Design Activity in the Process of Migrating Security Features to Cloud

L. Márquez, D. G. Rosado, H. Mouratidis and E. F. Medina

Abstract— **The importance of cloud computing is increasing enormously and receives a great attention from the scientific community. The Cloud Computing offers a wide range of benefits, but also a major challenge from the point of view of security, in fact security remains the main obstacle to success. Migration of legacy systems to the cloud gives us the opportunity to take control over security in legacy systems. The process called SMiLe2Cloud aims to solve the problem of secure migration legacy information systems to cloud. This paper aims to present a case study on the design of the migration of the security features of a legacy application to Cloud providers by using the process called SMiLe2Cloud.**

Keywords— **Cloud, security, migration, design, CSA.**

I. INTRODUCCION

UNO de los principales desafíos es la definición de Cloud Computing. Basado en la Cloud Security Alliance [1], Cloud Computing puede ser definido como: "un modelo para proporcionar acceso ubicuo, conveniente y bajo demanda a un conjunto de recursos de computación configurable (p. ej., redes, servidores, almacenamiento, aplicaciones y servicios)".

El nivel de importancia detrás de Cloud Computing se puede leer en el reciente informe publicado por la Comisión Europea titulado "Unleashing the Potential of Cloud Computing in Europe" [2]. En este informe se lleva a cabo una previsión del posible impacto del Cloud Computing que puede resultar en "una ganancia de más de 2,5 millones de nuevos puestos de trabajo, y un estímulo anual de 160 billones de euros al Producto Interior Bruto de la Unión Europea (sobre el 1%) para el año 2020".

Cloud Computing permite reducir el coste mejorando la utilización de los recursos, reduciendo los costes de administración y de infraestructuras y permitiendo ciclos de desarrollo más rápidos [3].

La esencia de la migración de sistemas heredados es el movimiento de un sistema existente a una nueva plataforma manteniendo la funcionalidad del sistema heredado causando el mínimo impacto al sistema operacional existente [4].

La migración de sistemas heredados es un procedimiento muy caro que tiene un riesgo de fallo muy elevado. Por ello antes de tomar la decisión de migrar, se debe hacer un estudio intensivo para cuantificar los riesgos y los beneficios que justifiquen la migración del sistema heredado [5, 6].

Según una encuesta llevada a cabo por PwC en el informe "The Future of IT Outsourcing and Cloud Computing" [7] el 62 % de los encuestados consideran la seguridad como la principal preocupación que los usuarios tienen en cuenta cuando mueven sus datos y aplicaciones al Cloud. Cloud Computing no introduce nuevos conceptos de seguridad que no se hayan estudiado previamente. La preocupación en la migración al Cloud es que la implementación de las medidas de seguridad depende de un tercero. Esta pérdida de control enfatiza la necesidad de transparencia por parte de los proveedores Cloud [8]. Sin embargo, en algunos casos los proveedores Cloud pueden ofrecer una mejor seguridad que una pequeña organización pueda lograr por sí misma.

El proceso denominado SMiLe2Cloud [9, 10] pretende resolver el problema de la migración con seguridad a la nube de sistemas de información heredados. El proceso SMiLe2Cloud consta de cinco actividades (extracción, análisis, diseño, despliegue y evaluación) dirigidas por 16 dominios de seguridad definidos por Cloud Security Alliance (en adelante CSA) en su Cloud Control Matrix v3 (en adelante CCM) [11].

El presente artículo pretende exponer un caso práctico sobre el diseño de la migración de las características de seguridad de una aplicación heredada a proveedores de Cloud utilizando para ello el proceso denominado SMiLe2Cloud. La estructura del artículo es como sigue: el capítulo II explica los distintos estándares de seguridad que CSA propone para el Cloud Computing, el capítulo III explica el proceso SMiLe2Cloud de migración de características de seguridad de una aplicación heredada al Cloud, el capítulo IV presenta el caso de estudio, el capítulo V expone la actividad de diseño de la migración de las características de seguridad y por último en el capítulo VI se exponen las conclusiones y el trabajo futuro.

II. INCUBADORA DE ESTÁNDARES DE SEGURIDAD CLOUD

Al igual que con todas las normas de sistemas de gestión, ISO/IEC 27001 [12] ha sido escrita de tal manera que se pueda aplicar a cualquier organización, grande o pequeña, en todas las industrias. Sin embargo, se considera que existen requisitos especiales específicos para Cloud Computing que o bien no están cubiertos o que necesitan ser cubiertos con mayor precisión.

CSA ha identificado dichas carencias en el entorno de las TI (Tecnologías de la Información) que están inhibiendo la

L. Mrquez, Spanish National Authority for Markets and Competition (CNMC), Madrid, Spain, luis.marquez@cnmc.es

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

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

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

contratación de servicios seguros y confiables en la nube por parte del mercado. CSA se posiciona como una incubadora de estándares de seguridad en Cloud, de forma que los proyectos de investigación utilizan metodologías ágiles para la rápida producción de resultados.

Por un lado CSA ha desarrollado un conjunto de guías de seguridad agrupadas en el documento "Guías de Seguridad de Áreas Críticas en Cloud Computing" que ya va por su tercera versión [1]. Este trabajo es un conjunto de las mejores prácticas de seguridad que CSA ha reunido en los dominios involucrados en el gobierno y las operaciones en Cloud.

Por otro lado CSA, unido a la British Standards Institution (en adelante BSI) está desarrollando un esquema de certificación de terceros para la seguridad en la nube llamada certificación STAR [13]. El plan incorpora los requisitos de la norma ISO 27001 y un índice de madurez para indicar cómo de bien la organización está cumpliendo con los requisitos específicos de la nube.

El esquema de certificación STAR se basa en la Matriz de Controles para la Nube (CCM) [11], que proporciona un conjunto adicional de controles para los proveedores de servicios Cloud. Los controles definidos en CCM están agrupados en 16 dominios: seguridad de aplicaciones e interfaces, cumplimiento y aseguramiento de las auditorías, gestión de la continuidad del negocio y resiliencia operacional, control de cambios y gestión de la configuración, seguridad de los datos y gestión del ciclo de vida de la información, seguridad del centro de datos, gestión de claves y cifrado, gobierno y gestión del riesgo, recursos humanos, gestión de identidades y accesos, seguridad de la infraestructura y virtualización, interoperabilidad y portabilidad, seguridad móvil anti-malware, gestión de incidentes de seguridad, gestión de la cadena de suministro, transparencia y responsabilidad y gestión de vulnerabilidades y amenazas. Para el desarrollo de CCM, CSA se ha basado en estándares existentes como la ISO 27001/27002 [12, 14], ISACA COBIT [15], PCI [16] y NIST [17].

III. SMILE2CLOUD: PROCESO DE MIGRACIÓN DE CARACTERÍSTICAS DE SEGURIDAD DE UNA APLICACIÓN HEREDADA

El proceso SMiLe2Cloud [9] consta de cinco actividades (extracción, análisis, diseño, despliegue y evaluación) dirigidas por los 16 dominios de seguridad definidos por CSA en CCM v3 [11] (ver Fig. 1). La actividad de extracción está enfocada al uso de la ingeniería inversa para extraer aspectos de seguridad desde el LIS (Legacy Information System) a un modelo de seguridad (SMiLe model) definido para nuestro proceso de migración. La segunda actividad es el análisis de los requisitos de seguridad (SecR), que está basada en la extensión de la metodología Secure Tropos [18] para el Cloud. La actividad de diseño está enfocada en la selección del modelo de servicio, el modelo de implementación y realizar la selección del proveedor Cloud basándose en el estándar STAR [13]. La actividad de despliegue está enfocada al despliegue de la especificación basada en un repositorio de patrones de migración al Cloud y en realizar la implementación del sistema. La quinta actividad es la evaluación donde se verifica y valida el modelo de seguridad migrado y se capturan 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.

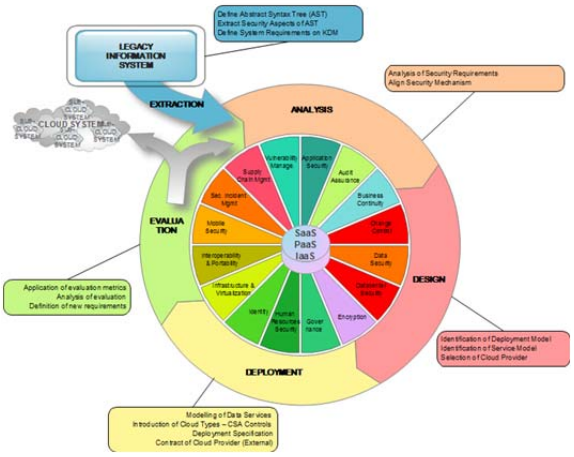

Figura 1. Proceso SMiLe2Cloud

A continuación, se describe en detalle la actividad de diseño, que es el principal objetivo del artículo, pero antes, se describe de forma breve, las dos actividades previas al diseño para poner en contexto al lector.

A. *Actividad de extracción y actividad de análisis*

La extracción es la actividad en la que los requisitos del sistema heredado son obtenidos a partir del propio código del sistema heredado y de la documentación del mismo. Se trata de un proceso de ingeniería inversa. Este proceso es realizado con la ayuda de herramientas 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. Esta actividad produce como salida los requisitos del sistema, especificados según el modelo SMiLe (objetivos, actores, planes, recursos y restricciones).

La actividad de análisis es la que se definen los requisitos de seguridad a implementar alineados con los diferentes dominios de seguridad propuestos por CSA en el CCM v3. En un primer paso se definen los requisitos de seguridad partiendo de los requisitos del sistema definidos en la actividad anterior. En un segundo paso se alinean estos requisitos de seguridad con los controles definidos en CCM v3. La salida de esta actividad es la especificación de los requisitos de seguridad del sistema alineados con los dominios del CSA, que servirá como entrada para la siguiente actividad, la actividad de diseño.

B. *Actividad de diseño*

La actividad de diseño está enfocada en la selección del modelo de servicio, del modelo de implementación y en la toma de decisión en la selección del proveedor Cloud basándose en la certificación STAR. Como entrada se cuenta con la especificación de los requisitos de seguridad obtenidos en la actividad anterior. Esta especificación de requisitos está alineada con CCM v3, de forma que se dispone de la lista de

controles que debe cumplir nuestro proveedor Cloud para alcanzar el nivel de seguridad requerido.

La actividad de diseño consta de dos tareas, "Identificación del modelo de implementación y modelo de servicio" y "Selección del proveedor Cloud". Para cada una de estas tareas, se muestra los roles o implicados en esta tarea, como pueden ser los ingenieros en seguridad o especialista Cloud, así como los artefactos de entrada y de salida para cada tarea. Se definirán los pasos de los que consta cada tarea así como las posibles guías, plantillas, técnicas o herramientas que se han usado en la aplicación de dicha tarea.

Así, para la primera tarea de "Identificación del modelo de implementación y modelo de servicio", se tiene como implicados o intervinientes a los ingenieros de seguridad, a los ingenieros de requisitos, a los especialistas Cloud y al arquitecto de sistemas. La única entrada para esta tarea es el artefacto de salida de la actividad anterior (actividad de análisis), y es la especificación de los requisitos de seguridad alineados con los dominios CSA, que se ha generado en la actividad de análisis. Las salidas que genera esta tarea son el modelo de implementación seleccionado y el modelo de servicio, que serán entradas para la siguiente tarea. Los pasos de que consta esta tarea son dos: identificar el modelo de implementación, e identificar el modelo de servicio partiendo de la especificación de requisitos de seguridad del sistema. Se tiene el CCM como plantilla para ayudar a la selección de proveedores y controles, y una herramienta que será desarrollado como soporte a esta actividad y al proceso completo.

La segunda tarea de esta actividad es "Selección del proveedor cloud". En esta tarea los implicados o roles que deben involucrarse son el ingeniero de seguridad, el diseñador y arquitecto de sistemas y el especialista cloud. Como artefactos de entrada se tiene a los dos generados en la tarea previa, el modelo de implementación y el modelo de servicio. Los artefactos de salida serán dos: el proveedor cloud seleccionado más apropiado que cumple con los requisitos de seguridad del sistema, y la lista de posibles controles de seguridad que los proveedores deberán proporcionar. Las guías o plantillas a usar son el registro STAR y la herramienta Smile2Cloud como soporte a la actividad.

La Fig. 2 muestra la representación gráfica de las principales tareas junto con los artefactos de entrada y salida usando la notación gráfica de SPEM 2.0.

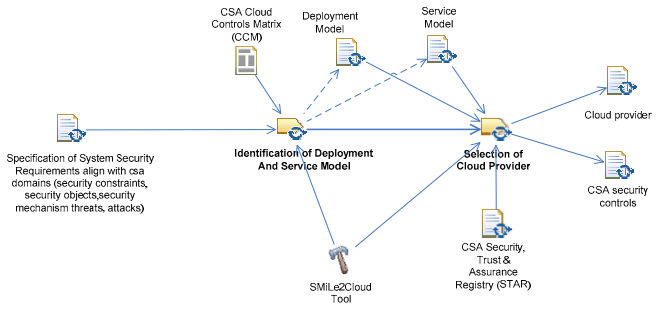

Figura 2. Actividad de diseño.

A continuación, se describe en detalle cada una de esas tareas de que consta la actividad de diseño, explicando cuál es el principal objetivo de cada tarea y los artefactos generados por cada una de ellas.

1) Identificación del modelo de implementación y modelo de servicio

Esta 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. Para ello, siguiendo la distinción que hace el NIST (National Institute of Standards and Technology) [19], se tienen tres modelos de servicio en Cloud (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) y Cloud Infrastructure as a Service (IaaS)) y cuatro modelos de implementación para Cloud (Cloud Pública, Cloud Privada, Cloud Comunitaria y Cloud Híbrida).

El resultado de esta tarea es la identificación del modelo de implementación y de servicio Cloud seleccionando el más apropiado y que encaja mejor con las características de nuestro sistema heredado, de los recursos disponibles y del nivel de seguridad que se quiera conseguir en el nuevo sistema cloud migrado. Para ello se alinea con CCM para obtener la información necesaria de qué modelo de implementación y qué modelo de servicio cubre mejor nuestras necesidades de seguridad.

2) Selección del proveedor Cloud

Una vez que se selecciona el modelo de implementación y el modelo de servicio, y se dispone de los requisitos de seguridad del sistema (SecR) alineados con los dominios CSA, se puede seleccionar el proveedor Cloud que mejor encaja con las necesidades de seguridad de acuerdo al estándar STAR. El estándar STAR proporciona, para cada proveedor Cloud, la lista de controles que implementa de entre los definidos en la matriz CCM v3.

De esta forma, al disponer de la lista de controles necesarios para cubrir los requisitos de seguridad definidos en la actividad de análisis, y disponer también la lista de proveedores Cloud que cumplen con dichos controles, se puede identificar la lista de proveedores Cloud que cumplen con los requisitos de seguridad.

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 análisis DAFO es una herramienta de gestión que facilita el proceso de planeación estratégica, proporcionando la información necesaria para la implementación de acciones y medidas correctivas, y para el desarrollo de proyectos de mejora. El nombre DAFO, responde a los cuatro elementos que se evalúan en el desarrollo del análisis: las debilidades, amenazas, fortalezas y oportunidades.

Para desarrollar la matriz DAFO será necesario seleccionar las fortalezas, oportunidades, amenazas y debilidades que mayor impacto puedan ocasionar sobre la organización. En la

caracterización de dichos elementos se consideran los factores económicos, técnicos, etc. Para su desarrollo, se recomienda la creación de un taller de expertos y desarrollar la técnica denominada tormenta de ideas (brainstorming).

La salida de esta tarea será el proveedor cloud más apropiado y que mejor encaje con los requisitos y controles de seguridad que será necesario implementar en el sistema destino, junto con la lista de controles de seguridad necesarios que cubren los requisitos de seguridad analizados y especificado en la actividad anterior, la actividad de análisis. La herramienta SMiLe2Cloud guía en el proceso de diseño.

IV. CASO DE EJEMPLO – REM

Para demostrar la aplicabilidad de la solución propuesta, para la actividad de diseño del proceso SMiLe2Cloud, se emplea un caso de estudio basado en la migración del sistema REM de la Comisión Nacional de los Mercados y la Competencia (CNMC).

Desde octubre de 2013, la CNMC es la nueva autoridad española para la regulación del cumplimiento de la ley de competencia así como la regulación de algunos otros sectores como las comunicaciones electrónicas, audio visual, energía, postal, aeroportuario y ferroviario. La autoridad ha sido creada para asegurar la competitividad y el buen funcionamiento de dichos mercados. Para alcanzar dichos objetivos la CNMC tiene una larga serie de herramientas. Una de estas herramientas es Registro de Entrada Masivo (en adelante REM).

REM es la aplicación utilizada por la CNMC para gestionar el intercambio de grandes cantidades de datos entre la comisión y las empresas con las que se relaciona. Debido a la naturaleza sensible de los datos que se manejan, el sistema debe cumplir una serie de requisitos de seguridad. Por ejemplo los usuarios de la aplicación deben tener un certificado criptográfico para llevar a cabo la autenticación, mientras que los datos transmitidos deben ser firmados y transmitidos a través de un canal seguro para garantizar su autenticidad, integridad y confidencialidad.

V. APLICACIÓN DE LA ACTIVIDAD DE DISEÑO DE SMILE2CLOUD AL CASO DE ESTUDIO

Como se ha comentado anteriormente la actividad de diseño propuesta en SMiLe2Cloud consta de dos tareas: "Identificación del modelo de implementación y del modelo de servicio" y "Selección del proveedor Cloud"

A. Identificación del modelo de implementación y modelo de servicio

1) Identificación del modelo de implementación

El NIST distingue entre los siguientes modelos de implementación: Cloud pública, Cloud privada, Cloud comunitaria y Cloud híbrida, como ya se ha mencionado en la sección III.B.

La aplicación REM es una aplicación de la CNMC. La CNMC como organismo autónomo no dispone de un Cloud privado en la actualidad. La CNMC es dependiente del Ministerio de Economía y Competitividad. Éste a su vez es dependiente de la Administración General del Estado (en adelante AGE). Entre los próximos retos de la AGE, en concreto en el informe CORA [20] propone la creación de una Cloud privada que preste servicio a las distintas administraciones públicas nacionales. De momento éste es sólo un proyecto, por lo que se descarta el uso de un Cloud privado, un Cloud comunitario o un Cloud híbrido.

Por ello el único modelo de implementación aplicable a nuestro caso de estudio es el Cloud público.

2) Identificación del modelo de servicio

Como se ha comentado anteriormente, el NIST distingue entre los siguientes modelos de servicio: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) y Cloud Infrastructure as a Service (IaaS).

En el modelo Cloud Software as a Service (SaaS) el usuario no gestiona ni controla las aplicaciones individuales disponibles como servicio. El software de REM es un software muy específico de la CNMC por lo que el modelo SaaS no aplica a nuestro caso de estudio.

En el modelo Cloud Platform as a Service (PaaS) el usuario no gestiona ni controla la infraestructura subyacente que incluye la red, los servidores, los sistemas operativos o el almacenamiento. La CNMC cuenta con personal altamente cualificado para la gestión de la infraestructura subyacente. Por ello se considera más adecuado a nuestro caso de estudio el modelo Cloud Infrastructure as a Service (IaaS).

El modelo Cloud Infrastructure as a Service (IaaS) proporciona la provisión de procesamiento, almacenamiento, interconexión de red y otros recursos de computación fundamentales donde el usuario es capaz de instalar y ejecutar software arbitrario que puede incluir sistemas operativos y aplicaciones. El usuario no gestiona ni controla la infraestructura Cloud subyacente, pero tiene el control de los sistemas operativos, el almacenamiento, las aplicaciones desplegadas y, posiblemente, control limitado sobre determinados componentes de red.

B. Selección del proveedor Cloud

1) Artefactos de entrada

La entrada a la actividad de diseño del proceso SMiLe2Cloud se basa en la especificación de requisitos de seguridad (SecR) alineada con los dominios CSA. Por tanto como punto de entrada se tiene la lista de los controles definidos en la Cloud Control Matrix v3 que son aplicables al caso de estudio. En la TABLA I se realiza un resumen del número de controles que son aplicables agrupados por dominio. En la primera columna se listan los 16 dominios definidos en CCM v3. En la segunda columna se indica el número de controles de estos dominios que son aplicables al caso de estudio, la aplicación REM. La tercera columna muestra el número total de controles definidos en CCM v3 para cada dominio.

TABLA I
CONJUNTO DE CONTROLES APLICABLES AL CASO DE ESTUDIO

Dominio	Controles REM	Controles CCMv3
Seguridad de Aplicaciones e Interfaces	4	4
Cumplimiento y aseguramiento de las Auditorías	2	3
Gestión de la Continuidad del Negocio y Resiliencia Operacional	8	12
Control de Cambios y Gestión de la	3	5

Configuración		
Seguridad de los Datos y Gestión del Ciclo de Vida de la Información	6	8
Seguridad del Centro de Datos	6	9
Gestión de Claves y Cifrado	2	4
Gobierno y Gestión del Riesgo	7	12
Recursos Humanos	7	12
Gestión de Identidades y Accesos	8	13
Seguridad de la Infraestructura y Virtualización	7	12
Interoperabilidad y Portabilidad	0	5
Seguridad móvil Anti-Malware	0	20
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, Investigaciones forenses en la nube	3	5
Gestión de la cadena de suministro, Transparencia y Responsabilidad	3	9
Gestión de vulnerabilidades y amenazas	1	3

A modo de ejemplo la TABLA II detalla los controles del dominio "Seguridad de los Datos y Gestión del Ciclo de Vida de la Información". En la primera columna se muestra la lista de controles y en la segunda columna se muestra si es aplicable en REM.

TABLA II
CONTROLES DEL DOMINIO "SEGURIDAD DE LOS DATOS Y GESTIÓN DEL CLICLO DE VIDA DE LA INFORMACIÓN

Seguridad de los Datos y Gestión del Ciclo de Vida de la Información.	**Aplicable a REM**
Clasificación	SI
Inventario de Datos / Flujos	NO
Transacciones de Comercio Electrónico	NO
Política de seguridad de manejo y etiquetado	SI
Fugas de Información	SI
Datos en entornos no de producción	SI
Propiedad/Servicio de los Datos	SI
Desechado Seguro	SI

Según la matriz CCM el control "Inventario de Datos / Flujos" no es aplicable al caso de ejemplo puesto que se ha seleccionado previamente el modelo de servicio IaaS y este control no es aplicable a IaaS.

Por otro lado el control "Transacciones de Comercio Electrónico" no es aplicable a nuestro caso de estudio porque REM no realiza transacciones de comercio electrónico.

Los demás controles del dominio "Seguridad de los Datos y Gestión del Ciclo de Vida de la Información" sí son aplicables a nuestro caso de estudio.

2) Selección del proveedor Cloud

Una vez que se ha seleccionado el modelo de implementación y el modelo de servicio, y se tienen los requisitos de seguridad del sistema (SecR) alineados con los dominios CSA, se puede seleccionar el proveedor Cloud que mejor encaja con las necesidades de seguridad de acuerdo al estándar STAR.

La certificación STAR indica el grado de cumplimiento de los proveedores Cloud respecto a los controles definidos en la matriz CCM. De esta forma se puede identificar los proveedores Cloud que garantizan el cumplimiento de las necesidades del sistema.

Está siendo desarrollada la herramienta SMiLe2Cloud para facilitar este proceso. Esta herramienta contiene una base de datos con los distintos proveedores Cloud y el grado de cumplimiento para cada uno de ellos. De esta forma se puede obtener automáticamente la lista de proveedores que encajan con las necesidades.

En este punto es importante destacar que sería aconsejable que el estándar STAR ofreciese en un formato abierto (Open Data) toda la información de la que dispone, de forma que cualquier modificación sea fácilmente integrable en aplicaciones de terceros como puede ser la herramienta SMiLe2Cloud.

Este caso de estudio se basa sólo en dos de los principales proveedores cloud. Según el informe "Top 100 Cloud Services Providers: 2014 Edition" [21] elaborado por el portal talkincloud.com destaca a AWS de Amazon como a Azure de Microsoft como los líderes destacados del tipo IaaS. Entre ambos tienen más del 55 % de la cuota de mercado, contando Amazon AWS con un 33% y Microsoft Azure con un 23%.

La TABLA III muestra el grado de cumplimiento de dichos proveedores con el dominio puesto como ejemplo anteriormente "Seguridad de los Datos y Gestión del Ciclo de Vida de la Información":

TABLA III
GRADO DE CUMPLIMIENTO DE LOS PROVEEDORES

Seguridad de los Datos y Gestión del Ciclo de Vida de la Información.	**AWS**	**Azure**
Clasificación	SI	SI
Inventario de Datos / Flujos	No aplicable	No aplicable
Transacciones de Comercio Electrónico	No aplicable	No aplicable
Política de seguridad de manejo y etiquetado	SI	SI
Fugas de Información	SI	SI
Datos en entornos no de producción	SI	SI
Propiedad/Servicio de los Datos	SI	SI
Desechado Seguro	SI	SI

Este mismo estudio se ha realizado para todos y cada uno de los controles definidos en la actividad de análisis.

Se obtiene como conclusión que ambos proveedores Cloud son adecuados para la gestión de la seguridad. Para escoger entre uno u otro proveedor Cloud se ha llevado a cabo por un lado un estudio de costes de ambos proveedores Cloud y por otro lado un análisis DAFO.

Para el estudio de costes se ha tenido en cuenta la infraestructura física de la aplicación REM que se detalla en la TABLA IV:

TABLA IV
INFRAESTRUCTURA FÍSICA DE REM.

Infraestructura	**Cantidad**
Servidores web	1
Servidores aplicaciones	1
Servidores bases de datos	1
Almacenamiento en cabina	1 TB
Backup	1 TB
VPN	1

Para simplificar todos los servidores se han escogido con la siguiente configuración: Linux como sistema operativo, 8 núcleos, 15 GB de memoria RAM y SSD.

La TABLA V muestra la comparativa de costes entre Microsoft Azure y Amazon AWS.

TABLA V
COMPARATIVA DE COSTOS.

Infraestructura	**Azure**	**AWS**
Servidores	585 €	681 €
Almacenamiento	91,87 €	107,6 €
Backup	201,07 €	40,9 €
VPN	152,74 €	96,9 €
Total	1.030,68 €	926,04 €

Complementario al estudio de costes se realiza un análisis DAFO de ambos proveedores Cloud en relación a nuestro caso de estudio.

La Fig. 3 muestra el análisis DAFO de Microsoft Azure y Amazon AWS en relación a REM.

Fortalezas	**Debilidades**
Azure Integración con tecnologías Microsoft Segundo líder de la industria (23%) ***AWS*** Líder de la industria (33%) Integración con la mayor parte de las tecnologías	***Azure*** Débil integración con tecnologías no Microsoft Mayor coste global ***AWS*** Se requieren conocimientos técnicos avanzados para el despliegue
Oportunidades	**Amenazas**
Azure Mayor crecimiento en el último año ***AWS*** En continuo crecimiento	***Azure*** Cierta opacidad en su integración con desarrollos Open Source ***AWS*** Demasiado volumen de negocio puede empeorar el servicio a una pequeña compañía

Figura 3. Análisis DAFO tecnología Microsoft Azure y Amazon AWS

Si se tiene en cuenta el análisis DAFO es importante destacar que tanto Microsoft Azure como Amazon AWS están ampliamente implantados en el mercado (más del 55% de la cuota de mercado como se indicaba anteriormente). Amazon AWS (33%) supera a Microsoft (23%) pero este último ha tenido un crecimiento superior según el informe "Top 100 Cloud Services Providers: 2014 Edition" [21] elaborado por el portal talkincloud.com.

Aunque ambos proveedores Cloud tienen una amplia implantación en el mercado, la débil integración de Microsoft Azure con tecnologías no Microsoft unido a su mayor coste determina que el proveedor Cloud elegido sea Amazon AWS.

VI. CONCLUSIONES

En este trabajo se ha explicado la actividad de diseño en el proceso de migración de características de Seguridad de los sistemas heredados al Cloud. Esta actividad es parte del proceso SMiLe2Cloud que propone la migración de las características de seguridad basándose en estándares y metodologías ampliamente aceptadas por el mercado.

La actividad de diseño se ha aplicado al caso de estudio de migración de la aplicación REM al Cloud. En concreto se ha aplicado con la migración a dos de los principales proveedores Cloud del mercado, Amazon AWS y Microsoft Azure.

Como trabajo futuro es destacable continuar con el proceso de migración de la aplicación REM al Cloud. Quedan pendientes la definición de la actividad de Despliegue y la actividad de Evaluación. En la actividad de Despliegue se han de definir un conjunto de patrones que ayuden con la migración. En la actividad de Evaluación se han de definir una serie de métricas para verificar que todo el proceso se ha llevado con éxito.

AGRADECIMIENTOS

Este trabajo 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" (España) y FEDER, y SEQUOIA (TIN2015-63502-C3-1-R) financiado por el "Ministerio de Economía y Competitividad" (España) y FEDER.

REFERENCIAS

[1] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011.
[2] European Commission, Unleashing the Potential of Cloud Computing in Europe. 2012, Communication from the commission to the European Parliament, the council, the European economic and social Committee and the Committee of the regions.
[3] Kushwah, V.S. and A. Saxena, A Security approach for Data Migration in Cloud Computing. International Journal of Scientific and Research Publications, 2013. 3(5).
[4] Wu, B., et al. Legacy system migration: A legacy data migration engine. in Proceedings of the 17th International Database Conference (DATASEM'97). 1997.
[5] Bisbal, J., et al., Legacy Information Systems: Issues and Directions. IEEE Softw., 1999. 16(5): p. 103-111.
[6] Bisbal, J., et al., A survey of research into legacy system migration. Technique report, 1997.
[7] PwC, The Future of IT Outsourcing and Cloud Computing. 2011.
[8] Ahronovitz, M., et al., Cloud computing use cases white paper. 2010.
[9] 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.
[10] Márquez, L., et al. A Framework for Secure Migration Processes of Legacy Systems to the Cloud. in Advanced Information Systems Engineering Workshops. 2015. Springer.
[11] Cloud Security Alliance. CLOUD CONTROLS MATRIX V3.0.1. 2014; Available from: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/.
[12] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. 2013.
[13] Cloud Security Alliance. CSA Security, Trust & Assurance Registry (STAR). 2014; Available from: https://cloudsecurityalliance.org/star/.
[14] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls. 2013.
[15] ISACA, COBIT5-A Business Framework for the Governance and Management of Enterprise IT. 2012.
[16] PCI, Data Security Standard, v3.1, in Requirements and Security Assessment Procedures. 2015.
[17] NIST. National Institute of Standards and Technology. 2015; Available from: http://gsi.nist.gov/global/index.cfm/L1-1.
[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] NIST, The NIST Definition of Cloud Computing, P. Mell and T. Grance, Editors. 2009, National Institute of Standards and Technology.

[20] CORA, Informe de progreso de la comisión para la reforma de las administraciones públicas. 2015.
[21] TalkinCloud, 2014 Talkin' Cloud 100: Top Cloud Service Providers, Aggregators and Brokers. 2014.

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.

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 Grid and Cloud Computing. 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 (Information Software Technology, Journal of Systems Architecture, Journal of Network and Computer Applications, etc.). He has been acting as a member of many conference program committees and as co-chairs of some workshops such as WOSIS (editions 2011, 2012, 2013, 2014, 2015) and WISSE (editions 2011, 2012, 2013, 2014, 2015). 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

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 Union-funding 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. In the past he has been Editor in Chief of the International Journal of Computer Science and Security and guest Editor in Chief of a special issue on Security Requirements Engineering at the Requirement Engineering Journal. He has been involved in the organization of various events related to his research interests, amongst others, as General Chair (International Workshop on Safety and Security in MAS, International Workshop on Information Systems Security Engineering), PC-Chair (1st International Workshop on Secure Requirements Engineering, International conference on Global e-security, CAiSE'11).

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.).