Propuesta metodológica de evaluación de seguridad para aplicaciones de Mobile Cloud Computing

***Diego Jara*[1], *Priscila Cedillo*[2]**

[1] Maestría en Gestión Estratégica de Sistemas de Información, Universidad de Cuenca, Av. 12 de abril y Av. Loja, Cuenca, Ecuador, 01.01.168.

[2] Departamento de Ciencias de la Computación, Universidad de Cuenca, Av. 12 de abril y Av. Loja, Cuenca, Ecuador, 01.01.168.

Autores para correspondencia: diego.jara@ucuenca.ec, priscila.cedillo@ucuenca.edu.ec

Fecha de recepción: 30 de julio de 2017 - Fecha de aceptación: 15 de agosto de 2017

RESUMEN

A raíz de los nuevos avances tecnológicos en los dispositivos móviles, éstos están siendo cada vez más utilizados para realizar tareas complejas, sin embargo existen temas que limitan su utilización en procesos que demandan muchos recursos, debido a sus limitaciones en procesamiento, tiempo de vida de la batería entre otros, de ahí que se ha considerado una opción apropiada el uso de la computación en la nube para realizar las tareas de alta complejidad y transferir los resultados al dispositivo móvil. Entonces, Mobile Cloud Computing se ha convertido en una buena y adecuada solución. Dada su adopción en muchas aplicaciones, se ha considerado un aspecto crítico el tema de la seguridad, siendo éste muchas veces el principal limitante para su masiva aceptación. Este trabajo propone una metodología para la evaluación de aplicaciones móviles basadas en plataformas cloud computing. Además, se ha propuesto un modelo de calidad basado en las características de la norma ISO/IEC 25010 para finalmente crear una metodología formal con la ayuda de la notación SPEM 2 (Software & System Process Engineering Meta-model Specification V2.0); constituyéndose este artículo en un aporte importante a la hora de realizar los estudios de seguridad en este ámbito.

Palabras clave: Cloud Computing, Mobile Cloud Computing, MCC, calidad, seguridad.

ABSTRACT

Mobile devices are increasingly used to perform complex tasks due to technological advances in mobile devices. However, there are issues that limit their use in processes that demand a lot of resources due to their processing limitations, the charge cycle of the battery among others. Hence a suitable option is the use of cloud computing to perform tasks of high complexity and transfer the results to the mobile device. Mobile Cloud Computing has become a good and appropriate solution. Given its adoption in many applications, the issue of security has been considered a critical issue, which is often the main limitation for its massive acceptance. This paper proposes a methodology for evaluating mobile applications based on cloud computing platforms. To do so, we propose a quality model based on the characteristics of ISO/IEC 25010, and designed finally a formal methodology with the help of the SPEM 2 (Software & System Process Engineering Meta-Model Specification V2.0) notation. This article can be of support when carrying out security studies in this area.

Keywords: Cloud Computing, Mobile Cloud Computing, MCC, quality, security.

1. INTRODUCCIÓN

Una nube es un conjunto virtual de recursos de computación que comprende ordenadores, servidores y sistemas que proporcionan recursos a los clientes (Khan, Naseem, Ahmad, & Khan, 2012). Por otra

parte, Buyya, Yeo, & Venugopal (2008) definen la computación en nube como un sistema computacional que se sirve de virtualización interna y un SLA, seguido de la asignación prevista de recursos. Además, otros trabajos destacan que el almacenamiento de datos en los servidores de la nube es uno de sus beneficios primordiales en la adopción de la misma (Hewitt, 2008), puesto que utiliza los recursos del dispositivo del usuario para obtener los datos desde el servidor.

La computación en nube es una tecnología que en la actualidad presenta mucha acogida dadas sus características intrínsecas de alta disponibilidad, agilidad, escalabilidad, elasticidad entre otras. Además, la computación en la nube proporciona las oportunidades de reducción de costes a través de una informática optimizada y eficiente (Khalid, 2010; Briscoe & Marinos, 2009; Zhang, Zhang, Chen, & Huo, 2010) que facilita el acceso efectivo y económico a los recursos con servicios constantemente disponibles en Internet (Khan, Mat Kiah, Khan, & Madani, 2013).

Dadas las ventajas de estas dos tecnologías, que al combinarlas dan lugar a Mobile Cloud Computing (MCC), se crea un nuevo concepto en donde la nube lleva a cabo el trabajo pesado de las tareas intensivas de computación y el almacenamiento de grandes cantidades de datos, mientras estos son recibidos y mostrados en un dispositivo móvil (Sarma Vittapu, Sunkari, Yoseph Abate, & Sreenivas, 2015). De ahí que esta nueva tecnología se concentra en la potencialidad de la computación en la nube (Ibukun & Daramola, 2015).

El presente artículo se distribuye de la siguiente manera: en el capítulo 1 presentamos una introducción a MCC, y los conceptos necesarios para entenderla. El capítulo 2 muestra los trabajos relacionados a la seguridad en MCC y la manera en que éstos están siendo abordados. El capítulo 3 presenta un modelo de calidad sobre la seguridad en entornos MCC, el mismo que está basado en la norma ISO/IEC 25010. El capítulo 5 por su parte plantea una propuesta metodológica para la evaluación de la seguridad en MCC. El capítulo 6 muestra el caso de estudio en el cual se pone a prueba el método propuesto. Finalmente, en el capítulo 6 se recogen las conclusiones respecto a este estudio.

2. TRABAJOS RELACIONADOS

Según Qureshi *et al.* (2011), hoy en día los teléfonos inteligentes se han construido teniendo en cuenta las características especiales de seguridad para protegerlos de un uso incorrecto o mal intencionado. La política de aplicaciones para dispositivos de Google (Google Apps Help, 2016) ofrece la facilidad a sus usuarios de bloquear de forma remota o borrar la información de un dispositivo móvil perdido o robado. Algunas medidas de respuesta, por ejemplo, la protección de acceso a la nube y protección integrada de la identidad dispositivo se pueden adoptar para mejorar la seguridad de los teléfonos inteligentes y las nubes.

Los SLA pueden cubrir términos relativos a la calidad de servicio, seguridad, tolerancia a fallos de funcionamiento, entre otros. Además, un proveedor de la nube también puede detallar en los SLA, limitaciones y obligaciones que los consumidores deben aceptar, aunque en caso de convenios mayores estos pueden ser acordados y re-negociados por las partes que intervienen (Badger, Grance, Patt Corner, & Voas, 2011).

En Myerson (2013) podemos encontrar un ejemplo de las mejores prácticas en cuanto al establecimiento de SLA apropiados, teniendo en cuenta las mencionadas perspectivas. Para el presente estudio se realiza una evaluación desde la perspectiva del usuario final (consumidor) que, según se extrae de Islam (2014), es uno de los puntos más débiles de la cadena de seguridad.

En Ye (2015) se muestra que los dispositivos móviles están reemplazando el escritorio tradicional como un portal principal a Internet, en consecuencia, la gente confía en éstos para manejar todo tipo de actividades diarias, como compras en línea y suscripción a servicios, así como el acceso a plataformas financieras y nubes de almacenamiento y gestión de información personal.

3. MODELO DE SEGURIDAD PARA MOBILE CLOUD COMPUTING.

En esta sección se ofrece una descripción de las sub-características, atributos y métricas planteadas para la evaluación de la seguridad en aplicaciones de Mobile Cloud Computing. Este modelo está alineado con el estándar ISO/IEC 25000 SQuaRE (ISO, 2005), el mismo que se descompone en sub-características y atributos. Por lo tanto, se adaptó la definición de estas sub-características y atributos con el fin de cubrir los aspectos específicos dirigidos a MCC. Además, existen varias perspectivas desde las cuales se puede abordar la calidad en MCC, den el presente artículo se abordará la calidad desde la perspectiva del usuario final de la aplicación móvil. En la Figura 1 se muestra el escenario típico de un ambiente MCC y desde el cual se puede identificar la aplicación móvil como parte de ella.

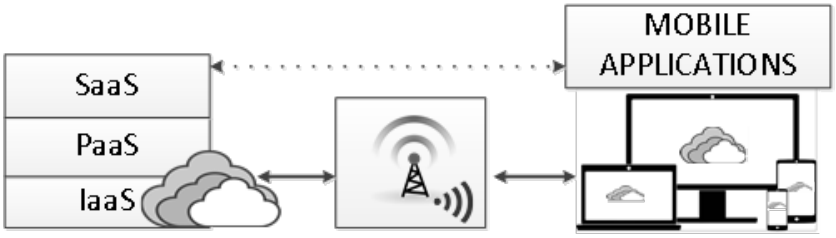

Figura 1. Escenario típico de Mobile Cloud Computing.

A continuación, se listan las diferentes sub-características que se adaptaron del modelo SQuaRE para la evaluación de un ambiente MCC y los atributos propuestos para este modelo de seguridad. Es importante explicar que, para la elaboración de este modelo, las métricas planteadas se basaron en una serie de recomendaciones y buenas prácticas obtenidas de certificaciones, planes de aseguramiento, sistemas de gestión de seguridad, normas y estándares internacionales como NIST, ENISA, CSA entre otros (Archer *et al.*, 2012; ENISA, 2009; Mell & Grance, 2011). Todas orientadas a prevenir los principales problemas de seguridad en MCC como lo plantea (Cloud Security Alliance, 2016) en su apartado de vulnerabilidades.

En la Tabla 1 se muestra un extracto de los diversos atributos y controles que se proponen para el presente modelo. Para verificar el modelo completo se puede acceder a la dirección web: https://goo.gl/hnkLrL.

Tabla 1. Extracto de un modelo de seguridad para MCC.

1. Confidentiality	1.1. Mobile Data Management	Se valora el servicio de manejo de los dispositivos móviles implementado por el sistema MCC	El servicio es ejecutable en todos los sistemas operativos móviles
			El sistema cuenta con opción de bloqueo remoto
	1.2. Control de accesos y gestión de identidades	Valoración de las características de control de accesos y la actividad de cada cuenta.	Cuenta con inventario de dispositivos móviles autorizados
			Alerta todos los ingresos de dispositivos móviles nuevos
	1.3. Seguridad en SLA	Se valoran las características elementales con las que debe contar un acuerdo SLA para MCC	¿Permite auditorías externas y certificaciones de seguridad?
			¿La normativa legal está acorde a la legislación del país del suscriptor del servicio?
	1.4. Calidad de encriptación	Se mide opciones ideales en cuanto a encriptación en ambientes MCC	Utiliza técnicas de cifrado fuertes (como AES-256, AES-192 o RSA)
			Utiliza formatos abiertos y validados, evitando en la medida de lo posible, el uso de técnicas de cifrado propietario.

	1.5. Test de seguridad	Se verifican las pruebas mínimas que deben realizarse a ambientes MCC	Realiza test de penetración externos e internos de seguridad a los móviles
			Mantiene un detalle de los terminales en los que se realizan los test y los utilizan únicamente con esos fines de prueba
	1.6. Manipulación de los datos del cliente	Se realiza una validación de los controles que se someten los datos de los usuarios	Brinda herramientas para etiquetado y clasificación de datos
			¿Entrega certificación de la destrucción por parte del proveedor de cloud computing o por un tercero?
	1.7. Prevención de ataques	Se mide las seguridades con las que debe contar un servicio MCC para prevenir ataques	Cuenta con un DLP (Data Loss Prevention) junto con la gestión que esto implica
			¿Presenta una certificación de seguridad conocida?
2. Integrity	2.1 Seguridad complementario	Se consulta sobre seguridades complementarias básicas respecto a instalaciones físicas del CSP	El servicio cuenta con responsables de la seguridad física, así como afines y otros
			Cuenta con autenticación biométrica
	2.4. Notificación y respuesta de incidentes de seguridad	Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes	Cuenta con un plan de emergencia por incidentes de seguridad
			Cuenta con un backup de servicios cloud.
	2.5. Gestión y control de cuentas de usuario	Se validan las medidas de seguridad en cuanto al monitoreo y revisión de los usuarios y sus cuentas de acuerdo con sus perfiles	Mantiene un registro del número total de cuentas
			Mide porcentaje de cuentas sin actividad
	2.8. Gestión de contenido antispam / correo electrónico	Se validan las acciones a tomar respecto a la incidencia de contenido spam a la app móvil	Monitoriza el número de correos electrónicos procesados
			Valida el número de correos electrónicos rechazados por restricciones de spam / contenido
5. Authenticity	5.1. Políticas de contraseña	Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad	Cuenta con políticas de caducidad de contraseñas
			Cuenta con autenticación en dos pasos
	5. 3. Contexto de uso	Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc.	¿Capacidad de detección mediante biometría del comportamiento?
			Detecta cambios de acceso al sistema, cambios de dirección IP incoherentes o franjas horarias

Los atributos mostrados en la Tabla 1 fueron considerados apropiados para realizar la posterior evaluación a las aplicaciones móviles. Para definir este tema se sometió todas las opciones a un consenso en el cual se consideró el tema de la perspectiva desde la cual se analiza la posibilidad de obtener información por parte del proveedor y la pertinencia de los controles para las pruebas.

4. METODOLOGÍA PARA LA EVALUACIÓN DE LA SEGURIDAD

En esta sección se define el método de evaluación de seguridad que será utilizado por el evaluador que, para el caso, es el usuario final. Con esto se pretende establecer la calidad del producto en temas de seguridad y el aporte de resultados que sean consistentes y replicables. El método adapta y extiende las características propuestas por el estándar ISO/IEC 25040 con el fin de evaluar la calidad en la seguridad de aplicaciones para MCC.

4.1. Definición del proceso con SPEM 2

En esta sección se detalla cómo, en base a lo señalado anteriormente, se llevará a cabo el proceso de evaluación correspondiente a la aplicación de la metodología de evaluación, para ello usaremos la notación SPEM 2 (Software & System Process Engineering Meta-model Specification V2.0) (OMG, 2008), propuesta por el grupo Object Management Group, que provee un marco formal para la definición de procesos de desarrollo de sistemas y de software, así como también para definir y describir sus elementos. El objetivo de su uso en este trabajo es el proveer una definición detallada del proceso de evaluación, adaptándola a la seguridad de aplicaciones para mobile cloud computing y guiar al evaluador para llevar a cabo los procesos de una manera simple y fácil de entender.

SPEM 2 (OMG, 2008) plantea tres elementos básicos: i) Tarea: que es el esfuerzo a realizar, ii) Rol: es quien realiza el esfuerzo, iii) Productos de trabajo: Entradas que se utilizan y salidas que éstos producen. Por medio de estos elementos se puede especificar “Quién (rol) realiza qué (tarea), para desde unas entradas conseguir unas salidas (productos de trabajo)”.

4.2. Método de Evaluación con SPEM 2

Como se señaló anteriormente, la metodología planteada se basa en la adaptación del estándar ISO/IEC 25040, en el cual se especifica un proceso para la evaluación de la seguridad, para ello los pasos de este proceso se muestran a continuación.

a. *Establecer los requisitos de evaluación*. En donde se establecen el propósito de la evaluación, se obtienen los requisitos de seguridad y se define el rigor de la evaluación.
b. *Especificar la evaluación*. Aquí se definen los criterios de decisión para la evaluación y las métricas.
c. *Diseñar la Evaluación.* Aquí se planifica las actividades de la evaluación.
d. *Ejecutar la Evaluación.* En esta etapa se realizan las mediciones y se aplican los criterios de decisión de las métricas y en general para la evaluación.
e. *Concluir la Evaluación.* Donde se revisa los resultados y se disponibiliza los datos de la evaluación.

En la Figura 2 se presenta todo el proceso con las respectivas tareas.

5. CASO DE ESTUDIO APP GMAIL (GOOGLE. INC)

Para el caso de estudio se utilizará el método de evaluación recientemente propuesto siguiendo la estructura mostrada en la Figura 2.

a. Especificación de los requisitos de evaluación

   En esta etapa se define el propósito u objetivo de la evaluación el cual es el análisis de las características de seguridad de la aplicación Gmail. También se define los requisitos que la aplicación debe cumplir, que para el caso práctico fue definido en el modelo de calidad mostrado en la Tabla 1 y que el detalle completo está en la URL: https://goo.gl/RNjGHa. Finalmente se genera un artefacto en el que se detalla los requisitos de evaluación a manera de plantilla para uso del evaluador. En este artefacto se deja constancia de: estado en el que se ejecutará la evaluación de seguridad, stackeholders involucrados y la lista de los atributos a evaluar.

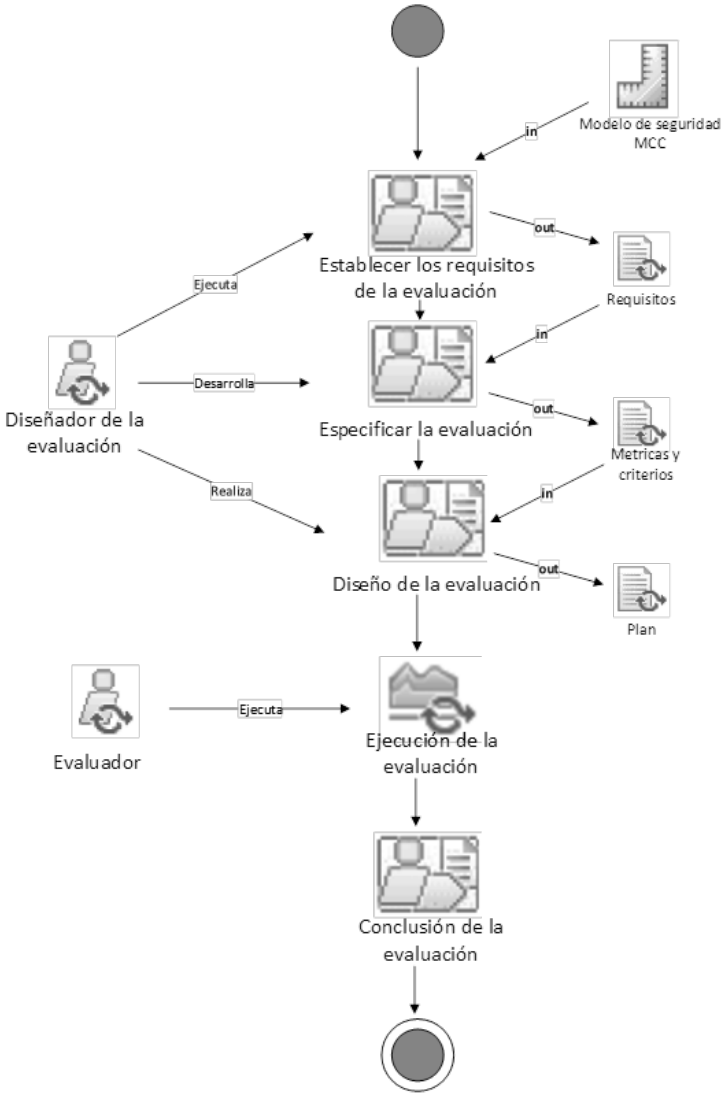

Figura 2. Proceso de evaluación de seguridad para aplicaciones.

b. Especificación de la Evaluación.

En esta fase se definen los atributos y métricas que se usaran, así como los umbrales que definirán la posterior valoración cualitativa que constara en el informe final. Estos atributos y métricas, así como los umbrales los señalamos por completo en la dirección web: https://goo.gl/aAtXAd.

c. Diseño de la Evaluación.

En esta fase se debe señalar que una de las restricciones que se afronta al momento de evaluar una *app* del mercado y de la cual no se es propietario. Se intentó obtener información respecto de aplicaciones realizadas por empresas locales, sin embargo, al ser un nicho de mercado emergente, el sigilo de la información es muy valorado, por temas de espionaje industrial y propiedad intelectual, lo que obliga de alguna manera a sesgar la búsqueda de aplicaciones basándose en la disponibilidad de la información necesaria para este caso de estudio. Para este ejemplo práctico se eligió la aplicación del gestor mail de Google: Gmail. Esta *app* aporta cierta información en su página web, pero la mayor parte de datos relacionados a la gestión de la seguridad se encontró en la plataforma “Google Cloud Platform” en el apartado de seguridad precisamente. El plan de evaluación que se seguirá será el de aplicar el Modelo de Seguridad para aplicaciones MCC, para ir evaluando el caso de estudio propuesto desde una visión global valorando cada proceso, control o política bajo la premisa de cumplimiento o no de la misma para cada atributo.

d. Ejecución de la Evaluación e Informe de Seguridad

Como paso final se ejecuta la evaluación de la aplicación basados en el plan de evaluación y requisitos levantados en las fases anteriores. A continuación, observamos el artefacto planteado en secciones anteriores, una plantilla que lleva la información acerca del estado en el cual se procedió a realizar la evaluación. En la Tabla 2 se muestra a manera de resumen los puntajes obtenidos y en la Figura 3 una gráfica de los umbrales máximos versus los puntajes obtenidos después de la evaluación realizada.

Plantilla Documento de Especificación de Requisitos de Evaluación

a) Stackeholders involucrados

-Usuario	X
-Comprador	
-Otros (Especificar)	

b) Lista de Atributos Por Evaluar

No.	Atributo	Código Atributo
1	1.1. Mobile Data Management	1.1
2	1.2. Control de accesos y gestión de identidades	1.2
3	1.3. Seguridad en SLA	1.3
4	1.4. Calidad de encriptación	1.4
5	1.5. Test de seguridad	1.5
6	1.6. Manipulación de los datos del cliente	1.6
7	1.7. Prevención de ataques	1.7
9	2.1 Seguridad Complementario	2.1
8	2.4. Notificación y respuesta de incidentes de seguridad	2.4
9	2.5. Gestión y control de cuentas de usuario	2.5
10	2.8. Gestión de contenido antispam / correo electrónico	2.8
11	3.1. No Repudio	3.1
12	4.1. Responsabilidad	4.1
13	5. 3. Contexto de uso	5.3

Plantilla 1. Documento de Especificación de Requisitos de Evaluación.

	MEDIDO	META
1.1. Mobile Data Management	25%	100%
1.2. Control de accesos y gestión de identidades	62%	100%
1.3. Seguridad en SLA	67%	100%
1.4. Calidad de encriptación	75%	100%
1.5. Test de seguridad	50%	100%
1.6. Manipulación de los datos del cliente	86%	100%
1.7. Prevención de ataques	64%	100%
2.1 Seguridad Complementario	70%	100%
2.4. Notificación y respuesta de incidentes de seguridad	86%	100%
2.5. Gestión y control de cuentas de usuario	71%	100%
2.8. Gestión de contenido anti-spam / correo electrónico	60%	100%
5.1. Políticas de contraseña	75%	100%
5. 3. Contexto de uso	0%	100%

Tabla 2. Resumen de resultados de la evaluación de seguridad.

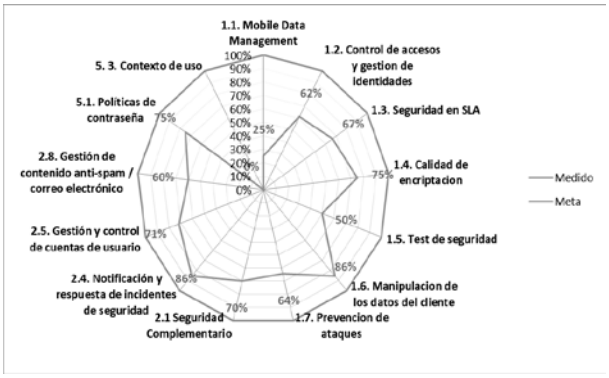

Figura 3. Resultados de la evaluación de seguridad de la *app* Gmail.

e. Discusión de resultados

De los resultados obtenidos y recopilados en la Tabla 2 existen algunos resultados que se consideró importante discutir y que se detallan a continuación.

- En la evaluación a la aplicación de correo Gmail con el modelo y metodología planteadas se obtuvo puntuaciones que, si dividimos en tres niveles como alto, medio y bajo, ordenaremos dentro de cada nivel a los diversos resultados obtenidos. Por ejemplo, se consideran dentro del nivel alto los puntajes con un puntaje mayor o igual al 70%, un nivel medio a los

puntajes comprendidos entre el 70% y el 50%, siendo puntajes menores al 50% considerados como un nivel bajo.

- Puntajes altos obtuvieron los atributos 1.4 - 1.6 - 2.1 - 2.4 - 2.5 y 5.1, principalmente por la información que la plataforma disponibiliza a quienes consultan los temas relacionados a seguridad. Al respecto se extrajo información como la relacionada a la manipulación de los datos del cliente, donde la plataforma establecía claramente los procesos y seguridades adoptadas o las vinculadas a las políticas de contraseñas donde se observó que mantienen reglas claras y estrictas al respecto. Por otra parte, se pudo observar que ninguno de los atributos considerados como el nivel más alto obtuvieron una puntuación de 100%, debido principalmente a la particularidad de la evaluación a la que fue sometida y que se señaló al principio del documento es recién una propuesta metodológica que se deberá continuar sometiendo a mejoras y estudios para profundizar y afinar criterios de medición.
- Entre los puntajes medios tenemos a los atributos 1.2 - 1.3 - 1.5 - 1.7 - 2.8, que obtuvieron puntajes menores y que se debe recalcar que se debió a que los atributos en mención están implementados de forma parcial o que no brindaron información suficiente respecto a uno o varios de los controles que componen cada atributo. Sin embargo, existen atributos como el de Test de Seguridad, en donde podrían aportar más información sobre como someten sus plataformas SaaS a revisión y pruebas de penetración, Hacking, etc. con el fin de incluir esta información en los SLA, que es otro de los atributos en los que podrían mejorar su puntaje.
- Los atributos que están en el nivel bajo son el 1.1 y 5.3 que corresponden a Mobile Data Management con un 25% y Contexto de uso 0%, respectivamente. El primer atributo hace referencia a las capacidades de la plataforma de controlar el dispositivo de forma remota, con el fin de salvaguardar la información ahí almacenada. Si bien la aplicación Gmail sí brinda opciones de borrado remoto y otras formas de controlar el acceso a las cuentas, no tiene más opciones ajustadas al dominio de la movilidad, puesto que un riesgo frecuente es el extravío o robo del dispositivo móvil en donde se mantiene información importante y que el mayor riesgo representa que es un dispositivo que cuenta con permisos de acceso Cloud. Por otra parte, el segundo atributo y que cabe señalar tiene la valoración más baja (0%), hace referencia al uso que la plataforma haga de los sensores y características particulares del dispositivo móvil con el fin de crear un perfil de uso particular del usuario, con esto se conseguiría distinguir patrones de uso diferentes y que puedan brindar alertas que desemboquen en incidentes de seguridad.

6. CONCLUSIONES

Una vez elaborado toda la propuesta metodológica se puede llegar a varias conclusiones que se detallan a continuación.

- Se puede concluir que las nuevas tecnologías de la comunicación e información traen consigo nuevos beneficios, pero también nuevos riesgos que muchas veces hacen dudar de su adopción, por tanto, es importante hacer un estudio profundo de la seguridad en estos ámbitos y tener en consideración los puntos de vista desde los cuales la seguridad puede ser abordada.
- Uno de los principales inconvenientes que se encontró fue el tema de las métricas para medición de la seguridad, las mismas que se encuentran en un estado de análisis, en su mayoría vinculadas a los costos, vulnerabilidades y cumplimientos de medidas de seguridad. Esto nos lleva a plantear que en trabajos futuros se podría profundizar más el estudio de métricas precisas que aporten información relevante respecto a un atributo o medida de mitigación de alguna vulnerabilidad.
- La elaboración del método planteado y su posterior aplicación en una *app* pública y comercial, disponible en el mercado, dejo ver que el tema de la seguridad, en primer lugar, está siendo cada vez mejor abordado y, en segundo lugar, la importancia de remitirse a los documentos de información complementaria que cada aplicación tiene, pues se observó que al momento de

instalar una aplicación móvil, es una práctica común el continuar con todo el proceso de instalación de la misma, sin prestar atención a estos temas.

- Es importante resaltar que existen características propias de MCC que fueron valoradas en el modelo y consecuentemente en el método de validación. Estas características ajustadas propiamente a las cualidades particulares de los dispositivos móviles fueron las que menores puntajes de cumplimiento obtuvieron en la evaluación, lo que da muestras que las aplicaciones a pesar de ejecutarse en dispositivos móviles aún tienen oportunidades de mejora en aspectos de seguridad relacionados a MCC.
- Las características y atributos evaluados fueron tomados de plataformas, instituciones y normas internacionales que han levantado varios temas referentes a seguridad en mobile cloud computing. Entre estos grupos están: Cloud Security Alliance, NIST, ENISA, donde se pudo encontrar información relevante ajustada a los requerimientos particulares necesarios para el presenta trabajo investigativo.

REFERENCIAS

About the Google Apps Device Policy for Android - Google Apps Help. (2016). Disponible en https://support.google.com/a/users/answer/190930?visit_id=1-636106337534220464-640974822&hl=en&rd=1

Archer, J., Boehme, A., Cullinance, D., Puhlmann, N., Kurz, P., Reavis, J. (2012). *Security guidance for critical areas of mobile computing*. Seattle, WA: Cloud Security Alliance, 60 pp. Disponible en https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf

Badger, L., Grance, T., Patt Corner, R., Voas, J. (2011). *Cloud computing synopsis and recommendations*. Special Publication (NIST SP) - 800-146. 81 p. Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Briscoe, G., Marinos, A. (2009). *Community cloud computing*. In: 1st International Conference on Cloud Computing. 11 p. arXiv:0907.2485v3 [cs.NI]. Disponible en http://eprints.lse.ac.uk/26516/1/community_cloud_computing_(LSERO_version).pdf

Buyya, R., Yeo, C. S., Venugopal, S. (2008). *Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities.* Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08, IEEE CS Press, Los Alamitos, CA, USA), 9 p. Disponible en https://arxiv.org/ftp/arxiv/papers/0808/0808.3558.pdf

Cloud Security Alliance. (2016). *The treacherous 12 cloud computing top threats in 2016*. 34 p. Disponible en https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

European Network and Information Security Agency (ENISA). Computación en nube: Beneficios, riesgos y recomendaciones para la seguridad de la información, 2009, 141, European Union.

Hewitt, C. (2008). ORGs for scalable, robust, privacy-friendly client cloud computing. *IEEE Internet Computing*, 12(5), 96-99. https://doi.org/10.1109/MIC.2008.107

Ibukun, E., Daramola, O. (2015). A systematic literature review of mobile cloud computing. *International Journal of Multimedia and Ubiquitous Engineering*, 10(12), 135-152. http://doi.org/10.14257/ijmue.2015.10.12.15

Islam, M. S. (2014). Systematic literature review: Security challenges of mobile banking and payments system. *International Journal of U- and E- Service, Science and Technology*, *7*(6), 107-116. https://doi.org/10.14257/ijunesst.2014.7.6.10

ISO/IEC. ISO/IEC 25010 Systems and Software quality requirements and evaluation (SQuaRE) - System and software quality models. (2011).

Khalid, A. (2010). *Cloud computing: Applying issues in small.* In: IEEE International Conference on

Signal Acquisition and Processing (ICSAP), pp. 278-281. https://doi.org/10.1109 /ICSAP.2010.78

Khan, A. N., Mat Kiah, M. L., Khan, S. U., Madani, S. A. (2013). Towards secure mobile cloud computing: A survey. *Future Generation Computer Systems*, *29*(5), 1278-1299. https://doi.org/10.1016/j.future.2012.08.003

Mell, P., Grance, T. (2011). *The NIST definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. Special Publication (NIST SP) - 800-145, 7 p. Disponible en https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Myerson, J. M. (2013). *Best practices to develop SLAs for cloud computing*. Develop a standard way to create service level agreements that multiple partners can use. Disponible en https://www.ibm.com/developerworks/cloud/library/cl-slastandards/index.html

OMG. (2008). *Software & Systems Process Engineering Meta-Model Specification V2.0*. 234 p. Disponible en https://www.omg.org/spec/SPEM/2.0/Beta2/About-SPEM/

Qureshi, S. S., Ahmad, T., Rafique, K., Shuja-ul-islam. (2011). *Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues*. In: IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), Beijing, China. pp. 467-471. https://doi.org/10.1109/CCIS.2011.6045111

Sarma Vittapu, M., Sunkari, V., Yoseph Abate, A., Sreenivas, N. (2015). A proposed solution to secure MCC uprising issue and challenges in the domain of cyber security.*Open Journal of Mobile Computing and Cloud Computing*, *2*(1).

Ye, Q. (2015). *Analyzing security property of android application implementation using formal method*. In: IEEE 20th Int. Conference on Engineering of Complex Computer Systems (ICECCS), Gold Coast, Australia, pp. 214-217. IEEE. https://doi.org/10.1109/ICECCS.2015.39

Zhang, S., Zhang, S., Chen, X., Huo, X. (2010). *Cloud computing research and development trend*. Second Conference on Cloud Computing Research and Development Trend. pp. 93-97. https://doi.org/10.1109/ICFN.2010.58