó antes, la tarea 1.4 es en sí misma un subproceso completo y es posible aplicar muchos métodos diferentes para llegar al objetivo final que es derivar el modelo SMiLe definitivo. Por ello, no tiene mucho sentido entrar a refinar la definición paso por paso de la tarea. Este refinamiento dependerá en gran medida del método que el analista haya elegido para derivar el modelo de seguridad definitivo. En único requisito real para el subproceso es que el modelo pueda ser realizado en términos del metamodelo de seguridad que ha sido definido; pero dado que nuestro metamodelo está muy próximo a la mayoría de los metamodelos actuales (especialmente a OSA) el analista no debería tener ningún problema para relacionar los conceptos de su propia elección con los del modelo SMiLe.

Actividad 2: Valoración

La actividad de valoración es en la que el modelo general de seguridad del sistema heredado es adaptado al nuevo entorno (en nuestro caso, a la nube). Comenzamos con un modelo SMiLe que no está específicamente adaptado al entorno de la nube y en dicho modelo estudiamos las fortalezas, debilidades, oportunidades y amenazas específicas que la nube incorpora. Esta actividad comienza con el modelo SMiLe (esto es, el modelo de seguridad del sistema heredado obtenido por ingeniería inversa) y es realmente la primera actividad de ingeniería directa del modelo de herradura que define nuestro proceso.

Los objetivos de esta actividad son los siguientes: refinar el modelo SMiLe para obtener un modelo SMiLe2Cloud (esto es, adaptar el modelo del sistema heredado con las amenazas específicas de la nube, los activos específicos en la nube, los escenarios específicos de la nube, los requisitos específicos de la nube, etc.); seleccionar un conjunto de proveedores de servicios en la nube y de proveedores de seguridad en la nube que, al menos parcialmente, cumplan con los requisitos de seguridad del modelo SMiLe2Cloud del sistema heredado según nuestra especificación de seguridad; y validar los modelos de servicio y de despliegue que pueden utilizarse dentro de los límites de dichas especificaciones de requisitos de seguridad.

La Fig. 9 muestra una representación gráfica de las tareas de la actividad de valoración junto con los artefactos de entrada y salida usando diagramas SPEM 2.0.

- A2.1 Definir la matriz DAFO (*Debilidades, Amenazas, Fortalezas y Oportunidades*) e incorporar los elementos específicos de la nube en el modelo SMiLe

Para cada uno de los requisitos en el SecRS, la próxima tarea es definir una matriz (DAFO) con las debilidades, fortalezas, oportunidades y nuevas amenazas que el modelo cloud plantea al LIS.

En este análisis, comprobamos las cuestiones específicas que son abordadas en los documentos de seguridad que se centran en entornos cloud. El objetivo del análisis DAFO es descubrir: si hay amenazas de seguridad en el modelo fuente LIS que no están presentes en el modelo de destino cloud (fortalezas); si existen nuevas amenazas de seguridad que son relevantes en la nube, si hay amenazas en el modelo de código LIS que no están presentes en el modelo de destino cloud que debe ser abordado (debilidades); si hay nuevos controles disponibles en el modelo de destino cloud que puedan reemplazar ventajosamente los controles actualmente en vigor en el modelo fuente no-cloud (oportunidades); y si existen controles establecidos en el modelo fuente no-cloud que no pueden ser integrados en un entorno cloud (amenazas).

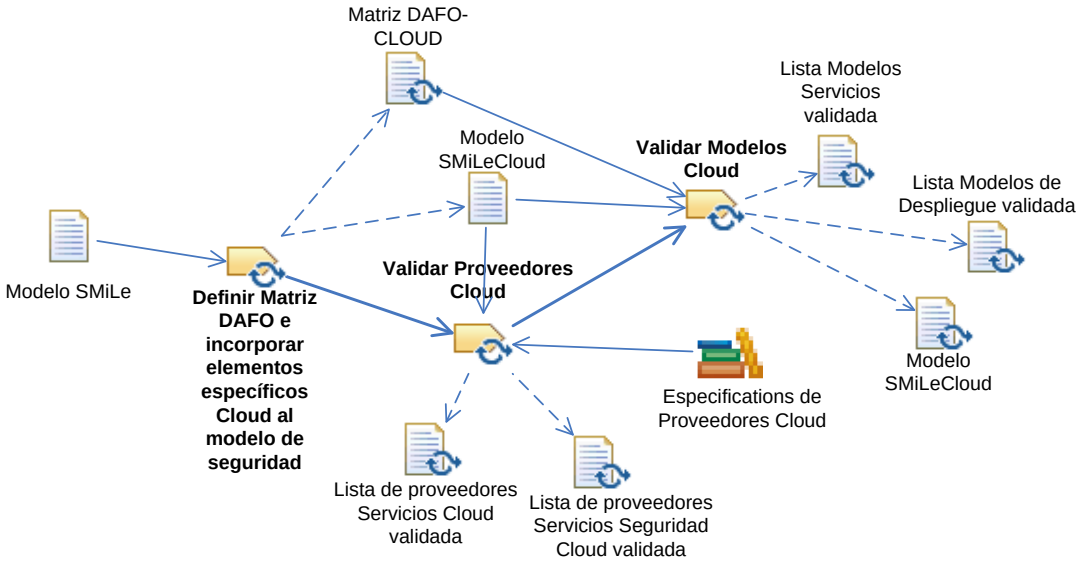

Fig. 9 Actividad de Valoración

El análisis DAFO implica una adaptación del modelo SMiLe que es refinado dentro del modelo SMiLe2Cloud con la incorporación de los activos cloud, las nuevas amenazas específicas cloud, una lista de los controles cloud propuestos que pueden sustituir a los controles existentes y una lista de los controles de seguridad del LIS que no pueden implementarse en entornos cloud.

En este punto nosotros introducimos controles específicos definidos en los 13 dominios del CSA (Cloud Security Alliance) (tomamos sólo los 13 dominios aparte del primero, es decir, el marco arquitectónico de la computación cloud, que es principalmente una introducción y descripción de los conceptos cloud) y mapeamos la matriz de control cloud proporcionada por el CSA dentro del modelo.

Algunos de los dominios y controles definidos por el CSA son sistemas amplios (por ejemplo, la DG-01 y controles IS-02). Todas las aplicaciones que son migradas al cloud deberían compartirlos, y sería posible la reutilización de los controles ya existentes desde otros ciclos del proceso de migración.

Esta tarea tiene dos pasos: validar la aplicabilidad de los controles CSA al LIS y refinar el modelo SMiLe dentro del modelo SMiLe2Cloud.

- A2.2 Validar proveedores en la nube

Una vez que la matriz DAFO se ha completado, el analista debe contrastarlo con el modelo SMiLe del LIS y comprobar la lista de proveedores de servicios cloud que puede abordar las especificaciones funcionales del LIS y extraer las especificaciones de seguridad que ofrecen dentro de los términos del acuerdo de nivel de servicio. El analista también debe comprobar cuáles términos relacionados con la seguridad del acuerdo a nivel de servicio están abiertos a negociación.

El analista adicionalmente validará un conjunto de proveedores de servicios de seguridad cloud, evaluando si se pueden entregar los controles que son necesarios para aliviar o implementar los controles necesarios que hemos identificado.

- A2.3 Validar modelos en la nube

Dado que las diferentes propuestas de modelos cloud (modelos de servicios y modelos de despliegue) forman parte de la arquitectura del modelo cloud y no del modelo de seguridad, no se debe tratar de cambiar los modelos seleccionados o propuestos definidos en la arquitectura LIS. Sin embargo, los modelos conducen a una diferencia en las restricciones de seguridad que el sistema migrado deberá enfrentar. Por tanto, es necesario validar si los modelos seleccionados o propuestos, de los proveedores seleccionados en el paso anterior, pueden o no cumplir con los requisitos de seguridad del LIS. Si no, el riesgo que no está cubierto por el requisito de seguridad no cumplido debe ser aceptado o un cambio en la arquitectura destino debe ser recomendada, proporcionando una lista de modelos aceptables que cumplen con los requisitos de seguridad.

Actividad 3: Análisis

La actividad de análisis es en la que definimos los requisitos de seguridad a implementar e identificamos el conjunto de servicios de seguridad contratables a proveedores específicos de seguridad como servicio (SecaaS) que se integrarán en nuestra aplicación una vez migrada a la nube. También se identificarán otros controles tales como las cláusulas estándar del SLA que

afectan a cuestiones de seguridad y también puede que volvamos a validar si los proveedores de servicio en caso de que algún proveedor concreto no pueda cumplir dentro de su marco contractual con los requisitos fundamentales de seguridad definidos.

La Fig. 10 muestra una representación gráfica de las tareas de la actividad de análisis junto con los artefactos de entrada y salida usando diagramas SPEM 2.0.

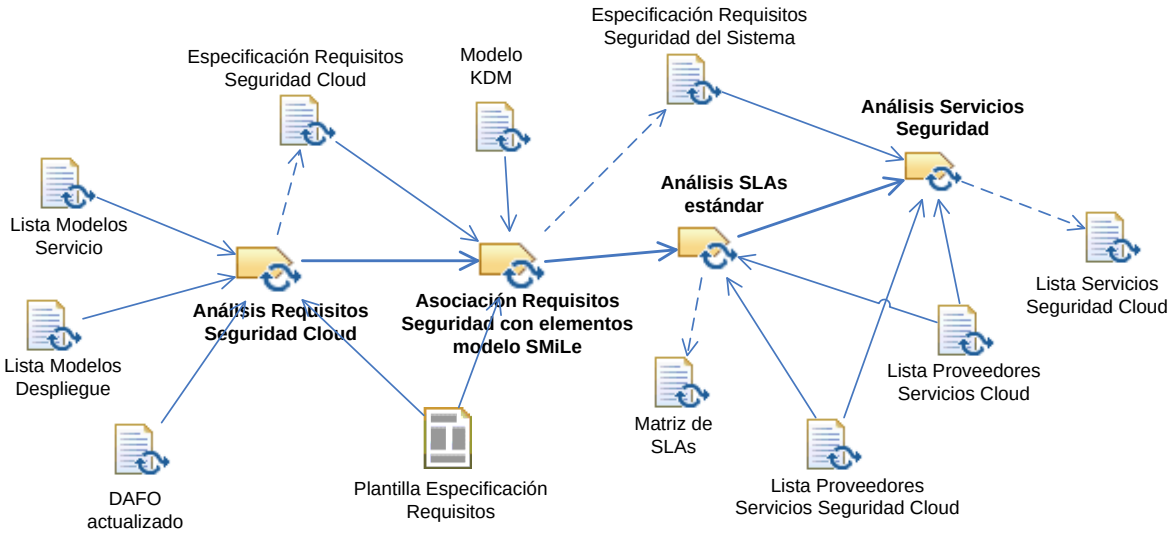

Fig. 10 Actividad de Análisis

- A3.1 Análisis de requisitos de seguridad en la nube

El modelo SMiLe2Cloud actualizado, proveedores cloud validados, modelos de servicio y despliegue son usados para derivar un conjunto de SecRS con la cual el sistema diseñado debe cumplir con el nuevo entorno. Los requisitos serán un subconjunto de requisitos del LIS que el LIS tenía y con los requisitos que se incluyeron en el desempeño del análisis DAFO.

Dos pasos son definidos en esta tarea: analizar los requisitos del LIS que ya no son necesarios y analizar los nuevos requisitos cloud que resulten aplicables.

Algunos de los requisitos del LIS original pueden ya no ser más aplicables al sistema destino, ya que el ecosistema cloud podría simplemente haberlos hecho redundantes o innecesarios. También es necesario tener en cuenta que no todos los controles cloud pueden ser aplicables al LIS; antes de continuar con el siguiente paso es necesario un análisis de la aplicabilidad de los nuevos requisitos cloud.

- A3.2 Asociación de los requisitos de seguridad con los elementos de SMiLe

Los artefactos obtenidos a partir de la tarea anterior deben ser utilizados para desarrollar un mapeo entre los requisitos de seguridad del LIS y una especificación formal de los requisitos de seguridad con la que el sistema destino debe cumplir para estar seguro de acuerdo con la especificación de la nueva arquitectura.

Estos requerimientos adoptan la forma de un conjunto de casos de uso de seguridad, una especificación completa UMLSec detallada o texto plano, y pueden ser tanto los requisitos que no son específicos del cloud como requisitos específicos de cloud.

Para este tipo de mapeo, trabajamos con plantillas que ayudan a facilitar la propia especificación. Un conjunto de reglas pueden ser identificadas y definidas con el fin de documentar más y después validar las especificaciones de los controles desarrollados o acordados en el SLA.

- A3.3 Análisis de los acuerdos estándar de nivel de servicio

Una vez que los requisitos de seguridad se han identificado y definido formalmente, es necesario seguir analizando el SLA estándar definido por los proveedores de la nube en busca de problemas de seguridad, políticas de seguridad, elementos de seguridad que pueden ser medidos, etc.

En esta tarea se extraen todas las cuestiones de seguridad relevantes que aparecen en el SLA de los proveedores validados o seleccionados, permitiendo así que las cláusulas de cada SLA sean mapeadas con los requisitos formalmente obtenidos en la tarea anterior.

- A3.4 Análisis de servicios de seguridad

La última tarea de esta actividad se ocupa de los servicios de seguridad actuales que son ofrecidos por los proveedores de servicios de seguridad. Una vez

más, esto puede implicar el análisis de SLA de estos proveedores y mapear algunas cláusulas del SLA en requisitos de las actividades anteriores.

Esta tarea nos permitirá obtener un conjunto de servicios de seguridad que deben integrarse en nuestro modelo de seguridad para el LIS.

Actividad 4: Diseño

En la actividad de diseño se definen los componentes propiamente dichos que forman el núcleo de la arquitectura de seguridad del sistema (cláusulas, controles personalizados, protocolos, etc.), y no sólo se define el diseño, sino que también se define la forma en la que deben ser validados y se planifican las actividades que serán necesarias en la migración real de la seguridad del sistema heredado.

La Fig. 11 muestra una representación gráfica de las tareas de la actividad de diseño junto con los artefactos de entrada y salida usando diagramas SPEM 2.0.

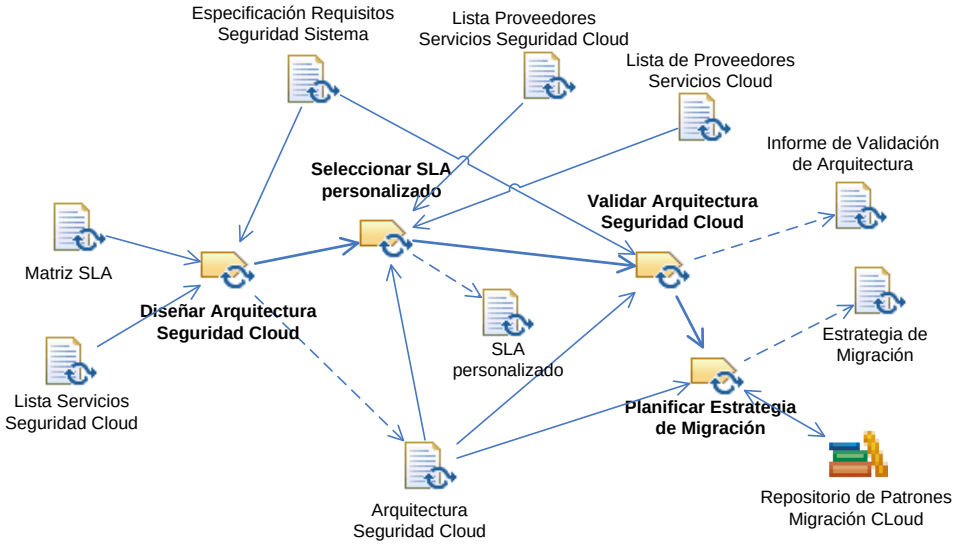

Fig. 11. Actividad de Diseño

- A4.1 Diseñar la arquitectura de seguridad básica para la nube

En esta tarea, se toma la especificación de los requisitos de seguridad y las cláusulas del SLA identificados en los pasos anteriores, junto con la lista de los anteriores servicios de seguridad cloud y se desarrolla la arquitectura de seguridad básica en términos de controles que se pueden ser integrados para cumplir con los requisitos de seguridad.

Si algunos requisitos no se pueden satisfacer plenamente dentro del SLA estándar y/o del SecSLA específica del proveedor de seguridad cloud, y la plataforma o modelo de nube nos permite hacer esto, podemos introducir nuevos controles para cumplir con los requisitos de seguridad que permanecen descubiertos por el SLA estándar y los servicios de seguridad cloud.

Esta tarea a veces implica el desarrollo de un diseño de una pieza de código o una interfaz para una pieza de código ya desarrollada. Por ejemplo, si es necesario implementar un conjunto de normas de seguridad basado en roles y la base de datos cloud elegida no es compatible con el concepto de rol, entonces será necesario integrar una clase con la que gestionar este rol en la aplicación, o para proponer otra base de datos que implementa el concepto de rol.

El artefacto principal que se extrae de esta tarea es la arquitectura de seguridad en la nube que incluye las cláusulas que constituyen la base de los servicios de seguridad, que se obtienen, ya sea del proveedor de servicios en la nube o el proveedor de servicios de seguridad en la nube, y controles personalizados que tienen que ser implementados en nuestra aplicación.

- A4.2 Diseñar los acuerdos personalizados de nivel de servicio

Siempre que sea posible, SLA (ya sea SLA general o SecSLA) debe ser personalizado para satisfacer las necesidades específicas del cliente.

La mayoría de los analistas cloud aconsejan que los contratos de servicio se adapten a las necesidades del cliente. En la práctica, esto sólo será un motivo de preocupación para los grandes clientes que pueden negociar contratos lucrativos. Por otra parte, es evidente que no todos los proveedores de servicios permitirán la personalización de los servicios y/o cláusulas hasta el grado deseado.

Sin embargo, una mera posibilidad siempre debe ser considerada. La personalización de un SLA a veces puede evitar la necesidad de desarrollar controles específicos, lo que sitúa la responsabilidad del control en manos del proveedor de servicio, en lugar de la nuestra. Esto debe hacerse tan a menudo como sea posible sin perder el control de la LIS y/o añadiendo nuevos riesgos para la privacidad de la información.

Este es el momento de diseñar las cláusulas que nos gustaría introducir. En el peor de los casos (si no se nos permite personalizar el SLA estándar) podremos utilizar la cláusula diseñada a medida, que es un medio para validar la arquitectura y posteriormente verificar y validar el modelo implementado.

- A4.3 Validar la arquitectura de seguridad específica de la nube

Una vez que la arquitectura de seguridad ha sido obtenida, y antes que la migración actual comience, tiene lugar la validación de la arquitectura. Esta validación involucra una revisión formal del diseño que hemos propuesto (ya sea SLA o controles personalizados). Después de esta validación, la aplicabilidad y viabilidad técnica de la arquitectura debería ser aclarada; es decir, todos los controles que se implementen a través de SLA deberían ser elegibles o dentro del ámbito SLA de los proveedores seleccionados y la responsabilidad de entregar el control siempre debe estar clara (es decir, cuando usamos dos proveedores de servicios, debemos asegurarnos que no hay ninguna posibilidad de que los contratos deleguen mutuamente la responsabilidad del control de seguridad). Como alternativa, los controles deben poder aplicarse como controles personalizados en el modelo seleccionado (es decir, en PaaS, el acceso está disponible para definir usuarios y otorgar permisos en una base de datos).

- A4.4 Planificar la estrategia de migración

Finalmente, la última tarea de la actividad de diseño es desarrollar un plan relativo a cómo la seguridad del LIS será implementada con recursos, horarios, logros, etc.

En este paso, una librería de patrones de migración cloud que facilita el propio proceso de migración será usado como un recurso (son patrones para mejorar el proceso de migración más que patrones para asegurar el propio proceso de migración).

El artefacto resultante de esta tarea es la estrategia actual para la migración de la seguridad del LIS una vez que la migración ha comenzado.

Actividad 5: Migración

Finalmente, la propia migración tiene lugar y es necesario contratar en la realidad los servicios y firmar los acuerdos de nivel de servicio y desarrollar los elementos de seguridad personalizados e implantarlos y configurarlos para dejar todos los controles de seguridad en condiciones de operación habitual.

La Fig. 12 muestra una representación gráfica de las tareas de la actividad de migración junto con los artefactos de entrada y salida usando diagramas SPEM 2.0.

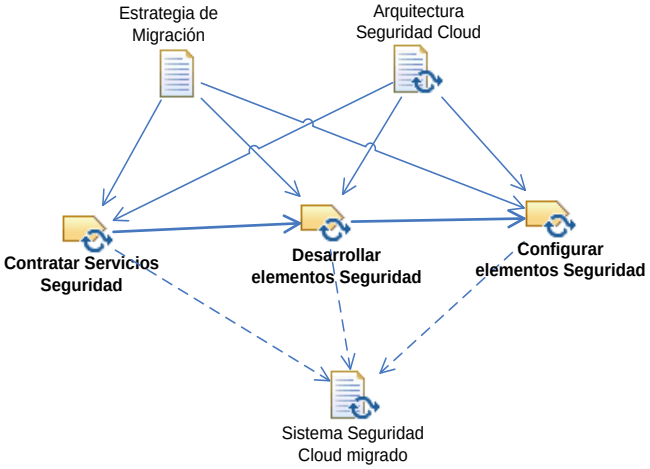

Fig. 12 Actividad de Migración

- A5.1 Contratar servicios de seguridad

En este punto tiene lugar la formalización del contrato. Este contrato puede ser un acuerdo de nivel de servicio con un proveedor de servicios de seguridad en la nube o pueden ser las cláusulas específicas de seguridad que se definen en los contratos con proveedores de servicios IaaS, PaaS o Saas.

Este proceso puede ser en ocasiones bastante largo, ya que puede implicar procedimientos legales y burocráticos y muchos pasos. Por ejemplo, en una administración pública puede implicar un proceso de contratación con publicación en diarios oficiales, vistas y pujas públicas, revisiones legales y otros elementos similares de garantía pública del proceso. Este tipo de burocracia es común a la mayoría de los contratos de suministros (como los de comunicaciones y los de energía).

Esta actividad será relativamente predecible si en la tarea de planificación que acometimos previamente se tuvieron en cuenta todas las peculiaridades del proceso de contratación de la organización que trata de migrar el sistema heredado y los proveedores de servicios seleccionados, pero puede ser realmente problemática si existe demasiada burocracia de por medio.

- A5.2 Desarrollar controles de seguridad a medida

Si nuestra arquitectura define controles de seguridad personalizados, ha llegado el momento de desarrollarlos. Por ejemplo, si hemos definido que nuestro sistema tundra una pieza de software que controlará los perfiles de usuario en una base de datos ofrecida por un proveedor de PaaS que no incorpora un sistema de roles internamente en la propia base de datos, será necesario desarrollar la pieza de software que realice la gestión del roles e integrarla en nuestras

aplicaciones y programas que desarrollan elementos funcionales; también será necesario en este punto hacer las pruebas unitarias de software de los controles de seguridad a medida.

Este tipo de tarea será habitual en algunos modelos de servicio (por ejemplo cuando estemos en presencia de IaaS) y será rara en otros (por ejemplo cuando se haya seleccionado el modelo SaaS).

- A5.3 Configurar controles de seguridad

Para los controles de seguridad personalizados definidos, contratados y/o implantados de forma personalizada en los pasos anteriores, normalmente es necesario realizar una función de despliegue en el sistema final. Además, si los controles necesitan algún tipo de configuración, en este punto deberán ser configurados y afinado su funcionamiento.

Actividad 6: Evaluación

Una vez que todo el proceso ha concluido y el sistema heredado sido movido a la nube de forma segura, es el momento de verificar y validar el sistema y los controles de seguridad.

La Fig. 13 muestra una representación gráfica de las tareas de la actividad de evaluación junto con los artefactos de entrada y salida usando diagramas SPEM 2.0.

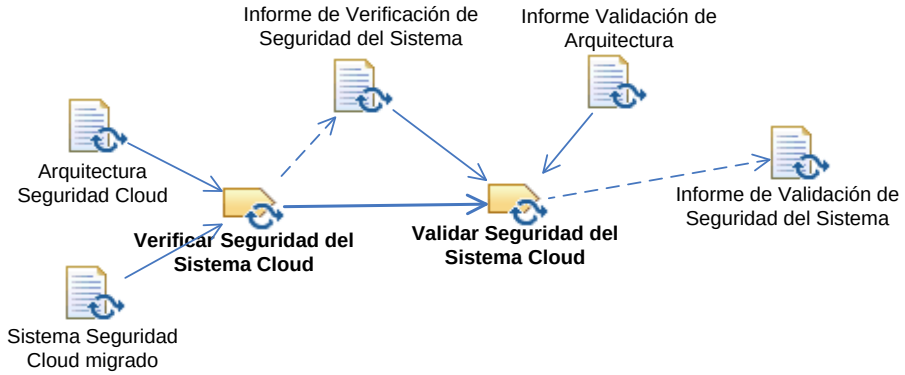

Fig. 13 Actividad de Evaluación

- A6.1 Verificar seguridad del sistema cloud

En actividades anteriores (durante el análisis y el diseño) algunos de los artefactos de salida eran entradas en la parte del proceso y del modelo de seguridad que trata con las cuestiones de pruebas, verificación y certificación de la seguridad.

En esta actividad, dichas pruebas son realizadas de forma que se pueda reunir evidencia suficiente para certificar o validar la seguridad del sistema.

Técnicamente, la verificación es el proceso de comprobación de que los propios requisitos son cubiertos por los controles implantados.

En algunos casos, la verificación será difícil puesto que la valoración del cumplimento de un servicio que ha sido contratado a veces requiere recursos no disponibles para el cliente un servicio en la nube, y a veces es necesario mantener una vigilancia contante (al menos durante una cantidad de tiempo considerable) sobre algunas métricas de seguridad definidas.

Sin embargo, en esta parte del proceso nosotros sólo nos enfocaremos en aquellos controles que pueden ser verificados mediante una actividad no recurrente y con herramientas de verificación al alcance del cliente del servicio en la nube (o sobre métricas a las que el cliente tiene acceso). Por ejemplo, si hemos firmado una clausula en un acuerdo de nivel de servicio que fija una serie de métricas de calidad sobre las contraseñas, podremos realizar una serie de intentos que pretendan definir una contraseña para un usuario escogido al azar en el sistema en funcionamiento con criterios de calidad de contraseña supuestamente insuficientes.

- A6.2 Validar seguridad del sistema cloud

Técnicamente, la validación es la actividad formal que hace que un sistema sea válido para el responsable de las cuestiones de seguridad de las tecnologías de la información: el administrador de la seguridad. La tarea consiste en revisar las evidencias obtenidas en la actividad anterior y en producir un documento que establece que la gestión de la seguridad está de acuerdo con la seguridad de los sistemas heredados (LIS) migrados a la nube de acuerdo con los requisitos especificados.

Actividad 7: Mejora

Dado que nuestro proceso tiene vocación de mejora continua (se trata de un ciclo de Deming) no finaliza con la validación real del sistema en funcionamiento.

Periódicamente, el responsable de la seguridad del sistema heredado deberá reunir nuevas evidencias que permitan asegurar que el sistema está permanentemente configurado según los requisitos y parámetros de seguridad definidos y que permita

renovar la validación. También estudiará mejoras que afecte al análisis DAFO, al análisis de seguridad en la nube o incluso a la lista de servicios en la nube que pueden ser considerados en las anteriores tareas.

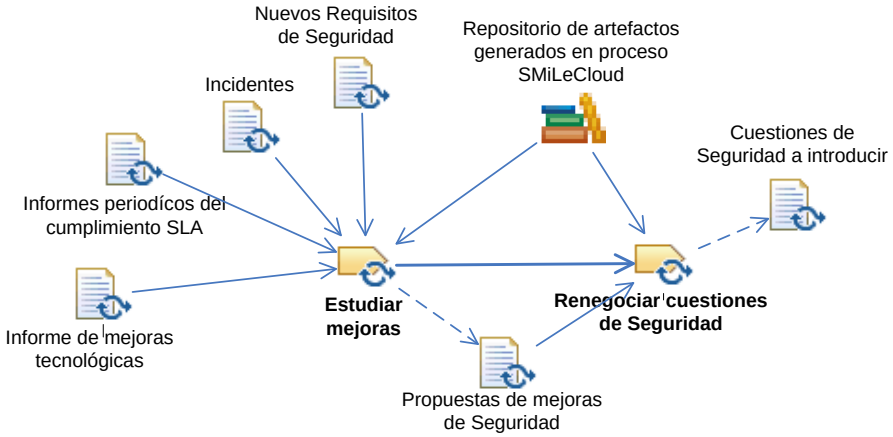

Fig. 14 Actividad de Mejora

La Fig. 14 muestra una representación gráfica de las tareas de la actividad de mejora junto con los artefactos de entrada y salida usando diagramas SPEM 2.0.

A7.1 Estudiar mejoras

La nube es un entorno cambiante. Algunos de los problemas que ahora están siendo objeto de estudio por parte de la mayor parte de los expertos, hace un par de años ni siquiera se conocían. En un par de años, puede que haya servicios completamente nuevos que ayuden a fortalecer la seguridad de un sistema heredado migrado a la nube. Además, dado que al mover un sistema a la nube, delegamos la responsabilidad sobre la aplicación de algunos controles, es necesaria y aconsejable que se vigilen los niveles y métricas definidos para asegurar su cumplimiento.

Incluso aunque el sistema esté operativo y funcionando, como ya hemos indicado, la verificación de algunas de las partes de ese sistema suponen un esfuerzo continuo para reunir evidencias adicionales que indiquen que la seguridad se mantiene en los niveles acordados y que los servicios de seguridad son proporcionados según las especificaciones del SecSLA.

Por ello, la actividad 6.1 debe ser repetida con cierta periodicidad y los resultados de esta actividad deben ser analizados y contrastados con los límites de las especificaciones de la arquitectura de seguridad propuesta.

Pero incluso si las especificaciones de seguridad fueran cubiertas en la forma en la que aparece escrito en los SecSLA, el hecho de que nuestro proceso sea un ciclo de Deming implica cierto tipo de reelaboración continua en busca de posibles mejoras al sistema de seguridad.

Estas mejoras pueden venir derivadas de avances técnicos en el campo de la seguridad o de la nube, de cambios producidos en los acuerdos estándar de nivel de servicio o en los propios servicios que el proveedor ofrece, de cambios legislativos que beneficien al cliente, etc. Cada vez que el sistema vuelva a ser evaluado, el informe de validación del sistema en el que se acepta la adecuación del sistema de seguridad conforme a los requisitos definidos, debería incluir una sección en la que la propuesta de mejoras sea estudiada y los cambios en los requisitos sean actualizados.

- A7.2 Renegociar cuestiones de seguridad

Finalmente, hemos definido una actividad que permita renegociar con los proveedores de servicios y proveedores de seguridad las incidencias de seguridad. Esta negociación es diferente de la que supone la renegociación de nuevos servicios.

Un incidente de seguridad puede ocurrir durante la operación del sistema y dicho incidente puede afectar al estado de seguridad general del sistema. Habitualmente, las políticas de contratación habituales existentes en los acuerdos de nivel de servicio indican penalizaciones aplicables si el proveedor no cumple con los requisitos cubiertos por el acuerdo de nivel de servicio.

Sin embargo, incluso si las penalizaciones están previstas, la mayoría de las cláusulas necesitan cierta interpretación que en ocasiones sólo se realiza cuando se presenta el caso real de aplicación del texto concreto del acuerdo de nivel de servicio que hace referencia a la situación concreta. En estos casos, el cliente puede necesitar negociar la interpretación de las cláusulas aplicables del contrato de servicios, las penalizaciones e incluso proponer cambios en la redacción del SLA.

D. Conclusiones

En este artículo hemos presentado un proceso que permite la migración de la seguridad o la migración segura a la nube de un sistema de información heredado. Comenzamos en el punto en el que el sistema ha sido objeto de un proceso de ingeniería inversa y tenemos disponibles una serie de modelos KDM que definen la parte funcional del sistema heredado. Desde este punto, ofrecemos una serie de actividades que permitirán evolucionar estas especificaciones en formato KDM en una arquitectura de seguridad para el sistema heredado y desde allí en un sistema objetivo migrado a la nube en forma segura; actualmente estamos desarrollando técnicas y plantillas para automatizar parcialmente el proceso de entrega de una arquitectura segura y para mapear la arquitectura de seguridad deseada en un modelo que de forma específica trate las cuestiones específicas de la nube como las amenazas específicas que la nube presenta, los requisitos de seguridad específicos para la nube, los controles específicos relacionados con la nube (ya sean en su forma de seguridad como servicio o como controles personalizados); todo ello con la intención de que una aplicación heredad que sea migrada a la nube cumpla estándares de seguridad en la nube tales como la matriz de controles de la CSA.

Nuestro trabajo futuro se enfocará en un ulterior refinamiento del propio proceso (ya que alguno de nosotros piensa que algunos aspectos del mismo pueden ser simplificados) y en el desarrollo de herramientas y patrones que permitan de forma semiautomática asistir al analista de seguridad en las actividades de obtención del modelo de seguridad del sistema heredado y la derivación del modelo de seguridad del sistema migrado a la nube a partir de aquél.

AGRADECIMIENTOS

Esta investigación es parte de los siguientes proyectos: SERENIDAD (PEII11-037-7035) financiado por la "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha" y FEDER, y SIGMA-CC (TIN2012-36904) financiado por el "Ministerio de Economía y Competitividad".

Un agradecimiento especial a Rafael Gómez Lago por su ayuda y labor realizada en esta investigación.

BIBLIOGRAFÍA

[1] Simmhan, Y., A.G. Kumbhare, B. Cao, and V.K. Prasanna, An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds, in IEEE International Conference on Cloud Computing, CLOUD 2011. 2011: Washington, DC, USA. p. 582-589.

[2] Gens, F. IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. IDC Exchange 2008 [cited 2012 20/10/2012]; Available from: http://blogs.idc.com/ie/?p=210.

[3] TOG, The Open Group Cloud Computing Survey. 2011, The Open Group.

[4] Jansen, W. and T. Grance, Guidelines on Security and Privacy in Cloud Computing. 2011.

[5] Winkler, J.R.V., in Securing the Cloud. Cloud Computing Security. Techniques and Tactics, B. Meine, Editor. 2011, Syngress, Elsevier. p. 25.

[6] Tobin, M. and B. Bass, Federal Application Modernization Road Trip: Express Lane or Detour Ahead? 2011, MeriTalk.

[7] Kundra, V., Federal Cloud Computing Strategy, U.S.C.I. Office, Editor. 2011.

[8] Rosado, D.G., R. Gómez, D. Mellado, and E. Fernández-Medina, Security Analysis in the Migration to Cloud Environments. Future Internet, 2012. 4(2): p. 469-487.

[9] Gómez, R., D.G. Rosado, D. Mellado, and E. Fernández-Medina, Security Criteria in Deciding on Migration of Systems to the Cloud, in 9th International Workshop on Security in Information Systems. 2012: Wroclaw, Poland. p. 93-100.

[10] CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011.

[11] Zhang, W., A. J.Berre, D. Roman, and H. Aage Huru, Migrating Legacy Applications to the Service Cloud, in OOPSLA 2009, Towards Best Practices in Cloud Computing. 2009.

[12] Seacord, R., D. Plakosh, and G. Lewis, Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices. 1st ed. 2003: Addison Wesley.

[13] OMG, Architecture-Driven Modernization. Knowledge Discovery Meta-Model (KDM), v1.3. 2011.

[14] Frey, S. and W. Hasselbrind, Model-Based Migration of Legacy Software Systems into the Cloud: The CloudMIG Approach, in 12 Workshop on Software-Reengineering of the GI-SRE. 2010.

[15] Zhou, H., H. Yang, and A. Hugill, An Ontology-Based Approach to Reengineering Enterprise Software for Cloud Computing, in IEEE 34th Annual Computer Software and Applications Conference. 2010: Seoul, Korea. p. 383-388.

[16] Vu, Q.H. and R. Asal, Legacy Application Migration to the Cloud: Practicability and Methodology, in IEEE Eighth World Congress on Services. 2012.

[17] [17]OSA. OSA Metamodel. 2012 [cited 2012; Available from: http://www.opensecurityarchitecture.org/cms/foundations/osa-metamodel.

[18] 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.

[19] Jürjens, J., UMLSec: Extending UML for Secure Systems Developments. Jean-Marc J´ez´equel, Heinrich Hussmann, and Stephen Cook, editors, UML 2002 — The Unified Modeling Language, LNCS, 2001. 2460: p. 412-425.

[20] Pérez-Castillo, R., I. García-Rodríguez de Guzmán, and M. Piattini, Knowledge Discovery Metamodel-ISO/IEC 19506: A standard to modernize legacy systems. Computer Standards & Interfaces, 2011(33): p. 519-532.

[21] Mellado, D., E. Fernández-Medina, and M. Piattini, A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems. Computers Standards & Interfaces, 2007. 29(2): p. 244-253.