UNIVERSIDAD DE CUENCA

Facultad de Ingeniería

Maestría en Gestión Estratégica de Tecnologías de la Información

"PROPUESTA METODOLÓGICA DE EVALUACIÓN DE SEGURIDAD PARAAPLICACIONES DE MOBILE CLOUD COMPUTING"

Trabajo de titulación previo a la obtención del título de Magíster en Gestión Estratégica de Tecnologías de la Información.

Autor:

Diego Xavier Jara Juárez
C.I. 0103544102

Directora:

Irene Priscila Cedillo Orellana.
C.I. 0102815842

Cuenca – Ecuador

2017

Resumen

Según el último informe Mobility Report realizado por el fabricante sueco Ericsson, se destaca que para el último trimestre del 2015 el total de líneas móviles en el mundo era de 7300 millones, una cifra que equivale al número de habitantes de la Tierra; así como también dentro del mismo trimestre, se vendieron 350 millones de *Smartphones*. Esta creciente tendencia del acceso al Internet desde dispositivos móviles, sumado al aumento de las capacidades de los mismos y a un mayor despliegue de redes de tercera y cuarta generación (3G/4G Long Term Evolution LTE) por sobre las redes Wifi, brindan a los usuarios una amplia gama de servicios y soluciones.

Sin embargo, la responsabilidad de seguridad, identificación personal y la misma evolución de la era post-aplicación son tres áreas en las que se muestran factores convergentes, los cuales Gartner ha identificado como el nexo de fuerzas para el 2020.

El incremento señalado de terminales móviles inteligentes, así como el aumento del acceso al internet desde estos dispositivos, junto a las múltiples necesidades planteadas han dado origen a un nuevo concepto de computación móvil en la nube o *Mobile Cloud Computing* (MCC), la misma que trata de la combinación de la computación móvil, la computación en la nube y el Internet móvil, donde se integran todas las ventajas de estas tecnologías.

En este trabajo, se pretende realizar un estudio profundo del estado del arte, que nos permita obtener un modelo de seguridad para aplicaciones desplegadas en ambientes de *Mobile Cloud Computing* (MCC), para posteriormente proponer una metodología de evaluación, que haga uso de este modelo.

La validación de este método, se la realizará a través de casos de estudio de aplicaciones existentes, en las que se aplique esta propuesta y que permitan realizar una evaluación de la misma.

Palabras Claves

Mobile Cloud Computing, Computación en la Nube, Seguridad, Calidad

Abstract

According to the latest Mobility Report by the Swedish manufacturer Ericsson; it is highlighted that by the last quarter of 2015 the total number of mobile lines in the world was 7300 million, which is the same than the number of inhabitants of the Earth; as well as, within the same quarter, 350 million smartphones were sold. This growing trend of Internet access from mobile devices, coupled with the increase of their capabilities and the greater deployment of third and fourth generation networks (3G / 4G Long Term Evolution LTE) over Wi-Fi networks, provide users, A wide range of services and solutions.

However, the responsibility for security, personal identification and the evolution of the post-implementation era are three areas in which convergent factors are shown, which Gartner has identified as the nexus of forces for 2020.

The increase in smart mobile terminals, as well as increased access to the internet from these devices, together with the needs raised, have given rise to a new concept of mobile computing in the cloud or Mobile Cloud Computing (MCC), which deals with the combination of mobile computing, cloud computing and mobile Internet, where all the advantages of the three are integrated.

Therefore, this study intends to carry out an in-depth literature review, which allows us to obtain a security model for applications deployed in Mobile Cloud Computing (MCC) environments, to subsequently is used by an evaluation method that makes use of this model.

The validation of this method has been made performed by means of proofs of concept or cases of study of existing applications in which this proposal is applied and that allow to make an evaluation of the same one.

Keywords.

Mobile Cloud Computing, Cloud Computing, Quality, Security

Índice

Índice de Tablas

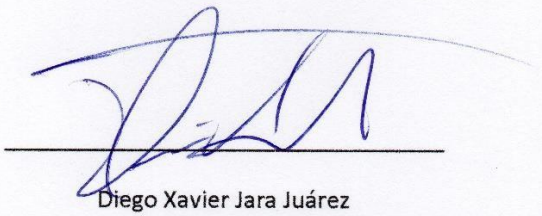
Índice de Figuras

Universidad de Cuenca
Cláusula de Licencia y Autorización para Publicación en el Repositorio Institucional

Diego Xavier Jara Juárez en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación "Propuesta Metodológica de Evaluación de Seguridad para Aplicaciones de Mobile Cloud Computing", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el Repositorio Institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, agosto de 2017



Diego Xavier Jara Juárez

C.I: 0103544102

Universidad de Cuenca
Cláusula de Propiedad Intelectual

Diego Xavier Jara Juárez, autor del trabajo de titulación "Propuesta Metodológica de Evaluación de Seguridad para Aplicaciones de Mobile Cloud Computing", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, agosto de 2017

Diego Xavier Jara Juarez

C.I: 0103544102

Agradecimientos

A Dios, por darme los dones y la esperanza de que, aunque hay tiempos difíciles siempre existe una nueva oportunidad con cada amanecer.

A mi directora de tesis Priscila Cedillo por su entrega y ayuda en la finalización de este trabajo. Gracias por su guía, consejos y por sus valiosas enseñanzas.

A mi esposa Verónica, por ser uno de los pilares y mi fortaleza en tiempos de flaqueza, enseñándome a mirar la vida con optimismo y alegría y sobre todo con ese amor que cada día me brinda. Gracias por mantener tu fe en mí.

A mi madre Yolanda, mi más grande ejemplo y la razón por la que Yo esté aquí. Las palabras no bastarían para agradecer lo mucho que ha hecho por mí, es mi mayor bendición.

A la Facultad de Ingeniería y al Centro de Postgrados en las personas de los ingenieros Juan Leonardo Espinoza, Diego Ponce y Xavier Salamea, por la oportunidad brindada para ser parte de este programa de postgrado.

A mis amigos de aulas y trabajos académicos: Boris, Juan y Pablo, quienes hicieron de este reto una oportunidad para aprender, no solo de los libros sino de su experiencia como brillantes profesionales.

A todas las personas que de una u otra manera estuvieron involucradas en la consecución de este logro.

Diego.

Dedicatoria

A:

Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

Mi esposa Verónica, por su amor y por ayudarme a construir un futuro mejor para nuestro hogar; por llenar mi mundo de alegrías y enseñanzas. Difícilmente habría logrado esto sin su apoyo.

Mi madre Yolanda, por darme la vida, quererme mucho, creer en mí y porque siempre me apoyó. Mamá gracias por motivarme a conseguir este título para mi futuro, todo esto te lo debo también a ti.

Mis abuelos Luis (QEPD) y Gloria (QEPD), por quererme y enseñarme siempre, esto también se lo debo a ustedes.

Todos mis amigos por compartir los buenos y malos momentos.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

Capitulo 1. Introducción

1.1 Antecedentes

Hoy en día la computación en la nube no sólo se limita a un computador personal, sino también ha influenciado y repercute intensamente en la tecnología móvil [1]. Entre las empresas que están adoptando esta tendencia tenemos a Google, Amazon y Microsoft [2], que ven a la computación en la nube, como nuevo paradigma para aplicaciones móviles.

Hace no mucho tiempo, la computación móvil tenía una visión enfocada al dispositivo móvil, en la que el almacenamiento de datos y el procesamiento de éstos se realizaba completamente en la unidad del usuario final, requiriendo una aplicación especializada para cada acción necesaria. Para ello el usuario acumulaba una vasta experiencia en la obtención y manejo de aplicaciones aisladas unas de otras, siendo necesaria una aplicación para cada actividad. Sin embargo, el concepto de individualidad manejado hasta aquí, no es del todo apegado a la realidad, debido a que las actividades de las personas representan más que actos aislados. Para ello la tendencia es de manejar una visión de la computación móvil en la nube [3] que permita sobrellevar estas limitaciones y desarrollar mejoras en las aplicaciones orientadas a este modelo de trabajo.

En los últimos años, esta perspectiva de computación en la nube, ha cobrado un impulso y está transformando la infraestructura de la computación de Internet. También las aplicaciones móviles y los dispositivos móviles se están desarrollando rápidamente. Se prevé que esta nueva visión traiga consigo innovación, donde los dispositivos móviles pueden utilizar las nubes para el procesamiento de datos, almacenamiento y otras operaciones. Es así que, dispositivos electrónicos tales como, teléfonos inteligentes, tabletas, computadores portátiles, están convergiendo en un nuevo campo de rápido crecimiento como lo es el Mobile Cloud Computing (MCC) [1], [4], [5]. Según el Mobile Cloud Computing Forum del año 2011 [6] se define a MCC como: "… a una infraestructura donde tanto el almacenamiento de datos como el procesamiento de datos ocurren fuera del dispositivo móvil. Las aplicaciones de nube móvil desplazan la capacidad de computación y el almacenamiento de datos lejos de los teléfonos móviles y hacia la nube, llevando las aplicaciones y la computación móvil a los usuarios de teléfonos inteligentes, pero a una gama mucho más amplia de suscriptores móviles"

Por tanto, MCC ofrece numerosas ventajas, de ahí, los hackers también están interesados en ella para cometer crímenes de diversa índole. Varios ataques tales como ingeniería social, ataques a la firma XML, la inyección de malware, la manipulación de datos, suplantación de cuentas, la saturación del tráfico, y el ataque a la red de área local inalámbrica, entre otros suponen un gran riesgo para los sistemas informáticos en la nube [7]. De hecho, existen muchos casos de empresas, que han sido víctimas de ataques a sus sistemas de cómputo en la nube.

Ante lo señalado, en cuanto al crecimiento y relevancia de MCC, es necesario realizar un estudio profundo sobre la seguridad, que nos de luces sobre las precauciones a tener en cuenta para conseguir una experiencia satisfactoria en cuanto al uso de esta tecnología.

1.2 Problemática y Justificación

Según el último estudio de predicciones elaborado por la empresa Gartner [8], asegura que hasta el 2020, el 95% de los fallos de seguridad serán culpa del usuario. Los problemas de seguridad siguen siendo la razón más común para evitar el uso de los servicios de nube pública para las empresas, las cuales prefieren pagar el costo de oportunidad al no permitir el acceso y consiguiente uso de estas plataformas a sus empleados.

Estándares de calidad tales como ISO 25010 [9], ISO 27001 [10] y SOC 2 [11], así como marcos de trabajo o modelos de validación se convertirán en herramientas para asegurar la calidad del producto en cuanto a seguridad, prácticamente obligatorios para cualquier empresa que se plantee estratégicamente el uso significativo de un servicio basado en la nube.

Es por ello, que este trabajo pretende elaborar un método para la evaluación de la seguridad de las aplicaciones para MCC, mediante un estudio profundo, que se apoye en un modelo de seguridad aquí propuesto, basado en la norma ISO/IEC 25010 [9], enfocada a la calidad de producto. Este método permitirá evaluar la seguridad de los aplicativos, siendo validado mediante su utilización en aplicaciones para MCC disponibles en el medio.

Con esto pretendemos generar un trabajo de investigación de actualidad, que permita valorar el estado actual en el que se desenvuelve la seguridad móvil y aportar significativamente a la evaluación de las aplicaciones y consecuentemente a la mejora de su seguridad.

1.3 Objetivos

Este trabajo tiene como objetivo general, definir una propuesta metodológica que permita evaluar la seguridad de las aplicaciones desplegadas en Mobile Cloud Computing (MCC), alineadas con la norma ISO 25000 SQuaRE para la evaluación de la calidad de productos de software.

Adicionalmente, se va a realizar un estudio del estado del arte para identificar el estado actual sobre Cloud Computing y Mobile Cloud, a fin de direccionar de manera objetiva la investigación que se presentará en este trabajo.

Como objetivos específicos que ayudarán a conseguir lo anteriormente expuesto tenemos:

- Entender como están enfocados los aspectos de seguridad en el campo de aplicaciones para MCC.
- Elaborar una lista de los tipos de ataques, comunes en las aplicaciones Mobile Cloud.
- Analizar cómo se abordan los estudios de investigación de la seguridad en aplicaciones en *MCC*.
- Elaborar un modelo de calidad basado en la norma ISO 25010, específicamente con la característica de Seguridad.
- Plantear una propuesta metodológica de evaluación de aplicaciones de (MCC).
- Evaluar la propuesta metodológica, en aplicaciones disponibles en el mercado, para verificar su validez y exponer sus resultados.

1.4 Alcance

El alcance del trabajo de investigación estará definido por: (i) la elaboración de un estado del arte sobre la seguridad de aplicaciones para MCC. (ii) además, se elaborará un modelo de calidad enfocado en la seguridad de las aplicaciones, para posteriormente

finalizar con (iii) la elaboración de un método de evaluación de la seguridad en aplicaciones móviles.

Cabe señalar que el modelo de calidad estará basado en la norma ISO 25010, puntualmente en la característica de seguridad y deberá cumplir con las sub-características correspondientes de: Confidencialidad, Integridad, No Repudio, Autenticidad y Responsabilidad; modelo de calidad que permitirá ser usado como un artefacto hacia la evaluación de productos de software de MCC.

Una vez desarrollado el método, se lo evaluará a través de casos de estudio.

Entregables:

- Revisión de la Literatura
- Modelo de seguridad para aplicaciones MCC
- Propuesta metodológica de evaluación de la seguridad para aplicaciones MCC.

1.5 Tareas de Investigación

El método de investigación a seguir involucra una serie de pasos que nos permitirán obtener los resultados esperados. A continuación, se detalla cada uno de ellos:

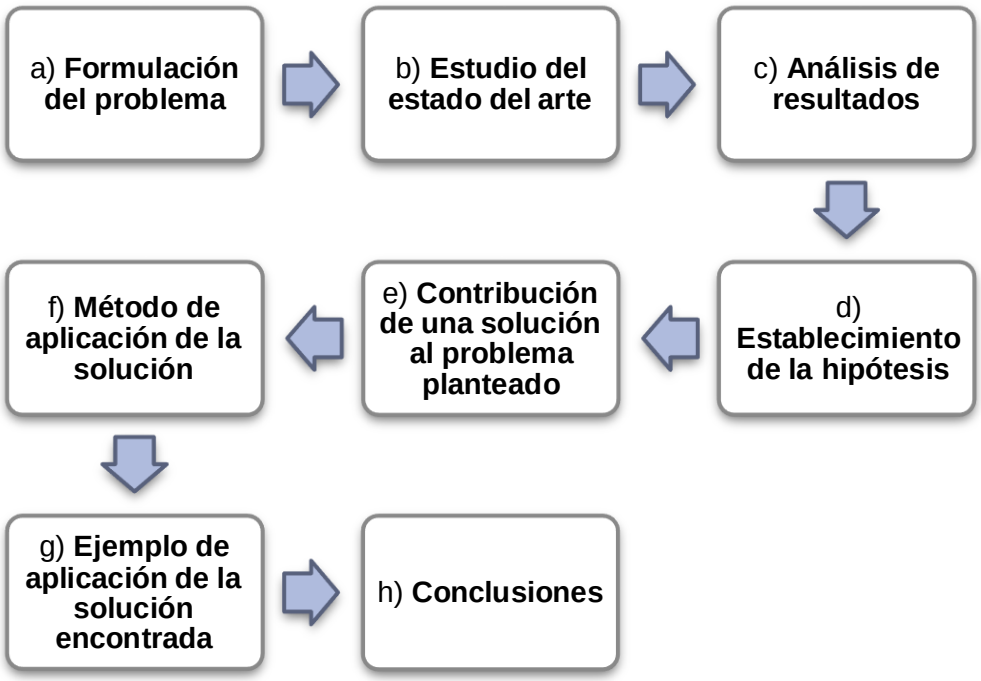


Figura 1-1 Tareas de Investigación utilizadas.

a) **Formulación del problema:** Se realizará una delimitación del mismo para poder tener un punto central y claro al cual atacar en el proceso de la búsqueda de la solución.

b) **Estudio del estado del arte:** Para el estado del arte se ha realizado un estudio consistente en un mapeo sistemático, que permitirán tener un estado actual de los aspectos de seguridad referentes a Mobile Cloud Computing.

c) **Análisis de resultados:** A continuación, después de realizar un análisis de los resultados de los estudios del estado del arte, se delimitaron los aspectos que se necesitan investigar en el presente trabajo.

d) **Establecimiento de la hipótesis:** Se encontró que existe una falta de estudios referentes a la seguridad en aplicaciones para MCC y en base a esto se delimito la hipótesis que se requiere esclarecer en la presente investigación.

e) **Contribución de una solución al problema planteado:** Se elaboró un modelo de Calidad para la Seguridad en aplicaciones para MCC, como base para la evaluación de la seguridad.

f) **Método de aplicación de la solución:** Se elaboró una metodología para la evaluación en la cual se tomará como entrada el modelo de seguridad propuesto.

g) **Ejemplo de aplicación de la solución encontrada:** En este paso se aplicará el método de evaluación de seguridad a tres aplicaciones MCC para verificar la validez del método propuesto.

h) **Conclusiones:** Se sacarán las principales conclusiones relacionadas al método de evaluación de seguridad MCC.

1.6 Estructura del Trabajo

El presente trabajo está compuesto por 7 capítulos distribuidos de la siguiente manera:

El **capítulo 1** brinda una introducción respecto el contexto y el alcance del trabajo, se indicará la metodología y la organización del mismo.

El **capítulo 2** recoge todo el marco tecnológico necesario para el desarrollo de la tesina, la taxonomía útil para el desarrollo del estado del arte y demás temas relacionados con el problema planteado.

El **capítulo 3** presenta el estado actual de la problemática mediante un mapeo sistemático, y se muestran las cifras de las clasificaciones con las cuales se tendrá una vista objetiva del problema.

Los **capítulos 4 y 5** muestran la contribución de este trabajo. El capítulo 4 contiene el modelo de seguridad de aplicaciones para MCC, compuesto por un conjunto de subcaracterísticas, atributos de calidad y métricas para medir los atributos.

El **capítulo 5**, muestra cómo realizar la evaluación de la seguridad de aplicaciones para MCC, mediante la aplicación del modelo propuesto.

En el **capítulo 6** se trata un caso de estudio en el cual se muestra cómo realizar la evaluación aplicando el modelo propuesto.

Finalmente, el **capítulo 7** contiene las conclusiones del trabajo.

Capitulo 2. Fundamento Tecnológico.

2.1 Cloud Computing

Los dispositivos móviles permiten a los usuarios ejecutar aplicaciones que se aprovechan de la creciente disponibilidad de capacidades de detección y un mejor intercambio de datos incorporados en los dispositivos móviles. Como resultado, las aplicaciones móviles se integran perfectamente con los flujos en tiempo real de datos y aplicaciones Web 2.0, tales como Mashups, abierta colaboración, redes sociales y comercio móvil [12] [13].

Los dispositivos móviles como teléfonos inteligentes, iPad’s o Tablets, se han vuelto parte cada vez más importante en nuestras vidas. La gente las está utilizando para realizar sus tareas diarias como compartir datos, ver películas, el pago de facturas, etc. Las aplicaciones mobile cloud han trasladado la potencia de cálculo y el almacenamiento

de datos fuera de los teléfonos móviles hacia la nube, llevando la informática y las aplicaciones no solo a los usuarios de teléfonos inteligentes sino a una gama mucho más amplia de suscriptores móviles. No obstante, estos dispositivos todavía tienen algunas limitaciones como la capacidad de procesamiento, la duración de la batería y el espacio de almacenamiento [14].

Cloud Computing (CC), que es el uso de los recursos informáticos que se entregan como un servicio a través de una red como Internet, donde el cobro-facturación se la realiza de acuerdo a la demanda, se compone de tres modelos de servicio: infraestructura como servicio (IaaS), plataforma como un servicio (PaaS) y software como servicio (SaaS). Gracias a CC, la función de almacenamiento es ahora poco menos que ilimitado y adicionalmente la potencia de cálculo se ha incrementado brindando la posibilidad de escalabilidad rápida cuando se necesite. Últimamente, los paradigmas de la nube proporcionan a los usuarios finales la capacidad de procesamiento de datos en paralelo, proporcionando los servidores para los distintos usuarios que no tienen esta característica en sus dispositivos [15]. Ahora el servicio SaaS, es cada vez más utilizado por las personas, pues se han dado cuenta que el sistema de almacenamiento en la nube es una estrategia muy rentable para sus aplicaciones, a pesar de que enfrentan algunas dificultades de rendimiento y sobre todo seguridad de acuerdo a varios estudios realizados.

Si un cliente puede acceder a sus datos y aplicaciones desde cualquier lugar, es posible que la privacidad del cliente se vea comprometida. Los dispositivos móviles al tener casi las mismas capacidades que una computadora de escritorio, da lugar a los mismos problemas relacionados con la seguridad y la privacidad.

A pesar de la enorme cantidad de trabajo e investigación para asegurar el entorno CC, todavía hay algunas áreas que requieren ser abordadas y más exploradas. Por ejemplo, la seguridad y la privacidad de los datos del usuario almacenados en los servidores de la nube, y la detección de intrusiones entre otros [16].

2.1.1 Arquitectura Cloud Computing

NIST (Instituto Nacional de Estándares y Tecnología) es una institución muy reconocida en todo el mundo por su trabajo en el campo de la tecnología de la información. NIST define la arquitectura Cloud Computing al describir cinco

características esenciales, tres modelos de servicios en la nube y cuatro modelos de implementación en la nube [17].

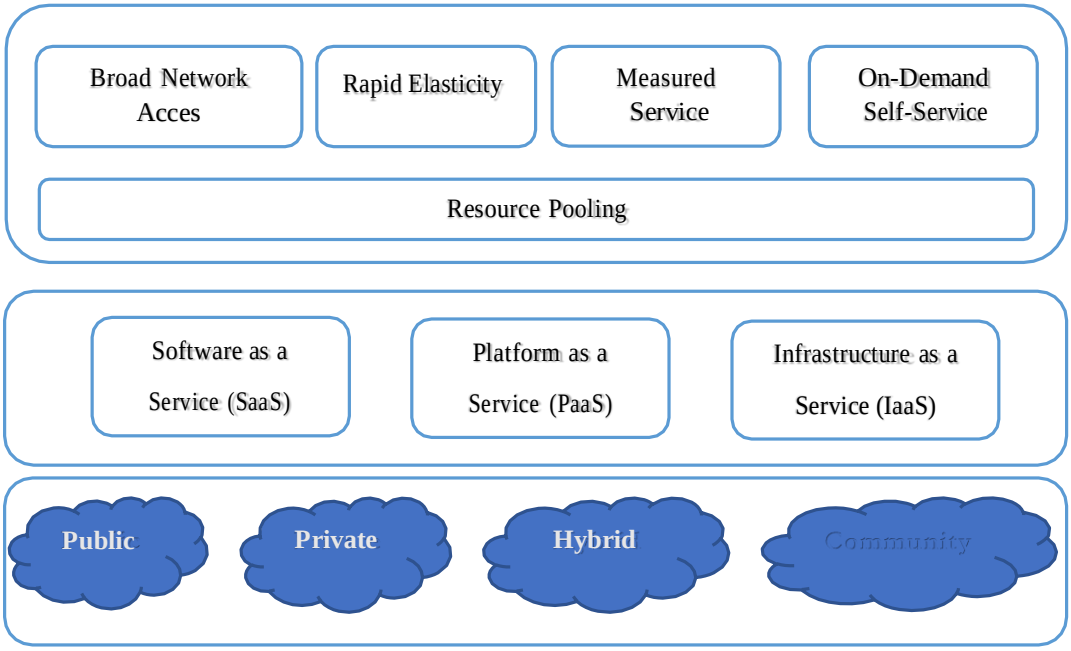


Figura 2-1 Modelo visual de la definición NIST de Cloud Computing [17]

2.1.2 Características esenciales de Cloud Computing

Como se describió anteriormente, hay 5 características esenciales de Cloud Computing donde se explica la relación y la diferencia con la informática tradicional.

- *On-demand-self-service*. El consumidor se vuelve el administrador de los servicios cuando sea necesario, sin la interacción con el proveedor de servicios.
- *Broad Network Access*. Cuenta con todas las capacidades sobre la red y accede a través de los medios disponibles.
- *Resource Pooling*. La reutilización de recursos informáticos permite que varios usuarios accedan tanto a recursos físicos y virtuales asignados dinámicamente, dependiendo de la demanda del consumidor.
- *Rapid Elasticity*. Los servicios se pueden desplegar rápida y elásticamente.
- *Measured Service*. Los sistemas de Cloud Computing controlan y optimizan automáticamente el uso de recursos proporcionando una capacidad de medición al tipo de servicios (por ejemplo, almacenamiento, procesamiento, ancho de banda o cuentas de usuario activas) [17].

2.1.3 Modelos de Servicio

La Figura 2-2 muestra los tres principales modelos de servicios y los productos que cada uno soporta. En general, hay tres diseños básicos de los modelos de cloud computing, como se describe a continuación:

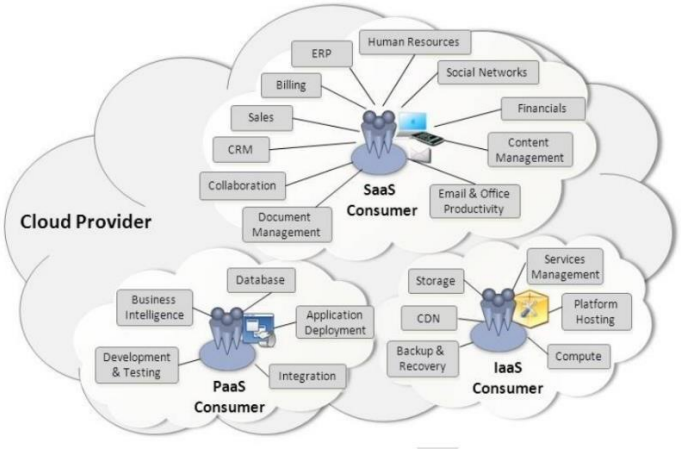


Figura 2-2 Ejemplo de servicios disponibles para un consumidor de la nube (NIST SP 500-292) [18].

Sin embargo, se puede encontrar literatura acerca de nuevos modelos de servicio como XaaS [19], SecaaS [20], ITaaS [21], .

La base para implementar estos modelos de servicios son la Virtualización y la multi-sesión. La virtualización permite que los recursos de la red estén disponibles siempre independientes de su ubicación física o la conexión física a la red. La multi-sesión se refiere al principio de arquitectura que permite el intercambio de recursos entre un gran número de usuarios[22].

2.1.3.1 Infrastructure as a Service (IaaS)

En una estructura IaaS, la infraestructura como servidores, CPU, almacenamiento, equipos de red y centros de datos, se entregan como un servicio bajo demanda. En lugar de comprar estos recursos, los clientes los obtienen como un servicio totalmente subcontratado durante el tiempo que los necesiten. El servicio se factura de acuerdo a los recursos consumidos. Amazon Elastic Compute Cloud (EC2), GoGrid y FlexiScale son algunos de los ejemplos de las nubes IaaS. Este tipo de nube también se denomina cloud de utilidad o nube de infraestructura.

El ejemplo más común de IaaS es el hosting[1], el cual provee de hardware como un servidor y software como un webserver[2]. Sin embargo, el concepto tradicional de hosting ha evolucionado, ya que no se requiere ningún compromiso a largo plazo y permite a los usuarios acceder a los recursos de acuerdo a sus necesidades.

Una nube IaaS presenta las siguientes características:

- Disponibilidad de un gran volumen de recursos computacionales tales como servidores, equipos de red, memoria, CPU, espacio en disco e instalaciones de centros de datos bajo demanda;
- Uso de infraestructuras de calidad empresarial a un costo reducido, permitiendo a las pequeñas y medianas empresas beneficiarse de las mejores virtudes de equipos computacionales;
- Escalabilidad dinámica de la infraestructura; La capacidad bajo demanda se puede escalar fácilmente hacia arriba y hacia abajo según las necesidades de recursos[23].

Desde otro punto de vista la infraestructura como servicio se refiere a la distribución de los recursos de hardware para ejecutar servicios, por lo general con la ayuda de la virtualización. Con IaaS, los usuarios tienen disponible los recursos existentes de manera escalable, es decir que si la demanda crece estos también lo harán. Este tipo de servicio generalmente viene acompañado del método de pago “pay as you go” en el cual se pagará solo por los recursos consumidos [24].

2.1.3.2 Platform as a Service (PaaS)

Platform as a Service o plataforma como servicio, es aquella que ofrece a los desarrolladores, plataformas y desarrollo de aplicaciones como servicio sin el costo ni la complejidad de la compra y gestión de infraestructura adicional. De esta forma se brinda las facilidades para la construcción y entrega de aplicaciones completas en Internet [25].

---

[1] Hosting. - Es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web

[2] Webserver. - programa informático el cual procesa páginas web generalmente en código http.

En el modelo PaaS, la plataforma y las herramientas para el desarrollo de aplicaciones y los sistemas *middleware*[3] son alojados por un proveedor y ofrecidos a los desarrolladores de aplicaciones, permitiéndoles simplemente codificar y desplegar sin interactuar directamente con la infraestructura subyacente. La plataforma proporciona la mayoría de las herramientas e instalaciones necesarias para construir y entregar aplicaciones y servicios tales como instalaciones de flujo de trabajo para el diseño, desarrollo, pruebas, implementación y hospedaje de aplicaciones, así como servicios de aplicaciones como integración de servicios web, integración de bases de datos, almacenamiento, versión de aplicaciones y comunicación y colaboración del equipo. Ejemplos de PaaS incluyen Google App Engine, Microsoft Azure, los servicios Web de Amazon y el IDE NetBeans de Sun Microsystems. La nube PaaS también se llama cloud de la plataforma o cloudware.

2.1.3.3 Software as a Service (SaaS)

Software as a service ó Software como servicio también se denominan nubes de software. En el modelo SaaS, una aplicación es alojada por un proveedor de la nube y entregada como un servicio a los usuarios, principalmente a través de Internet o una red dedicada [26]. Elimina la necesidad de instalar y ejecutar la aplicación localmente en la computadora de un usuario y, por lo tanto, libra a los usuarios del mantenimiento y actualizaciones de hardware y software. La licencia de software no es propiedad del usuario. Los servicios son facturados, dependiendo de su uso. Por lo tanto, los costos de usar un servicio se convierten en un gasto continuo en lugar de un enorme gasto inicial de capital en el momento de la compra.

Ejemplos de SaaS incluyen Webmail, Google Apps, Force.com CRM, contabilidad online de Quicken, Business Suite de software de NetSuite, Sun Java Communications Suite y Paychex sistema de gestión de nómina.

Para el usuario final, SaaS es un concepto simple, se inicia una sesión en la aplicación a través de internet y trabaja de forma rápida y fiable sin importar donde se encuentre físicamente la aplicación. En cuanto a costos de implementación, obviamente

[3] *Middleware. - Es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones.*

SaaS es un producto altamente rentable y la mayoría de empresas lo tomaran como un gasto mensual del cual pueden prescindir en casos de emergencia [27].

En este último nivel del Cloud se brinda el servicio completo a la organización brindándole el software que esta requiere como ERP, CMR, SAP y así un sin número de soluciones completas para el manejo personalizado de su negocio.

2.1.4 Modelos de despliegue.

Se observan cuatro escenarios para la formación de Cloud Computing, Private Cloud, Public Cloud, Hybrid Cloud y Community Cloud. Entre estos escenarios es que se dispone de un abanico de opciones que utilizan usuarios y desarrolladores. Cabe destacar que estos escenarios son implementados en los Datacenters[4], los mismos que dependiendo de su disposición pueden tener un enfoque interno, externo o combinado.

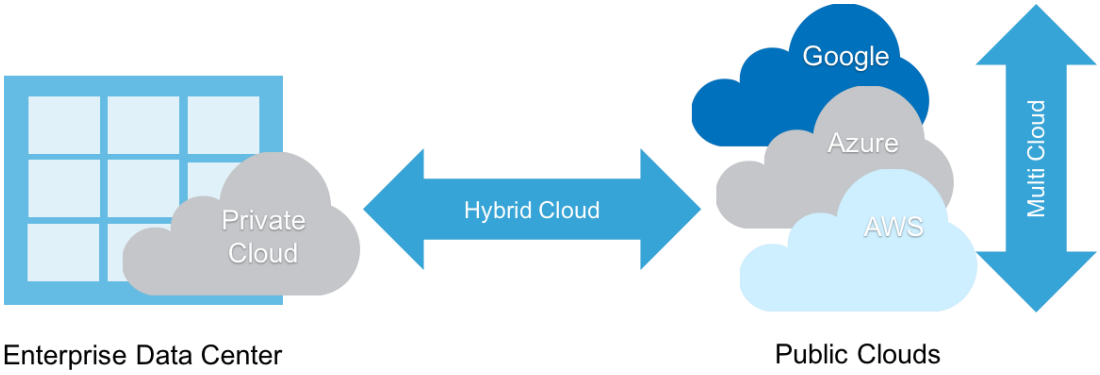


Figura 2-3 Modelos de despliegue.

2.1.4.1 Private Cloud

La nube privada o Private Cloud es considerada la primera etapa en el desarrollo de Cloud Computing, debido a que éstas se implementan en las grandes empresas por equipos de TI. Estas nubes privadas se ejecutarán en Datacenters seguros fuera de la empresa, vinculando a todas las oficinas de la compañía a través de túneles cifrados por la Internet pública o VPN[5]. Una vez comunicada de forma segura la nube con todas las

[4] Datacenters. - Significa centro de procesamiento de datos (CPD) es aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización

[5] *VPN. - Virtual Private Network*

sucursales de la empresa, esta se dispondrá a colocar sus datos y aplicaciones en la nube, siempre de manera segura y privada [28].

Inicialmente las nubes privadas se componen casi enteramente de los recursos internos, una nube privada puede combinar recursos de una nube externa como interna para satisfacer las necesidades de un sistema o aplicación, destacando que la empresa está en control total de la gestión unificada de la nube.

2.1.4.2 Public Cloud

El escenario conocido como Public Cloud se da en el momento en el cual las empresas necesitan mover datos o aplicaciones desde su interior al exterior. El escenario que se crea con la interconexión de varias nubes públicas es conocido como External Cloud [11].

Las nubes externas involucran recursos y servicios TI que son vinculados fuera del establecimiento, a modelo de un hosting. Estos recursos y servicios son vendidos con las cualidades de Cloud Computing: el auto-servicio, pay as you go[6], administración de recursos de forma dinámica y escalabilidad infinita. Cabe señalar que estos recursos no son del todo controlados por el cliente [12].

2.1.4.3 Hybrid Cloud

Una nube híbrida es una combinación de dos o más de los modelos de nube anteriores. En este modelo, una empresa utiliza nubes tanto públicas como privadas, implementando sus servicios menos críticos y de bajo riesgo en una nube pública y aplicaciones centrales críticas en su nube privada interna. Un modelo híbrido permite la implementación selectiva abordando las preocupaciones sobre seguridad, cumplimiento y pérdida de control, así como la habilitación de la adopción de nubes públicas que ofrecen beneficios de costos y más opciones de aplicación.

Incluso la nube híbrida puede ser un buen paso intermedio antes de pasar la mayoría de las aplicaciones a la nube, ya que es algo menos riesgoso. Por lo tanto, sería

[6] *Pay as You Go. - Pago por Consumo.*

interesante pasar algunas aplicaciones más útiles para la nube a ésta y en el momento que sea más cómoda, mover las que sean necesarias.

2.1.4.4 Community Cloud

Nube comunitaria es un modelo de despliegue en el que una infraestructura es implementada para un uso específico de una comunidad que comparten intereses comunes y que tienen acceso exclusivo. El mismo que puede ser administrado por alguien de la comunidad, un tercero como proveedor o una combinación de ambos.

AcademyOne Navigator Suite (dirigido a académicos y estudiantes) y Asite Solutions (específicamente diseñado para la industria de la construcción) son ejemplos de este tipo de nubes [23].

2.1.5 Beneficios del Cloud Computing

Los beneficios clave de adoptar una nube incluyen la reducción de capital y costos operativos, flexibilidad mejorada, escalabilidad en cuanto a la demanda, despliegue de aplicaciones de una manera más fácil y rápida, facilidad de uso y disponibilidad de vastos recursos de nube para cada tipo de aplicación o uso. Muchas aplicaciones, incluyendo correo electrónico, creación de documentos de oficina y mucho almacenamiento de datos continúan moviéndose hacia las nubes para aprovechar los beneficios de este nuevo paradigma en TI.

Para que los usuarios puedan hacer uso de los recursos de la nube desde cualquier parte del mundo en cualquier momento, sólo se necesita una conexión a Internet y un navegador Web. La nube permite a los usuarios ejecutar incluso aplicaciones de computación intensiva o de almacenamiento intensivo, ya que todas sus necesidades de computación y almacenamiento se obtienen de la nube.

Las nubes públicas eliminan los gastos de capital importantes para el hardware y las tarifas de licencia iniciales para el software, así como los problemas del mantenimiento y la actualización de hardware y software por parte de los usuarios. Las aplicaciones en la nube se pueden implementar instantáneamente y simultáneamente a miles de usuarios en diferentes ubicaciones alrededor del mundo, y pueden actualizarse con regularidad. Además, a medida que las nubes proporcionan una continuidad mejorada de los negocios y la seguridad de los datos, son particularmente atractivas para las

pequeñas y medianas empresas, así como para las empresas en áreas propensas a desastres. Los desarrolladores de aplicaciones pueden utilizar las nubes para probar sus ideas sin tener que invertir en su propia infraestructura.

En la última década, la red basada en la computación y las aplicaciones en demanda han mejorado la computación en nube que ha comandado una enorme atención a la investigación desde 2007 [29]. De acuerdo con [30], y como se ha reseñado en párrafos anteriores, cloud computing se refiere a un catálogo de servicios prestados por un grupo de ordenadores orientados a Internet. El clúster tiene servidores de bajo costo, administración de recursos bien organizada que proporciona un nuevo modelo de suplemento, consumo y entrega para servicios de TI, que son escalables, independientes del dispositivo, confiables, rápidas y convenientes. La red de próxima generación presenta una ventaja de la ubicuidad y movilidad a través de la tecnología de redes inalámbricas que proporcionan Internet en dispositivos móviles. El hecho de reunir las capacidades de la computación en nube y la computación móvil dio origen a un nuevo paradigma llamado computación en nube móvil (MCC). El objetivo de MCC es utilizar técnicas de computación en nube para el almacenamiento y procesamiento de datos en dispositivos móviles, reduciendo así las limitaciones de los dispositivos móviles en términos de potencia computacional baja y limitada capacidad de almacenamiento.

2.1.6 Aspectos generales de Cloud Computing

Como se ha establecido y se reforzara durante el desarrollo del presente trabajo la necesidad de satisfacer las necesidades de los sistemas de computación más exigentes, ha producido una necesaria evolución de las arquitecturas de cálculo, fundamentalmente basada en la ejecución de procesos de forma simultánea en múltiples equipos informáticos.

A lo largo del presente estudio se eligió utilizar el término en idioma inglés cloud computing y no el de computación en nube en idioma español según la traducción de la Unión Internacional de Telecomunicaciones (UIT) y la Unión Europea; Esta decisión se basó principalmente a que el termino en idioma inglés aparece citado con mayor frecuencia en la mayor parte de los artículos científicos consultados, así como en los libros especializados. Con el fin de observar los importantes temas a revisar en esta tesina, se presenta una serie de aspectos importantes a considerar enfocados básicamente a la

seguridad.

2.1.6.1 Seguridad

El proveedor de Cloud debe asegurarse de que el cliente no se enfrenta a ningún problema como la pérdida de datos o el robo de datos. También existe la posibilidad de que un usuario malintencionado pueda penetrar en la nube haciéndose pasar por un usuario legítimo, infectando toda la nube y afectando así a muchos clientes que comparten la nube infectada. Hay varios problemas dentro de la seguridad en la computación en la nube. El reciente acontecimiento en el mundo de las TI incluye muchos ataques a los datos almacenados en la nube que afectaron directamente la seguridad [31]. Como todos los datos de usuario se almacenan en la nube, la seguridad es definitivamente, sin duda, uno de los principales problemas a tratar.

2.1.6.2 Ancho de banda

Las preocupaciones por la seguridad han dominado durante mucho tiempo la mayor parte de la conversación en la nube y han causado que muchas compañías deliberen sobre cómo empezar en la nube. Pero si bien el foco ha estado en la seguridad en la nube, otros potenciales cuellos de botella serian como el requisito de ancho de banda. Dado que el ancho de banda rara vez es un problema para las empresas que exploran la nube de una manera pequeña. Pero a medida que comienzan a expandir su huella de la nube y ejecutar aplicaciones orientadas a la producción, el movimiento de datos toma una escala completamente diferente. A medida que las empresas comiencen a mover las cargas de trabajo reales a la nube, es natural que busquen un mayor ancho de banda. La capacidad de transmisión y recepción del canal, en definitiva, se convirtieron en un problema grande para la empresa que depende directamente de las soluciones al tema de ancho de banda.

2.1.6.3 Consumo de energía

Los servicios ofrecidos por proveedores en la nube como Amazon, Microsoft, IBM y Google se implementan en miles de servidores distribuidos en múltiples centros de datos distribuidos geográficamente. Los costos de electricidad involucrados en el funcionamiento de una gran infraestructura de nube de múltiples centros de datos pueden ser enormes. De hecho, los proveedores de servicios en la nube a menudo deben pagar por el pico de potencia que extraen, así como la energía que consumen. Reducir estos altos costos de operación es uno de los desafíos que enfrentan los proveedores de servicios

en la nube.

2.1.6.4 Recuperación de desastres y continuidad de los negocios

La recuperación de desastres es otro de los principales problemas en el cloud computing. Si un cliente almacena sus datos en la nube proporcionada por un proveedor de servicios y éste sufre la pérdida repentina de la empresa quedando en una posición que le obliga a apagar el servidor de datos, entonces los datos del cliente están en un estado incierto. No puede ser recuperado por el cliente y el proveedor de servicios en la nube es también incapaz de responder ante el cliente en estos problemas, esto es la recuperación de desastres y el problema de continuidad de negocio en la computación en nube.

2.1.6.5 Disponibilidad

Los problemas de disponibilidad en el cloud computing son similares a la recuperación de desastres y la continuidad del negocio. El servidor de datos presente en el proveedor de servicios en la nube debe proporcionar un servicio ininterrumpido al lado del cliente, con el fin de evitar el tiempo de inactividad en el lado del usuario. En la nube, el tiempo de inactividad o la pérdida de datos pueden paralizar rápidamente el flujo de trabajo e imponer costos sustanciales, que pueden ir desde el tiempo y el dinero gastados en reparaciones y lapsos de productividad, hasta la incapacidad de cumplir con los niveles de servicio estipulados en los SLA [31].

2.1.6.6 Service Level Agreement (SLA)

TM Forum define en [32] a los SLAs como las expectativas entre dos o más partes en cuanto a temas de calidad de servicio, prioridades y responsabilidades. En el mismo documento el Consejo de Clientes de Cloud Standards considera los SLAs en la nube como expectativas escritas para el servicio entre consumidores y proveedores de la nube.

Básicamente un SLA proporciona orientación a los responsables de la toma de decisiones sobre qué esperar y qué debe tener en cuenta al evaluar y comparar los SLA de los usuarios finales de los proveedores de cloud computing. Quienes toman estas decisiones también deben evaluar los SLAs que un proveedor de cloud computing tiene con terceros, centros de datos empresariales, proveedores de red entre otros pues de manera indirecta también influye en el servicio que reciba como usuario.

Un SLA no debe ser fruto de una negociación rápida. Por ello acelerar el proceso

de negociación de los términos y condiciones en el SLA no permite que las partes

entiendan las expectativas del otro, especialmente cuando cada parte tiene una percepción diferente de lo que significa una determinada terminología o determinado proceso parte del servicio. Por ello es importante el detalle en el contrato de servicio establecido bajo éste SLA, debido a que en el momento de la evaluación serán las condiciones establecidas en este documento, los que servirán para valorar el cumplimiento o no de lo acordado sobre todo en temas de seguridad, que es lo que nos compete tratar en este trabajo.

2.2 Mobile Cloud Computing

Se define a Mobile Cloud Computing como "el enriquecimiento de la tecnología de la computación móvil que aprovecha los recursos elásticos unificados de diversas nubes y tecnologías de red, cuyo objeto es la funcionalidad sin restricciones, el almacenamiento y la movilidad para servir a una multitud de dispositivos móviles en cualquier lugar y en cualquier momento a través del canal de Ethernet o Internet en entornos heterogéneos y plataformas basadas en el principio de pago-por-uso" [33].

El foro MCC define al Mobile Cloud Computing como sigue [6]:

“La computación en la nube móvil en su forma más simple, se refiere a una infraestructura donde tanto el almacenamiento de datos como el procesamiento de datos ocurren fuera del dispositivo móvil. Las aplicaciones mobile cloud desplazan la capacidad de computación y el almacenamiento de datos de los teléfonos móviles hacia la nube, llevando las aplicaciones y el MC a los usuarios de teléfonos inteligentes, pero a una gama mucho más amplia de suscriptores móviles”.

Aepona [34] describe a MCC como un nuevo paradigma para aplicaciones móviles por el cual el procesamiento y almacenamiento de datos se mueven desde el dispositivo móvil a plataformas de computación potentes y centralizadas ubicadas en nubes. A continuación, se accede a estas aplicaciones centralizadas a través de la conexión inalámbrica basada en un cliente nativo o navegador web en los dispositivos móviles.

Alternativamente, MCC se puede definir como una combinación de web móvil y CC [35], [36], que es la herramienta más popular para los usuarios de móviles para acceder a las aplicaciones y servicios en Internet.

En pocas palabras, MCC proporciona a los usuarios móviles los servicios de procesamiento y almacenamiento de datos en las nubes. Los dispositivos móviles no

necesitan una configuración potente (por ejemplo, velocidad de la CPU y capacidad de memoria) porque todos los complicados módulos informáticos pueden procesarse en las nubes.

2.2.1 Arquitectura Mobile Cloud Computing

MCC utiliza enfoques de aumento computacional (los cálculos se ejecutan de forma remota en lugar de en el dispositivo) mediante los cuales los dispositivos móviles pueden utilizar recursos computacionales basados en la nube [37]. En MCC, hay cuatro tipos de recursos basados en la nube, estos son, las nubes inmóviles distantes, las entidades de computación inmóvil cercanas, las entidades de computación móvil cercanas, y el recurso híbrido (combinación de los otros tres modelos)[37][38]. Los servicios cloud gigantes tales como Amazon EC2 están en los grupos inmóviles lejanos mientras que el *cloudlet* o los sustitutos son el miembro de las entidades informáticas inmóviles próximas. Los teléfonos inteligentes, las tabletas, los dispositivos móviles (smartphones, tablets, phablets) y los dispositivos de computación portátiles forman parte del tercer grupo de recursos basados en la nube, que es una entidad informática móvil cercana. [1]

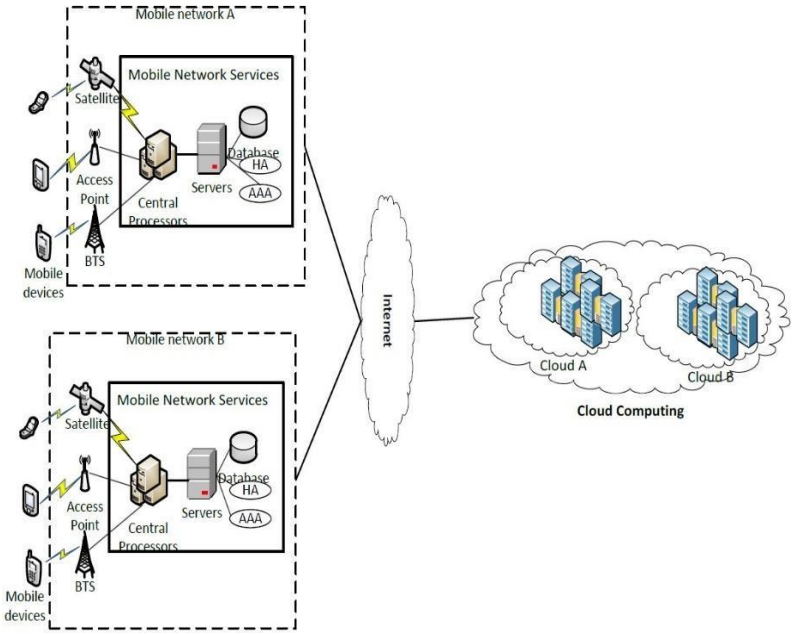


Figura 2-4 Arquitectura MCC [39]

Se puede considerar que un cloudlet es un dispositivo pequeño que se encuentra cerca, tal vez en una cafetería. Cuando sea necesario, el dispositivo descarga los datos del

usuario desde una ubicación centralizada, permitiendo el acceso local por parte del

usuario y reduciendo la latencia. Cuando haya terminado, los datos del usuario pueden ser devueltos a la ubicación centralizada, si es necesario. Este proceso ocurre de forma invisible para el usuario [40].

Un cloudlet [41] es un clúster de computadoras ricos en recursos informáticos bien conectados a Internet y disponibles para su uso por dispositivos móviles cercanos. Por lo tanto, cuando los dispositivos móviles no quieren desconectarse de la nube pueden encontrar un cloudlet cercano. De esta manera, los usuarios móviles pueden satisfacer la demanda en tiempo real y con baja latencia, únicamente con acceso inalámbrico al cloudlet. Si no hay un cloudlet en las inmediaciones, el dispositivo móvil puede utilizar el modo por defecto enviando las solicitudes a una nube remota, o en el peor de los casos, haciendo uso únicamente de sus propios recursos.

2.2.2 Taxonomía de problemas en Mobile cloud computing

Se presenta una taxonomía de los problemas en MCC basada en asuntos relacionados con los niveles operativos, usuario final y servicio, así como en áreas de seguridad, conocimiento del contexto y gestión de datos, como se ilustra en la 0. Los criterios para definir la taxonomía se basan en las cuestiones clave de la computación en la nube móvil, y cómo se han abordado estos temas en la academia:

- Problemas a nivel operacional
- Problemas a nivel de usuario final
- Problemas a nivel de servicio y aplicación
- Privacidad, seguridad y confianza
- Conocimiento del contexto
- Gestión de datos

Estos puntos en el nivel superior de la taxonomía son aplicables a muchas áreas, y no sólo a MCC. Las similitudes sirven para la comparación sobre cómo la computación en la nube móvil se relaciona con otros campos. En la Figura 2-5 se muestra de manera más detallada la taxonomía de problemas mencionada.

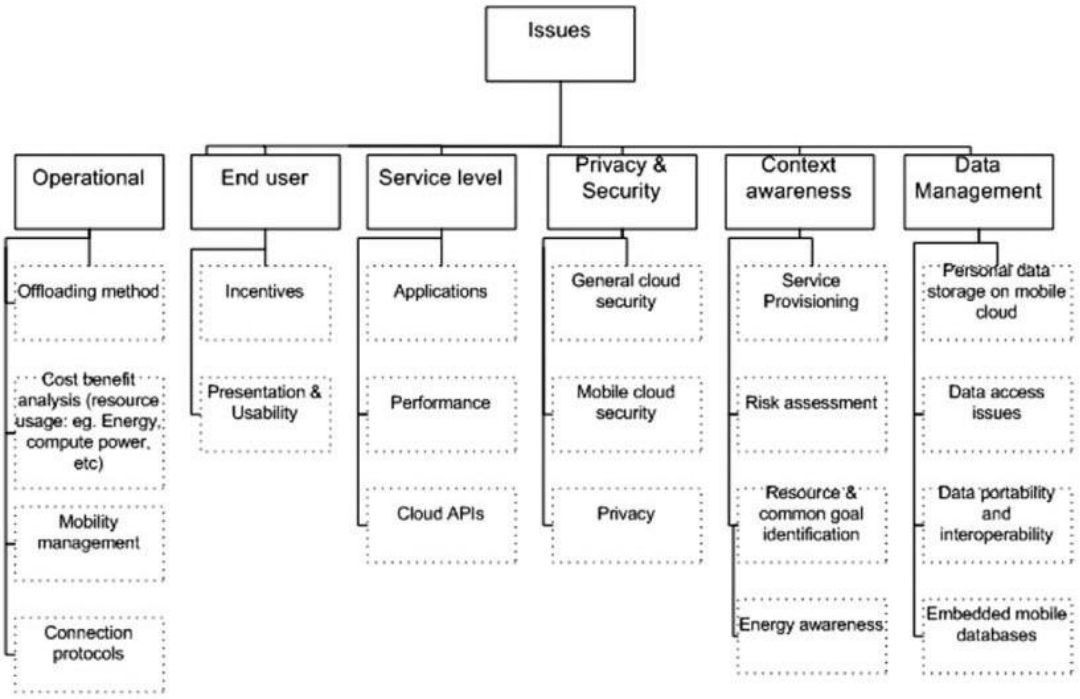


Figura 2-5 Taxonomía de problemas en Mobile Cloud Computing [1]

2.2.2.1 Privacidad, seguridad y confianza

Ya sea descargando cálculos intensivos o almacenamiento de datos, el uso de la nube para dispositivos móviles plantea cuestiones de seguridad y problemas de confianza. En [42] se describen los peligros potenciales en el uso de servicios en la nube para dispositivos móviles. Debido a la baja capacidad de almacenamiento de dispositivos móviles, muchos usuarios están empezando a almacenar datos como contactos, calendarios y SMS en las nubes. Sin embargo, estos servicios en la nube se declaran vulnerables y los usuarios pueden perder sus datos si los servicios salen del negocio, o simplemente si los servicios fallan debido a problemas tecnológicos.

En consecuencia, MCC hereda las amenazas de seguridad de la computación en nube convencional en los casos en que la definición de nube móvil significa conectar dispositivos móviles a una nube remota. En este caso, el servidor de nube remoto sería el mismo que un proveedor de computación en nube convencional, lo que hace que las amenazas generales de seguridad en la nube sean válidas. Al mismo tiempo, las nubes móviles presentan un grupo de problemas que son específicos de los dispositivos móviles que descargan trabajos a través de los canales de comunicación inalámbrica. Por otra parte, las preocupaciones de seguridad que son específicos de los dispositivos móviles,

como los ataques de agotamiento de la batería [43], *botnets*[7] móviles y ataques dirigidos [44] también deben ser considerados.

Seguridad general en la nube

En [45] se describe siete riesgos de seguridad que los usuarios deben considerar en la computación en nube:

1. Acceso privilegiado al usuario: la descarga de datos sensibles a la nube significaría la pérdida de control físico, lógico y personal directo sobre los datos.

2. Cumplimiento normativo: los proveedores de servicios en la nube deben estar dispuestos a someterse a auditorías externas y certificaciones de seguridad.

3. Ubicación de los datos: la ubicación física exacta de los datos del usuario no es transparente, lo que puede dar lugar a confusión sobre jurisdicciones específicas y compromisos sobre los requisitos locales de privacidad.

4. Segregación de datos: dado que los datos de nube suelen almacenarse en un espacio compartido, es importante que los datos de cada usuario estén separados de otros con esquemas de cifrado eficientes.

5. Recuperación: es imperativo que los proveedores de la nube proporcionen mecanismos adecuados de recuperación de datos y servicios en caso de fallo tecnológico u otro desastre.

6. Apoyo investigativo: dado que la explotación forestal y los datos para múltiples clientes pueden estar ubicados en un mismo lugar, la actividad inadecuada o ilegal en caso de que se produzcan puede ser muy difícil de investigar.

[7] *Botnet es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de*

forma remota [82]

7. Viabilidad a largo plazo: aseguramiento de que los datos de los usuarios serían seguros y accesibles incluso si la propia empresa en la nube se fuera a operar.

Seguridad en Mobile Cloud

La seguridad de una nube móvil introduce los siguientes desafíos como se describe en [46], donde los autores proponen un modelo de seguridad para aplicaciones elásticas compuestas de weblets[8] que se pueden migrar hacia y desde una nube a un dispositivo móvil:

- autenticación entre los weblets que se distribuirían entre la nube y el dispositivo,
- autorización para weblets que podrían estar ejecutándose en entornos de nube relativamente poco confiables para acceder a datos de usuario confidenciales, y
- establecimiento y verificación de nodos de nube de ejecución de weblet de confianza.

Las amenazas de seguridad se clasifican como amenazas a dispositivos móviles, amenazas a la plataforma en la nube y contenedor de aplicaciones y amenazas a los canales de comunicación.

Privacidad

Con el incidente con respecto a CarrierIQ donde se instalaron y recopilaron información de teléfonos móviles [47], es importante que los usuarios de teléfonos móviles tengan transparencia y opciones. Los usuarios deben ser conscientes de qué información personal es exactamente visible para el público y tener control sobre sus datos personales que se almacenan en sus teléfonos inteligentes. Es vital que los datos personales que se comparten, se lo hacen con el consentimiento de los usuarios, y que pueden optar por cualquier programa de recopilación de datos en cualquier momento.

---

[8] ***Weblets*** *da soporte para servir recursos que estén dentro del JAR, o accesibles desde una URL o incluso en la propia aplicación web, y todo esto es tema de configuración. Es decir* ***Weblets*** *proporciona una interfaz y varias*

implementaciones [83]

En una mobile cloud en la que el recurso compartido de dispositivos móviles funciona con otros dispositivos móviles, la principal preocupación son los dispositivos maliciosos. En un entorno en el que los usuarios del dispositivo son desconocidos y la nube móvil se forma de manera oportunista, esta es una preocupación muy seria. Aunque la Infraestructura de clave pública (PKI) es un método apropiado para el problema de seguridad, la problemática radica en que dibuja una sobrecarga operativa alta que no es práctica en dispositivos móviles con restricción de recursos. Además, las conexiones entre los dispositivos en una nube móvil son altamente dinámicas. En un momento dado, nuevos dispositivos pueden unirse mientras que los dispositivos actuales pueden estar saliendo. En tal escenario, la frecuencia de solicitudes de autenticación de usuario aumentará hasta tal punto que podría resultar en recursos insuficientes para realizar operaciones de clave asimétrica y transmitir mensajes pesados [48]. Por otra parte, el concepto cloudlet [40] es útil en este escenario: los cloudlets podrían funcionar como la infraestructura local a la que se pueden descargar las operaciones PKI.

Además de un esquema de autorización, los usuarios de la nube móvil también deben tener la capacidad de cambiar su configuración de privacidad y dictar qué información se puede ver, por ejemplo, su información de ubicación.

2.2.2.2 Conocimiento del contexto

Schilit et al. [49] describe los tres aspectos importantes del contexto como: la ubicación del usuario, otros usuarios cercanos y los recursos en el entorno del usuario. Por ejemplo, en la perspectiva de un usuario móvil, 'contexto' significa cosas tales como iluminación, nivel de ruido, conectividad de red, costes de comunicación, ancho de banda de comunicación e incluso la situación social.

Los sistemas con conciencia de contexto son capaces de utilizar la información contextual para cambiar automáticamente sus configuraciones para adaptarse al contexto [50]. Este comportamiento es muy útil en el caso de los sistemas móviles, ya que estos tratan con un entorno de ejecución que está sujeto a cambios constantes. En el caso de mobile cloud computing, la conciencia del contexto se puede utilizar en la formación de nubes de recursos, así como la información de procesamiento. Por ejemplo, un dispositivo puede inferir su ubicación a través de GPS, Bluetooth o algunas otras formas de

posicionamiento y utilizar esa información para prepararse para el próximo procesamiento.

2.2.2.3 Conciencia de la energía

Debido a que un dispositivo móvil funciona con un suministro finito de energía contenida en su batería, la energía es uno de los recursos clave que debe utilizarse con cuidado [51]. En el contexto de las nubes móviles, el costo de participación (como el consumo de energía) debe ser menor que el beneficio obtenido [52]. Además, permitirá que el dispositivo móvil tome las medidas apropiadas a nivel de componentes para minimizar el consumo innecesario de energía y, por lo tanto, alargar la vida útil del sistema mediante la descarga de componentes de software innecesarios, la redistribución de componentes intensivos en energía a hosts más ingeniosos y la colocación de hosts de comunicación frecuente sugerido en [53]. Por estas razones, ser consciente del uso de energía de un dispositivo es vital.

2.2.2.4 Gestión de datos

Para muchos usuarios y proveedores de la nube, la administración de datos en la nube plantea muchas complicaciones. En mobile cloud computing, como sugiere el propio nombre, los datos que normalmente eran del dominio del autor de éstos ahora estan en un ambiente en el que pueden ser accesibles o compartidos con varios usuarios. Para muchos usuarios móviles, esto plantea cuestiones de privacidad y seguridad. Sumado a esto el asunto de la representacion de datos en dispositivos móviles varía, y en una nube móvil heterogénea, esto conduciría a problemas con la portabilidad y la interoperabilidad. Los cálculos en una nube móvil se extenderían a través de un sistema de archivos distribuido, donde varios dispositivos podrían tener que acceder y modificar archivos.

Además, se debe tener en cuenta el acceso a archivos desde móviles a través de redes inalámbricas. En una nube móvil, las ubicaciones geográficas de los usuarios no son fijas y el ancho de banda debe conservarse debido a los costes de acceso a los datos. Sin embargo, también es vital que las bases de datos móviles contengan políticas para protegerse contra la pérdida de datos, al tiempo que garantiza que se ajusta a las restricciones de movilidad.

2.2.3 Ventajas en Mobile Cloud Computing

El cloud computing móvil proporcionará muchos beneficios y ventajas para los proveedores de cloud computing, operadores de redes móviles y consumidores de cloud computing tales como [54]:

- Compartir información y aplicaciones sin necesidad de hardware y software complejos y costosos, ya que el procesamiento de datos se ejecuta en la nube;
- Características y funcionalidades mejoradas de los dispositivos móviles a través de nuevas aplicaciones en la nube;
- Fácil acceso a MCC a través de un navegador móvil;
- Posibilidad de que una aplicación sea compartida y accedida por muchos usuarios de dispositivos móviles;
- Mayor alcance y difusión de aplicaciones de MCC;
- Aumento de la energía de la batería de los dispositivos móviles;
- Mejora de la capacidad de almacenamiento de datos y la capacidad de procesamiento, ya que MCC permitirá a los usuarios móviles almacenar / acceder y procesar los grandes datos como el modelado de la visualización de gráficos 3D y la animación en ecología, soluciones climáticas globales, riesgos financieros, Proyectos, etc., a través de las redes inalámbricas y móviles en la nube donde reside el sistema de computación de alto rendimiento (HPC);
- Mayor nivel de disponibilidad que el entorno Cloud Computing convencional;
- Mayor fiabilidad, ya que los datos y las aplicaciones informáticas se almacenan y copian en varios ordenadores; y
- Posibilidad de un sistema de aprendizaje a distancia en el entorno de MCC.

2.2.4 Riesgos de Mobile Cloud Computing

La seguridad de las transacciones financieras, las aplicaciones empresariales y el acceso no autorizado, que se ejecutan desde una ubicación remota y la transmisión de información por aire, son los desafíos más complicados que deben abordar conjuntamente los desarrolladores de aplicaciones móviles, proveedores de servicios de red inalámbrica y departamentos de TI.

Adicionalmente instituciones como la Cloud Security Alliance [55]han planteado las vulnerabilidades más comunes para ambientes mobile computing y cloud computing, ente los que figuran:

- Pérdida de datos de dispositivos perdidos, robados o desmantelados.
- Información que roba el malware móvil
- Pérdida de datos a través de aplicaciones de terceros mal escritas.
- Vulnerabilidades en dispositivos, SO, diseño y aplicaciones de terceros.
- Wi-Fi no seguro, acceso a la red y puntos de acceso inseguros.
- Los mercados de aplicaciones no garantizados o fraudulentos.
- NFC y la piratería basada en la proximidad.
- Brechas de datos.
- Gestión insuficiente de identidades, credenciales y acceso.
- Interfaces y API no seguros.
- Vulnerabilidades del sistema.
- Secuestro de cuenta.
- Empleados maliciosos.
- Vulnerabilidades de tecnología compartida.

Adicionalmente también están los temas de gobierno, riesgo, recuperación de desastres, seguridad física, consideraciones legales, respuesta a incidentes e investigación que son temas igual de importantes y que pueden ser temas de estudio e investigación.

2.3 Estándar ISO 25000 (SQuaRE)

ISO es la Organización Internacional de Normalización [56] y es la entidad internacional encargada de favorecer normas de fabricación, comercio y comunicación en todo el mundo.

La norma ISO 25000 es la evolución de las normas ISO/IEC 9126 Y 14598 debido a la necesidad de evolución en la forma de evaluar el software por ello se consiguió que sea una guía para el uso de las nuevas series de estándares internacionales llamados: Requisitos y Evaluación de Calidad de Productos de Software (SQuaRE).

Entre sus objetivos está el permitir una mayor eficacia en la definición del software, para ello plantea la evaluación de productos intermedios consiguiendo al final una mejora en la calidad del producto.

Esta familia de normas ISO/IEC 25000 se encuentra compuesta por cinco divisiones. Como se muestra en la Figura 2-6 a continuación

Figura 2-6 Organización de las series SQuaRE.

2.3.1 Características y Atributos de Calidad de SQuaRE

El modelo de calidad representa la piedra angular en el cual se cimientan las características de calidad que se van a tener en cuenta para la evaluación de las propiedades del software.

La calidad de producto software será el grado en el cual el usuario percibe que se satisfacen los requisitos de calidad aportando de esta manera un valor. Siendo a su vez estos requisitos los que se encuentran representados en el modelo de calidad definido por el estándar ISO/IEC 25010 (2011) que se encuentra compuesto por ocho características que se muestran en la Figura 2-7 y se describen a continuación

Figura 2-7 Norma ISO/IEC 25010 [57]

Como se ha podido observar el estándar SQuaRE tiene detallado una serie de características y sub-características que completan la norma. Para los fines del presente trabajo se seleccionó la característica de Seguridad.

2.3.2 Característica de Seguridad.

Según ISO 25010 [58] la característica de seguridad la define como: "Capacidad de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos". La misma que se subdivide a su vez en las siguientes sub-características:

Confidencialidad. Capacidad de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente.

Integridad. Capacidad del sistema o componente para prevenir accesos o modificaciones no autorizados a datos o programas de ordenador.

No repudio. Capacidad de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente.

Responsabilidad. Capacidad de rastrear de forma inequívoca las acciones de una entidad.

Autenticidad. Capacidad de demostrar la identidad de un sujeto o un recurso.

Capitulo 3. Estado del Arte.

En este capítulo se muestran los estudios que se han realizado a lo largo de esta tesina para de esta manera tener una visión global sobre la Evaluación de Seguridad para Mobile Cloud Computing (MCC).

En primer lugar, se detallará el método aplicado para la recolección de la información que será útil en el presente capítulo.

En la sección 3.2 se presenta un mapeo sistemático sobre la Seguridad para Aplicaciones de Mobile Cloud Computing, en donde se han analizado aspectos relacionados a la seguridad, el tipo de enfoque, el tipo de validación de los estudios, en qué ámbito se usan estas aplicaciones, los riesgos y amenazas a los que están sujetos las plataformas basadas en Cloud.

3.1 Introducción a los Estudios de Mapeos Sistemáticos de la Literatura.

El método elegido, que consiste en un mapeo sistemático de la literatura, se basa en la metodología propuesta por [59], [60], que tuvo sus raíces en revisiones bibliográficas realizadas en el campo de las Ciencias Humanas y la Medicina, pero en los últimos años se han propuesto adaptaciones para otras disciplinas como la ingeniería.

Un mapeo sistemático en el área de la ingeniería del software es un método para construir un esquema de clasificación y estructurar un campo de interés en la ingeniería del software. El análisis de los resultados se centra en frecuencias de publicaciones por categorías [61].

El fin de un mapeo sistemático es el de identificar las áreas en las cuales es necesario conducir una revisión sistemática.

El proceso completo de un mapeo comprende tres fases: 1) Planificación de la búsqueda, 2) Conducción de la búsqueda y, 3) reporte de resultados. Ver Figura 3-1.

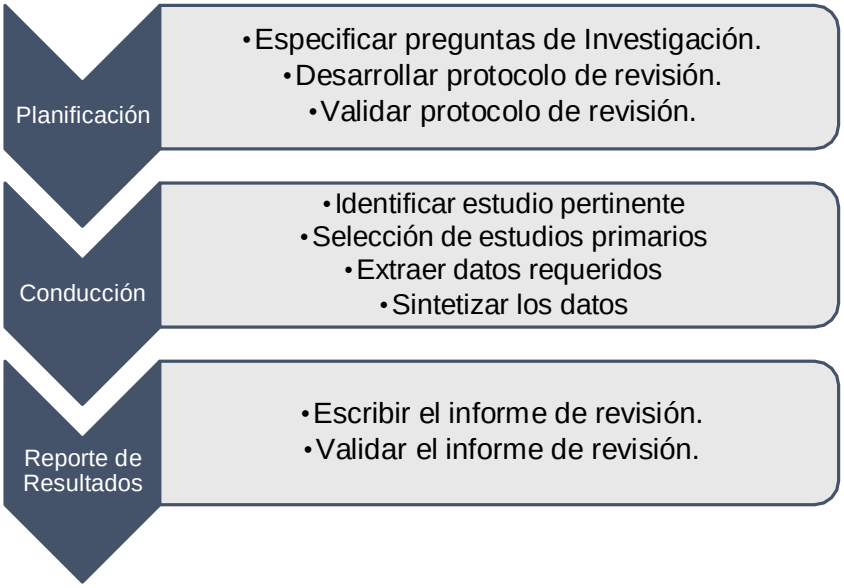


Figura 3-1 Proceso completo Revisión Sistemática.

3.2 Mapeo Sistemático sobre la seguridad de aplicaciones MCC

Con el fin de elaborar un estado del arte preciso se ha realizado una exhaustiva búsqueda sobre los estudios en cuanto a seguridad de aplicaciones para MCC. Para ello se ha empleado un método que permita ubicar toda la información actual mediante un Mapeo Sistemático.

Se va a realizar el mapeo sistemático basados en trabajos como [59], [62] donde se definen tres etapas:

- Planificación.
- Conducción.
- Informes.

3.2.1 Fase de Planificación.

La etapa de planificación está compuesta por seis pasos:

- Establecimiento de la pregunta de investigación y sub-preguntas.
- Definición de la estrategia de búsqueda.
- Selección de estudios primarios.
- Evaluación de calidad.
- Definición de la estrategia de extracción de datos.
- Selección de métodos de síntesis.

En esta fase fue donde se identificaron estudios relacionados a seguridad en Cloud Computing como [63], donde elabora un estado del arte de la seguridad pero enfocado al sistema Cloud sin adentrarse en las opciones móviles. Por otra parte se hallaron revisiones sistemáticas de la literatura como [64]–[66], donde se encontró valiosa información respecto a problemas en ambientes cloud y como se está llevando a cabo los estudios en plataformas cloud especializadas como Mobile Healtcare, sin embargo también centrados en las generalidades de Cloud Computing pudiendo mejorar los aspectos enfocados a seguridad fundamentalmente. Revisiones de la literatura así como encuestas para Mobile Cloud Computing como [67]–[69] también abordan los temas en cuanto a vulnerabilidades y las causas de la no adopción de este nuevo paradigma de trabajo y gestión.

Se puede señalar también que existen modelos de calidad basados en las perspectivas de cloud computing, o mobile cloud como se reseña en [69]–[73] entre otros, que plantean modelos y marcos de trabajo enfocados en distintos puntos de vista como la gestión, control sin embargo no se hallaron trabajos que resuman los resultados de una manera documentada los métodos de búsqueda, procesos de extracción o el análisis de datos y que adicionalmente estén enfocados en Seguridad específicamente para Mobile Cloud Computing.

Pregunta de Investigación

Siguiendo las guías ya antes mencionadas la meta del estudio es hallar como se están llevando a cabo los estudios en cuanto a seguridad en Mobile Cloud Computing, así como hallar las principales vulnerabilidades a las cuales están expuestas las aplicaciones basadas en estas plataformas, es así que la pregunta planteada es:

¿Cómo se enfoca la Seguridad de MCC y cuáles son posibles problemas en este campo?

Para responder a la pregunta de investigación, se ha propuesto 3 sub-preguntas que sirvieron de guía para consolidar un tema tan extenso como la seguridad en las aplicaciones MCC. Las preguntas son las siguientes:

RQ1: ¿Cómo se analizan los aspectos de seguridad en el campo de las aplicaciones para MCC?

RQ2: ¿Qué tipo de ataque de seguridad ocurre comúnmente en aplicaciones MCC?

RQ3: ¿Cómo se realizan las investigaciones de seguridad para las aplicaciones MCC?

La respuesta a estas preguntas de investigación proporcionara una visión general de los enfoques de investigación actuales y ayudara a identificar áreas de investigación no cubiertas por los artículos científicos encontrados hasta ahora. Además, las respuestas a las preguntas anteriores permiten construir una clasificación de amenazas de seguridad, técnicas de ataque, arquitectura y tipos de modelos de computación en la nube estudiados.

Estrategia de búsqueda

Este mapeo sistemático se llevó a cabo mediante una búsqueda electrónica en dos bibliotecas digitales: la Biblioteca Digital ACM y la Biblioteca Digital IEEE Xplore. Su objetivo es proporcionar una cobertura completa de las citas bibliográficas de todos los principales editores en el campo de la informática. Además, se realizó búsquedas manuales en varias conferencias y "workshops" con el fin de abarcar posibles estudios que aborden el tema motivo de esta investigación.

La metodología, que se utiliza para una cobertura completa, es realizar una búsqueda avanzada en estas bases de datos para acumular citas bibliográficas de los principales escritores de artículos científicos en el campo de mobile computing y cloud computing. Esta estrategia de búsqueda podría, inevitablemente, omitir algunos artículos útiles, por ejemplo, porque puede haber algunos autores que no están incluidos en estas bases de datos o que sus artículos son muy cortos o no muy importantes. Por otra parte, la comunidad de investigación ha mostrado interés en MCC progresivamente a partir de 2010 hasta la fecha, por lo tanto, es esencial articular la tendencia en MCC de investigación. Así, el período cubierto fue de los últimos seis años, es decir, los estudios publicados entre 2010 y 2016.

Para buscar automáticamente las bibliotecas digitales seleccionadas, planeamos utilizar la siguiente cadena de búsqueda descrita en la Tabla 3-1:

Tabla 3-1 Cuadro de búsqueda

Concept	Sub-String	Connector	Alternative Terms
Security	Secur*	and	Secure, Security
Mobile Cloud	Mobile Cloud	or	Mobile Cloud
MCC	MCC	And	MCC

Applications	Application	Or	Application*, App
Software	Software	Or	Software
Services	Service	and	Service, Services
Security AND (Mobile Cloud OR MCC) AND (Application OR Software OR Service)			

Adicionalmente, se ha buscado manualmente en las ediciones de las siguientes revistas, libros y conferencias como se muestran en las tablas Tabla 3-2 y Tabla 3-30:

Tabla 3-2 Conferencias y Workshops para búsqueda manual

CONFERENCE NAME	ACRONIM	CORE
International Conference on Computing, Networking and Communications	ICNC	B
International Conference on Advances in Mobile Computing and Multimedia	MOMM	B
Annual Computer Security Applications Conference	ACSAC	A
Computational Intelligence in Security for Information Systems	CISIS	B
IFIP International Information Security Conference	IFIP SEC	B
Information Security Conference	ISC	B
Information Security Practice and Experience Conference	ISPEC	B
International Workshop on Security	IWSEC	B

Tabla 3-3 Libros y revistas para búsqueda manual

SJR QUARTILE	JOURNAL NAME	RANK
Q1	ACM Transactions on Information and System Security	11
Q1	Pervasive and Mobile Computing	25
Q1	Computers and Security	31
Q1	Computer Journal	54

La búsqueda se realiza aplicando la cadena de búsqueda a los mismos metadatos (es decir, título, resumen y palabras clave) de cada artículo para todas las fuentes (la sintaxis de la cadena de búsqueda se adaptará para que se aplique en cada biblioteca digital).

Selección de estudios primarios

Cada estudio es recuperado de la búsqueda automatizada y evaluado con el fin de decidir si debe incluirse o no considerando su título, resumen y palabras clave. Las discrepancias en la selección se resolverán por consenso después de revisar el documento completo.

Se incluirán los estudios que cumplan al menos uno de los siguientes criterios de inclusión:

- Estudios que presentan aspectos de seguridad en aplicaciones de MCC.
- Estudios sobre ataques comunes a aplicaciones MCC.

Se excluirán los estudios que cumplan al menos uno de los siguientes criterios:

- Documentos introductorios para ediciones especiales, libros y talleres.
- Informes duplicados del mismo estudio en diferentes fuentes.
- Trabajos cortos con menos de cinco páginas.
- Artículos no escritos en idioma inglés.

Estrategia de Extracción de datos

La estrategia de extracción de datos empleada se basa en proporcionar un conjunto de respuestas posibles para cada sub-pregunta de investigación que se había definido. Esta estrategia asegura la aplicación de los mismos criterios de extracción de datos a todos los trabajos seleccionados y facilita su clasificación.

De acuerdo con lo anterior, se establecieron los criterios de extracción, que sirven para la clasificación de los artículos y estudios científicos. Los criterios se proponen considerando la pertinencia del tema en respuesta a las preguntas establecidas en las secciones anteriores.

Además, cada criterio se subdivide en varias opciones con las cuales mapear cada artículo. La clasificación de cada criterio se muestra a continuación en la Tabla 3-4

Tabla 3-4 Subdivisión Criterios de Extracción

RQ1: ¿Cómo se analizan los aspectos de seguridad en el campo de las aplicaciones para MCC?		
EC1	Modelo de Servicio	IaaS
		PaaS
		SaaS
		Secaas
		Xaas
EC2	Modelos de despliegue	Publico
		Privado
		Comunitario

		Hibrido
EC3	Características según NIST	Puesta en común de recursos
		Servicio medido para facturación
		Amplio acceso a la red
		Elasticidad rápida
		Autoservicio bajo demanda
EC4	Soluciones MCC existentes	Cloudlets
		CloneCloud
		Cuckoo
		Carmen
		Calling the cloud
		Clone2Clone
		Chroma
		Hyrax
		MAUI
		MAPCloud
		MobiCloud
		Scavenger
		Spectra
		SCAMPI
		ThinkAir
		VOLARE
		others
EC5	Modelos de Integración	REST
		SOAP
		Web Services
		Application Programming Interfaces (API)
		virtualization
		network infrastructure
EC6	Tipo de Encriptación	Encryption Public Key
		Encryption Private Key
RQ2: ¿Qué tipo de ataque de seguridad ocurre comúnmente en aplicaciones MCC?		
EC7	Ataques aplicaciones y servicios Web	SQL injection
		Cross-Site Scripting (XSS)
		Cross-Site Request Forgery (CSRF)
		session hijacking
		Distributed Denial of Service (DDoS)
EC8	Riesgos generales de seguridad en la nube que deben considerarse	Empleados maliciosos en el proveedor de CC
		Datos de localización
		Pérdida o pérdida de datos

		Secuestro de cuenta en línea
		Intercepción de datos: API insegura
		Spoofing - Pishing
		Ingeniería social
		Ataques de fuerza bruta
		Sniffer
		Infección por virus
		Hombre en el medio
EC9	Formas de expresar las necesidades de seguridad	SLA based
		Multi-model based
		VM_focussed
EC10	Seguridades a tener en cuenta para las aplicaciones	Aseguramiento del ciclo de vida de desarrollo de la app
		Abordar las amenazas comunes de seguridad
		Autenticación y control de acceso
		Cifrado de datos sensibles y críticos
		Rastreabilidad y no repudio
		normas de seguridad
EC11	Tipo de Seguridad	Seguridad del producto
		Seguridad del proceso
		Seguridad de datos
		Seguridad en uso
EC12	Subcaracterísticas Norma ISO 25010	Confidencialidad
		Integridad
		No repudio
		Responsabilidad
		Autenticidad
RQ3: ¿Cómo se realizan las investigaciones de seguridad para las aplicaciones MCC?		
EC13	Método de Validación	Experimentos
		Prototipo
		Caso de estudio
		Prueba de conceptos
		Encuesta
EC14	Entidad que Investiga	Industria
		Académico
EC15	Aspecto de la investigación	Seguridad de datos / archivos
		Seguridad de las aplicaciones móviles

Métodos de Síntesis

Hemos aplicado métodos de síntesis cuantitativos y cualitativos. La síntesis cuantitativa está basada en:

- Contar los estudios primarios que son clasificados en cada respuesta desde nuestro criterio.
- Definir gráficos de burbujas para mostrar las frecuencias de la combinación de resultados desde diferentes sub-preguntas de investigación. Un gráfico de burbujas es básicamente un eje x-y con burbujas en las intersecciones de las categorías. Este es útil para proveer un mapa y dar una rápida visión de un campo de investigación [53].

La síntesis cualitativa está basada en incluir algunos estudios representativos para cada criterio considerando los resultados de cada evaluación de la seguridad.

3.2.2 Fase de Conducción

Con la aplicación del protocolo de revisión daremos resultados preliminares. Los resultados se seleccionarán de acuerdo con los criterios de inclusión.

Aquí obtendremos una tabla en la que podemos resumir los resultados de la etapa de realización, la fuente de las búsquedas automáticas, los estudios potenciales y los estudios seleccionados.

En esta etapa pudimos encontrar algunos estudios que posiblemente se han publicado en más de una revista / conferencia y en este caso, seleccionaremos sólo la versión más completa del estudio. Casi pudimos encontrar algunos estudios aparecidos en más de una fuente. En este caso, deberíamos tener en cuenta una sola vez según nuestro orden de búsqueda, que es el siguiente: ACM, IEEE Xplore, etc.

La búsqueda para identificar los estudios primarios las bibliotecas digitales IEEE Xplore y ACM fue realizada el 9 de septiembre de 2016. La aplicación del protocolo de revisión trajo los siguientes resultados:

- En la búsqueda bibliográfica realizada a las bases de datos se identificaron 268 publicaciones (227 de IEEE Xplore y 41 de ACM). Luego de aplicar los

criterios de inclusión y exclusión documentados anteriormente, fueron finalmente seleccionados (78 de IEEE Xplore y 5 de ACM).

- En la revisión manual de la bibliografía de otras fuentes se encontraron 28 publicaciones potencialmente relevantes que después del proceso de extracción documentado nos quedamos con 8 estudios (2 de CISIS Y 6 DE IFIP SEC).

Algunos estudios han sido publicados en más de una revista/conferencia. En este caso, se ha seleccionado solamente la versión más completa del estudio. Los estudios que aparecen en más de una fuente fueron tomadas en cuenta solamente una vez y por regla se planteó que solo los artículos que se listan en la biblioteca digital IEEE Xplore.

3.2.3 Reporte de resultados

Un resumen de los resultados del estudio realizado se muestra en la Tabla 3-5

Tabla 3-5 Mapeo Sistemático. Resultados según criterios de extracción

Criterio	**Posibles Respuestas**	**#** Estudios	**%** Porcentaje
C1. Modelo de Servicio	IaaS	19	20.88%
	PaaS	54	59.34%
	SaaS	44	48.35%
	Secaas	28	30.77%
	Xaas	4	4.40%
C2. Modelos de despliegue	Public	16	17.58%
	Private	82	90.11%
	Community	6	6.59%
	Hybrid	24	26.37%
C3. Características NIST	Puesta en común de recursos	20	21.98%
	Servicio medido o facturación	4	4.40%
	Amplio acceso a la red	61	67.03%
	Elasticidad rápida	7	7.69%
	Autoservicio bajo demanda	10	10.99%
C4. Seguridad de red según ISO / IEC 27001 y GB / T22239	Seguridad Física	4	4.40%
	Seguridad del Entorno	52	57.14%
	Seguridad de la Red	34	37.36%
	Seguridad en host	7	7.69%
C5. Soluciones Mobile Cloud Computing Existentes	Cloudlets	3	3.30%
	CloneCloud	4	4.40%
	Cuckoo	2	2.20%
	Carmen	0	0.00%
	Calling the cloud	0	0.00%
	Clone2Clone	0	0.00%
	Chroma	0	0.00%
	Hyrax	1	1.10%
	MAUI	5	5.49%
	MAPCloud	0	0.00%
	MobiCloud	3	3.30%
	Scavenger	0	0.00%
	Spectra	0	0.00%

	SCAMPI	0	0.00%
	ThinkAir	3	3.30%
	VOLARE	0	0.00%
	others	2	2.20%
C6. Modelo de integración	REST	3	3.30%
	SOAP	1	1.10%
	Web Services	1	1.10%
	Application Programming Interfaces (API)	5	5.49%
	Virtualization	7	7.69%
	Network infrastructure	1	1.10%
C7. Tipo de cifrado	Encryption Public Key	20	21.98%
	Encryption Private Key	32	35.16%
C8. Ataques aplicaciones y servicios Web	SQL injection	0	0.00%
	Cross-Site Scripting (XSS)	2	2.20%
	Cross-Site Request Forgery (CSRF)	0	0.00%
	Session hijacking	24	26.37%
	Distributed Denial of Service (DDoS)	6	6.59%
C9. Riesgos generales de seguridad en la nube que deben considerarse	Empleados maliciosos en el proveedor CC	12	13.19%
	Localización de los datos	8	8.79%
	Perdida de datos	43	47.25%
	Robo de cuenta en línea	24	26.37%
	Intercepción de datos – API inseguras	25	27.47%
	Spoofing - Pishing	13	14.29%
	Ingeniería Social	5	5.49%
	Ataques de fuerza bruta	15	16.48%
	Sniffer	40	43.96%
	Virus Infection	10	10.99%
	Man in the middle	48	52.75%
C10 Formas de expresar las necesidades de seguridad	SLA based	5	5.49%
	multi-model based	0	0.00%
	VM_focussed	7	7.69%
C11. Seguridades a tener en cuenta para las aplicaciones	Ciclo de vida de desarrollo de software seguro	8	8.79%
	Abordar las amenazas comunes de seguridad	8	8.79%
	Autenticación y control de acceso	61	67.03%
	Cifrado de datos sensibles y críticos	45	49.45%
	Rastreabilidad y no repudio	30	32.97%
	Adopción de las normas de seguridad	5	5.49%
C12. Tipo de seguridad	Seguridad del producto	16	17.58%
	Seguridad del proceso	40	43.96%
	Seguridad de datos	20	21.98%
	Seguridad en uso	40	43.96%
C13. Subcaracterísticas Norma ISO 25010	Confidencialidad	73	80.22%
	Integridad	73	80.22%
	No repudio	32	35.16%
	Responsabilidad	22	24.18%
	Autenticidad	58	63.74%
C14. Método de Validación	Experimentos	8	8.79%
	Prototipo	5	5.49%
	Casos de estudio	5	5.49%
	Pruebas de Concepto	60	65.93%

	Encuestas	2	2.20%
C15. Entidad que Investiga	Industria	4	4.40%
	Academia	80	87.91%
C16. Aspecto de la investigación	Seguridad de datos / archivos	34	37.36%
	Seguridad de las aplicaciones móviles...	54	59.34%

Respecto al criterio C1 "Modelo de Servicio", los resultados indican que la mayoría de estudios enfocaban el modelo de servicio PaaS con un 59.34% seguido de un 48.35% de modelos SaaS, 30.77% para SecaaS y 20.88% para IaaS. Esto nos da muestras que los estudios se empiezan a interesar no solo en las plataformas sino también en las aplicaciones móviles para plataformas Cloud.

El criterio C2 "Modelos de despliegue", nos muestra que los mayores desarrollos los está haciendo la parte privada con un 90.11% de los artículos consultados. Esto se empata con el hecho que se ha convertido en una tecnología emergente y como un nicho de negocio es la parte privada, es decir las empresas, las que aprovechan estas nuevas formas de gestión.

Respecto al criterio C3: "Características NIST" se encontró que la mayoría de los artículos se enfocan en el acceso a la red con un 67.03%. Además, temas como la puesta en común de recursos obtuvieron un 21.98%.

Según el criterio C4: "Seguridad de red según ISO / IEC 27001 y GB / T22239" una de los principales temas sobre los que se trabaja en ambientes MCC es en la seguridad del entorno, con una valoración de 57.14%. También se ocupan en la seguridad de la red con 37.36% de artículos donde hacen referencia a estos criterios.

Respecto al criterio C5: "Soluciones Mobile Cloud Computing Existentes" los resultados fueron escasos. Se presume que debido a que son modelos que no están del todo desarrollados, en etapas de prueba o simplemente usan tecnologías cerradas no los pueden validar con la frecuencia necesaria para levantar estudios al respecto.

Según el criterio C6: "Modelo de integración" se obtuvo información respecto a las API y la virtualización como formas de integración con porcentajes de 5.49% y 7.69% respectivamente.

El criterio C7: “Tipo de cifrado” estableció que el 21.98% de los documentos consultados enfocan aspectos relacionados a la encriptación con clave pública para MCC mientras que 35.16% se enfocaron en encriptación por clave privada.

En lo que se refiere a tipos de ataques y vulnerabilidades de aplicaciones para mobile cloud computing resaltamos hallazgos como en el criterio C9 “Riesgos generales de seguridad en la nube que deben considerarse” el 47.25% de los artículos establecen que uno de las preocupaciones más recurrentes, es la perdida de los datos del usuario. Otro dato importante en este criterio fue que el 43.96% de los artículos se enfocan en riesgos vinculados a ataques de tipo Sniffer y un 52.75% en ataques relacionados a Hombre en el medio (Man in the Middle).

Respecto al criterio C12 “Tipo de Seguridad”, los resultados indican que la seguridad en proceso y la seguridad en el uso (ambos con un 43%) son los datos en los que más se enfocan los artículos y sus investigaciones, seguidos por la seguridad de los datos con un 21% de los artículos.

Según el criterio C13 “Subcaracterísticas Norma ISO 25010”, se relacionó que tanto la confidencialidad y la integridad, ambas con un 80.22% de artículos, son los temas más tratados y relacionados a seguridad MCC. La autenticación también es un tema muy discutido con el 63.74% de los artículos y en menor medida el no repudio y la responsabilidad.

Con respecto al criterio C14 “Método de Validación”, los resultados muestran que la mayoría de estudios (65.93%) han presentado Pruebas de conceptos para validar sus enfoques. También se halló que se realizaron pocos experimentos (8.79%), y en menor medida casos de estudio (5%), prototipos (5%) y apenas existen estudios que se sirvan de encuestas como métodos de validación.

Finalmente, en lo que respecta al criterio C15 “Entidad que Investiga” se encontró que 87.91% de los artículos revisados, corresponden a estudios realizados desde el área académica y la industria aporta apenas un 4.4% en investigación. Esto no quiere decir que la industria no esté generando investigación, al contrario, se plantea una interrogante alrededor de la pregunta, ¿Por qué la industria no está generando contenido formal respecto a seguridad MCC? La respuesta a esta pregunta podría ser tema de próximos estudios más centrados hacia este particular.

Para observar de manera más amigable los hallazgos del mapeo sistemático se optó por combinar criterios como el de la 0. A partir de la gráfica, podemos concluir que un gran número de investigaciones se centran en ataques como un hombre en el medio, Sniffer o secuestro de sesión y los riesgos consecuentes, así como preocupaciones referentes a la pérdida o fuga de la información. Teniendo en cuenta los modelos de implementación y modelos de servicio, ratificamos como se señaló anteriormente que las nubes privadas son las que acumulan más artículos en contraste con las nubes comunitarias que tienen un número mínimo de estudios. Por otro lado, SaaS y PaaS son los modelos de servicio más abordados, mientras que modelos como IaaS y XaaS casi no son analizados.

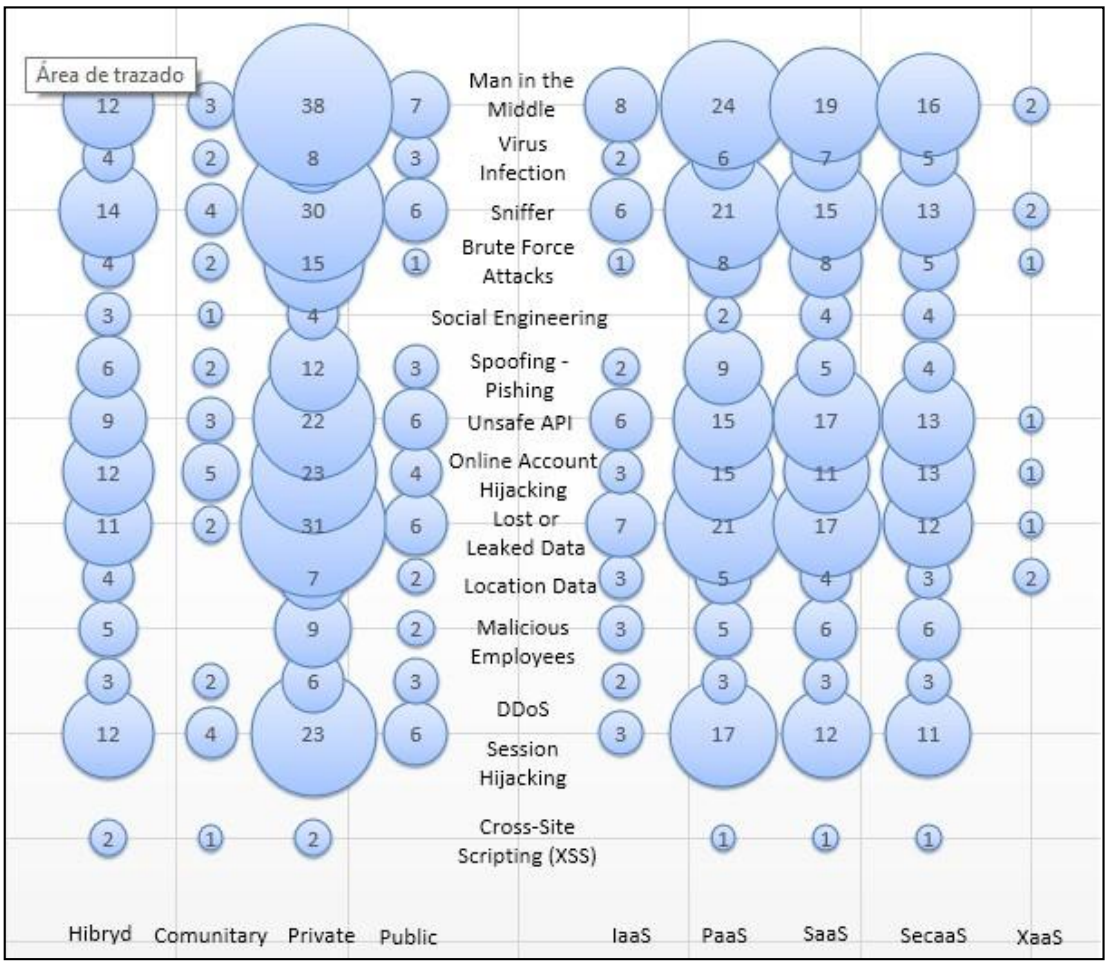


Figura 3-2 Comparación entre los criterios C1, C2 y C8-C9

En la Figura 3-2, Figura 3-3 y Figura 3-4 se muestras otra comparación entre criterios

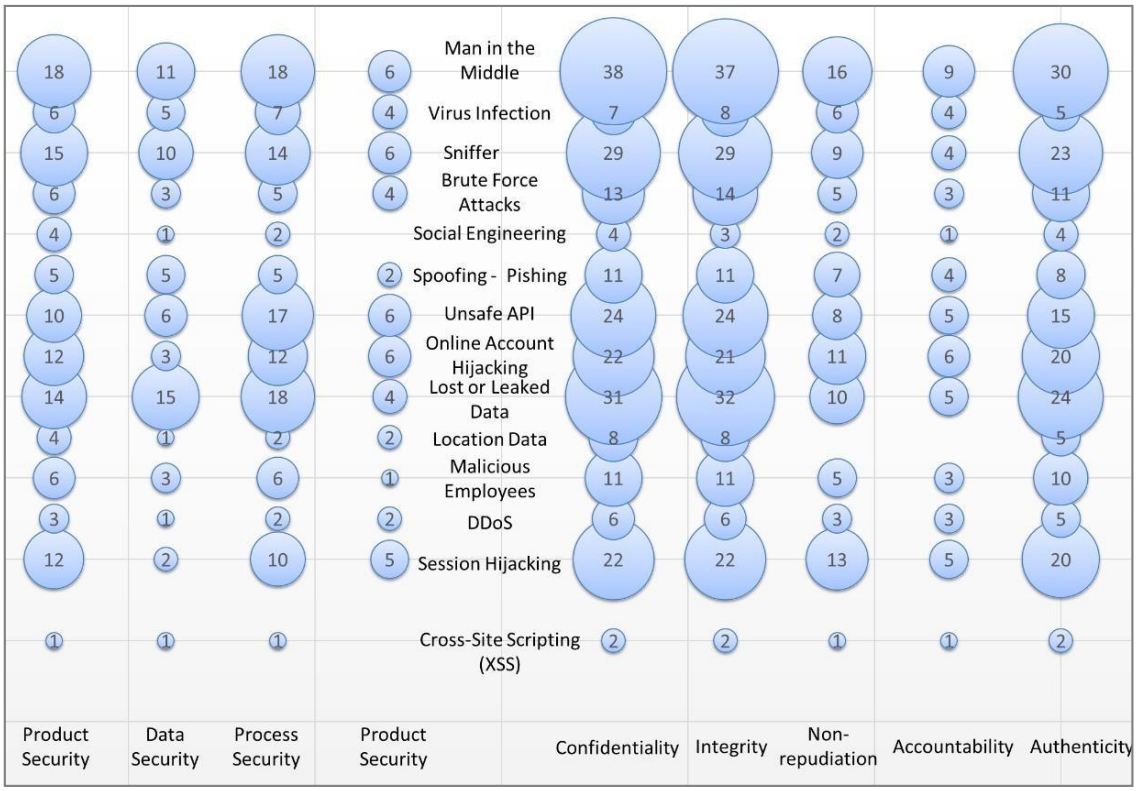


Figura 3-3 Comparación entre criterios C12, C13 – C8, C9.

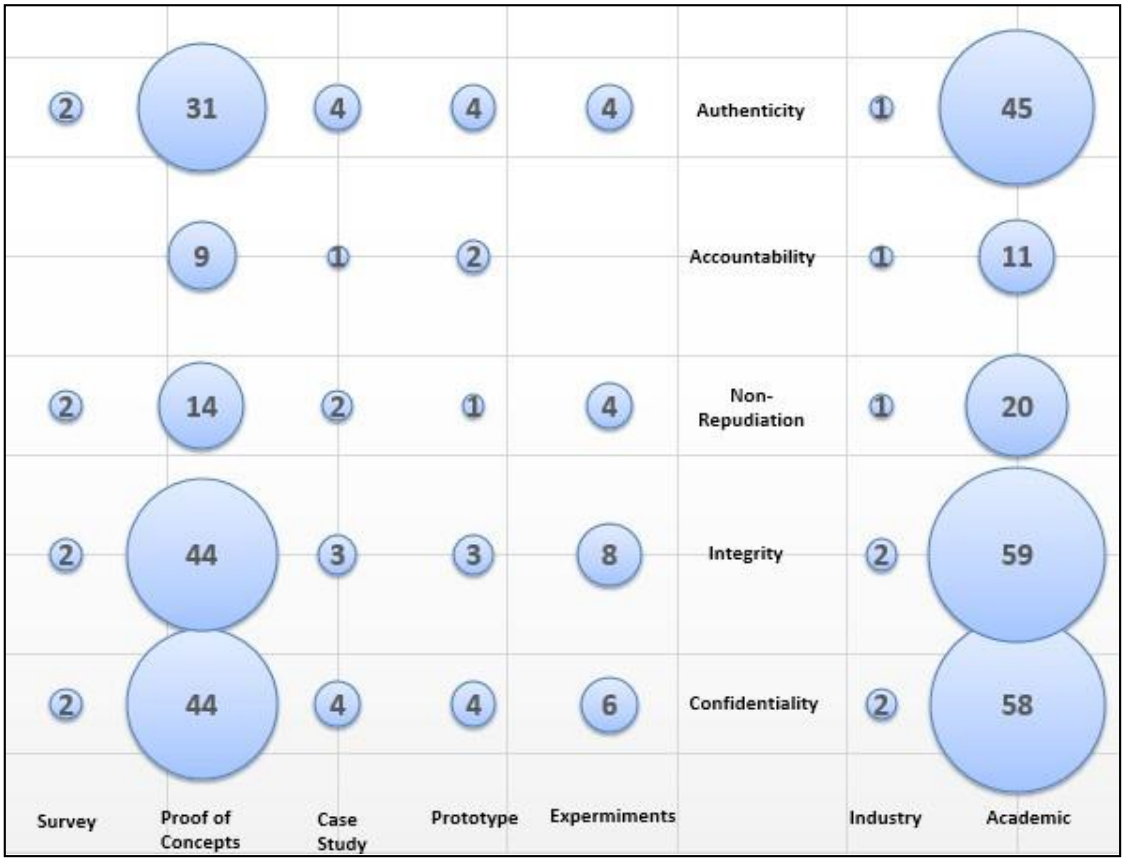


Figura 3-4 Comparación de criterios C13 vs C14, C15d

Dificultades en la Validación

Las principales dificultades de este estudio son: el sesgo en el ámbito de las preguntas de investigación, publicación y selección, la imprecisión en la extracción de datos y errores en la clasificación.

El ámbito de nuestra pregunta de investigación fue limitada a los temas referentes a la seguridad en aplicaciones SaaS para MCC. Sin embargo, existieron temas muy interesantes y que pudieron dejarse de lado debido a la relevancia de la publicación, el tamaño del articulo o la conferencia – revista en la cual esta publicada.

Los sesgos de publicación se refieren al problema de preferir los resultados positivos sobre los negativos para su publicación [74]. Se tiene conciencia de esta es una limitación inherente a las fuentes bibliográficas. Además, no se consideró otras fuentes bibliográficas tales como Springer Link o ScienceDirect lo que puede haber afectado a la completitud de nuestro mapeo sistemático. Además, nuestra búsqueda bibliográfica fue conducida en septiembre del año 2016, algunos estudios no estuvieron aún indexados en ese momento y pudieron no haber sido considerados.

Finalmente, se intentó aliviar la imprecisión en la extracción de los datos y la falta de una adecuada clasificación mediante la resolución de discrepancias por consenso.

Capitulo 4. Modelo de Seguridad para Mobile Cloud Computing

Con un crecimiento explosivo de las aplicaciones móviles y emergentes del concepto de computación en la nube, la MCC se ha convertido en una tecnología potencial para los usuarios de servicios móviles. MCC integra la tecnología de la computación en nube con el entorno móvil y ha tomado parte importante hilo de discusión en el mundo de las TI desde 2009. La ABI Research indicaba que se espera que el número de abonados a MCC crecería de 42,8 millones (1,1% del total de móviles usuarios) en 2008 a 998 millones (19% de los usuarios móviles totales) en 2014. A pesar de este hito alcanzado, el crecimiento de los suscriptores móviles de computación en nube es aún por debajo de las expectativas. El 74% de los ejecutivos de TI y los directores de información no están dispuestos a adoptar servicios en la nube debido a los riesgos asociados con la seguridad y la privacidad [75].. A pesar de los diversos esfuerzos para superar estos inconvenientes, hay una serie de lagunas y retos que aún existen en las políticas de seguridad de Mobile Cloud Computing [76].. Los problemas de seguridad en Mobile Cloud Computing incluyen principalmente la autenticación, autorización, seguridad de la aplicación, la privacidad de la ubicación y la seguridad de los datos.

Visión general de la arquitectura MCC y su seguridad

Hay varios modelos de servicios de computación en la nube. Huang, Xing y Wu [77] presentaron un estudio exhaustivo para establecer los modelos existentes de servicios de computación en la nube móvil. Su investigación distingue la construcción y la integración de dos entidades involucradas en MCC, el *cyber physical system* (CPS) y el cyber virtual system (CVS), en el que el CPS está principalmente compuesto por entidades inteligentes y móviles tanto físicas, y el CVS está formado principalmente por recursos y servicios virtualizados basados en la nube. Tradicionalmente, el cloud computing se ha clasificado en tres modelos de servicio: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS). Además, la computación en nube puede ser considerada desde varias perspectivas, estas perspectivas se basan en los roles de la participación del usuario. Hemos extrapolado estas perspectivas a MCC, considerando el punto de vista de sus actores (es decir, proveedores de servicios, consumidores y *bróker*).

En la Figura 4-1 se presenta el escenario que motiva nuestro modelo de seguridad. Aunque el mobile cloud computing tiene tres modelos de servicio, los servicios proporcionados por el modelo SaaS y sus interacciones con aplicaciones móviles se consideran en el modelo de seguridad presentado en este documento (es decir, enlazado por la línea puntiaguda). Además, no se tienen en cuenta las líneas de comunicación o los problemas de transmisión física.

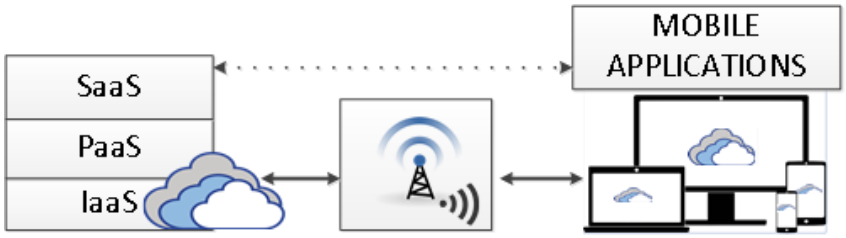


Figura 4-1 Mobile Cloud Computing security evaluation scenario

4.1 Un modelo de seguridad para MCC

Aquí se ofrece una descripción de las sub-características, atributos y métricas planteadas para la verificación de seguridad en Mobile Cloud Computing. Este modelo es una adaptación del estándar ISO / IEC 25000 SQuaRE [57], que se desglosa en sub-características y atributos, teniendo en cuenta las principales características de seguridad en las aplicaciones MCC relacionadas con la calidad del producto de las mismas. Por lo tanto, se adaptó la definición de estas sub-características y atributos, con el fin de adaptarlos a la naturaleza MCC.

Con el fin de construir el modelo de calidad, se consideró que la seguridad en Mobile Cloud Computing se puede validar desde tres perspectivas diferentes: (i) la aplicación de dispositivos móviles, (ii) la red física y (iii) la infraestructura de cloud computing. Para los fines de este estudio se opta por considerar al canal de comunicación o red física como un canal ideal además considerando que el método está basado en las aplicaciones y las posteriores validaciones serán desde la perspectiva del usuario final no se considera para el modelo la perspectiva del CSP (Cloud Service Provider).

A continuación, se muestran las sub-características que se adaptaron desde el modelo SQuaRE para la evaluación de MCC, con los atributos específicos relacionados con el dominio de aplicaciones MCC. Todos los atributos incluidos en el modelo de calidad deberían tenerse en cuenta durante la evaluación de las aplicaciones para garantizar su seguridad, sin embargo, cabe señalar que podrían existir escenarios en los

cuales no sea posible someter estos atributos a evaluación por las condiciones propias de la app y sus funciones intrínsecas.

Algo importante para la elaboración de este modelo, es que 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, EISA y otros). Todas orientadas a prevenir los principales problemas de seguridad en MCC como lo plantea [78] en su apartado de vulnerabilidades.

4.1.1 Confidencialidad (Confidentiality).

Según [58] la confidencialidad es el grado en que un producto o sistema permite que los datos sean accesibles solo por las personas autorizadas.

La primera subcaracterística del modelo de seguridad de MCC es la confidencialidad, que se desglosa en otras sub-características y atributos. La Tabla 4-1 **¡Error! No se encuentra el origen de la referencia.** muestra la sub-característica y sus a tributos específicos junto con la heurística de cada una.

El detalle completo de subcaracterísticas junto con atributos, así como controles y métricas con sus fórmulas de cálculo se muestran en el URL: https://mcc821.wordpress.com/2017/08/10/_trashed/

Tabla 4-1 Subcaracterísticas de Confidencialidad

Sub – Característica	Atributos	Heurística
1. Confidencialidad	1.1. Administración de Datos en el móvil	Medición del servicio de manejo de los dispositivos móviles implementado por el sistema MCC
	1.2. Control de accesos y gestión de identidades	Valoración de las características de control de accesos y la actividad de cada cuenta.
	1.3. Seguridad en SLA	Medición de las características elementales con las que debe contar un acuerdo SLA para MCC
	1.4. Calidad de encriptación	Opciones ideales en cuanto a encriptación en ambientes MCC
	1.5. Test de seguridad	Verificación de las pruebas mínimas que deben realizarse a aplicaciones móviles en ambientes MCC
	1.6. Manipulación de los datos del cliente	Validación de los controles a los que se someten los datos de los usuarios
	1.7. Prevención de ataques	Medición de las seguridades con las que debe contar un servicio MCC para prevenir ataques
	1.8. Gobierno y políticas BYOD	Validación de las condiciones que debe cumplir un terminal que pertenece al usuario final BYOD (Bring Your Own Device)

4.1.2 Integridad (Integrity)

Según [57] es la capacidad del sistema o componente para prevenir intrusiones no autorizadas a los datos o programas de ordenador. La Tabla 4-2 muestra los atributos junto con la explicación del control que realiza.

Tabla 4-2 Subcaracterística de Integridad

Subcaracterística	Atributos	Heurística
2. Integridad	2.1 Seguridad Complementaria	Se consulta sobre seguridades complementarias básicas respecto a instalaciones físicas del CSP
	2.2 Buenas prácticas de prevención	Se validan las precauciones que puede tomar un proveedor CSP para evitar posibles ataques a su integridad
	2.3 Seguridad en el desarrollo de código	Se verifican procedimientos en cuanto al desarrollo de aplicaciones móviles para MCC
	2.4 Notificación y respuesta de incidentes de seguridad	Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes
	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
	2.6 Auditorias	Se verifica las acciones ideales para temas de auditorías al servicio cloud
	2.7 Estado del Antivirus	Se mide los controles básicos que deben implementar respecto a los antivirus
	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

4.1.3 No Repudio (Non-Repudiation)

Según [79] el no repudio es el grado en que se puede demostrar que las acciones o eventos han sucedido, de tal forma que los eventos o acciones no pueden ser negados más tarde por parte del autor. La Tabla 4-3 muestra la descripción de los atributos y explicación correspondiente

Tabla 4-3 Subcaracterística de No Repudio

Subcaracterística	Atributo	Heurística

3. No Repudio	No Repudio	Se validan las distintas opciones con las que se puede evitar la negación de una acción por parte de su autor

4.1.4 Responsabilidad (Accountability)

Según la definición de la norma ISO 25010 la responsabilidad es el "grado en el que las acciones de una entidad pueden atribuirse únicamente a esta". La Tabla 4-4 muestra la descripción y atributo correspondiente a esta subcaracterística.

Tabla 4-4 Subcaracterística de Responsabilidad

Subcaracterística	Atributo	Heurística
4. Responsabilidad	Validación de Responsabilidad	Se mide la capacidad del sistema de controlar el tema de la responsabilidad

4.1.5 Autentificación (Authenticity)

Según [79] la autenticación es: "grado en el que la identidad de un sujeto o recursos pueden probar ser quien dicen ser." En la Tabla 4-5 se muestran los atributos junto con las descripciones vinculadas a los controles correspondientes.

Tabla 4-5 Subcaracterística de Autentificación.

Subcaracterística	Atributo	Heurística
5. Autentificación	Políticas de contraseña	Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad
	IDM Identity Management	se valida el cumplimiento de características de un servicio de gestión de identidades
	Contexto de uso	Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc.

Capitulo 5. Método de Evaluación de la Seguridad para aplicaciones de Mobile Cloud Computing.

En esta sección se define de manera detallada el método de evaluación de seguridad que será utilizada por los diferentes evaluadores, ya sea el comprador del producto o un evaluador independiente. Esto permite establecer la calidad del producto en cuanto a seguridad y el aporte de resultados serán consistentes y replicables. El método adapta y extiende las características propuestas en el estándar ISO/IEC 25040 con el fin de evaluar la calidad en la seguridad de aplicaciones para MCC.

La creciente tasa de adopción de sistemas basados en plataformas cloud computing sumado a los beneficios de la movilidad requiere de un proceso formal de evaluación de varias características inherentes a estas tecnologías. Al analizar la literatura, se encuentra que una de las principales preocupaciones de los stakeholders es lo concerniente a la seguridad.

Al hablar de stakeholders incluimos a desarrolladores, compradores, usuarios o clientes de aplicaciones móviles para cloud computing.

Es importante que las características de calidad en seguridad sean planteadas, monitoreadas y evaluadas basados en las mejores prácticas de seguridad, que a su vez sean ampliamente aceptadas. Los modelos de calidad en el SQuaRE nos sirven para validar estas características importantes para posteriormente establecer requerimientos de cumplimiento y satisfacción, así como las mediciones consecuentes.

Según la norma ISO el comprador es aquel que adquiere un producto de software, pudiendo ser este personalizado o no, y especifica los requisitos de calidad para el proveedor y evalúa una potencial adquisición bajo estos requisitos.

Los evaluadores independientes por otro lado deben evaluar los productos finales para asegurar la calidad. Para un enfoque de evaluación independiente se debe proporcionar requisitos y recomendaciones para la implementación práctica de la evaluación, donde las partes necesitan entender, aceptar y confiar en los resultados de la misma. Esta evaluación podría realizarse a solicitud del stakeholder sea éste un desarrollador, adquirente o cualquier otra parte.

En este apartado se diseñará el proceso de la evaluación y qué información será recolectada durante el mismo. Para poner en práctica el método de evaluación propuesto, se empleará como artefacto de entrada el modelo definido en el capítulo 4, el mismo que, como se ha comentado en secciones anteriores, y que tiene como base el estándar ISO/IEC 25010 [58].

Como se mencionó anteriormente, en este capítulo se presenta un método para la evaluación de la calidad, tomando de base el estándar SQuaRE, específicamente su división ISO 2504n en su versión 3 lanzada el 14 de junio de 2009, que consiste de los siguientes estándares:

- **Estándar ISO / IEC 25040 – Modelo de referencia de evaluación y guía**: contiene los requisitos generales para la especificación y evaluación de la calidad del software y aclara los conceptos generales. Proporciona una descripción de proceso para evaluar la calidad del producto de software y establece los requisitos para la aplicación de este proceso. El proceso de evaluación es la base para la evaluación de la calidad del producto de software para diferentes propósitos y enfoques.
- **Estándar ISO / IEC 25041 – Módulos de evaluación:** define la estructura y contenido de la documentación a ser usada para describir un módulo de evaluación. Estos módulos de evaluación contienen la especificación del modelo de calidad (por ejemplo, características, subcaracterísticas y las correspondientes métricas de calidad interna, externa o en uso), los datos asociados y la información sobre la aplicación planeada del modelo y de la información sobre su aplicación actual. Los módulos de evaluación apropiados son seleccionados para cada evaluación. En algunos casos puede ser necesario desarrollar nuevos módulos de evaluación.
- **Estándar ISO / IEC 25045 – Módulos de evaluación para la recuperación:** Provee la especificación para evaluar las sub-características de recuperación definidas bajo la característica de confiabilidad del modelo de calidad. Este determina las medidas externas de la calidad de software de resistencia y del índice de recuperación autónoma cuando el sistema de información esté compuesto de uno o más productos de software, la ejecución de las transacciones está sujeta a una

serie de distracciones. Una distracción puede ser un fallo operacional (por ejemplo, un apagado abrupto o un proceso de sistema operativo que haga caer al sistema) o un evento (por ejemplo, un incremento significante de usuarios al sistema).

5.1 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 & Sistema Process Engineering Meta-model Specification V2.0) [80], 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 adaptándole 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.

El Metamodelo SPEM 2.0 es un modelo basado en MOF (Meta Object Facility) que reutiliza otras especificaciones de OMG. Y que se dedica a definir, implementar, medir y mejorar proceso de la ingeniería de software.

SPEM se encarga de establecer procesos relacionados a la Ingeniería de Software. Es así como detalla los elementos mínimos necesarios que permitan definir dichos procesos sin añadir aspectos del dominio particular. La idea central de SPEM 2 está basada en tres elementos básicos: rol, producto de trabajo y tarea.

Tarea: Esfuerzo a realizar.

Rol: Quien realiza el esfuerzo.

Productos de trabajo: Entradas que se utilizan y salidas que éstos producen.

Por medio de estos elementos se puede especificar “Quien (rol) realiza qué (tarea) para desde unas entradas conseguir unas salidas (productos de trabajo)”.

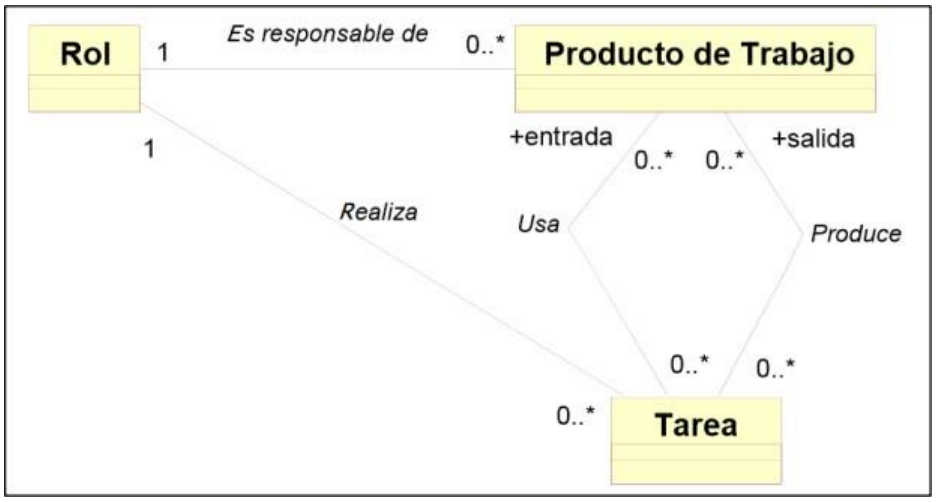


Figura 5-1 Metamodelo SPEM [81]

Según SPEM el subconjunto de primitivas de modelado más comúnmente usadas se muestra a continuación en la Tabla 5-1.

Tabla 5-1 Nomenclatura SPEM2

Icono	Nombre	Descripción
	Definición de Rol	Conjunto de habilidades, competencias y responsabilidades relacionadas, de un individuo o de un grupo.
	Definición de Tarea	Unidad de trabajo asignable y gestionable, identificando el trabajo que se ejecuta por los roles. Puede dividirse en varios pasos.
	Definición de Producto de trabajo	Producto usado o producido por las Tareas. Existen dos tipos de productos: Artefacto de naturaleza tangible (modelo, documento, código, archivos, etc.) y Entregable para empaquetar productos con fines de entrega a un cliente interno o externo. Se pueden asociar entre ellos mediante relaciones de agregación, composición e impacto.
	Categoría	Clasificación de elementos como Tareas, Roles y Productos en base a los criterios que desee el ingeniero de procesos. Existen diversos tipos de categorías: Conjunto de Roles (para Roles), Disciplina (para Tareas), Dominio (para Productos),
	Guías	Información adicional relacionada con otros elementos. Los sub-tipos de guías pueden ser (entre otros): Activo Reutilizable, Directriz, Documentación, plantillas. El icono presentado es genérico, pero se pueden emplear
	Uso de Rol Uso	Representación del rol que lleva a cabo una Tarea o Actividad dentro de un proceso determinado. Hace referencia a una Definición de Rol (elemento de Contenido).
	Uso de Tarea	Representación de una tarea atómica dentro de un proceso determinado. Hace referencia a una Definición de Tarea (elemento de Contenido).
	Uso de Producto de Trabajo	Representación de un Producto de Trabajo de entrada o salida, relacionado con una Actividad o Tarea. Hace referencia a una Definición de un Producto de Trabajo (elemento de Contenido)
	Actividad Fase Iteración	Representación de un conjunto de Tareas que se ejecutan dentro del proceso, junto con sus Roles y Productos asociados. Si únicamente se quiere representar una agrupación de tareas, se puede usar los elementos Actividad o Fase (incluido por retro-compatibilidad y más empleado en tareas de desarrollo), o bien si es un conjunto de tareas que se repite un determinado número de veces, se puede usar el elemento Iteración.
	Paquete de Proceso	Representación de un paquete agrupando todos los elementos del proceso

Ventajas de utilizar SPEM:

- Se puede disponer de modelos de Procesos de software en formato procesable por computador.
- Facilita la comprensión y comunicación entre las personas puesto que propicia un conocimiento homogéneo.
- Da soporte a la mejora de procesos. Da soporte a la gestión de procesos.
- Guía la automatización de procesos y da soporte para la ejecución automática.

5.2 Método de Evaluación con SPEM 2

Como primer paso para la definición de la aplicación del modelo de evaluación será especificar los parámetros iniciales de evaluación. Cabe señalar que las perspectivas desde las cuales se plantea evaluar la seguridad de aplicaciones para MCC, son las del punto de vista del comprador y del evaluador independiente. No se plantea realizar el análisis desde la perspectiva del desarrollador ya que se asumirá que se parte de una aplicación ya funcional y ya publicada como servicio SaaS.

Sin embargo, podemos graficar el proceso de construcción de dicha aplicación.

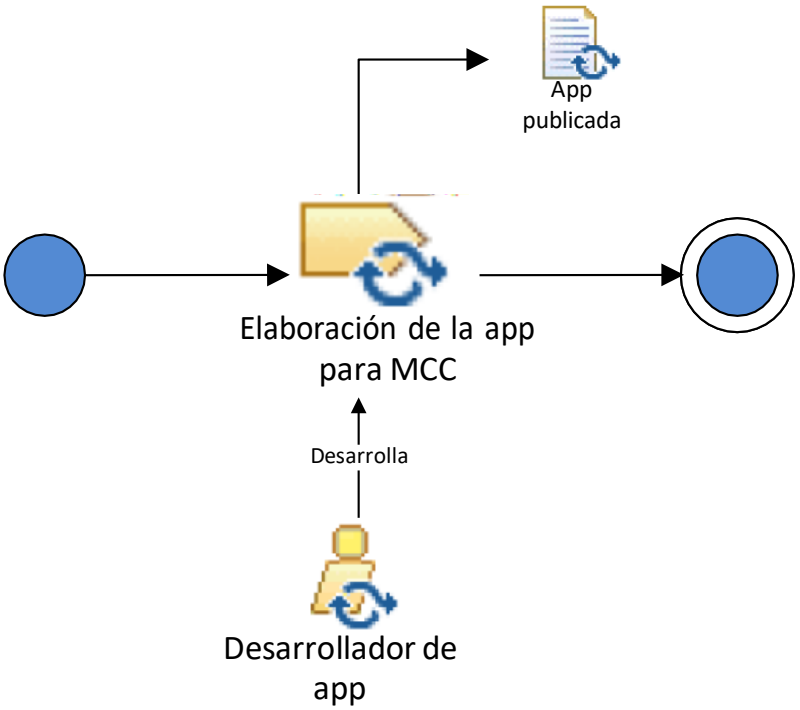


Figura 5-2 Proceso de construcción de una app

Como se definió anteriormente, el proceso de evaluación de la seguridad para aplicaciones para MCC parte desde el proceso de evaluación de calidad propuesto en el estándar 2504n considerando que cada fase del mismo se ha adaptado a las necesidades del producto aquí estudiado.

La división 2504n de la norma SQuaRE, propone un método de evaluación de la calidad basado en cinco fases principales detalladas en el siguiente gráfico:

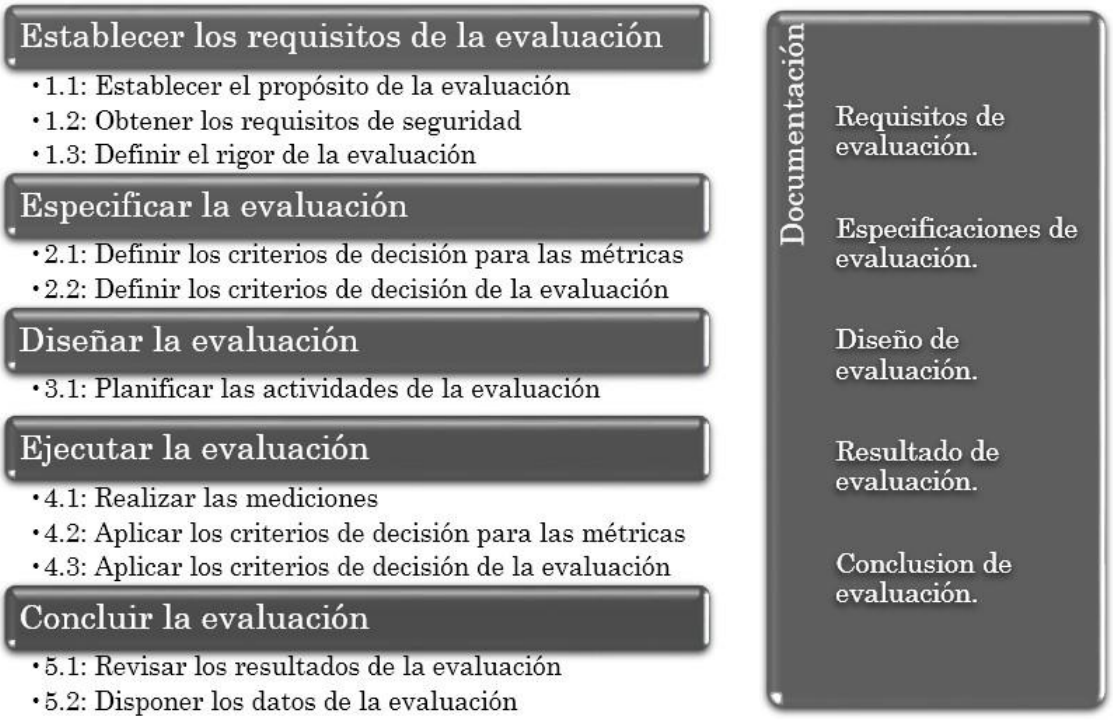


Figura 5-3 Pasos del proceso de evaluación de la seguridad de aplicaciones para MCC

Para el caso de las aplicaciones de MCC, se adaptó cada tarea descrita en la tabla anterior. A continuación, se presenta cada fase con sus respectivas tareas y su detalle en la Figura 5-4.

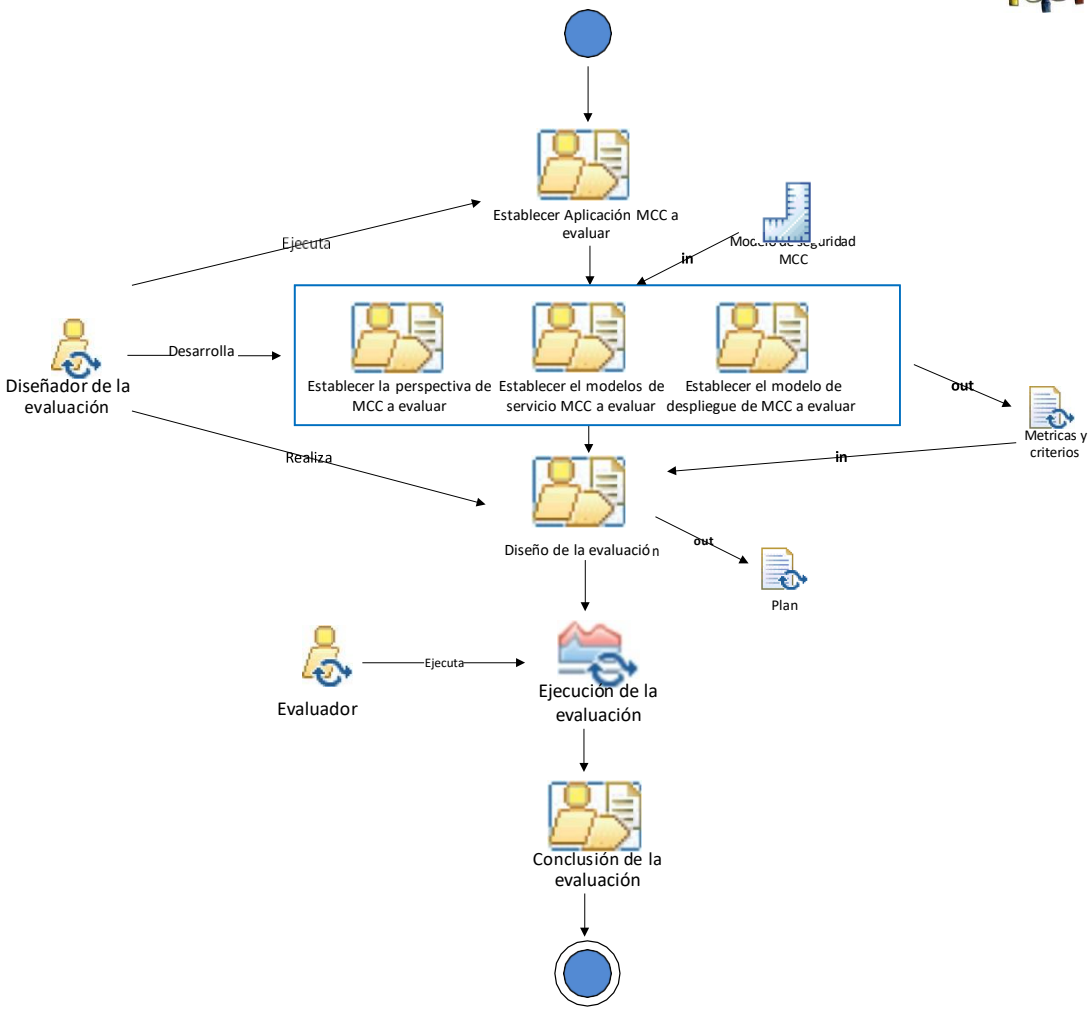


Figura 5-4 Proceso de evaluación de seguridad para aplicaciones.

5.2.1 Especificación de los Requisitos de Evaluación

Etapa en la cual se identifica y se declara explícitamente los requerimientos que se deben considerar previo al diseño de la evaluación de la seguridad. En la Figura 5-5 se muestran los diferentes procesos y salidas obtenidas en esta etapa.

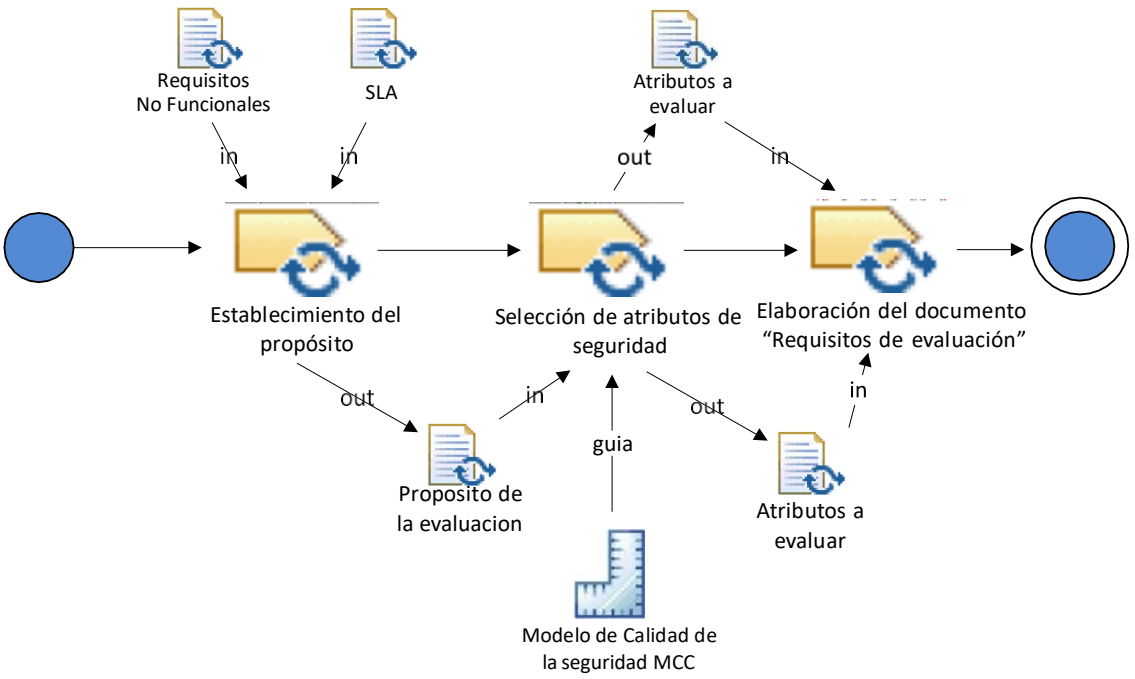


Figura 5-5 Especificación de los “Requisitos de Evaluación”

a) Establecimiento del Propósito de la Evaluación de la seguridad.

Esta tarea consiste en determinar que la evaluación se realizara el momento que el usuario final utilice el producto terminado es decir la aplicación SaaS para MCC. Para ello es necesario seleccionar la aplicación a evaluar y obtener el SLA como documentación formal para nuestra revisión.

b) Especificación de atributos de Seguridad.

Esta tarea consiste en especificar qué requisitos de calidad debe cumplir la evaluación, así como también quien los solicita.

- El evaluador debe asegurar que los stakeholders de la app sean identificados. Para ello se requiere la información necesaria para identificarlos a todos; los mismos que pueden ser una persona, parte u organización y pueden estar involucrados en la evaluación. Uno es un stakeholder como el desarrollador, adquiriente, usuario, etc. Otro es aquel que requiere la evaluación y necesita información sobre la calidad de software, patrocina la evaluación y requiere un reporte de la evaluación.

- Un artefacto importante a manera de guía será el Modelo de Calidad de la Seguridad desarrollado en secciones anteriores donde se seleccionarán las subcaracterísticas y los atributos a evaluar.

c) Elaboración del Documento de Requisitos de Evaluación.

Una vez reunida toda la información anteriormente detallada, se elaborará un documento que refleje los requisitos de la evaluación. Para ello se pueden usar plantillas, las mismas que contendrán la información de las tareas precedentes. En el Apéndice C, encontramos la Plantilla 1 Documento de Especificación de Requisitos de Evaluación.

5.2.2 Especificación de la Evaluación

En esta fase se especifica detalladamente la evaluación que se realizará, qué artefactos se van a evaluar, qué métricas se aplicarán y de qué manera, qué umbrales se considerarán adecuados para los resultados obtenidos, cómo se combinan los resultados y cómo se reportan los problemas que sean detectados.

En la Figura 5-6 se muestra las tareas a realizar en esta fase.

a) Selección de Atributos Por Evaluar.

En esta sección se escoge los atributos que serán sujeto de evaluación. Para ello tomamos como referencia nuevamente el modelo de calidad planteado en capítulos anteriores. Este nos brinda una serie de atributos que serán incluidos en el informe para la posterior verificación.

Los métodos de evaluación deberán ser documentados, teniendo en cuenta las acciones a ser ejecutadas para conseguir los resultados de la evaluación.

b) Selección de Métricas Por Emplear

Una vez fijados los atributos de seguridad que se evaluaran, el modelo de calidad definido anteriormente ayudara a establecer las correspondientes métricas asociadas a cada uno de estos atributos. Cabe recalcar que estas métricas se elaboraron basadas en una serie de buenas prácticas de seguridad a manera de checklist, cuya evaluación por cumplimiento brinda la información necesaria para la construcción de las métricas del atributo correspondiente.

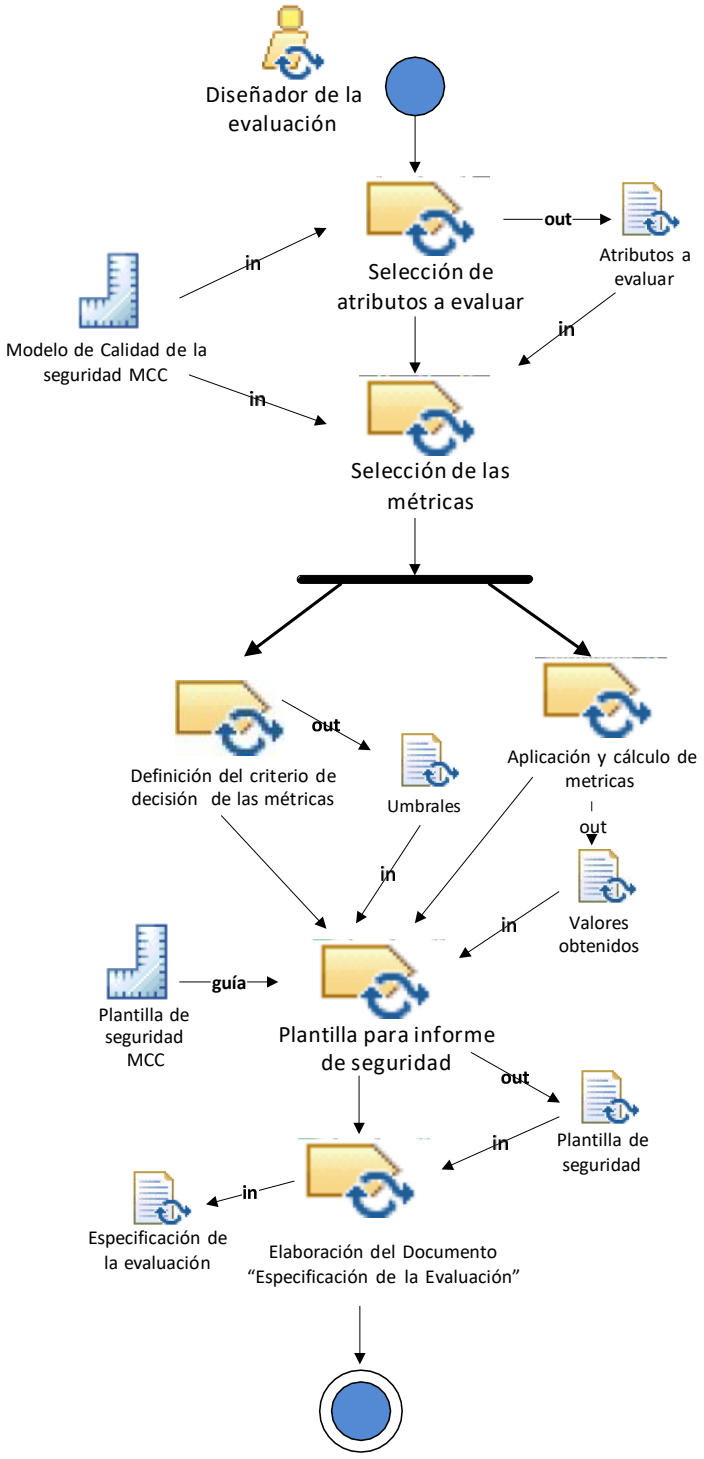


Figura 5-6 Especificación de la evaluación

c) Definición del Criterio de Decisión para las Métricas.

El criterio de decisión deberá ser establecido para las métricas seleccionadas.

Los criterios de decisión son umbrales numéricos usados para determinar el nivel de confianza en una aplicación analizada. Aquí se obtendrá una fórmula para calcular el estado de la app bajo evaluación.

Comúnmente en temas de seguridad se establecen practicas ideales para evitar incidentes de seguridad, sin embargo, asegurar una infraestructura o para el caso del presente trabajo una aplicación, al 100% es una realidad muy difícil de conseguir. Para ello se intenta abarcar la mayor cantidad de precauciones basados en estudios formales y en cierta medida en prácticas comunes del mercado sobre las vulnerabilidades del sistema, con esto se conseguiría disminuir el riesgo al mínimo. Por ello se han definido umbrales que pueden ser dinámicos y flexibles de acuerdo a las necesidades y al contexto de la aplicación MCC evaluada. Con esto se consigue que el método planteado no deje por fuera aplicaciones que, por tener umbrales de medición extremos, sean considerados como no aptos para su uso. Además, existe la conciencia que hay tecnologías MCC en el mercado, que no brindan mayor información por tratarse de un nicho de negocio y la confidencialidad de las empresas no lo permite, como se mostrara en el apartado de conclusiones.

d) Definición de la Plantilla para el Informe de Seguridad

Esta tarea consiste en diseñar un documento que presente los problemas de seguridad detectados para así emprender obtener elementos de juicio para consecuentes decisiones. El documento consta de los siguientes campos:

ID de la métrica	*XXX* Código único de identificación de la métrica bajo análisis
Nombre del indicador	Nombre del atributo en análisis.
Propósito del indicador	Explicación o heurística del atributo evaluado con las diferentes métricas y controles relacionados a cada uno.
Controles asociados	ID. Sub-característica / … / ID. Atributo. Campo donde se muestra las sub-características de las que proviene.
Perspectiva MCC	Se indica la perspectiva desde la que se está evaluando
Modelo de Despliegue	Se puede seleccionar si es MCC: Publico, Privado, Hibrido, Comunitario.
Modelos de Servicio MCC	Opciones de servicio a ser evaluado: IaaS, PaaS o SaaS
Formula	Descripción de la forma de calculo

Escala	Unidades de medida (ej. porcentaje)
Nivel para el cumplimiento	Resultado objetivo con el que el indicador o atributo es considerado como aceptable
Medición	Registro de los valores obtenidos de acuerdo al cumplimiento de cada uno de los controles verificados en cada atributo
Nivel de cumplimiento	Valoración numérica obtenida como resultado de la medición planteada.

5.2.3 Diseño de la Evaluación

Se formaliza el diseño de la evaluación, usando como entradas el resumen de la especificación de evaluación obtenido en la etapa anterior, como se observa en la 0.

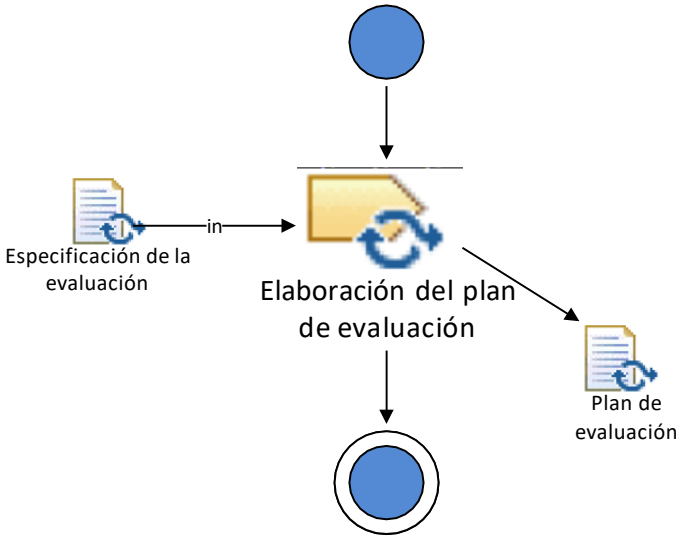


Figura 5-7 Diseño de la evaluación

a) Elaboración del plan de evaluación

En base a los requerimientos levantados en etapas anteriores se elabora un plan de evaluación de seguridad el mismo que debe evitar tareas duplicadas y definir puntos de decisión en el proceso de la evaluación el cual determina cuando y porque la evaluación puede ser considerada completada y debería parar. Esto debería ser hecho para disminuir el riesgo de errores y para reducir el esfuerzo de evaluación planeado.

5.2.4 Ejecución de la Evaluación e Informe de Seguridad

En esta fase con la obtención del plan de evaluación y las especificaciones de los atributos y métricas observadas se llevará a cabo la evaluación y posterior elaboración del informe con resultados respecto a la seguridad, proceso que se grafica en la Figura

5-8

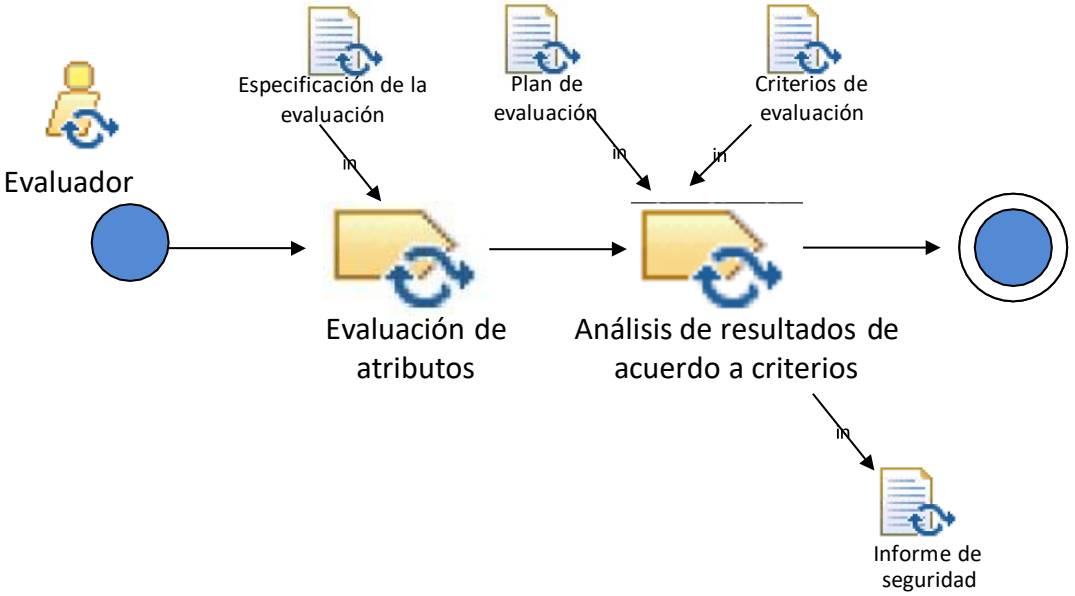


Figura 5-8 Fase "Ejecución de la evaluación"

Para la mencionada evaluación es importante considerar que éste es un proceso iterativo el mismo que puede repetirse según sea necesario. En esta fase se tendrá en cuenta dos tareas principales:

a) Evaluación por Atributos

En esta tarea se realiza la validación de los atributos de seguridad sobre la aplicación para Mobile Cloud Computing. Para esto se consulta los documentos que cada propietario a compartido en sus sitios web designados para ello. De esta manera se procederá a verificar cada ítem del checklist evaluando su cumplimiento o no. Con la información obtenida se podría ya elaborar un informe previo respecto al estado de la seguridad de la app evaluada, donde conste las novedades detectadas conforme a la plantilla elaborada en la fase de especificación.

b) Análisis de resultados de acuerdo a criterios

En esta fase se analiza los resultados obtenidos en cada atributo respecto a las especificaciones y criterios de evaluación elaborados en los apartados anteriores, luego del cual se podrá entregar un informe final sobre la seguridad de la aplicación.

Este informe debería:

1. Establecer un apropiado grado de confianza en el que la app es capaz de reunir los requerimientos de seguridad de la evaluación.

2. Identificar las oportunidades de mejora tanto en los requerimientos de la evaluación, así como posibles necesidades de evaluaciones adicionales para cuantificar estas oportunidades de mejora.

3. Identificar vulnerabilidades o riegos relacionados a la plataforma MCC.

4. Identificar documentación adicional complementaria a ser considerada para una nueva evaluación o auditoria.

c) Elaboración del Informe de Seguridad

Para esta etapa se procede con la elaboración del informe de seguridad el mismo que deberá incluir la plantilla de seguridad que incluirá el análisis de atributos, así como los criterios de evaluación que son tareas definidas en esta fase.

5.2.5 Finalización de la Evaluación

En esta fase se muestra en la Figura 5-9 las siguientes tareas:

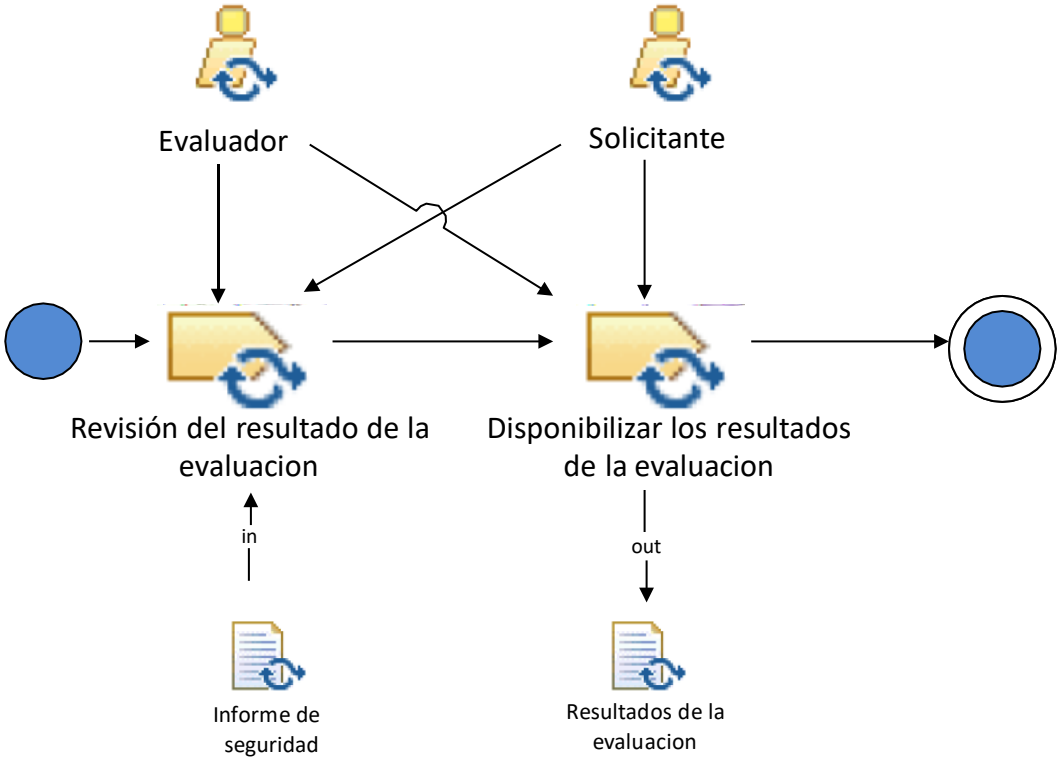


Figura 5-9 Finalizar la evaluación

a) Revisar el Resultado de la Evaluación

El evaluador y el que solicitó la evaluación debe llevar a cabo una revisión conjunta de los resultados de la evaluación.

Los comentarios del reporte de la evaluación deben ser dispuestos e incluidos en la versión final del reporte.

b) Disponer Datos de la Evaluación

Cuando la evaluación se ha completado, los datos y los ítems de evaluación deben ser dispuestos de acuerdo a los requerimientos del solicitante de la evaluación.

Capitulo 6. Aplicación del Método de Evaluación

En este capítulo se presenta la forma en la que el método de evaluación de seguridad aquí planteado puede ser puesto en práctica, para ello se ha puesto a modo de caso de estudio tres aplicaciones móviles basadas en Cloud Computing y que son las que más sobresalen en sus especialidades, para de esta manera proveer ejemplos que sirvan de guía para la evaluación de la calidad de la seguridad y den una idea clara de cómo poner en práctica cada una de las tareas que se encuentran en las fases de la evaluación.

En la sección 6.1 se presenta cada uno de las *app's* a evaluar, incluyendo una breve explicación sobre su funcionalidad.

En la sección 6.2 se presenta la aplicación del método de evaluación propuesto en este trabajo sobre cada una de las aplicaciones anteriormente citadas.

Por último, en la sección 6.3 se recogen las lecciones aprendidas tras la aplicación del método de evaluación y se hacen recomendaciones basadas en la experiencia de la ejecución del método de evaluación.

Cabe señalar que la metodología propuesta aplica tanto para aplicaciones públicas y privadas, por lo tanto, los controles y métricas planteadas se aplican indistintamente para los diferentes servicios MCC.

6.1 Aplicaciones Mobile Cloud Computing Por Evaluar

En esta sección se presentará una breve descripción sobre cada uno de los casos de estudio seleccionados para ejecutar la evaluación de la seguridad. Se tendrá en cuenta el tipo de *app's*, que funcionalidad tienen y qué servicios prestan al usuario.

6.1.1 Gmail (Plataforma Google)

Como primer ejemplo tenemos a Gmail de Google https://mail.google.com, que es el cliente de correo electrónico nativo de la empresa Google Inc. Google es por esencia la plataforma cloud de servicios integrados más relevante de los últimos años, debido principalmente a la importante incursión de su buscador en el día a día de las labores de millones de usuarios de computadores y dispositivos móviles.

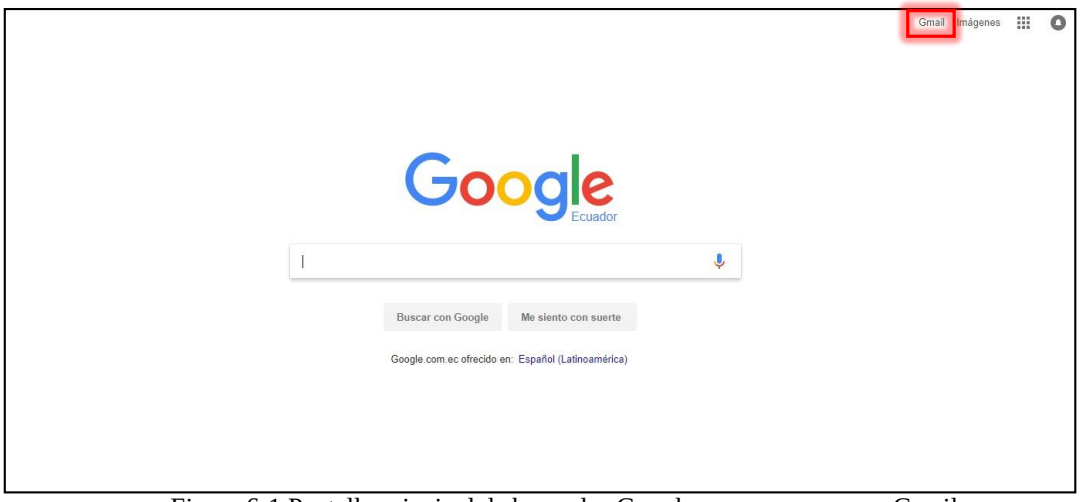


Figura 6-1 Pantalla principal de buscador Google y acceso a su app Gmail.

Según la Figura 6-1 podemos observar que por defecto aparece la opción del buscador de esta plataforma y en la parte superior derecha el acceso directo hacia su gestor de correo Gmail. Esto para computadores de escritorio o portátiles que ingresen por un navegador convencional sin embargo también cuenta con una app móvil.

Esta aplicación puede ser descargada directamente ingresando desde un dispositivo móvil a la aplicación Play Store, que es el mercado o almacén de aplicaciones exclusivo de los dispositivos con sistema operativo Android y de la tienda App Store para dispositivos con sistema operativo iOS de Apple.

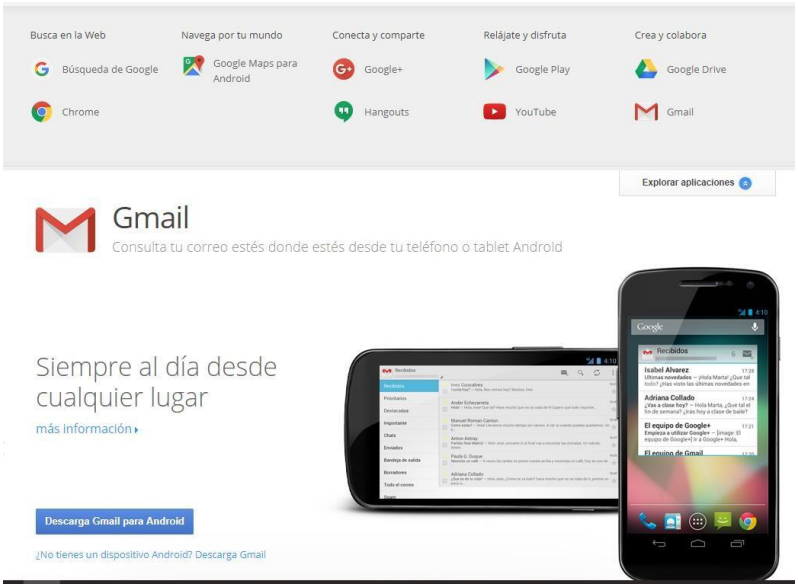


Figura 6-2 App Gmail de Google

Según la propia tienda Play Store, esta aplicación ha sido descargada cerca de cinco mil millones de veces ($5x10^9$) lo que brinda una idea del impacto de esta app en el mundo del cloud computing.

Google al ser una de las plataformas más utilizadas a nivel, tanto de computadores de escritorio como de dispositivos móviles, cuenta entre sus servicios con una plataforma Cloud donde se pudo encontrar la mayor información respecto a su modelo de seguridad Figura 6-3 aquí informa acerca de políticas, seguridad física, datos, gestión, etc.

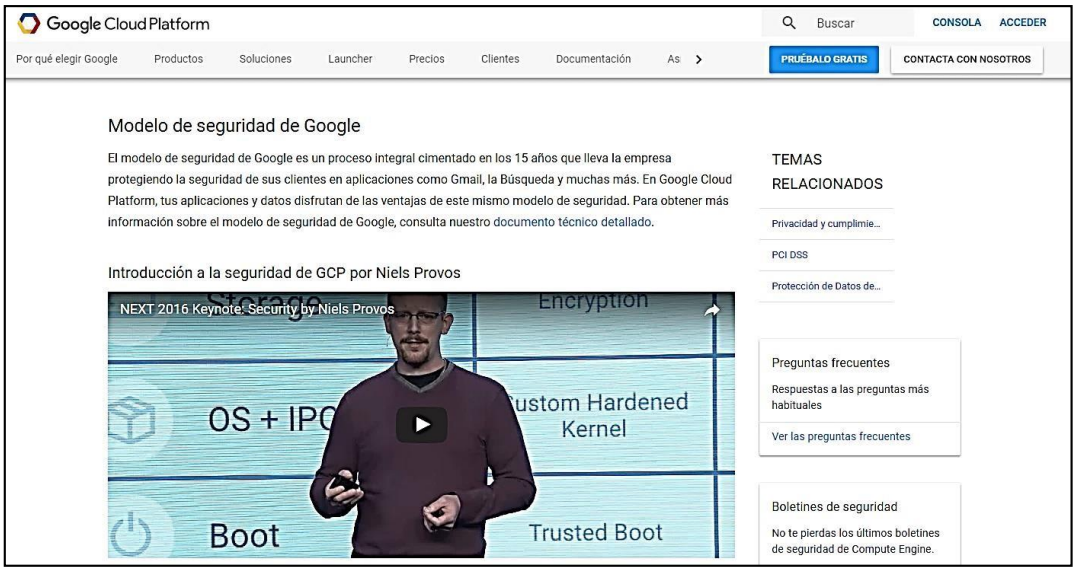


Figura 6-3 Google Cloud Platform y su apartado que trata de seguridad.

6.1.2 Office 365 (Microsoft)

Otra aplicación bajo análisis será Office 365 [9] , que encierra un paquete de utilitarios de la empresa Microsoft, estos son: Word, Excel, PowerPoint, One Note, etc. Y que en esta versión brinda al usuario la posibilidad de utilizar estas aplicaciones desde dispositivos de escritorio, así como en dispositivos móviles al basarse en una plataforma Cloud Computing.

[9] *https://www.microsoft.com/es-es/store/d/Office-365-Home/CFQ7TTC0K5DM/007R?icid=Cat-Office365-mosaic_linknav-1-home*

Figura 6-4 Portal Office 365

Este paquete de aplicaciones se puede utilizar de una manera independiente cada una, lo que hace que sea muy versátil para diversos dispositivos y requerimientos. Cada aplicación por su parte, al contar con una suscripción a office 365 funcionara en conjunto con la plataforma cloud de este proveedor simulando un ambiente de oficina en la nube móvil. En la tienda de aplicaciones para sistemas operativos Android (Play Store) cada aplicación suma más de cien millones ($100x10^6$) de descargas.

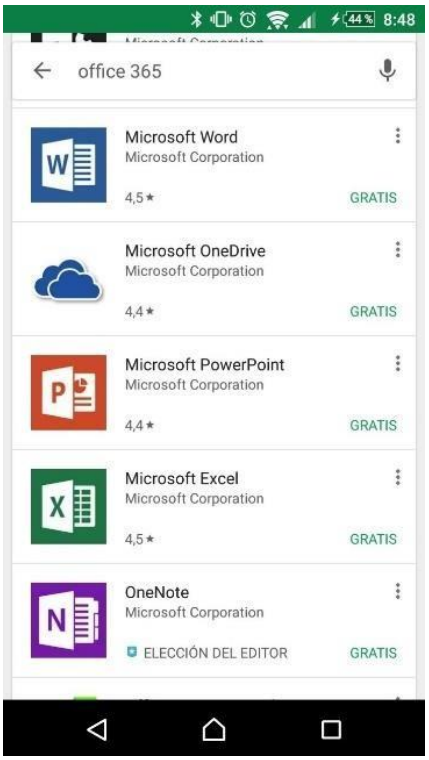


Figura 6-5 Paquete de aplicaciones de Office 365

En cuanto a lo referente a seguridad el portal de esta aplicación donde aborda estos temas es el de Microsoft Trust Center, en el apartado de "Seguridad de Microsoft Office 365"[10] y que se muestra en la Figura 6-6.

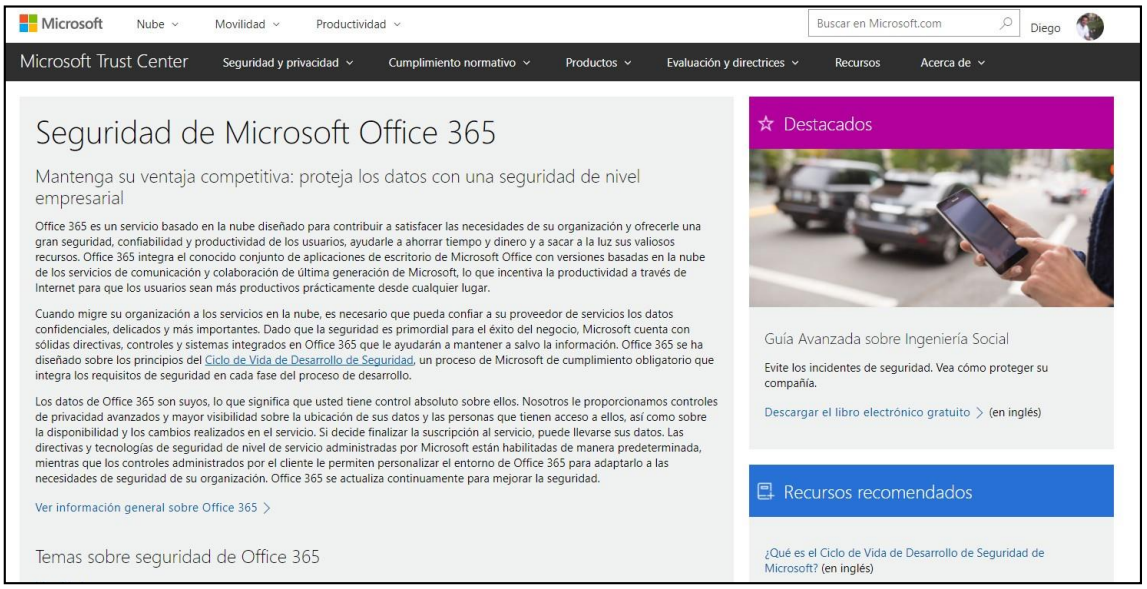


Figura 6-6. Portal Microsoft Trust Center – Office 365

6.1.3 Salesforce

Finalmente, se escogió la aplicación Salesforce[11] que es una de las principales plataformas de CRM [12] (Customer Relationship Management) y que basa su funcionamiento en la tecnología cloud. Salesforce tiene su propia app móvil Salesforce1 que recopila diferentes recursos de la plataforma principal para la administración de los temas vinculados a servicio al cliente, ventas, marketing y comunidades.

[10] *https://www.microsoft.com/es-xl/trustcenter/security/office365-security*
[11] *https://www.salesforce.com/mx/*
[12] *https://es.wikipedia.org/wiki/Customer_relationship_management*

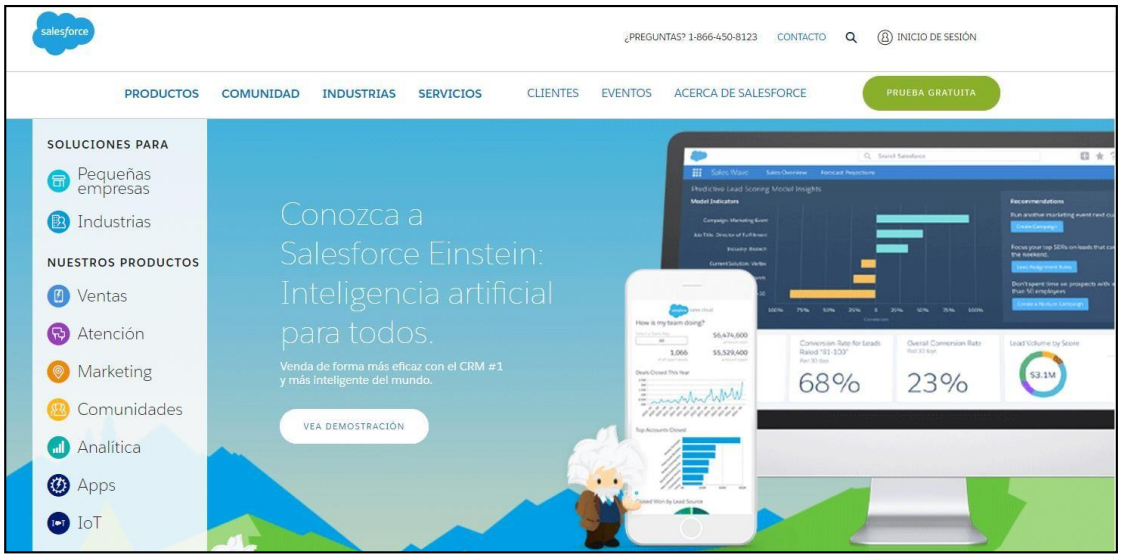


Figura 6-7 Portal Salesforce.com

Como se mencionó anteriormente la app móvil de esta plataforma se llama Salesforce1 disponible para descargas para los diferentes sistemas operativos móviles en App Store y Play Store. En esta última lleva alrededor de cinco millones ($5x10^6$) de descargas

Figura 6-8 Aplicación Salesforce1

En cuanto a los temas de seguridad vinculados a la plataforma y consecuentemente a la app Salesforce1, en la página Salesforce Trust[13] se encontró la información necesaria para el respectivo análisis, que motiva este trabajo en desarrollo.

6.2 Aplicación del Método de Evaluación de Seguridad

En esta sección se utilizará el método de evaluación propuesto en este trabajo en cada una de las aplicaciones antes mencionadas. Se presentará paso a paso cada una de las fases y sus tareas involucradas al momento de la evaluación, siguiendo la estructura presentada a continuación:

1. Requisitos de la evaluación.
2. Especificación de la Evaluación.
3. Diseño de la evaluación.
4. Ejecución de la evaluación e informe de usabilidad

Fase 1: Especificación de los Requisitos de Evaluación.

En esta fase definimos el propósito de la evaluación considerando las apps a evaluar, requisitos establecidos por los stakeholder y los atributos de seguridad de cada aplicación.

a) Establecimiento del Propósito de la Evaluación.

El objetivo es realizar una evaluación de la seguridad de la aplicación móvil cuya base de funcionamiento es una plataforma cloud computing, es decir, se evaluará las características de seguridad de la aplicación que se seleccionó.

b) Selección de los Atributos de Seguridad.

Los requisitos de seguridad son lo que debe cumplir la aplicación a modo de ejemplo tanto por el proveedor como por el usuario final, siendo estos dos los principales stakeholders envueltos en el método de evaluación descrito aquí.

[13] *https://trust.salesforce.com/es/*

Para ello utilizaremos los atributos planteados para aplicaciones MCC en el modelo de calidad propuesto en el capítulo 4, debido a que se quiere enfocar especialmente en este tipo de app´s.

Por tanto, los atributos a medirse están especificados en la Tabla 6-1 Atributos para evaluación de la seguridad de app´s para MCC:

Tabla 6-1 Atributos para evaluación de la seguridad de app´s para MCC

Atributos Por Evaluar	
1	1.1. Administración de Datos en el móvil
2	1.2. Control de accesos y gestión de identidades
3	1.3. Seguridad en SLA
4	1.4. Calidad de encriptación
5	1.5. Test de seguridad
6	1.6. Manipulación de los datos del cliente
7	1.7. Prevención de ataques
8	2.1 Seguridad Complementario
9	2.4. Notificación y respuesta de incidentes de seguridad
10	2.5. Gestión y control de cuentas de usuario
11	2.8. Gestión de contenido antispam / correo electrónico
12	5.1. Políticas de contraseña
13	5.3. Contexto de uso

c) Elaboración del Documento de Requisitos de Evaluación.

En esta tarea fijaremos un documento que refleje los requisitos de la evaluación, para ello elaboraremos una plantilla, que contendrá la información de los atributos que se analizaran en el método de evaluación.

Fase 2: Especificación de la Evaluación

En esta fase se especifica detalladamente la evaluación que se realizará, qué artefactos se van a evaluar, qué métricas se aplicarán y de qué manera, qué umbrales se considerarán adecuados para los resultados obtenidos, cómo se combinan los resultados y cómo se reportan los problemas que sean detectados.

a) Selección de Atributos Por Evaluar.

En esta sección se escoge los atributos que serán sujeto de evaluación. Para ello tomamos como referencia nuevamente el modelo de calidad planteado en capítulos

anteriores. Este nos brinda una serie de atributos que serán incluidos en el informe para la posterior verificación.

Los métodos de evaluación deberán ser documentados, teniendo en cuenta las acciones a ser ejecutadas para conseguir los resultados de la evaluación.

b) Selección de Métricas Por Emplear

Una vez fijados los atributos de seguridad que se evaluaran, el modelo de calidad definido anteriormente ayudara a establecer las correspondientes métricas asociadas a cada uno de estos atributos. Cabe recalcar que estas métricas se elaboraron basadas en una serie de buenas prácticas de seguridad a manera de checklist, cuya evaluación por cumplimiento brinda la información necesaria para la construcción de las métricas del atributo correspondiente.

Tabla 6-2 Métricas a ser evaluadas en el caso de estudio Gmail

Atributo	Métrica	Umbrales
1.1. Administración de Datos en el móvil	(Componentes MDM implementados) / (# total de componentes)	RANGOS: 1 a 0.75 = Ideal 0.625 a 0.375 = Mejorable menor a 0.375 = Deficiente
1.2. Control de accesos y gestión de identidades	(Controles implementados) / (# total de controles)	RANGOS: 1 a 0.692 = Ideal 0.615 a 0.308 = Mejorable menor a 0.308 = Deficiente
1.3. Seguridad en SLA	(Seguridades implementadas en el SLA) / (# total de seguridades SLA)	RANGOS: 1 a 0.667 = Ideal 0.583 a 0.333 = Mejorable menor a 0.333 = Deficiente
1.4. Calidad de encriptación	(Características implementadas) / (# total de características)	RANGOS: 1 a 0.75 = Ideal 0.625 a 0.375 = Mejorable menor a 0.375 = Deficiente
1.5. Test de seguridad	(Componentes de test implementados) / (# total de componentes)	RANGOS: 1 a 0.667 = Ideal 0.5 a 0.333 = Mejorable menor a 0.333 = Deficiente
1.6. Manipulación de los datos del cliente	(Seguridades de datos disponibles) / (# total de Seguridades)	RANGOS: 1 a 0.714 = Ideal 0.714 a 0.429 = Mejorable menor a 0.429 = Deficiente
1.7. Prevención de ataques	(Seguridades-prevenciones implementadas) / (# total de seguridades)	RANGOS: 1 a 0.786 = Ideal 0.714 a 0.357 = Mejorable menor a 0.357 = Deficiente
2.1 Seguridad Complementario	(Seguridades complementarias disponibles) / (# total de seguridades)	RANGOS: 1 a 0.6 = Ideal 0.5 a 0.3 = Mejorable menor a 0.3 = Deficiente

2.4. Notificación y respuesta de incidentes de seguridad	(Acciones implementadas) / (# total de acciones a implementar)	RANGOS: 1 a 0.714 = Ideal 0.571 a 0.286 = Mejorable menor a 0.286 = Deficiente
2.5. Gestión y control de cuentas de usuario	(Controles implementados) / (# total de controles disponibles)	RANGOS: 1 a 0.714 = Ideal 0.643 a 0.357 = Mejorable menor a 0.357 = Deficiente
2.8. Gestión de contenido antispam / correo electrónico	(Componentes implementados) / (# total de componentes)	RANGOS: 1 a 0.8 = Ideal 0.6 a 0.4 = Mejorable menor a 0.4 = Deficiente
5.1. Políticas de contraseña	(Políticas implementadas) / (# total de componentes)	RANGOS: 1 a 0.75 = Ideal 0.625 a 0.375 = Mejorable menor a 0.375 = Deficiente
5. 3. Contexto de uso	(Componentes implementados) / (# total de componentes)	RANGOS: 1 = Ideal menor a 1 = Deficiente

c) Definición del Criterio de Decisión para las Métricas.

Los criterios de decisión los vemos establecidos conjuntamente en la Tabla 6-2**¡Error! No se encuentra el origen de la referencia.** en la columna de "Umbrales".

d) Definición de la Plantilla para el Informe de Usabilidad

Para la presentación de problemas de usabilidad se usa una plantilla propuesta en el capítulo que especifica el método de evaluación.

Fase 3: 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, es la información respecto a seguridad que el dueño-creador de la aplicación pueda proveer. Se intento obtener información respecto de aplicaciones realizadas por empresas locales, sin embargo, como señalamos en apartados anteriores 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 obligó a de alguna manera sesgar la búsqueda de aplicaciones a analizar basándose en la disponibilidad de la información necesaria para este caso de estudio.

a) Plan de Evaluación

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.

Fase 4: Ejecución de la Evaluación e Informe de Seguridad

En esta fase se recibe la especificación detallada del plan de evaluación, así como los requisitos de calidad de la evaluación que se tienen ya disponibles, así también ya se han especificado las métricas para evaluar las apps y se pueden obtener los resultados para rellenar los informes correspondientes. Las tareas de esta fase son:

a) Evaluación por Atributos

Aquí se procede a realizar las validaciones de las características de seguridad vinculadas a cada atributo según lo planteado en el modelo de calidad. Estos atributos están divididos en varios ítems que se verificara si la aplicación las adopta o no, asignándoles una puntuación: Si = 1 y No = 0.

6.2.1 Evaluación de app Gmail

En este apartado se evaluará la seguridad de la app Gmail, considerando como guía el modelo de calidad planteado en el capítulo 4, donde se definió una serie de atributos con sus controles específicos y una métrica que engloba cada uno, para una valoración final.

1. Administración de Datos en el móvil

Aquí procedemos a analizar los controles que se considera importantes de implementar para un correcto programa de MDM. Estos controles se muestran a continuación en la Tabla 6-3 junto con el resultado de evaluación por cumplimiento o no de los mismos.

Tabla 6-3 Controles correspondientes el atributo 1.1.

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	El servicio es ejecutable en todos los sistemas operativos móviles	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	El sistema cuenta con opción de Bloqueo remoto	Evaluación por cumplimiento: (SI=1, NO=0)	0 *

3	El sistema tiene una opción de Borrado remoto	Evaluación por cumplimiento: (SI=1, NO=0)	1 *
4	Previene la transferencia no autorizada de información sensible hacia fuera del dispositivo	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Proporciona opciones de desactivación remota de los módulos de comunicación	Evaluación por cumplimiento: (SI=1, NO=0)	0
6	Ofrece inicio de sesión único (SSO) para todas las aplicaciones	Evaluación por cumplimiento: (SI=1, NO=0)	0
7	Informa a los administradores de seguridad cualquier intento de instalación de apps no autorizadas según listado documentado	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Posee opciones de implementación de geo vallas virtuales	Evaluación por cumplimiento: (SI=1, NO=0)	0

De la información relevante respecto a este atributo podemos señalar que la aplicación normalmente no tiene control sobre el dispositivo móvil que es en esencia lo más importante de un sistema de manejo de dispositivos móviles remoto. Sin embargo, se puede validar también que implementa seguridades basadas en estas características como el borrado remoto o bloqueo remoto, pero con la asistencia de todo el ambiente del sistema operativo Android. Para un sistema operativo diferente su alcance sería el de borrar la información retirando los permisos de acceso de manera remota.

El artefacto que resume el puntaje obtenido se adjunta a continuación en la Tabla 6-4

Tabla 6-4 Evaluación atributo 1.1 de Seguridad

ID de la métrica	1.1
Nombre del indicador	1.1. Mobile Data Management
Propósito del indicador	Se valora el servicio de manejo de los dispositivos móviles implementado por el sistema MCC
Controles asociados	1. Confidentiality/ Atributo: 1.1
Perspectiva MCC	Usuario: _X Proveedor:___Bróker:___Otros:
Modelo de Servicio MCC evaluado	IaaS: _____PaaS: _____SaaS: _X__Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:___Hibrido:___Comunitario:
Formula	(Componentes MDM implementados) / (# total de componentes)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	2
Nivel de cumplimiento	0.25

RANGOS:

1 a 0.75 = Ideal
0.625 a 0.375 = Mejorable
menor a 0.375 = Deficiente

Para este atributo que obtuvo un nivel de cumplimiento de 0.25 = 25%, según el rango planteado el nivel de cumplimiento es “Deficiente”.

2. Control de accesos y gestión de identidades

En este atributo lo que se busca es que se implemente las mejores prácticas de control de accesos y de la actividad de cada cuenta. Los controles planteados se observan en la tabla detallada a continuación.

N°	***Controles por evaluar***	***Medición***	***Resultados***
1	Cuenta con inventario de dispositivos móviles autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Alerta todos los ingresos de dispositivos móviles nuevos	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Revisa y deshabilita cualquier cuenta que no pueda asociarse con un proceso de empresa y/o propietario	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Calcula la incidencia de dispositivos no autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	N/A
5	Establece un proceso de revocado automático del acceso al sistema cloud deshabilitando cuentas inmediatamente después de la terminación de un vínculo con empleado o contratista.	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Supervisa regularmente el uso de todas las cuentas, desconectando automáticamente los usuarios después de un período estándar de inactividad	Evaluación por cumplimiento: (SI=1, NO=0)	0
7	Maneja un perfil de uso típico por usuario	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Monitoriza cambios en configuración o actividad de usuarios	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Monitoriza las sesiones en busca de actividades inusuales	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Valida configuración de dispositivos: autenticados y autorizados antes del acceso	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Implementa monitoreo del tráfico de datos por usuario	Evaluación por cumplimiento: (SI=1, NO=0)	0
12	¿Gestiona listas negras públicas?	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	Asigna a los dispositivos móviles autorización de acceso caducable	Evaluación por cumplimiento: (SI=1, NO=0)	1

Para este atributo señalamos que los controles parametrizados en esta aplicación no se pueden determinar que sean definitivos por el hecho que la aplicación no comparte cierta información, quizá por no considerarla relevante o por temas de políticas internas.

Tabla 6-5 Evaluación atributo 1.2 de Seguridad

ID de la métrica	1.2
Nombre del indicador	1.2. Control de accesos y gestión de identidades
Propósito del indicador	Valoración de las características de control de accesos y la actividad de cada cuenta.
Controles asociados	1. Confidentiality/ Atributo: 1.2
Perspectiva MCC	Usuario: _X_ Proveedor:_____Bróker:_____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____PaaS:_____SaaS: _X__Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:___Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	0.62

El resultado obtenido es de 0.62 es decir un 62% y de acuerdo a los umbrales planteados el cumplimiento de este indicador es “mejorable”.

RANGOS:

1 a 0.692 = Ideal

0.615 a 0.308 = Mejorable

menor a 0.308 = Deficiente

3. Seguridad en SLA

Aquí se validan características consideradas importantes y que debe contar un acuerdo SLA para MCC. Se considera un acuerdo de nivel de servicio valido para una aplicación pública y gratuita, a todos los ofrecimientos y garantías que ésta mantenga publicada en su página web. De esta manera se plantean los siguientes controles mostrados en la Tabla 6-6

Tabla 6-6 controles de evaluación atributo 1.3

N°	***Controles por evaluar***	***Medición***	***Resultados***
1	¿Permite auditorías externas y certificaciones de seguridad?	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿La normativa legal está acorde a la legislación del país del suscriptor del servicio?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	¿Provee información sobre incidentes de seguridad de manera periódica?	Evaluación por cumplimiento: (SI=1, NO=0)	1

4	Permite que los informes, registros y servicios de terceros se sometan a auditoría y revisión	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Informa acerca del tratamiento que se dará a los datos del cliente.	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Ofrece opciones en cuanto al formato de disponibilidad de datos aptos para móviles	# de formatos disponibles / total de formatos posibles	0
7	¿Establece garantías en la encriptación de los datos en reposo?	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Informa acerca del uso de canales de comunicación protegidos y cifrados en el caso de migración de servidores físicos, aplicaciones o datos a sistemas cloud	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Establece acciones por modificación unilateral del contrato	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Garantiza que los logs y los datos de los incidentes se gestionan de una forma centralizada	Evaluación por cumplimiento: (SI=1, NO=0)	0
11	¿Define por contrato la política de copias de seguridad?	Evaluación por cumplimiento: (SI=1, NO=0)	1*
12	¿Establece garantías respecto al aislamiento de los datos en reposo?	Evaluación por cumplimiento: (SI=1, NO=0)	1

Como se informó en párrafos anteriores esta app “Gmail” es pública y gratuita, al igual que otras aplicaciones del fabricante Google. Bajo ese escenario se elabora el control correspondiente, por lo tanto, no existe un contrato físico legal que sea firmado y reconocido por las partes involucradas.

Tabla 6-7 Evaluación atributo 1.3 de Seguridad

ID de la métrica	1.3
Nombre del indicador	1.3. Seguridad en SLA
Propósito del indicador	Valoración de las características de control de accesos y la actividad de cada cuenta.
Controles asociados	1. Confidentiality/ Atributo: 1.3
Perspectiva MCC	Usuario: _X_ Proveedor:____Bróker:____Otros: _____
Modelo de Servicio MCC evaluado	IaaS:____PaaS:____SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: X_ Privado:___Hibrido:___Comunitario: ____
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	0.67

De acuerdo a lo anteriormente establecido el cumplimiento de este atributo alcanzo el 0.67=67% que está dentro del rango como ideal

RANGOS:

1 a 0.667 = Ideal

0.583 a 0.333 = Mejorable

menor a 0.333 = Deficiente

4. Calidad de encriptación.

Se mide opciones ideales en cuanto a encriptación en ambientes MCC, varias de ellas se plantean más como recomendaciones en el ámbito del cifrado. Los controles planteados los vemos en la Tabla 6-8.

Tabla 6-8 Controles del atributo 1.4.

N°	***Controles por evaluar***	***Medición***	***Resultados***
1	Utiliza técnicas de cifrado fuertes (como AES-256, AES-192 o RSA)	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Utilizar formatos abiertos y validados, evitando en la medida de lo posible, el uso de técnicas de cifrado propietario.	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Usa controles de protección de claves como KEK90 (Clave de Cifrado de Claves) o equivalentes	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Evitar utilizar estándares antiguos de encriptación tales como Data Encryption Standard (DES)	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Utiliza técnicas de cifrado de red estándar incluyendo SSL21, VPNs22, y SSH23	Evaluación por cumplimiento: (SI=1, NO=0)	0
6	¿Utiliza Secure Sockets Layer?	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Transport Layer Security (TLS)	Evaluación por cumplimiento: (SI=1, NO=0)	1

Como se esperaba la información respecto al cifrado no estaba difundida al detalle, pero se hace alusión al uso de métodos de cifrado SSL y TLS. También se encontró que Gmail tiene certificaciones PCi DSS v3.1 y cumple auditorias como: SSAE16 / ISAE 3402 tipo II, ISO 270XX, lo cual garantiza el tema de cifrado de una manera indirecta. La Tabla 6-9 muestra el resultado de la evaluación

Tabla 6-9 Evaluación atributo 1.4 de Seguridad

ID de la métrica	1.4
Nombre del indicador	1.4. Calidad de encriptación
Propósito del indicador	Se mide opciones ideales en cuanto a encriptación en ambientes MCC

Controles asociados	1. Confidentiality/ Atributo: 1.4
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:___Otros: _____
Modelo de Servicio MCC evaluado	IaaS:___PaaS:___SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario: __
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	0.75

Según los rangos planteados el cumplimiento respecto a este atributo, un resultado de 0.75 = 75% equivale a "ideal".

RANGOS:

1 a 0.75 = Ideal

0.625 a 0.375 = Mejorable

menor a 0.375 = Deficiente

5. Test de seguridad

Se verifican las pruebas recomendables que deben realizarse a ambientes MCC. Para ello los controles se detallan en Tabla 6-10

Tabla 6-10 Controles a evaluar atributo 1.5

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Realiza test de penetración externos e internos de seguridad a los móviles	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Mantiene un detalle de los terminales en los que se realizan los test y los utilizan únicamente con esos fines de prueba	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Realiza pruebas a terminales móviles en los que involucre ingeniería social	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Realiza pruebas periódicas de verificación de acceso a aplicaciones no autorizadas	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Cuenta con un listado detallado de vulnerabilidades del sistema cloud	Evaluación por cumplimiento: (SI=1, NO=0)	1

6	Realiza test a los terminales móviles donde se validan los parches de seguridad necesarios	Evaluación por cumplimiento: (SI=1, NO=0)	1

En lo que se refiere a test de penetración la plataforma por si toma precauciones al respecto sin embargo también brinda la oportunidad de realizar pruebas de penetración sin necesidad de aprobaciones adicionales únicamente con el condicionamiento del cumplimiento de las Políticas de uso aceptable y de las Condiciones de servicio. Adicionalmente aclara que las pruebas a realizar deben afectar única y exclusivamente a los proyectos propios y no a los demás clientes. En la Tabla 6-11 observamos el artefacto con el que se obtuvo la calificación de la app.

Tabla 6-11 Evaluación atributo 1.5 de Seguridad

ID de la métrica	1.5
Nombre del indicador	1.5. Test de seguridad
Propósito del indicador	Se verifican las pruebas mínimas que deben realizarse a ambientes MCC
Controles asociados	1. Confidentiality/ Atributo: 1.5
Perspectiva MCC	Usuario: _X_ Proveedor:____Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:____PaaS:___SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: X_ Privado:___Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	3
Nivel de cumplimiento	50%

Para el rango medido se valida que el cumplimiento del atributo fue de 1=100% que equivale a “ideal”, principalmente por el tema de la apertura que la plataforma da para realizar pruebas y por las certificaciones que mantiene.

6. Manipulación de los datos del cliente

Se realiza una validación de los controles que se someten los datos de los usuarios, principalmente enfocados en la manipulación y eliminación de éstos. Para estas evaluaciones se plantean los controles de la Tabla 6-12

Tabla 6-12 Controles del atributo 1.6

N°	***Controles a evaluar***	***Medición***	***Resultados***

1	Brinda herramientas para etiquetado y clasificación de datos	Evaluación por cumplimiento: (SI=1, NO=0)	N/A
2	¿Entrega certificación de la destrucción por parte del proveedor de cloud computing o por un tercero?	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	¿Permite la portabilidad de la información a sistemas propios o de otros proveedores?	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Asegura que los datos no son recuperables mediante ningún medio forense informático	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Posee políticas y procedimientos para la eliminación segura y completa de los datos terminales móviles	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	¿Utiliza técnicas de borrado seguras para unidades de almacenamiento que serán reutilizadas?	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Cuenta con políticas y procedimientos para la eliminación segura de equipos móviles de los usuarios	Evaluación por cumplimiento: (SI=1, NO=0)	1

En la Tabla 6-13 se muestran la calificación obtenida

Tabla 6-13 Evaluación atributo 1.6

ID de la métrica	1.6
Nombre del indicador	1.6. Manipulación de los datos del cliente
Propósito del indicador	Se realiza una validación de los controles que se someten los datos de los usuarios
Controles asociados	1. Confidentiality/ Atributo: 1.6
Perspectiva MCC	Usuario: _X_ Proveedor:____Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:____ PaaS:____ SaaS: _X__Otros: _____
Modelo de Despliegue MCC evaluado	Publico: X_ Privado:___Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	5
Nivel de cumplimiento	86%

Se observa que alcanza una calificación de 0.86=86% lo que se adjudica un cumplimiento “Ideal” de acuerdo a los rangos planteados.

RANGOS:

1 a 0.714 = Ideal

0.714 a 0.429 = Mejorable

menor a 0.429 = Deficiente

7. Prevención de ataques

Se mide las seguridades con las que se recomienda debería contar un servicio MCC para prevenir ataques, los controles se muestran en la Tabla 6-14

Tabla 6-14 Controles a evaluar de atributo

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con un DLP junto con la gestión que esto implica	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿Presenta una certificación de seguridad conocida?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	CSP garantice que los logs y los datos de los incidentes se gestionan de una forma centralizada	Evaluación por cumplimiento: (SI=1, NO=0)	n/a
4	Configuración del sistema operativo se habilita sólo los puertos, protocolos y servicios necesarios para satisfacer las necesidades empresariales	Evaluación por cumplimiento: (SI=1, NO=0)	n/a
5	Soporta controles técnicos como: antivirus, monitoreo de integridad de archivos y registro de dispositivos finales	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Los entornos de producción y no producción deben estar separados	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	La separación de los entornos puede incluir: firewalls de inspección con estado, fuentes de autenticación de dominio	Evaluación por cumplimiento: =1 por cada sistema	0
8	Avisos al usuario sobre actividades, en tiempo real	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Cortafuegos de perímetro para restringir tráfico no autorizado	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Configuración de seguridad habilitada con cifrado fuerte para la autenticación y la transmisión	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Cuenta con servicios de detección de patrones de tráfico para datos en tránsito	Evaluación por cumplimiento: (SI=1, NO=0)	0
12	Cuenta con técnicas de defensa en profundidad (p. Ej., Análisis de paquetes profundos, estrangulamiento del tráfico y retención en negro)	Evaluación por cumplimiento: (SI=1, NO=0)	0
13	El proveedor utilizará API abiertas y publicadas para garantizar el soporte para la interoperabilidad	Evaluación por cumplimiento: (SI=1, NO=0)	0
14	Validación remota de la versión / parche del software de dispositivos móviles	Evaluación por cumplimiento: (SI=1, NO=0)	n/a

En cuanto a prevención de ataques existe información que la aplicación no informa y la plataforma propietaria tampoco, por ello en algunos controles los listamos como n/a. En el cuadro a continuación mostramos la información de la evaluación.

Tabla 6-15 Evaluación atributo 1.7

ID de la métrica	1.7
Nombre del indicador	1.7. Prevención de ataques
Propósito del indicador	Se mide las seguridades con las que debe contar un servicio MCC para prevenir ataques
Controles asociados	1. Confidentiality/ Atributo: 1.7
Perspectiva MCC	Usuario: X Proveedor:___Broker:___Otros: _____
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: X Privado:___Hibrido:____Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	64%

El cumplimiento de este atributo obtuvo una calificación de 0.64=64% que se ajusta como “Mejorable” de acuerdo a los rangos planteados.

RANGOS:

1 a 0.786 = Ideal

0.714 a 0.357 = Mejorable

menor a 0.357 = Deficiente

8. Seguridad Complementario

En este apartado se observan características relacionadas con la protección de las instalaciones físicas y el acceso a los centros de datos en donde estén alojados los servicios cloud. Los controles se listan en la Tabla 6-16

Tabla 6-16 Controles para evaluación de atributo 2.1

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	El servicio cuenta con responsables de la Seguridad física, así como afines y otros	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Autenticación Biométrica	Evaluación por cumplimiento: (SI=1, NO=0)	1

3	Sistemas de Identificación	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Métodos de Verificación	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	CCTV	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Guardias	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Redundancia Energética	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Redundancia de Comunicaciones	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Monitoreo periódico de accesos autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Actualización periódica de permisos de acceso	Evaluación por cumplimiento: (SI=1, NO=0)	0

En la Tabla 6-17 a continuación se indican los resultados de evaluación.

Tabla 6-17 Resultados evaluación atributo 2.1

ID de la métrica	2.1
Nombre del indicador	2.1 Seguridad Complementario
Propósito del indicador	Se consulta sobre seguridades complementarias básicas respecto a instalaciones físicas del CSP
Controles asociados	2. Integridad/ Atributo: 2.1
Perspectiva MCC	Usuario: X_ Proveedor:___Broker:____Otros: _____
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: X_ Privado:___Hibrido:___Comunitario: _____
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	70%

De acuerdo al nivel de cumplimiento que fue de 0.7=70%, está dentro del nivel "ideal" según el rango planteado.

RANGOS:

1 a 0.615 = Ideal

0.538 a 0.308 = Mejorable

menor a 0.308 = Deficiente

9. Notificación y respuesta de incidentes de seguridad

Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes. Los controles sugeridos se indican en la Tabla 6-18

Tabla 6-18 Controles para evaluación de atributo 2.4

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con un plan de emergencia por incidentes de seguridad	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿Cuenta con un firewall a nivel de aplicación?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Notifica sobre procedimientos de copia de seguridad en terminal móvil en caso de un incidente	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	¿Cuenta con herramientas de registro incidentes de aplicaciones?	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Cuenta con un plan de recuperación de desastres	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Cuenta con un backup de servicios cloud.	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Brinda una respuesta de incidentes automatizada	Evaluación por cumplimiento: (SI=1, NO=0)	1

En la Tabla 6-19 se observa el resumen de la evaluación del atributo, que tiene resultados esperados, debido a que la plataforma cuenta con certificaciones que contemplan eventos e incidentes de seguridad.

Tabla 6-19 Resultados de evaluación atributo 2.4

ID de la métrica	2.2
Nombre del indicador	2.2. Buenas prácticas de prevención
Propósito del indicador	Se validan las precauciones que puede tomar un proveedor CSP para evitar posibles ataques a su integridad
Controles asociados	2. Integridad/ Atributo: 2.2
Perspectiva MCC	Usuario: X Proveedor:___Broker:___Otros: _____
Modelo de Servicio MCC evaluado	IaaS:____PaaS:____SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:___Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	0
Nivel de cumplimiento	0%

La calificación de nivel de cumplimiento obtenida de 0.86=86% equivale a “Ideal” de acuerdo a los rangos planteados

RANGOS:

1 a 0.714 = Ideal

0.571 a 0.286 = Mejorable

menor a 0.286 = Deficiente

10. 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 a sus perfiles. Aquí en particular se asumen como usuarios a los distintos dispositivos en los que se puede activar la aplicación y que a su vez tienen accesos a los datos y configuraciones principales. En la Tabla 6-20 se muestran los controles para el atributo mencionado.

Tabla 6-20 Controles para atributo 2.5

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Maneja un listado general de cuentas	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Maneja un porcentaje de cuentas sin actividad	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Se mide el porcentaje de cuentas sin actividad en los últimos 30 días / 60 días	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Se mide porcentaje de cuentas con perfil de administrador	Evaluación por cumplimiento: (SI=1, NO=0)	n/a
5	Posee cuentas de servicio o test	Evaluación por cumplimiento: (SI=1, NO=0)	0
6	Proporciona autenticación fuerte y control de acceso para el perfil de administración	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Presenta monitoreo de las sesiones en busca de actividades inusuales	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Incluye monitoreo y envío de alertas sobre el uso de información etiquetada como crítica	Evaluación por cumplimiento: (SI=1, NO=0)	0
9	Mantiene políticas de asignación y control para usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
10	Proporciona monitoreo de actividad de usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Posee una actualización y revisión periódica de lista de usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	0
12	Cuenta con políticas internas y cumplimiento de normativas como SOX, PCI e HIPAA	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	Emplea herramientas como SAPM (Shared Account Password Management o Gestión de Contraseñas de Cuentas Compartidas)	Evaluación por cumplimiento: (SI=1, NO=0)	1

14	Posee un listado del número total de cuentas y sus perfiles	Evaluación por cumplimiento: (SI=1, NO=0)	1

Como señala en su página, Gmail indica que se ajusta a certificaciones que aseguran el tema de la gestión de cuentas y usuarios. En la Tabla 6-21 se observa el resultado de la medición.

Tabla 6-21 Resultado evaluación atributo 2.5

ID de la métrica	2.5
Nombre del indicador	2.5. Gestión y control de cuentas de usuario
Propósito del indicador	Se validan las medidas de seguridad en cuanto al monitoreo y revisión de los usuarios y sus cuentas de acuerdo a sus perfiles
Controles asociados	2. Integridad/ Atributo: 2.5
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:___Otros: _____
Modelo de Servicio MCC evaluado	IaaS:____PaaS:____SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: X_ Privado:___Hibrido:___Comunitario: ____
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	9
Nivel de cumplimiento	0.71

De acuerdo a la tabla el cumplimiento de este atributo es de 0.71=71% que lo sitúa como ideal.

RANGOS:

1 a 0.714 = Ideal

0.643 a 0.357 = Mejorable

menor a 0.357 = Deficiente

11. Gestión de contenido anti-spam / correo electrónico

Se considero apropiado someter este atributo a evaluación debido a que la app es fundamentalmente para gestión, envió y recepción de correos electrónicos. La Tabla 6-22 muestra los atributos.

Tabla 6-22 Controles para evaluación atributo 2.8

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Monitoriza el número de correos electrónicos procesados	Evaluación por cumplimiento: (SI=1, NO=0)	1

2	Valida el número de correos electrónicos rechazados por restricciones de spam / contenido	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Realiza un control de MB de correo electrónico rechazado (ancho de banda utilizado por el móvil)	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Controla el número de correos electrónicos salientes con contenido inapropiado	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Lleva controles acerca del porcentaje de falsa identificación de spam	Evaluación por cumplimiento: (SI=1, NO=0)	1

En esta evaluación no se encontró información referente a los controles 3 y 4 sin embargo se estima que esos controles los deben realizar internamente o de lo contrario existen otro tipo de controles que suplan lo planteado. Los resultados los observamos a continuación.

Tabla 6-23 Resultados evaluación atributo 2.8

ID de la métrica	2.8
Nombre del indicador	2.8. Gestión de contenido anti-spam / correo electrónico
Propósito del indicador	Se validan las acciones a tomar respecto a la incidencia de contenido spam a la app móvil
Controles asociados	2. Integridad/ Atributo: 2.8
Perspectiva MCC	Usuario: _X_ Proveedor:____Broker:___Otros: _____
Modelo de Servicio MCC evaluado	IaaS:____PaaS:____SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:___Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	3
Nivel de cumplimiento	60%

De acuerdo a este resultado el cumplimiento de este atributo es 0.6=60% lo que indica que es “mejorable” según el rango de umbrales planteados. Pero se puede mejorar el mismo únicamente implementando uno de los controles que ya se señaló no hay información, convirtiendo ese resultado como “ideal”.

RANGOS:

1 a 0.8 = Ideal

0.6 a 0.4 = Mejorable

menor a 0.4 = Deficiente

12. Políticas de contraseña

Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad. En la Tabla 6-24 observamos los controles a evaluar.

Tabla 6-24 Controles a evaluar atributo 5.1

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Posee una política de caducidad de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Posee políticas sobre regulación de longitud de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Cuenta con política de autenticación en dos pasos	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Cuenta con política sobre complejidad de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Política sobre uso de autenticaciones biométricas	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Las claves deben tener propietarios identificables (claves de enlace a las identidades) y habrá políticas de administración clave.	Evaluación por cumplimiento: (SI=1, NO=0)	0
7	¿Existen políticas donde se definen y documentan todos los requisitos y niveles de confianza para el acceso de los clientes?	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Política sobre implementación de interfaz estándar OAuth 2.0 o equivalentes?	Evaluación por cumplimiento: (SI=1, NO=0)	1

En este apartado observamos que el tema de autenticación es muy valorado y por lo tanto se ve reflejado a continuación en el resultado de la misma.

Tabla 6-25 Resultado evaluación de atributo 5.1

ID de la métrica	5.1
Nombre del indicador	5.1. Políticas de contraseña
Propósito del indicador	Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad
Controles asociados	5. Authenticity/ Atributo: 5.1
Perspectiva MCC	Usuario: _X_ Proveedor:____Broker:____Otros: ____
Modelo de Servicio MCC evaluado	IaaS:___PaaS:___SaaS: _X_ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:___Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%

Medición	6
Nivel de cumplimiento	75%

Respecto al cumplimiento de este atributo, la calificación obtenida es de 0.75=75% que lo encasilla en un estado “Ideal”.

RANGOS:

1 a 0.75 = Ideal

0.625 a 0.375 = Mejorable

menor a 0.375 = Deficiente

13. Contexto de uso

Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc. De esta manera se podrá obtener un perfil del usuario respecto al uso, lugares, etc. En la Tabla 6-26

Tabla 6-26 Controles para evaluar atributo 5.3

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Capacidad de detección mediante biometría del comportamiento	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Detecta cambios de acceso al sistema, cambios de dirección IP incoherentes o franjas horarias	Evaluación por cumplimiento: (SI=1, NO=0)	0

Al someter a las aplicaciones a estos controles referentes al contexto de uso ninguno de ellos los cumplía. No se quiere decir que por ello es vulnerable, sino se plantea como oportunidades de mejora para fortalecer los procesos de autenticación y uso.

Tabla 6-27 Resultado evaluación

ID de la métrica	5.3
Nombre del indicador	5. 3. Contexto de uso
Propósito del indicador	Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc.
Controles asociados	5. Authenticity/ Atributo: 5.3
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros: _____

Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	0
Nivel de cumplimiento	0%

En este caso el atributo según el nivel de cumplimiento se tiene una valoración "mejorable".

Resumiendo, la aplicación tiene oportunidades de mejora en atributos como la implementación de Administración de Datos en el móvil como el más crítico y en los demás atributos obtuvo una valoración en su mayoría como ideal según el modelo. En la Figura 6-9 se muestra de manera gráfica lo indicado.

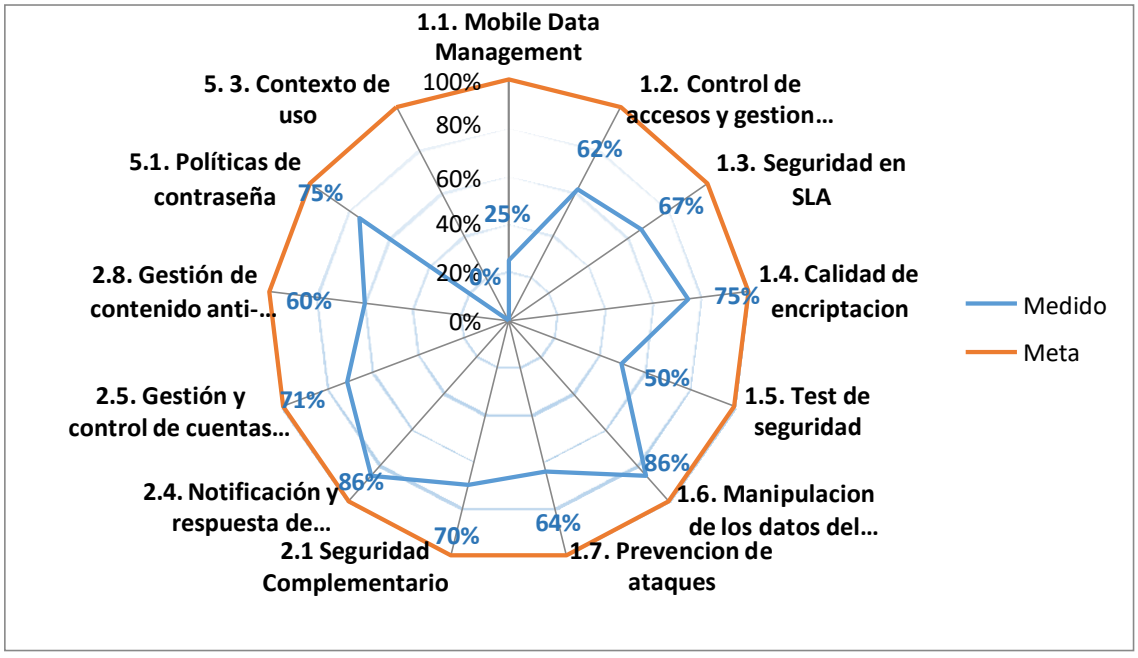


Figura 6-9 Resumen de evaluación de seguridad app Gmail

6.2.2 Evaluación de app Office 365

En este apartado se evaluará la seguridad de la app Office 365, considerando como guía el mismo modelo de calidad planteado en el capítulo 4.

1. Administración de Datos en el móvil (1.1)

Aquí procedemos a analizar los controles que se considera importantes de implementar para un correcto programa de MDM. Estos controles se muestran a continuación en la Tabla 6-28 junto con el resultado de evaluación por cumplimiento o no de los mismos.

Tabla 6-28 Controles correspondientes el atributo 1.1.

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	El servicio es ejecutable en todos los sistemas operativos móviles	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	El sistema cuenta con opción de Bloqueo remoto	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	El sistema tiene una opción de Borrado remoto	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Previene la transferencia no autorizada de información sensible hacia fuera del dispositivo	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Proporciona opciones de desactivación remota de los módulos de comunicación	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Ofrece inicio de sesión único (SSO) para todas las aplicaciones	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Informa a los administradores de seguridad cualquier intento de instalación de apps no autorizadas según listado documentado	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Posee opciones de implementación de geo vallas virtuales	Evaluación por cumplimiento: (SI=1, NO=0)	0

De la información relevante respecto a este atributo podemos señalar que la aplicación normalmente no tiene control sobre el dispositivo móvil que es en esencia lo más importante de un sistema de manejo de dispositivos móviles remoto. Sin embargo, se puede validar también que implementa seguridades basadas en estas características como el borrado remoto o bloqueo remoto, pero con la asistencia de todo el ambiente del sistema operativo Android. Para un sistema operativo diferente su alcance sería el de borrar la información retirando los permisos de acceso igual de manera remota.

El artefacto que resume el puntaje obtenido se adjunta a continuación en la Tabla 6-29

Tabla 6-29 Evaluación atributo 1.1 de Seguridad

ID de la métrica	1.1
Nombre del indicador	1.1. Mobile Data Management

Propósito del indicador	Se valora el servicio de manejo de los dispositivos móviles implementado por el sistema MCC
Controles asociados	1. Confidentiality/ Atributo: 1.1
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario: __
Formula	(Componentes MDM implementados) / (# total de componentes)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	0.875

RANGOS:

1 a 0.75 = Ideal

0.625 a 0.375 = Mejorable

menor a 0.375 = Deficiente

Para este atributo que obtuvo un nivel de cumplimiento de 0.875 = 87.5%, según el rango planteado el nivel de cumplimiento es “Ideal”.

2. Control de accesos y gestión de identidades

En este atributo lo que se busca es que se implemente las mejores prácticas de control de accesos y de la actividad de cada cuenta. Los controles planteados se observan en la Tabla 6-30

Tabla 6-30 Controles para evaluar 1.2 de Seguridad

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con inventario de dispositivos móviles autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Alerta todos los ingresos de dispositivos móviles nuevos	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	Revisa y deshabilita cualquier cuenta que no pueda asociarse con un proceso de empresa y/o propietario	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Calcula la incidencia de dispositivos no autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	N/A

5	Establece un proceso de revocado automático del acceso al sistema cloud deshabilitando cuentas inmediatamente después de la terminación de un vínculo con empleado o contratista.	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Supervisa regularmente el uso de todas las cuentas, desconectando automáticamente los usuarios después de un período estándar de inactividad	Evaluación por cumplimiento: (SI=1, NO=0)	0
7	Maneja un perfil de uso típico por usuario	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Monitoriza cambios en configuración o actividad de usuarios	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Monitoriza las sesiones en busca de actividades inusuales	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Valida configuración de dispositivos: autenticados y autorizados antes del acceso	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Implementa monitoreo del tráfico de datos por usuario	Evaluación por cumplimiento: (SI=1, NO=0)	0
12	¿Gestiona listas negras públicas?	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	Asigna a los dispositivos móviles autorización de acceso caducable	Evaluación por cumplimiento: (SI=1, NO=0)	1

Para este atributo señalamos que los controles parametrizados en esta aplicación no se pueden determinar que sean definitivos por el hecho que la aplicación no comparte cierta información, quizá por no considerarla relevante o por temas de políticas internas. En la Tabla 6-31 se muestra los resultados de la evaluación de los atributos

Tabla 6-31 Evaluación atributo 1.2 de Seguridad

ID de la métrica	1.2
Nombre del indicador	1.2. Control de accesos y gestión de identidades
Propósito del indicador	Valoración de las características de control de accesos y la actividad de cada cuenta.
Controles asociados	1. Confidentiality/ Atributo: 1.2
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	9
Nivel de cumplimiento	0.77

El resultado obtenido es de 0.77 es decir un 77% y de acuerdo a los umbrales planteados el cumplimiento de este indicador es “Ideal”.

RANGOS:

1 a 0.692 = Ideal

0.615 a 0.308 = Mejorable

menor a 0.308 = Deficiente

3. Seguridad en SLA

Aquí se validan características consideradas importantes y que debe contar un acuerdo SLA para MCC. Se considera un acuerdo de nivel de servicio valido para una aplicación pública y gratuita, a todos los ofrecimientos y garantías que ésta mantenga publicada en su página web. De esta manera se plantean los siguientes controles mostrados en la Tabla 6-32

Tabla 6-32 controles de evaluación atributo 1.3

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	¿Permite auditorías externas y certificaciones de seguridad?	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿La normativa legal está acorde a la legislación del país del suscriptor del servicio?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	¿Provee información sobre incidentes de seguridad de manera periódica?	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Permite que los informes, registros y servicios de terceros se sometan a auditoría y revisión	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Informa acerca del tratamiento que se dará a los datos del cliente.	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Ofrece opciones en cuanto al formato de disponibilidad de datos aptos para móviles	# de formatos disponibles / total de formatos posibles	0
7	¿Establece garantías en la encriptación de los datos en reposo?	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Informa acerca del uso de canales de comunicación protegidos y cifrados en el caso de migración de	Evaluación por cumplimiento: (SI=1, NO=0)	1

	servidores físicos, aplicaciones o datos a sistemas cloud		
9	Establece acciones por modificación unilateral del contrato	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Garantiza que los logs y los datos de los incidentes se gestionan de una forma centralizada	Evaluación por cumplimiento: (SI=1, NO=0)	0
11	¿Define por contrato la política de copias de seguridad?	Evaluación por cumplimiento: (SI=1, NO=0)	1*
12	¿Establece garantías respecto al aislamiento de los datos en reposo?	Evaluación por cumplimiento: (SI=1, NO=0)	1

Como se informó en párrafos anteriores esta app "office365" es privada y solo para usuarios bajo suscripción con costo. Bajo ese escenario se elabora el control correspondiente, por lo tanto, no existe un contrato físico legal que sea firmado y reconocido por las partes involucradas.

Tabla 6-33 Evaluación atributo 1.3 de Seguridad

ID de la métrica	1.3
Nombre del indicador	1.3. Seguridad en SLA
Propósito del indicador	Valoración de las características de control de accesos y la actividad de cada cuenta.
Controles asociados	1. Confidentiality/ Atributo: 1.3
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	8
Nivel de cumplimiento	0.75

De acuerdo a lo mostrado el cumplimiento de este atributo alcanzo el 0.75=75% que está dentro del rango como ideal

RANGOS:

1 a 0.667 = Ideal

0.583 a 0.333 = Mejorable

menor a 0.333 = Deficiente

4. Calidad de encriptación.

Se mide opciones ideales en cuanto a encriptación en ambientes MCC, varias de ellas se plantean más como recomendaciones en el ámbito del cifrado. Los controles planteados los vemos en la Tabla 6-34

Tabla 6-34 Controles del atributo 1.4.

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Utiliza técnicas de cifrado fuertes (como AES-256, AES-192 o RSA)	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Utilizar formatos abiertos y validados, evitando en la medida de lo posible, el uso de técnicas de cifrado propietario.	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Usa controles de protección de claves como KEK90 (Clave de Cifrado de Claves) o equivalentes	Evaluación por cumplimiento: (SI=1, NO=0)	
4	Evitar utilizar estándares antiguos de encriptación tales como Data Encryption Standard (DES)	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Utiliza técnicas de cifrado de red estándar incluyendo SSL21, VPNs22, y SSH23	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	¿Utiliza Secure Sockets Layer?	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Transport Layer Security (TLS)	Evaluación por cumplimiento: (SI=1, NO=0)	1

En esta revisión también no se halló mucha información respecto al, pero se hace alusión al uso de métodos de cifrado SSL y TLS. También se encontró que office365 cumple con normativas como: Cláusulas modelo de la UE, FedRAMP, FERPA, FISMA, Contrato de asociación empresarial de HIPAA, ISO/IEC 27001, G-Cloud v6 Official de Reino Unido. La Tabla 6-33 muestra el resultado de la evaluación

Tabla 6-35 Evaluación atributo 1.4 de Seguridad

ID de la métrica	1.4
Nombre del indicador	1.4. Calidad de encriptación
Propósito del indicador	Se mide opciones ideales en cuanto a encriptación en ambientes MCC
Controles asociados	1. Confidentiality/ Atributo: 1.4
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje

Nivel para el cumplimiento	100%
Medición	7
Nivel de cumplimiento	0.88

Según los rangos planteados el cumplimiento respecto a este atributo, un resultado de 0.88 = 88% equivale a "ideal".

RANGOS:

1 a 0.75 = Ideal

0.625 a 0.375 = Mejorable

menor a 0.375 = Deficiente

5. Test de seguridad

Se verifican las pruebas recomendables que deben realizarse a ambientes MCC. Para ello los controles se detallan en Tabla 6-36

Tabla 6-36 Controles a evaluar atributo 1.5

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Realiza test de penetración externos e internos de seguridad a los móviles	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Mantiene un detalle de los terminales en los que se realizan los test y los utilizan únicamente con esos fines de prueba	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	Realiza pruebas a terminales móviles en los que involucre ingeniería social	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Realiza pruebas periódicas de verificación de acceso a aplicaciones no autorizadas	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Cuenta con un listado detallado de vulnerabilidades del sistema cloud	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Realiza test a los terminales móviles donde se validan los parches de seguridad necesarios	Evaluación por cumplimiento: (SI=1, NO=0)	0

En lo que se refiere a test de penetración la plataforma no informa al tema puntualmente, sin embargo, de la información que tiene disponible en la página web se tomó los datos para la valoración correspondiente. En la Tabla 6-37 observamos el artefacto con el que se obtuvo la calificación de la app.

Tabla 6-37 Evaluación atributo 1.5 de Seguridad

ID de la métrica	1.5
Nombre del indicador	1.5. Test de seguridad
Propósito del indicador	Se verifican las pruebas mínimas que deben realizarse a ambientes MCC
Controles asociados	1. Confidentiality/ Atributo: 1.5
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	3
Nivel de cumplimiento	50%

Para el rango medido se valida que el cumplimiento del atributo fue de 0.33=33% que equivale a "Deficiente", sin embargo, cabe aclarar que la valoración se ve afectada porque no se halló información relacionada a test de seguridad.

RANGOS:
1 a 0.667 = Ideal
0.5 a 0.333 = Mejorable
menor a 0.333 = Deficiente

6. Manipulación de los datos del cliente

Se realiza una validación de los controles que se someten los datos de los usuarios, principalmente enfocados en la manipulación y eliminación de éstos. Para estas evaluaciones se plantean los controles de la Tabla 6-38.

Tabla 6-38 Controles del atributo 1.6

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Brinda herramientas para etiquetado y clasificación de datos	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	¿Entrega certificación de la destrucción por parte del proveedor de cloud computing o por un tercero?	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	¿Permite la portabilidad de la información a sistemas propios o de otros proveedores?	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Asegura que los datos no son recuperables mediante ningún medio forense informático	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Posee políticas y procedimientos para la eliminación segura y completa de los datos terminales móviles	Evaluación por cumplimiento: (SI=1, NO=0)	1

6	¿Utiliza técnicas de borrado seguras para unidades de almacenamiento que serán reutilizadas?	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Cuenta con políticas y procedimientos para la eliminación segura de equipos móviles de los usuarios	Evaluación por cumplimiento: (SI=1, NO=0)	1

En la Tabla 6-39 se muestra la calificación obtenida

Tabla 6-39 Evaluación atributo 1.6

ID de la métrica	1.6
Nombre del indicador	1.6. Manipulación de los datos del cliente
Propósito del indicador	Se realiza una validación de los controles que se someten los datos de los usuarios
Controles asociados	1. Confidentiality/ Atributo: 1.6
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	5
Nivel de cumplimiento	71%

Se observa que alcanza una calificación de 0.71=71% lo que se adjudica un cumplimiento “Ideal” de acuerdo a los rangos planteados.

RANGOS:

1 a 0.714 = Ideal

0.714 a 0.429 = Mejorable

menor a 0.429 = Deficiente

7. Prevención de ataques

Se mide las seguridades con las que se recomienda debería contar un servicio MCC para prevenir ataques, los controles se muestran en la Tabla 6-40

Tabla 6-40 Controles a evaluar de atributo

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con un DLP junto con la gestión que esto implica	Evaluación por cumplimiento: (SI=1, NO=0)	1

2	¿Presenta una certificación de seguridad conocida?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	CSP garantice que los logs y los datos de los incidentes se gestionan de una forma centralizada	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Configuración del sistema operativo se habilita sólo los puertos, protocolos y servicios necesarios para satisfacer las necesidades empresariales	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Soporta controles técnicos como: antivirus, monitoreo de integridad de archivos y registro de dispositivos finales	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Los entornos de producción y no producción deben estar separados	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	La separación de los entornos puede incluir: firewalls de inspección con estado, fuentes de autenticación de dominio	Evaluación por cumplimiento: =1 por cada sistema	1
8	Avisos al usuario sobre actividades, en tiempo real	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Cortafuegos de perímetro para restringir tráfico no autorizado	Evaluación por cumplimiento: (SI=1, NO=0)	1
10	Configuración de seguridad habilitada con cifrado fuerte para la autenticación y la transmisión	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Cuenta con servicios de detección de patrones de tráfico para datos en tránsito	Evaluación por cumplimiento: (SI=1, NO=0)	0
12	Cuenta con técnicas de defensa en profundidad (p. Ej., Análisis de paquetes profundos, estrangulamiento del tráfico y retención en negro)	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	El proveedor utilizará API abiertas y publicadas para garantizar el soporte para la interoperabilidad	Evaluación por cumplimiento: (SI=1, NO=0)	1
14	Validación remota de la versión / parche del software de dispositivos móviles	Evaluación por cumplimiento: (SI=1, NO=0)	0

En este análisis tampoco se halló información respecto de la prevención de análisis, por lo que se tuvo que analizar basados en la información disponible.

ID de la métrica	1.7
Nombre del indicador	1.7. Prevención de ataques
Propósito del indicador	Se mide las seguridades con las que debe contar un servicio MCC para prevenir ataques
Controles asociados	1. Confidentiality/ Atributo: 1.7
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros: _____

Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	11
Nivel de cumplimiento	0.79

El cumplimiento de este atributo obtuvo una calificación de 0.79=79% que se ajusta como "Ideal" de acuerdo a los rangos planteados.

RANGOS:

1 a 0.786 = Ideal

0.714 a 0.357 = Mejorable

menor a 0.357 = Deficiente

8. Seguridad Complementario

En este apartado se observan características relacionadas con la protección de las instalaciones físicas y el acceso a los centros de datos en donde estén alojados los servicios cloud. Los controles se listan en la Tabla 6-41

Tabla 6-41 Controles para evaluación de atributo 2.1

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	El servicio cuenta con responsables de la Seguridad física, así como afines y otros	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Autenticación Biométrica	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Sistemas de Identificación	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Métodos de Verificación	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	CCTV	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Guardias	Evaluación por cumplimiento: (SI=1, NO=0)	1

7	Redundancia Energética	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Redundancia de Comunicaciones	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Monitoreo periódico de accesos autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Actualización periódica de permisos de acceso	Evaluación por cumplimiento: (SI=1, NO=0)	1

En la Tabla 6-42 a continuación se indican los resultados de evaluación.

Tabla 6-42 Resultados evaluación atributo 2.1

ID de la métrica	2.1
Nombre del indicador	2.1 Seguridad Complementario
Propósito del indicador	Se consulta sobre seguridades complementarias básicas respecto a instalaciones físicas del CSP
Controles asociados	2. Integridad/ Atributo: 2.1
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	9
Nivel de cumplimiento	90%

De acuerdo al nivel de cumplimiento que fue de 0.9=90%, está dentro del nivel "ideal" según el rango planteado.

RANGOS:

1 a 0.615 = Ideal

0.538 a 0.308 = Mejorable

menor a 0.308 = Deficiente

9. Notificación y respuesta de incidentes de seguridad

Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes. Los controles sugeridos se indican en la Tabla 6-43

Tabla 6-43 Controles para evaluación de atributo 2.4

N°	*Controles a evaluar*	*Medición*	*Resultados*
1	Cuenta con un plan de emergencia por incidentes de seguridad	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿Cuenta con un firewall a nivel de aplicación?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Notifica sobre procedimientos de copia de seguridad en terminal móvil en caso de un incidente	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	¿Cuenta con herramientas de registro incidentes de aplicaciones?	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Cuenta con un plan de recuperación de desastres	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Cuenta con un backup de servicios cloud.	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Brinda una respuesta de incidentes automatizada	Evaluación por cumplimiento: (SI=1, NO=0)	1

En la .

Tabla 6-44 se observa el resumen de la evaluación del atributo, que tiene resultados muy buenos debido principalmente a que se ajusta al enfoque recomendado por el Instituto Nacional de Normalización y Tecnología (NIST) en la normativa NIST 800-61.

Tabla 6-44 Resultados de evaluación atributo 2.4

ID de la métrica	2.4
Nombre del indicador	2.4. Notificación y respuesta de incidentes de seguridad
Propósito del indicador	Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes
Controles asociados	2. Integridad/ Atributo: 2.4
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario: __
Formula	$(Numero\ de\ componentes\ que\ cumple)/(Numero\ total\ de\ componentes\ planteados)$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	86%

La calificación de nivel de cumplimiento obtenida de 0.86=86% equivale a “Ideal” de acuerdo a los rangos planteados

RANGOS:

1 a 0.714 = Ideal

0.571 a 0.286 = Mejorable

menor a 0.286 = Deficiente

10. 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 a sus perfiles. Aquí en particular se asumen como usuarios a los distintos dispositivos en los que se puede activar la aplicación y que a su vez tienen accesos a los datos y configuraciones principales. En la Tabla 6-45 se muestran los controles para el atributo mencionado.

Tabla 6-45 Controles para atributo 2.5

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Maneja un listado general de cuentas	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Maneja un porcentaje de cuentas sin actividad	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Se mide el porcentaje de cuentas sin actividad en los últimos 30 días / 60 días	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Se mide porcentaje de cuentas con perfil de administrador	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Posee cuentas de servicio o test	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Proporciona autenticación fuerte y control de acceso para el perfil de administración	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Presenta monitoreo de las sesiones en busca de actividades inusuales	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Incluye monitoreo y envío de alertas sobre el uso de información etiquetada como crítica	Evaluación por cumplimiento: (SI=1, NO=0)	0
9	Mantiene políticas de asignación y control para usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1

10	Proporciona monitoreo de actividad de usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Posee una actualización y revisión periódica de lista de usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
12	Cuenta con políticas internas y cumplimiento de normativas como SOX, PCI e HIPAA	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	Emplea herramientas como SAPM (Shared Account Password Management o Gestión de Contraseñas de Cuentas Compartidas)	Evaluación por cumplimiento: (SI=1, NO=0)	1
14	Posee un listado del número total de cuentas y sus perfiles	Evaluación por cumplimiento: (SI=1, NO=0)	1

En esta sección se tuvo que realizar consultas al documento: *"Microsoft Intune Datasheet"* donde especifica los diversos controles de cuentas y dispositivos. En la Tabla 6-46 se observa el resultado de la medición.

Tabla 6-46 Resultado evaluación atributo 2.5

ID de la métrica	2.5
Nombre del indicador	2.5. Gestión y control de cuentas de usuario
Propósito del indicador	Se validan las medidas de seguridad en cuanto al monitoreo y revisión de los usuarios y sus cuentas de acuerdo a sus perfiles
Controles asociados	2. Integridad/ Atributo: 2.5
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	12
Nivel de cumplimiento	0.86

De acuerdo a la tabla el cumplimiento de este atributo es de 0.86=86% que lo sitúa como ideal.

RANGOS:

1 a 0.714 = Ideal

0.643 a 0.357 = Mejorable

menor a 0.357 = Deficiente

11. Gestión de contenido anti-spam / correo electrónico

Se considero apropiado someter este atributo a evaluación debido a que la app es tiene una importante aplicación en el mercado que es la app Outlook que es básicamente para gestión, envió y recepción de correos electrónicos.

Tabla 6-47 Controles para evaluación atributo 2.8

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Monitoriza el número de correos electrónicos procesados	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Valida el número de correos electrónicos rechazados por restricciones de spam / contenido	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Realiza un control de MB de correo electrónico rechazado (ancho de banda utilizado por el móvil)	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Controla el número de correos electrónicos salientes con contenido inapropiado	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Lleva controles acerca del porcentaje de falsa identificación de spam	Evaluación por cumplimiento: (SI=1, NO=0)	1

En esta evaluación no se encontró información referente a los controles 3 y 4 sin embargo se estima que esos controles los deben realizar internamente o de lo contrario existen otro tipo de controles que suplan lo planteado. Los resultados los observamos a continuación.

ID de la métrica	2.8
Nombre del indicador	2.8. Gestión de contenido anti-spam / correo electrónico
Propósito del indicador	Se validan las acciones a tomar respecto a la incidencia de contenido spam a la app móvil
Controles asociados	2. Integridad/ Atributo: 2.8
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	80%

De acuerdo a este resultado el cumplimiento de este atributo es del 80% lo que indica que es “ideal”

RANGOS:
1 a 0.8 = Ideal
0.6 a 0.4 = Mejorable
menor a 0.4 = Deficiente

12. Políticas de contraseña

Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad. En la Tabla 6-48 observamos los controles a evaluar.

Tabla 6-48 Controles a evaluar atributo 5.1

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Posee una política de caducidad de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Posee políticas sobre regulación de longitud de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Cuenta con política de autenticación en dos pasos	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Cuenta con política sobre complejidad de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Política sobre uso de autenticaciones biométricas	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Las claves deben tener propietarios identificables (claves de enlace a las identidades) y habrá políticas de administración clave.	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	¿Existen políticas donde se definen y documentan todos los requisitos y niveles de confianza para el acceso de los clientes?	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Política sobre implementación de interfaz estándar OAuth 2.0 o equivalentes?	Evaluación por cumplimiento: (SI=1, NO=0)	0

En este apartado observamos que el tema de autenticación es muy valorado y por lo tanto se ve reflejado a continuación en el resultado de la misma.

Tabla 6-49 Resultado evaluación de atributo 5.1

ID de la métrica	5.1
Nombre del indicador	5.1. Políticas de contraseña
Propósito del indicador	Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad
Controles asociados	5. Authenticity / Atributo: 5.1
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros: _____

Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario:
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	75%

Respecto al cumplimiento de este atributo, la calificación obtenida es de 75% que lo encasilla en un estado "Ideal".

13. Contexto de uso

Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc. De esta manera se podrá obtener un perfil del usuario respecto al uso, lugares, etc. En la Tabla 6-50

Tabla 6-50 Controles para evaluar atributo 5.3

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Capacidad de detección mediante biometría del comportamiento	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Detecta cambios de acceso al sistema, cambios de dirección IP incoherentes o franjas horarias	Evaluación por cumplimiento: (SI=1, NO=0)	0

Al someter a las aplicaciones a estos controles referentes al contexto de uso ninguno de ellos los cumplía. No se quiere decir que por ello es vulnerable, sino se plantea como oportunidades de mejora para fortalecer los procesos de autenticación y uso.

Tabla 6-51 Resultado evaluación

ID de la métrica	5.3
Nombre del indicador	5. 3. Contexto de uso
Propósito del indicador	Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc.
Controles asociados	5. Authenticity/ Atributo: 5.3
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico: _X_ Privado:____Hibrido:___Comunitario: ___
Formula	$(Numero\ de\ componentes\ que\ cumple)/$ $(Numero\ total\ de\ componentes\ planteados)$

Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	1
Nivel de cumplimiento	50%

En este caso el atributo según el nivel de cumplimiento se hace merecedor a una valoración “mejorable”.

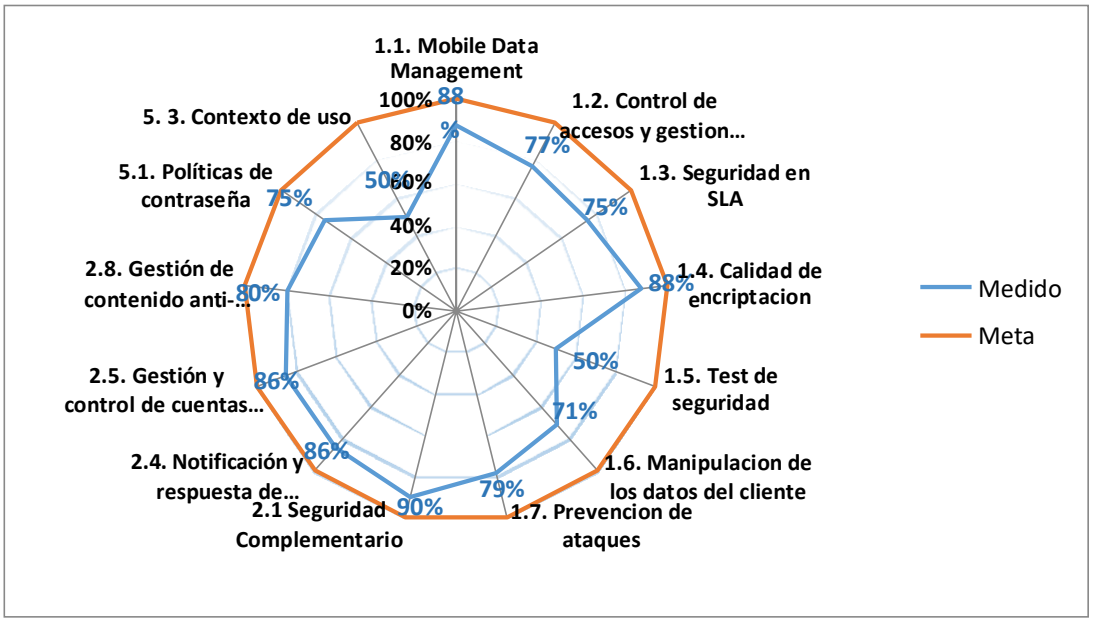


Figura 6-10 Resumen grafico de la evaluación.

6.2.3 Evaluación de app Salesforce

Salesforce es una empresa responsable de una de las plataformas de CRM más relevantes de los últimos tiempos el mismo cuyo software está basado en la nube. En este apartado se evaluará la seguridad de esta aplicación, considerando como guía el modelo de calidad planteado en el capítulo 4, donde se definió una serie de atributos con sus controles específicos y una métrica que engloba cada uno, para una valoración final.

1. Administración de Datos en el móvil (1.1)

Aquí procedemos a analizar los controles que se considera importantes de implementar para un correcto programa de MDM. Estos controles se muestran a continuación en la Tabla 6-52 junto con el resultado de evaluación por cumplimiento o no de los mismos.

Tabla 6-52 Controles correspondientes el atributo 1.1.

N°	*Controles a evaluar*	*Medición*	*Resultados*
1	El servicio es ejecutable en todos los sistemas operativos móviles	Evaluación por cumplimiento: (SI=1, NO=0)	
2	El sistema cuenta con opción de Bloqueo remoto	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	El sistema tiene una opción de Borrado remoto	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Previene la transferencia no autorizada de información sensible hacia fuera del dispositivo	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Proporciona opciones de desactivación remota de los módulos de comunicación	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Ofrece inicio de sesión único (SSO) para todas las aplicaciones	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Informa a los administradores de seguridad cualquier intento de instalación de apps no autorizadas según listado documentado	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Posee opciones de implementación de geo vallas virtuales	Evaluación por cumplimiento: (SI=1, NO=0)	0

La aplicación Salesforce1 no maneja opciones de MDM sin embargo en toda la página en la que trata el tema de seguridad[14] informa sobre las medidas de prevención que están relacionadas a temas vinculados a MDM.

El artefacto que resume el puntaje obtenido se adjunta a continuación en la Tabla 6-53

Tabla 6-53 Evaluación atributo 1.1 de Seguridad

ID de la métrica	1.1
Nombre del indicador	1.1. Mobile Data Management
Propósito del indicador	Se valora el servicio de manejo de los dispositivos móviles implementado por el sistema MCC
Controles asociados	1. Confidentiality/ Atributo: 1.1
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X___ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___

[14] *https://trust.salesforce.com/es/security/*

Formula	(Componentes MDM implementados) (# total de componentes)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	0.75

RANGOS:

1 a 0.75 = Ideal

0.625 a 0.375 = Mejorable

menor a 0.375 = Deficiente

Para este atributo que obtuvo un nivel de cumplimiento de 0.62 = 62%, según el rango planteado el nivel de cumplimiento es “Mejorable”.

2. Control de accesos y gestión de identidades

En este atributo lo que se busca es que se implemente las mejores prácticas de control de accesos y de la actividad de cada cuenta. Los controles planteados se observan en la Tabla 6-54

Tabla 6-54 Controles a Evaluar para atributo 1.2

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con inventario de dispositivos móviles autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Alerta todos los ingresos de dispositivos móviles nuevos	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Revisa y deshabilita cualquier cuenta que no pueda asociarse con un proceso de empresa y/o propietario	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Calcula la incidencia de dispositivos no autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Establece un proceso de revocado automático del acceso al sistema cloud deshabilitando cuentas inmediatamente después de la terminación de un vínculo con empleado o contratista.	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Supervisa regularmente el uso de todas las cuentas, desconectando automáticamente los usuarios después de un período estándar de inactividad	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Maneja un perfil de uso típico por usuario	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Monitoriza cambios en configuración o actividad de usuarios	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Monitoriza las sesiones en busca de actividades inusuales	Evaluación por cumplimiento: (SI=1, NO=0)	1

10	Valida configuración de dispositivos: autenticados y autorizados antes del acceso	Evaluación por cumplimiento: (SI=1, NO=0)	0
11	Implementa monitoreo del tráfico de datos por usuario	Evaluación por cumplimiento: (SI=1, NO=0)	1
12	¿Gestiona listas negras públicas?	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	Asigna a los dispositivos móviles autorización de acceso caducable	Evaluación por cumplimiento: (SI=1, NO=0)	1

Dentro de las políticas que la aplicación Salesforce1 maneja y sumado a las recomendaciones que propone en la plataforma Trust Salesforce se ha podido realizar la evaluación comparando los controles propuestos con lo indicado en este portal. La Tabla 6-55

Tabla 6-55 Evaluación atributo 1.2 de Seguridad

ID de la métrica	1.2
Nombre del indicador	1.2. Control de accesos y gestión de identidades
Propósito del indicador	Valoración de las características de control de accesos y la actividad de cada cuenta.
Controles asociados	1. Confidentiality/ Atributo: 1.2
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	(*Numero de componentes que cumple*)/ (*Numero total de componentes planteados*)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	10
Nivel de cumplimiento	0.77

El resultado obtenido es de 0.77 es decir un 7% y de acuerdo a los umbrales planteados el cumplimiento de este indicador es “Ideal”.

RANGOS:

1 a 0.692 = Ideal

0.615 a 0.308 = Mejorable

menor a 0.308 = Deficiente

3. Seguridad en SLA

Aquí se validan características consideradas importantes y que debe contar un acuerdo SLA para MCC. Se considera un acuerdo de nivel de servicio valido para una aplicación pública y gratuita, a todos los ofrecimientos y garantías que ésta mantenga publicada en su página web. De esta manera se plantean los siguientes controles mostrados en la Tabla 6-56

Tabla 6-56 Controles de evaluación atributo 1.3

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	¿Permite auditorías externas y certificaciones de seguridad?	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿La normativa legal está acorde a la legislación del país del suscriptor del servicio?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	¿Provee información sobre incidentes de seguridad de manera periódica?	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Permite que los informes, registros y servicios de terceros se sometan a auditoría y revisión	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Informa acerca del tratamiento que se dará a los datos del cliente.	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Ofrece opciones en cuanto al formato de disponibilidad de datos aptos para móviles	# de formatos disponibles / total de formatos posibles	0
7	¿Establece garantías en la encriptación de los datos en reposo?	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Informa acerca del uso de canales de comunicación protegidos y cifrados en el caso de migración de servidores físicos, aplicaciones o datos a sistemas cloud	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Establece acciones por modificación unilateral del contrato	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Garantiza que los logs y los datos de los incidentes se gestionan de una forma centralizada	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	¿Define por contrato la política de copias de seguridad?	Evaluación por cumplimiento: (SI=1, NO=0)	1
12	¿Establece garantías respecto al aislamiento de los datos en reposo?	Evaluación por cumplimiento: (SI=1, NO=0)	1

Salesforce y su aplicación Salesforce1 brindan únicamente una prueba gratuita con una vigencia caducable. Bajo ese escenario el SLA es temporal y no es completo si comparamos a la opción de uso completa de la aplicación, sin embargo, fue posible levantar el informe del atributo evaluado que se muestra en la Tabla 6-57

Tabla 6-57 Evaluación atributo 1.3 de Seguridad

ID de la métrica	1.3
Nombre del indicador	1.3. Seguridad en SLA
Propósito del indicador	Valoración de las características de control de accesos y la actividad de cada cuenta.
Controles asociados	1. Confidentiality/ Atributo: 1.3
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	9
Nivel de cumplimiento	0.75

De acuerdo a lo anteriormente establecido el cumplimiento de este atributo alcanzo el 0.75=75% que está dentro del rango como ideal

RANGOS:

1 a 0.667 = Ideal

0.583 a 0.333 = Mejorable

menor a 0.333 = Deficiente

4. Calidad de encriptación.

Se mide opciones ideales en cuanto a encriptación en ambientes MCC, varias de ellas se plantean más como recomendaciones en el ámbito del cifrado. Los controles planteados los vemos en la Tabla 6-8

Tabla 6-58 Controles del atributo 1.4.

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Utiliza técnicas de cifrado fuertes (como AES-256, AES-192 o RSA)	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Utilizar formatos abiertos y validados, evitando en la medida de lo posible, el uso de técnicas de cifrado propietario.	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Usa controles de protección de claves como KEK90 (Clave de Cifrado de Claves) o equivalentes	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Evitar utilizar estándares antiguos de encriptación tales como Data Encryption Standard (DES)	Evaluación por cumplimiento: (SI=1, NO=0)	0

5	Utiliza técnicas de cifrado de red estándar incluyendo SSL21, VPNs22, y SSH23	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	¿Utiliza Secure Sockets Layer?	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Transport Layer Security (TLS)	Evaluación por cumplimiento: (SI=1, NO=0)	1

En este caso también todo lo que se refiere a cifrado no estaba difundida al detalle, pero se hace alusión al uso de métodos de cifrado SSL y TLS 1.1. Por otra parte, Salesforce mantiene un conjunto completo de certificaciones de cumplimiento normativo ISO, AICPA, PCIDSS, NIST, TRUSTe, etc. La Tabla 6-59 muestra el resultado de la evaluación

Tabla 6-59 Evaluación atributo 1.4 de Seguridad

ID de la métrica	1.4
Nombre del indicador	1.4. Calidad de encriptación
Propósito del indicador	Se mide opciones ideales en cuanto a encriptación en ambientes MCC
Controles asociados	1. Confidentiality/ Atributo: 1.4
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	(*Numero de componentes que cumple*)/ (*Numero total de componentes planteados*)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	0.75

Según los rangos planteados el cumplimiento respecto a este atributo, un resultado de 0.75 = 75% equivale a “ideal”.

RANGOS:

1 a 0.75 = Ideal

0.625 a 0.375 = Mejorable

menor a 0.375 = Deficiente

5. Test de seguridad

Se verifican las pruebas recomendables que deben realizarse a ambientes MCC. Para ello los controles se detallan en Tabla 6-60

Tabla 6-60 Controles a evaluar atributo 1.5

N°	*Controles a evaluar*	*Medición*	*Resultados*
1	Realiza test de penetración externos e internos de seguridad a los móviles	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Mantiene un detalle de los terminales en los que se realizan los test y los utilizan únicamente con esos fines de prueba	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Realiza pruebas a terminales móviles en los que involucre ingeniería social	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Realiza pruebas periódicas de verificación de acceso a aplicaciones no autorizadas	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Cuenta con un listado detallado de vulnerabilidades del sistema cloud	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Realiza test a los terminales móviles donde se validan los parches de seguridad necesarios	Evaluación por cumplimiento: (SI=1, NO=0)	0

En lo que se refiere a test de penetración la plataforma por si toma precauciones al respecto y son esas precauciones las que se valoraron en la calificación del atributo. En la Tabla 6-61 observamos el artefacto con el que se obtuvo la calificación de la app.

Tabla 6-61 Evaluación atributo 1.5 de Seguridad

ID de la métrica	1.5
Nombre del indicador	1.5. Test de seguridad
Propósito del indicador	Se verifican las pruebas mínimas que deben realizarse a ambientes MCC
Controles asociados	1. Confidentiality/ Atributo: 1.5
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	4
Nivel de cumplimiento	67%

Para el rango medido se valida que el cumplimiento del atributo fue de 0.67=67% que equivale a “mejorable”, principalmente por el tema de la apertura que la plataforma da para realizar pruebas y por las certificaciones que mantiene.

6. Manipulación de los datos del cliente

Se realiza una validación de los controles que se someten los datos de los usuarios, principalmente enfocados en la manipulación y eliminación de éstos. Para estas evaluaciones se plantean los controles de la Tabla 6-62.

Tabla 6-62 Controles del atributo 1.6

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Brinda herramientas para etiquetado y clasificación de datos	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	¿Entrega certificación de la destrucción por parte del proveedor de cloud computing o por un tercero?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	¿Permite la portabilidad de la información a sistemas propios o de otros proveedores?	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Asegura que los datos no son recuperables mediante ningún medio forense informático	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Posee políticas y procedimientos para la eliminación segura y completa de los datos terminales móviles	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	¿Utiliza técnicas de borrado seguras para unidades de almacenamiento que serán reutilizadas?	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Cuenta con políticas y procedimientos para la eliminación segura de equipos móviles de los usuarios	Evaluación por cumplimiento: (SI=1, NO=0)	1

En la Tabla 6-63 se muestran la calificación obtenida

Tabla 6-63 Evaluación atributo 1.6

ID de la métrica	1.6
Nombre del indicador	1.6. Manipulación de los datos del cliente
Propósito del indicador	Se realiza una validación de los controles que se someten los datos de los usuarios
Controles asociados	1. Confidentiality/ Atributo: 1.6
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	6
Nivel de cumplimiento	86%

Se observa que alcanza una calificación de 0.86=86% lo que se adjudica un cumplimiento "Ideal" de acuerdo a los rangos planteados.

RANGOS:

1 a 0.714 = Ideal

0.714 a 0.429 = Mejorable

menor a 0.429 = Deficiente

7. Prevención de ataques

Se mide las seguridades con las que se recomienda debería contar un servicio MCC para prevenir ataques, los controles se muestran en la Tabla 6-64

Tabla 6-64 Controles a evaluar de atributo 1.7

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con un DLP junto con la gestión que esto implica	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿Presenta una certificación de seguridad conocida?	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	CSP garantice que los logs y los datos de los incidentes se gestionan de una forma centralizada	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Configuración del sistema operativo se habilita sólo los puertos, protocolos y servicios necesarios para satisfacer las necesidades empresariales	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Soporta controles técnicos como: antivirus, monitoreo de integridad de archivos y registro de dispositivos finales	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Los entornos de producción y no producción deben estar separados	Evaluación por cumplimiento: (SI=1, NO=0)	
7	La separación de los entornos puede incluir: firewalls de inspección con estado, fuentes de autenticación de dominio	Evaluación por cumplimiento: =1 por cada sistema	1
8	Avisos al usuario sobre actividades, en tiempo real	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Cortafuegos de perímetro para restringir tráfico no autorizado	Evaluación por cumplimiento: (SI=1, NO=0)	1
10	Configuración de seguridad habilitada con cifrado fuerte para la autenticación y la transmisión	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Cuenta con servicios de detección de patrones de tráfico para datos en tránsito	Evaluación por cumplimiento: (SI=1, NO=0)	1
12	Cuenta con técnicas de defensa en profundidad (p. Ej., Análisis de	Evaluación por cumplimiento: (SI=1, NO=0)	1

	paquetes profundos, estrangulamiento del tráfico y retención en negro)		
13	El proveedor utilizará API abiertas y publicadas para garantizar el soporte para la interoperabilidad	Evaluación por cumplimiento: (SI=1, NO=0)	
14	Validación remota de la versión / parche del software de dispositivos móviles	Evaluación por cumplimiento: (SI=1, NO=0)	

Algo que se pudo identificar en el análisis de la aplicación Salesforce 1 fue que brinda una opción de certificación reconocida por Salesforce Inc. Dentro de la cual se pudo sacar cierta información relacionada a varios atributos incluido este último. En la Tabla 6-65

Tabla 6-65 Resultados evaluación atributo 1.7

ID de la métrica	1.7
Nombre del indicador	1.7. Prevención de ataques
Propósito del indicador	Se mide las seguridades con las que debe contar un servicio MCC para prevenir ataques
Controles asociados	1. Confidentiality/ Atributo: 1.7
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	9
Nivel de cumplimiento	0.64

El cumplimiento de este atributo obtuvo una calificación de 0.64=64% que se ajusta como “Mejorable” de acuerdo a los rangos planteados.

RANGOS:

1 a 0.786 = Ideal

0.714 a 0.357 = Mejorable

menor a 0.357 = Deficiente

8. Seguridad Complementario

En este apartado se observan características relacionadas con la protección de las instalaciones físicas y el acceso a los centros de datos en donde estén alojados los servicios cloud. Los controles se listan en la Tabla 6-16

Tabla 6-66 Controles para evaluación de atributo 2.1

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	El servicio cuenta con responsables de la Seguridad física, así como afines y otros	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Autenticación Biométrica	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	Sistemas de Identificación	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Métodos de Verificación	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	CCTV	Evaluación por cumplimiento: (SI=1, NO=0)	0
6	Guardias	Evaluación por cumplimiento: (SI=1, NO=0)	0
7	Redundancia Energética	Evaluación por cumplimiento: (SI=1, NO=0)	0
8	Redundancia de Comunicaciones	Evaluación por cumplimiento: (SI=1, NO=0)	0
9	Monitoreo periódico de accesos autorizados	Evaluación por cumplimiento: (SI=1, NO=0)	0
10	Actualización periódica de permisos de acceso	Evaluación por cumplimiento: (SI=1, NO=0)	0

En la Tabla 6-67 a continuación se indican los resultados de evaluación. Para este atributo puntual no se encontró información acerca de las seguridades de las instalaciones físicas por lo que en este atributo la calificación es 0.

Tabla 6-67 Resultados evaluación atributo 2.1

ID de la métrica	2.1
Nombre del indicador	2.1 Seguridad Complementario
Propósito del indicador	Se consulta sobre seguridades complementarias básicas respecto a instalaciones físicas del CSP
Controles asociados	2. Integridad/ Atributo: 2.1
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$(Numero\ de\ componentes\ que\ cumple)/(Numero\ total\ de\ componentes\ planteados)$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	0
Nivel de cumplimiento	0%

De acuerdo al nivel de cumplimiento que fue de 0=0%, está dentro del nivel "Deficiente" según el rango planteado.

RANGOS:

1 a 0.615 = Ideal

0.538 a 0.308 = Mejorable

menor a 0.308 = Deficiente

9. Notificación y respuesta de incidentes de seguridad

Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes. Los controles sugeridos se indican en la Tabla 6-68

Tabla 6-68 Controles para evaluación de atributo 2.4

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Cuenta con un plan de emergencia por incidentes de seguridad	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	¿Cuenta con un firewall a nivel de aplicación?	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	Notifica sobre procedimientos de copia de seguridad en terminal móvil en caso de un incidente	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	¿Cuenta con herramientas de registro incidentes de aplicaciones?	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Cuenta con un plan de recuperación de desastres	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Cuenta con un backup de servicios cloud.	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	Brinda una respuesta de incidentes automatizada	Evaluación por cumplimiento: (SI=1, NO=0)	1

Se observa el resumen de la evaluación del atributo, que tiene resultados esperados, debido a que la plataforma cuenta con certificaciones que contemplan eventos e incidentes de seguridad.

Tabla 6-69 Resultados de evaluación atributo 2.4

ID de la métrica	2.4
Nombre del indicador	2.4. Notificación y respuesta de incidentes de seguridad
Propósito del indicador	Se califica la capacidad del servicio en cuanto a respuesta y notificación de incidentes

Controles asociados	2. Integridad/ Atributo: 2.4
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros: _____
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	(*Numero de componentes que cumple*)/ (*Numero total de componentes planteados*)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	5
Nivel de cumplimiento	71%

La calificación de nivel de cumplimiento obtenida de 0.71=71% equivale a "Ideal" de acuerdo a los rangos planteados

RANGOS:

1 a 0.714 = Ideal

0.571 a 0.286 = Mejorable

menor a 0.286 = Deficiente

10. 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 a sus perfiles. Aquí en particular se asumen como usuarios a los distintos dispositivos en los que se puede activar la aplicación y que a su vez tienen accesos a los datos y configuraciones principales. En la Tabla 6-70 se muestran los controles para el atributo mencionado.

Tabla 6-70 Controles para atributo 2.5

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Maneja un listado general de cuentas	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Maneja un porcentaje de cuentas sin actividad	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Se mide el porcentaje de cuentas sin actividad en los últimos 30 días / 60 días	Evaluación por cumplimiento: (SI=1, NO=0)	
4	Se mide porcentaje de cuentas con perfil de administrador	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Posee cuentas de servicio o test	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Proporciona autenticación fuerte y control de acceso para el perfil de administración	Evaluación por cumplimiento: (SI=1, NO=0)	1

7	Presenta monitoreo de las sesiones en busca de actividades inusuales	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Incluye monitoreo y envío de alertas sobre el uso de información etiquetada como crítica	Evaluación por cumplimiento: (SI=1, NO=0)	1
9	Mantiene políticas de asignación y control para usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
10	Proporciona monitoreo de actividad de usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
11	Posee una actualización y revisión periódica de lista de usuarios con privilegios	Evaluación por cumplimiento: (SI=1, NO=0)	1
12	Cuenta con políticas internas y cumplimiento de normativas como SOX, PCI e HIPAA	Evaluación por cumplimiento: (SI=1, NO=0)	1
13	Emplea herramientas como SAPM (Shared Account Password Management o Gestión de Contraseñas de Cuentas Compartidas)	Evaluación por cumplimiento: (SI=1, NO=0)	1
14	Posee un listado del número total de cuentas y sus perfiles	Evaluación por cumplimiento: (SI=1, NO=0)	1

Basados en las certificación y demás normas de cumplimiento se realiza el análisis del atributo de control de cuentas de usuario. En la Tabla 6-21 se observa el resultado de la medición.

Tabla 6-71 Resultado evaluación atributo 2.5

ID de la métrica	2.5
Nombre del indicador	2.5. Gestión y control de cuentas de usuario
Propósito del indicador	Se validan las medidas de seguridad en cuanto al monitoreo y revisión de los usuarios y sus cuentas de acuerdo a sus perfiles
Controles asociados	2. Integridad/ Atributo: 2.5
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X___ Otros: _____
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$\frac{(Numero\ de\ componentes\ que\ cumple)}{(Numero\ total\ de\ componentes\ planteados)}$
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	13
Nivel de cumplimiento	0.93

De acuerdo a la tabla el cumplimiento de este atributo es de 0.93=93% que lo sitúa como ideal.

RANGOS:

1 a 0.714 = Ideal

0.643 a 0.357 = Mejorable

menor a 0.357 = Deficiente

11. Gestión de contenido anti-spam / correo electrónico

Se considero apropiado someter este atributo a evaluación debido a que la app es fundamentalmente para gestión, envió y recepción de correos electrónicos.

Tabla 6-72 Controles para evaluación atributo 2.8

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Monitoriza el número de correos electrónicos procesados	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Valida el número de correos electrónicos rechazados por restricciones de spam / contenido	Evaluación por cumplimiento: (SI=1, NO=0)	0
3	Realiza un control de MB de correo electrónico rechazado (ancho de banda utilizado por el móvil)	Evaluación por cumplimiento: (SI=1, NO=0)	0
4	Controla el número de correos electrónicos salientes con contenido inapropiado	Evaluación por cumplimiento: (SI=1, NO=0)	0
5	Lleva controles acerca del porcentaje de falsa identificación de spam	Evaluación por cumplimiento: (SI=1, NO=0)	0

En esta evaluación no se encontró información al respecto sin embargo dentro de la aplicación existe opciones de configuración de correo electrónico y se establece las debidas protecciones embebidas en la misma aplicación. Los resultados los observamos a continuación.

Tabla 6-73 Resultado de evaluación de atributo 2.8

ID de la métrica	2.8
Nombre del indicador	2.8. Gestión de contenido anti-spam / correo electrónico
Propósito del indicador	Se validan las acciones a tomar respecto a la incidencia de contenido spam a la app móvil
Controles asociados	2. Integridad/ Atributo: 2.8
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros:
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	$(Numero\ de\ componentes\ que\ cumple)/(Numero\ total\ de\ componentes\ planteados)$
Escala	Porcentaje

Nivel para el cumplimiento	100%
Medición	0
Nivel de cumplimiento	0%

De acuerdo a este resultado el cumplimiento de este atributo es de 0% lo que indica que es "deficiente" pero se debe realizar un análisis más a profundidad obteniendo más información al respecto.

RANGOS:
1 a 0.8 = Ideal
0.6 a 0.4 = Mejorable
menor a 0.4 = Deficiente

12. Políticas de contraseña

Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad. En la Tabla 6-74 observamos los controles a evaluar.

Tabla 6-74 Controles a evaluar atributo 5.1

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Posee una política de caducidad de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
2	Posee políticas sobre regulación de longitud de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
3	Cuenta con política de autenticación en dos pasos	Evaluación por cumplimiento: (SI=1, NO=0)	1
4	Cuenta con política sobre complejidad de contraseñas	Evaluación por cumplimiento: (SI=1, NO=0)	1
5	Política sobre uso de autenticaciones biométricas	Evaluación por cumplimiento: (SI=1, NO=0)	1
6	Las claves deben tener propietarios identificables (claves de enlace a las identidades) y habrá políticas de administración clave.	Evaluación por cumplimiento: (SI=1, NO=0)	1
7	¿Existen políticas donde se definen y documentan todos los requisitos y niveles de confianza para el acceso de los clientes?	Evaluación por cumplimiento: (SI=1, NO=0)	1
8	Política sobre implementación de interfaz estándar OAuth 2.0 o equivalentes?	Evaluación por cumplimiento: (SI=1, NO=0)	1

En este apartado observamos que el tema de autenticación es muy valorado y por lo tanto se ve reflejado a continuación en el resultado de la misma.

Tabla 6-75 Resultado evaluación de atributo 5.1

ID de la métrica	5.1
Nombre del indicador	5.1. Políticas de contraseña
Propósito del indicador	Se verifica el cumplimiento de condiciones que hacen que la implementación de contraseñas se ajuste a las mejores prácticas de seguridad

Controles asociados	5. Authenticity/ Atributo: 5.1
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros: _____
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:
Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	(*Numero de componentes que cumple*)/ (*Numero total de componentes planteados*)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	8
Nivel de cumplimiento	100%

Respecto al cumplimiento de este atributo, la calificación obtenida es del 100% que lo encasilla en un estado "Ideal".

13. Contexto de uso

Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc. De esta manera se podrá obtener un perfil del usuario respecto al uso, lugares, etc. En la Tabla 6-76 se muestra los controles de este atributo

Tabla 6-76 Controles para evaluar atributo 5.3

N°	***Controles a evaluar***	***Medición***	***Resultados***
1	Capacidad de detección mediante biometría del comportamiento	Evaluación por cumplimiento: (SI=1, NO=0)	0
2	Detecta cambios de acceso al sistema, cambios de dirección IP incoherentes o franjas horarias	Evaluación por cumplimiento: (SI=1, NO=0)	0

Al someter a las aplicaciones a estos controles referentes al contexto de uso ninguno de ellos los cumplía. No se quiere decir que por ello es vulnerable, sino se plantea como oportunidades de mejora para fortalecer los procesos de autenticación y uso.

Tabla 6-77 Resultado evaluación

ID de la métrica	5.3
Nombre del indicador	5. 3. Contexto de uso
Propósito del indicador	Verifica posibles vulnerabilidades basado en opciones propias de los dispositivos móviles como el GPS, giroscopio, etc.
Controles asociados	5. Authenticity/ Atributo: 5.3
Perspectiva MCC	Usuario: _X_ Proveedor:___Broker:____Otros: _____
Modelo de Servicio MCC evaluado	IaaS:_____ PaaS:_____ SaaS: _X__ Otros:

Modelo de Despliegue MCC evaluado	Publico:___Privado: _X_ Hibrido:___Comunitario: ___
Formula	(*Numero de componentes que cumple*)/ (*Numero total de componentes planteados*)
Escala	Porcentaje
Nivel para el cumplimiento	100%
Medición	0
Nivel de cumplimiento	0%

En este caso el atributo según el nivel de cumplimiento la valoración es "mejorable".

RANGOS:
1 = Ideal
menor a 1 = Mejorable

6.3 Conclusiones de la aplicación del Método de Evaluación

La aplicación del Método de Evaluación propuesto, nos ha permitido obtener los resultados deseados, ya que mediante este Método conseguimos evaluar los artefactos deseados, mostramos los problemas hallados, aplicamos los controles correspondientes con sus consecuentes métricas resultantes.

Este capítulo ha mostrado, cómo se aplica el método de evaluación de la seguridad para aplicaciones MCC propuesto en este trabajo. Para ello se basó en el modelo de calidad de seguridad SQuaRE.

Es necesario resaltar que, al ser aplicaciones provistas por terceros, estas pueden fallar, o no estar disponibles o como ya sucedió en el presente análisis no brindar suficiente información, lo que hace necesario tener en cuenta varios aspectos que ayuden a solventar este tipo de problemas.

Por medio de la aplicación de casos de estudio reales, se ha podido dar una retroalimentación al modelo, mejorarlo y además descubrir aspectos que a simple vista son difíciles de divisar. Además, se tomaron la mayoría de atributos y se aplicaron, a fin de conocer cómo podrían ser usadas las métricas, los umbrales y en definitiva todos los pasos que engloba la evaluación.

Cabe señalar que existen atributos que no fueron tomados en cuenta por su relación a las diferentes aplicaciones para MCC, para tener un rango de acción y no dejar

por fuera del análisis aplicaciones y tratar de disminuir el sesgo al momento de la evaluación.

Capitulo 7. Conclusiones

En este capítulo se recogen las conclusiones generales de este trabajo, los trabajos futuros propuestos con miras a la continuación de esta investigación y las publicaciones realizadas como resultados de esta tesina.

7.1 Conclusiones

Las aplicaciones MCC son parte del día a día de millones de usuarios alrededor del mundo, por lo tanto, es muy importante contar con un proceso formal para la evaluación de parámetros relacionados entre otros los que tienen que ver con la seguridad.

La motivación principal de esta tesina de Master, es el contar con este método que permita la evaluación de la seguridad de aplicaciones desplegadas en plataformas móviles para Cloud Computing. Sin embargo, se tiene la conciencia de que este es el primer paso para la formalización de este método el mismo que después de las debidas pruebas documentadas y avales de los entes competentes podrá pasar de una "Propuesta Metodológica" a un "Método" formal.

Dentro de las posibilidades que se identificó durante la elaboración del presente trabajo, ha sido la opción de evaluar no solo la app final sino también la plataforma SaaS en donde se despliegan este tipo de aplicaciones basadas en Cloud Computing. Al igual que se podrían integrar diversas perspectivas, no solo desde el usuario final que es muy limitada, sino también desde la perspectiva del proveedor, del bróker o incluso desde el medio de transporte. Para ello se deberían levantar más controles y métricas que abarquen temas puntuales que involucren las perspectivas mencionadas.

También se ha tenido en cuenta el producto final, al cual incluso se han dirigido los casos de estudio, y en el que se ve globalmente la aplicación, los controles y métricas obtenidas para así llegar a la obtención de la presente propuesta.

Según los objetivos planteados en el primer capítulo:

1. Revisión de la Literatura relacionada a las aplicaciones MCC y la seguridad.
2. Elaboración de un Modelo de seguridad para aplicaciones MCC.

3. Finalmente levantar una: Propuesta metodológica de evaluación de la seguridad para aplicaciones MCC.

4. Ejemplificar por medio de casos de estudio la metodología planteada.

Se puede decir que todos y cada uno de ellos han sido abordados y satisfechos:

El objetivo 1 fue conseguido mediante un mapeo sistemático después del cual se detectó que hay una falta de trabajos que se enfoquen en la seguridad de aplicaciones móviles para Cloud. También aportó enormemente al entendimiento del estado del arte en tema Mobile Cloud Computing, cuáles son las brechas en la investigación en estos temas y qué falta por recorrer en los mismos.

El objetivo 2, fue abordado con un estudio de los estándares involucrados y cómo estos pueden aplicarse. Para ello se estudió el estándar ISO 25000 SQuaRE y sus predecesores, para finalmente elaborar un Modelo de Seguridad extendido y adaptado para aplicaciones MCC y a la última norma ISO 25000 SQuaRE, puntualmente la característica de Seguridad.

Con respecto al objetivo 3, se definió el proceso de evaluación empleando para ello la notación SPEM, contribuyendo a proporcionar una especificación guiada y detallada del método para los evaluadores. Este método de evaluación utiliza como artefacto principal de entrada el Modelo de Seguridad detallado en el capítulo 4.

Por último, el objetivo 4 se cumplió aplicando el método de evaluación a tres casos de estudio donde se muestran los pasos a seguir definidos en la propuesta metodológica de evaluación y que permiten evaluar la seguridad de estas aplicaciones.

Como se puede observar los objetivos de la tesina fueron abarcados en su totalidad y vale la pena destacar que a nivel académico se ha logrado un claro entendimiento del tema, de cómo se puede contribuir a la seguridad tomando como base estándares y cómo esta resulta una forma clara de presentar un modelo y un proceso de evaluación que al estar definido con una notación conocida como lo es SPEM puede contribuir claramente y sin ambigüedades a evaluar aplicaciones para MCC sin embargo esta metodología se puede extender a aplicaciones de cualquier tipo, ayudando a desarrolladores y los diferentes stackeholders a obtener productos de calidad.

Referencias.

[1] N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing: A survey,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 1, pp. 84–106, Jan. 2013.

[2] R. Krutz, R. Dean, and R. D. V. Ronald L. Krutz, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing [Kindle Edition]*. Wiley Publishing, 2010.

[3] S. S. Qureshi, T. Ahmad, and K. Rafique, “Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues,” *2011 IEEE Int. Conf. Cloud Comput. Intell. Syst.*, pp. 467–471, 2011.

[4] C. Wang, P. Zou, Z. Liu, and J. Wang, “CS-DRM: A Cloud-based SIM DRM Scheme for Mobile Internet,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2011, p. 14:1--14:30, 2011.

[5] S. Abolfazli, Z. Sanaei, M. Shiraz, and A. Gani, “MOMCC: Market-oriented architecture for Mobile Cloud Computing based on Service Oriented Architecture,” *Proc. 1st IEEE Int. Conf. Commun. China Work.*, pp. 8–13, 2012.

[6] Y. Wang, R. Chen, and D. C. Wang, “A Survey of Mobile Cloud Computing Applications : Perspectives and Challenges,” *Wirel. Pers. Commun.*, pp. 1–29, 2014.

[7] Cloud Security Alliance, “Top Threats to Cloud Computing,” *Security*, no. March, pp. 1–14, 2010.

[8] Gartner, “Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing,” 2016. [Online]. Available: https://www.gartner.com/doc/3142020?refval=&pcp=mpe. [Accessed: 10-Mar-2016].

[9] ISO, “ISO/IEC 25010:2011 - Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models,” 2011. [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=35733. [Accessed: 21-Mar-2016].

[10] ISO, “ISO/IEC 27001:2013 - Information technology -- Security techniques --

Information security management systems -- Requirements," 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. [Accessed: 21-Mar-2016].

[11] SSAE 16, "SOC 2 Report – Trust Services Principles | The SSAE 16 Reporting Standard - SOC 1 - SOC 2 - SOC 3," 2015. [Online]. Available: http://www.ssae-16.com/soc-2/. [Accessed: 21-Mar-2016].

[12] A. Wright, "Get smart," *Technology*, pp. 1–3.

[13] D. Kovachev, D. Renzel, R. Klamma, and Y. Cao, "Mobile community cloud computing: Emerges and evolves," *Proc. - IEEE Int. Conf. Mob. Data Manag.*, pp. 393–395, 2010.

[14] T. M. Maarouk, D. E. Saidouni, and M. Khergag, "Towards a calculus for distributed, real-time and mobile systems," *J. Softw.*, vol. 7, no. 3, pp. 564–574, 2012.

[15] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Trans. Serv. Comput.*, vol. 5, no. 2, pp. 220–232, Apr. 2012.

[16] Y. J. Larios Olivos, "Guía metodológica para la protección de datos en la utilización de la computación en la nube." 2014.

[17] C. C. V, "Security Guidance Critical Areas of Focus for," *Security*, vol. 1, no. December, pp. 1–76, 2009.

[18] F. Liu, J. Tong, J. Mao, and R. Bohn, "NIST Cloud Computing Security Reference Architecture," *NIST Spec. ...*, vol. 500, no. 299, pp. 1–204, 2013.

[19] P. Martin and K. Brohman, "CLOUDQUAL: A Quality Model for Cloud Services," *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1527–1536, 2014.

[20] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," *Cloud Secur. Alliance*, vol. 2, no. 1, 2011.

[21] K. Mohiuddin, A. Islam, A. Alam, and A. Ali, "24X7X365: Mobile Cloud Access," in *Proceedings of the CUBE International Information Technology*

Conference on - CUBE '12, 2012, p. 544.

[22] M. A. Maldonado Revelo, "Diseño e Implementación de una Red de Servicios basada en los conceptos de Cloud Computing," ESCUELA POLITECNICA DEL EJERCITO, 2013.

[23] S. MurugESan and I. Bojanova, Eds., *Encyclopedia of Cloud Computing*, FIRST 1st. 2016.

[24] B. Ohlman, A. Eriksson, and R. Rembarz, "What Networking of Information Can Do for Cloud Computing," 2009.

[25] P. Mell and T. Grance, "NIST SP 800-145 - The NIST Definition of Cloud Computing.," vol. 145, no. September, p. 7, 2011.

[26] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," 2011.

[27] A. Dver., "Enemy Of Saas?," 2008.

[28] J. D. Lasica, *Identity in the Age of Cloud Computing: The next-generation Internet's impact on business, governance and social interaction*. 2009.

[29] Y. Chen, W.-S. Ku, J. Feng, P. Liu, and Z. Su, "Secure Distributed Data Storage in Cloud Computing," in *Cloud Computing*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011, pp. 221–248.

[30] H. Qi and A. Gani, "Research on mobile cloud computing: Review, trend and perspectives," *2012 2nd Int. Conf. Digit. Inf. Commun. Technol. its Appl. DICTAP 2012*, pp. 195–202, 2012.

[31] "Análisis de amenazas y ataques a la seguridad de la nube | ITSitio Distribución." [Online]. Available: http://distribucion.itsitio.com/es/analisis-de-amenazas-y-ataques-a-la-seguridad-de-la-nube/. [Accessed: 10-Jul-2017].

[32] J. M. Myerson, "Best practices to develop SLAs for cloud computing Develop a standard way to create service level agreements that multiple partners can use," pp. 1–9, 2013.

[33] S. A. Z. Sanaei A. Gani, R. Buyya, "Heterogeneity in Mobile Cloud Computing:Taxonomy and Open Challenges," *IEEE Commun. Surv. Tutorials*

(Accepted Publ., pp. 1–24, 2013.

[34] AEPONA, "Mobile Cloud Computing Solution Brief." 2010.

[35] L. Liu, R. Moulic, and D. Shea, "Cloud Service Portal for Mobile Device Management," in *2010 IEEE 7th International Conference on E-Business Engineering*, 2010, pp. 474–478.

[36] J. H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications," *Proc. 24th ACM SIGPLAN Conf. companion Object oriented Program. Syst. Lang. Appl.*, pp. 627–634, 2009.

[37] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: Motivation, taxonomies, and open challenges," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 337–368, 2014.

[38] A. U. R. Khan, M. Othman, F. Xia, and A. N. Khan, "Context-Aware Mobile Cloud Computing and Its Challenges," *IEEE Cloud Comput.*, vol. 2, no. 3, pp. 42–49, May 2015.

[39] P. Kulkarni and R. Khanai, "Addressing mobile Cloud Computing security issues: A survey," in *Communications and Signal Processing (ICCSP), 2015 International Conference on*, 2015, pp. 1463–1467.

[40] M. Satyanarayanan, P. Bahl, R. Cáceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.

[41] P. Gómez, "Técnicas de Mantenimiento de Qos en MCC," 2015.

[42] O. Kharif, "Perils of the Mobile Cloud.," *McGraw-Hill Co.*, 2009.

[43] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of wi-fi and bluetooth battery exhaustion attacks on mobile devices," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2010, pp. 1–9.

[44] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa)," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications - HotMobile '10*, 2010, pp. 43–47.

[45] J. Brodkin, "Gartner: Seven cloud-computing security risks," *Infoworld*, vol. 2008,

pp. 1–3, 2008.

[46] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," *Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW '09*, p. 127, 2009.

[47] "Carrier IQ Rootkit Reportedly Logs Everything On Millions Of Phones [Updated] | PCWorld." [Online]. Available: http://www.pcworld.com/article/245229/carrier_iq_rootkit_logs_everything_on_millions_of_phones.html. [Accessed: 06-Mar-2017].

[48] M. Fahrmair, W. Sitou, and B. Spanfelner, "Security and privacy rights management for mobile and ubiquitous computing," *Work. UbiComp Priv.*, 2005.

[49] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," *Mob. Comput. Syst. Appl.*, pp. 1–7, Dec. 1994.

[50] B. D. Noble, M. Satyanarayanan, D. Narayanan, J. E. Tilton, J. Flinn, and K. R. Walker, "Agile application-aware adaptation for mobility," *ACM SIGOPS Oper. Syst. Rev.*, vol. 31, no. 5, pp. 276–287, 1997.

[51] J. R. Lorch and A. J. Smith, "Software strategies for portable computer energy management," *IEEE Pers. Commun.*, vol. 5, no. 3, pp. 60–73, 1998.

[52] K. Mansley, A. R. Beresford, and D. Scott, "The Carrot Approach: Encouraging Use of Location Systems BT - UbiComp 2004: Ubiquitous Computing," *UbiComp 2004 Ubiquitous Comput.*, vol. 3205, no. Chapter 22, pp. 366–383, 2004.

[53] C. Seo, S. Malek, and N. Medvidovic, "Estimating the energy consumption in pervasive java-based systems," in *6th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2008*, 2008, pp. 243–247.

[54] S. Kitanov and T. Janevski, "State of the Art: Mobile Cloud Computing," *2014 Sixth Int. Conf. Comput. Intell. Commun. Syst. Networks*, pp. 153–158, 2014.

[55] J. Archer, A. Boehme, D. Cullinance, N. Puhlmann, P. Kurz, and J. Reavis, "Security Guidance for Critical Areas of Mobile Computing," *Cloud Secur. Alliance*, no. December, pp. 1–60, 2012.

[56] Iso/Iec, "INTERNATIONAL STANDARD ISO / IEC Information technology —

Security techniques — Information security management systems — Overview and Vocabulary 2014," vol. 2014, 2014.

[57] ISO, "ISO 25010," 2005. [Online]. Available: http://iso25000.com/index.php/normas-iso-25000/iso-25010.

[58] ISO/IEC, "ISO/IEC 25010 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models." 2011.

[59] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, no. TR/SE-0401, p. 28, 2004.

[60] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," *Engineering*, vol. 2, p. 1051, 2007.

[61] A. Méndez-porras, C. Quesada-lópez, and M. Jenkins, "Automated Testing of Mobile Applications : A Systematic Map and Review," *CIBSE 2015 - XVIII Ibero-American Conf. Softw. Eng.*, pp. 195–208, 2015.

[62] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," *Information and Software Technology*, vol. 51, no. 1. pp. 7–15, 2009.

[63] L. F. B. Soares, D. A. B. Fernandes, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Cloud Security: State of the Art," in *Security, Privacy and Trust in Cloud Systems*, S. Nepal and M. Pathan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 3–44.

[64] H. Yang and M. Tate, "A Descriptive Literature Review and Classification of Cloud Computing Research.," *Commun. Assoc. Inf. Syst.*, vol. 31, pp. 35–60, 2012.

[65] L. C. Jersak, A. C. Costa, D. A. Callegari, L. C. Jersak, C. Adriana, and D. A. Callegari, "A Systematic Review on Mobile Health Care A Systematic Review on Mobile Health Care," no. 73, 2013.

[66] V. Khatibi and E. Khatibi, "Issues on Cloud Computing: A Systematic Review," *Int. Conf. Comput. Tech. Mob. Comput.*, pp. 212–216, 2012.

[67] E. Ibukun and O. Daramola, "A systematic literature review of mobile cloud computing," *Int. J. Multimed. Ubiquitous Eng.*, vol. 10, no. 12, pp. 135–152, 2015.

[68] M. R. Rahimi, J. Ren, C. H. Liu, A. V Vasilakos, and N. Venkatasubramanian, "Mobile Cloud Computing: A Survey, State of Art and Future Directions," *Mob. Netw. Appl.*, vol. 19, no. 2, pp. 133–143, 2014.

[69] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wirel. Commun. Mob. Comput.*, no. February 2015, pp. 421–430, 2011.

[70] D. Goyal and M. B. Krishna, "Secure framework for data access using Location based service in Mobile Cloud Computing," in *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1–6.

[71] D. Huang, X. Zhang, M. Kang, and J. Luo, "MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication," in *Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on*, 2010, pp. 27–34.

[72] W. D. Yuefa and G. Yaqiang, "Data security model for cloud computing," *... Inf. Secur. ...*, no. c, pp. 23–43, 2009.

[73] D. B. Hoang and L. Chen, "Mobile Cloud for Assistive Healthcare (MoCAsH)," in *Proceedings of the 2010 IEEE Asia-Pacific Services Computing Conference*, 2010, pp. 325–332.

[74] P. Cedillo, A. Fernandez, A. Insfran, and S. Abrahão, "Quality of Web Mashups: A Systematic Mapping Study," *Proc. ICWE 2013 Int. Work. Compos. QWE, MDWE, DMSSW, Emot. CSE, SSN, PhD Symp.*, vol. 8295, pp. 66–78, 2013.

[75] A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Futur. Gener. Comput. Syst.*, vol. 29, no. 5, pp. 1278–1299, Jul. 2013.

[76] D. Dev and K. L. Baishnab, "A Review and Research Towards Mobile Cloud Computing," in *Proceedings of the 2014 2Nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2014, pp. 252–256.

[77] D. Huang, T. Xing, and H. Wu, "Mobile cloud computing service models: a user-

centric approach," *IEEE Netw.*, vol. 27, no. 5, pp. 6–11, 2013.

[78] Cloud Security Alliance, "The Treacherous 12 Cloud Computing Top Threats in 2016," *Security*, no. February, pp. 1–34, 2016.

[79] I. 9126, "Draft International Standard Iso / Iec Fdis," vol. 1991, 1991.

[80] Omg, "Software & Systems Process Engineering Meta-Model Specification V2.0," no. April, p. 236, 2008.

[81] I. P. Cedillo Orellana, "Un Método de Evaluación de Usabilidad de Mashups Basado en la Composicionalidad de sus Componentes," 2013.

[82] kaspersky, "¿QUÉ ES UN ATAQUE MAN-IN-THE-MIDDLE? – Blog oficial de Kaspersky Lab." [Online]. Available: https://blog.kaspersky.com.mx/que-es-un-ataque-man-in-the-middle/469/. [Accessed: 28-Aug-2017].

[83] "Weblet - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Weblet. [Accessed: 29-Aug-2017].

Apéndices - Plantillas

Documento de Especificación de Requisitos de Evaluación

a) Perspectiva desde la que se Ejecutará la Evaluación de Seguridad MCC (Marcar con una X).

Usuario:	
Bróker:	
Proveedor:	
Otros: _____	

b) Modelo de despliegue MCC (Marcar con una X).

- Publico	
- Privado	
- Hibrido	
- Otros (Especificar)	

c) Lista de Atributos a Evaluar

No.	**Atributo**	**Código Atributo**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		

Plantilla 1 Documento de Especificación de Requisitos de Evaluación.

Apéndice B - Plantillas de Casos de Estudio

Documento de Especificación de Requisitos de Evaluación

a) Perspectiva desde la que se Ejecutará la Evaluación de Seguridad MCC (Marcar con una X)

Usuario:	X
Bróker:	
Proveedor:	
Otros: _____	

b) Modelo de despliegue MCC (Marcar con una X).

- Publico	
- Privado	
- Hibrido	
- Otros (Especificar)	

c) Lista de Atributos a Evaluar

No.	Atributo	Código Atributo
1	1.1. Administración de Datos en el móvil	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
8	1.8. Gobierno y políticas BYOD	1.8
9	2.1 Seguridad Complementario	2.1
10	2.2. Buenas prácticas de prevención	2.2
11	2.3. Seguridad en el desarrollo de código	2.3
12	2.4. Notificación y respuesta de incidentes de seguridad	2.4
13	2.5. Gestión y control de cuentas de usuario	2.5
14	2.6. Auditorias	2.6
15	2.7. Estado del Antivirus	2.7
16	2.8. Gestión de contenido anti-spam / correo electrónico	2.8
17	3.1. No Repudio	3.1
18	4.1. Responsabilidad	4.1
19	5.1. Políticas de contraseña	5.1
20	5.2. IDM - Identity Management	5.2
21	5. 3. Contexto de uso	5.3

Plantilla 2 Plantilla de Requisitos de Evaluación Gmail

Apéndice C - Plantillas de Casos de Estudio

Documento de Especificación de Requisitos de Evaluación

a) Perspectiva desde la que se Ejecutará la Evaluación de Seguridad MCC (Marcar con una X).

Usuario:	X
Bróker:	
Proveedor:	
Otros: _____	

b) Modelo de despliegue MCC (Marcar con una X).

- Publico	
- Privado	
- Hibrido	
- Otros (Especificar)	

c) Lista de Atributos a Evaluar

No.	Atributo	Código Atributo
1	1.1. Administración de Datos en el móvil	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
8	1.8. Gobierno y políticas BYOD	1.8
9	2.1 Seguridad Complementario	2.1
10	2.2. Buenas prácticas de prevención	2.2
11	2.3. Seguridad en el desarrollo de código	2.3
12	2.4. Notificación y respuesta de incidentes de seguridad	2.4
13	2.5. Gestión y control de cuentas de usuario	2.5
14	2.6. Auditorias	2.6
15	2.7. Estado del Antivirus	2.7
16	2.8. Gestión de contenido anti-spam / correo electrónico	2.8
17	3.1. No Repudio	3.1
18	4.1. Responsabilidad	4.1
19	5.1. Políticas de contraseña	5.1
20	5.2. IDM - Identity Management	5.2
21	5. 3. Contexto de uso	5.3

Plantilla 2 Plantilla de Requisitos de Evaluación Office365

Apéndice D - Plantillas de Casos de Estudio

Documento de Especificación de Requisitos de Evaluación

a) Perspectiva desde la que se Ejecutará la Evaluación de Seguridad MCC (Marcar con una X)

Usuario:	X
Bróker:	
Proveedor:	
Otros: _____	

d) Modelo de despliegue MCC (Marcar con una X).

- Publico	
- Privado	
- Hibrido	
- Otros (Especificar)	

b) Lista de Atributos a Evaluar

No.	Atributo	Código Atributo
1	1.1. Administración de Datos en el móvil	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
8	1.8. Gobierno y políticas BYOD	1.8
9	2.1 Seguridad Complementario	2.1
10	2.2. Buenas prácticas de prevención	2.2
11	2.3. Seguridad en el desarrollo de código	2.3
12	2.4. Notificación y respuesta de incidentes de seguridad	2.4
13	2.5. Gestión y control de cuentas de usuario	2.5
14	2.6. Auditorias	2.6
15	2.7. Estado del Antivirus	2.7
16	2.8. Gestión de contenido anti-spam / correo electrónico	2.8
17	3.1. No Repudio	3.1
18	4.1. Responsabilidad	4.1
19	5.1. Políticas de contraseña	5.1
20	5.2. IDM - Identity Management	5.2
21	5. 3. Contexto de uso	5.3

Plantilla 2 Plantilla de Requisitos de Evaluación Salesforce

Apéndice E: Bibliografía Mapeo Sistemático de Seguridad

Bibliografía IEEE Xplore

[1] A. Afianian, S. S. Nobakht, and M. B. Ghaznavi-Ghoushchi, "Energy-efficient secure distributed storage in mobile cloud computing," in *2015 23rd Iranian Conference on Electrical Engineering*, 2015, pp. 740–745.

[2] K. Akherfi, H. Harroud, and M. Gerndt, "A mobile cloud middleware for data storage and integrity," in *Cloud Technologies and Applications (CloudTech), 2015 International Conference on*, 2015, pp. 1–7.

[3] M. M. Alam, S. Hati, D. De, and S. Chattopadhyay, "SeCure Sharing Of Mobile Device Data Using Public Cloud," in *Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference* -, 2014, pp. 149–154.

[4] S. L. Albuquerque and P. R. L. Gondim, "Security in Cloud-Computing-Based Mobile Health," *IT Prof.*, vol. 18, no. 3, pp. 37–44, May 2016.

[5] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V Vasilakos, K. Li, and A. Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds," *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–10, 2015.

[6] M. Aloqaily, B. Kantarci, and H. T. Mouftah, "On the impact of quality of experience (QoE) in a vehicular cloud with various providers," in *2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy)*, 2014, pp. 94–98.

[7] H. S. Alqahtani and G. Kouadri-Mostefaou, "Multi-clouds Mobile Computing for the Secure Storage of Data," in *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, 2014, pp. 495–496.

[8] P. Angin, B. Bhargava, and Z. Jin, "A Self-Cloning Agents Based Model for High-Performance Mobile-Cloud Computing," in *2015 IEEE 8th International Conference on Cloud Computing*, 2015, pp. 301–308.

[9] P. Angin, B. Bhargava, and R. Ranchal, "Tamper-resistant autonomous agents-based mobile-cloud computing," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, 2016, pp. 843–847.

[10] L. Apiecionek, T. Kosowski, H. Kruszynski, M. Piotrowski, and R. Palka, "The concept of integration tool for the civil and military service cooperation during emergency response operations," in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–7.

[11] C. A. Ardagna, M. Conti, M. Leone, and J. Stefa, "An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments," *IEEE Trans. Serv. Comput.*, vol. 7, no. 3, pp. 373–386, Jul. 2014.

[12] G. Arfaoui, S. Gharout, and J. Traor, “Trusted Execution Environments: A Look under the Hood,” in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on*, 2014, pp. 259–266.

[13] A. Awad, A. Matthews, and B. Lee, “Secure cloud storage and search scheme for mobile devices,” in *MELECON 2014 - 2014 17th IEEE Mediterranean Electrotechnical Conference*, 2014, pp. 144–150.

[14] A. Awad, A. Matthews, Y. Qiao, and B. Lee, “Chaotic Searchable Encryption for Mobile Cloud Storage,” *IEEE Trans. Cloud Comput.*, vol. PP, no. 99, pp. 1–14, 2015.

[15] M. R. Baharon, Q. Shi, and D. Llewellyn-Jones, “A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing,” in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 618–625.

[16] M. Bahrami, “Cloud Computing for Emerging Mobile Cloud Apps,” in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on*, 2015, pp. 4–5.

[17] P. Balboni and B. Iafelice, “Mobile cloud for enabling the EU eHealth sector Regulatory issues and opportunities,” in *Telecom World (ITU WT), 2011 Technical Symposium at ITU*, 2011, pp. 51–56.

[18] L. Baleh, L. Suciu, and J.-M. Bonnin, “Enriched connectivity-as-a-service for dynamic Mobile-Cloud,” in *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, 2012, pp. 655–660.

[19] C. Barz, A. Diefenbach, F. Abut, M. Wilmes, P. Sevenich, P. Simon, and N. Bret, “The CoNSIS approaches to network management and monitoring,” in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–8.

[20] Y. Baseri, A. Hafid, and S. Cherkaoui, “K-anonymous location-based fine-grained access control for mobile cloud,” in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2016, pp. 720–725.

[21] R. Baskarane, P. Archana, A. Priyadharshini, and P. Hemalatha, “MC2 for enhancing the lifetime of a cellular device,” in *International Conference on Information Communication and Embedded Systems (ICICES2014)*, 2014, pp. 1–6.

[22] K. Bicakci, D. Unal, N. Ascioglu, and O. Adalier, “Mobile Authentication Secure Against Man-in-the-Middle Attacks,” in *Proceedings of the 2014 2Nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2014, pp. 273–276.

[23] T. H. Bloebaum and K. Lund, "CoNSIS: Demonstration of SOA interoperability in heterogeneous tactical networks," in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–7.

[24] W. K. Bodin, D. Jaramillo, S. K. V Marimekala, and J. Borowski, "Think smart and communicate fast! Are you mobile in the Cloud?," in *2014 11th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT)*, 2014, pp. 1–6.

[25] J. Bong, Y. Suh, and Y. Shin, "Fast user authentication method considering mobility in multi clouds," in *International Conference on Information Networking*, 2016, vol. 2016–March, pp. 445–448.

[26] S. Bouzefrane and L. V. Thinh, "Trusted Platforms to Secure Mobile Cloud Computing," *2014 IEEE Intl Conf High Perform. Comput. Commun. 2014 IEEE 6th Intl Symp Cybersp. Saf. Secur. 2014 IEEE 11th Intl Conf Embed. Softw. Syst*, pp. 1068–1075, 2014.

[27] J. Brunel, R. Pacalet, S. Ouaarab, and G. Duc, "SecBus, a Software/Hardware Architecture for Securing External Memories," in *2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2014, pp. 277–282.

[28] L. Cailleux, "A new security service for future military messaging," in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–8.

[29] F. Carriedo and M. Beltran, "Mobile Cloud Computing to Provide Mobiquity as a Service on Telecommunication Vertical Clouds," in *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2015, pp. 211–220.

[30] B. Cha, S. Park, S. Shim, and J. Kim, "Secured mVoIP Service over Cloud and Container-Based Improvement," in *Advanced Information Networking and Applications (AINA), 2015 IEEE 29th International Conference on*, 2015, pp. 791–795.

[31] C. Chang, S. N. Srirama, and M. Liyanage, "A Service-Oriented Mobile Cloud Middleware Framework for Provisioning Mobile Sensing as a Service," in *Parallel and Distributed Systems (ICPADS), 2015 IEEE 21st International Conference on*, 2015, pp. 124–131.

[32] N. Che, Z. Chen, X. Zheng, and G. Chen, "Mobile Cloud Based System Architecture for Remote-Resident Multimedia Discovery and Access," in *Proceedings of the 2013 10th Web Information System and Application Conference*, 2013, pp. 361–364.

[33] E. Y. Chen and M. Itoh, "Virtual smartphone over IP," in *2010 IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2010, pp. 1–6.

[34] L. Chen and D. B. Hoang, "Addressing Data and User Mobility Challenges in the Cloud," in *Proceedings of the 2013 IEEE Sixth International Conference on Cloud Computing*, 2013, pp. 549–556.

[35] L. Chen, X. Zheng, and G. Chen, "A system architecture for intelligent logistics system," in *Proceedings - 2013 International Conference on Cloud Computing and Big Data, CLOUDCOM-ASIA 2013*, 2013, pp. 426–431.

[36] L. Chen, Y. Duan, M. Qiu, J. Xiong, and K. Gai, "Adaptive Resource Allocation Optimization in Heterogeneous Mobile Cloud Systems," in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 2015, pp. 19–24.

[37] C. Chilipirea, A. C. Petre, C. Dobre, and F. Pop, "Enabling Mobile Cloud Wide Spread Through an Evolutionary Market-Based Approach," *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–8, 2015.

[38] P. K. Chouhan, F. Yao, and S. Sezer, "Software as a service: Understanding security issues," in *2015 Science and Information Conference (SAI)*, 2015, pp. 162–170.

[39] T.-T. Chu and C.-T. Chiu, "A cost-effective minutiae disk code for fingerprint recognition and its implementation," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2016, pp. 981–985.

[40] Q. Dai, H. Yang, Q. Yao, and Y. Chen, "An improved security service scheme in mobile cloud environment," in *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, 2012, vol. 1, pp. 407–412.

[41] S. M. Daisy, R. S. Shaji, and J. P. Jayan, "Asymetric key based data communication under mobile cloud system," in *Communication Technologies (GCCT), 2015 Global Conference on*, 2015, pp. 559–564.

[42] N. R. Darve and D. P. Theng, "Comparison of biometric and non-biometric security techniques in mobile cloud computing," in *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, 2015, pp. 213–216.

[43] S. Das, M. Khatua, S. Misra, and M. Obaidat, "Quality-assured Secured Load Sharing in Mobile Cloud Networking Environment," *IEEE Trans. Cloud Comput.*, vol. PP, no. 99, pp. 1–1, 2015.

[44] S. R. Das, S. Chita, N. Peterson, B. A. Shirazi, and M. Bhadkamkar, "Home automation and security for mobile devices," in *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2011, pp. 141–146.

[45] K. David, D. Dixit, and N. Jefferies, "2020 Vision," *IEEE Veh. Technol. Mag.*, vol. 5, no. 3, pp. 22–29, Sep. 2010.

[46] D. Dennisen, F. Abut, D. Glosel, J. Bogenfeld, C. Barz, I. Aktas, K. Wehrle, and P. Sevenich, "Using cross-layer design to detect jamming attacks in the CoNSIS scenario," in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–7.

[47] D. Dev and K. L. Baishnab, "A Review and Research Towards Mobile Cloud Computing," in *2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2014, pp. 252–256.

[48] S. Dey, S. Sampalli, and Q. Ye, "Message digest as authentication entity for mobile cloud computing," in *2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC)*, 2013, pp. 1–6.

[49] S. Dey, S. Sampalli, and Q. Ye, "A Context-Adaptive Security Framework for Mobile Cloud Computing," in *2015 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, 2015, pp. 89–95.

[50] S. Dolev, I. H. Shtacher, B. Shapira, Y. Elovici, G. Messalem, D. Mimran, and M. Kopeetsky, "Exploiting simultaneous usage of different wireless interfaces for security and mobility," in *Second International Conference on Future Generation Communication Technologies (FGCT 2013)*, 2013, pp. 21–26.

[51] A. C. Donald and L. Arockiam, "A secure authentication scheme for MobiCloud," in *2015 International Conference on Computer Communication and Informatics (ICCCI)*, 2015, pp. 1–6.

[52] M. Dong, R. Ranjan, A. Y. Zomaya, and M. Lin, "Guest Editorial on Advances in Tools and Techniques for Enabling Cyber–Physical–Social Systems—Part I," *IEEE Trans. Comput. Soc. Syst.*, vol. 2, no. 3, pp. 38–40, Sep. 2015.

[53] H. Duan, X. Han, and Y. Wang, "Safety management study of construction enterprises - Based on data of Mcc Jingtang Construction Corporation (JTMCC)," *2010 Int. Conf. E-Product E-Service E-Entertainment, ICEEE2010*, pp. 1–5, Nov. 2010.

[54] M. A. Elgendy, A. Shawish, and M. I. Moussa, "MCACC: New approach for augmenting the computing capabilities of mobile devices with Cloud Computing," in *2014 Science and Information Conference*, 2014, pp. 79–86.

[55] J. Eloff and A. Singh, "The extended supply chain: A virtual collaborative ecosystem to enhance and drive innovation," in *2011 6th International Conference on Pervasive Computing and Applications*, 2011, pp. 2–2.

[56] D. I. Fadaraliki and S. Rajendran, "Process offloading from android device to cloud using JADE," in *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, 2015, pp. 1–5.

[57] K. Gai, Z. Du, M. Qiu, and H. Zhao, "Efficiency-Aware Workload Optimizations of Heterogeneous Cloud Computing for Capacity Planning in Financial Industry,"

in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 2015, pp. 1–6.

[58] K. Gai, M. Qiu, B. Thuraisingham, and L. Tao, "Proactive Attribute-based Secure Data Schema for Mobile Cloud in Financial Industry," in *Proceedings of the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conf on Embedded Software and Systems*, 2015, pp. 1332–1337.

[59] B. Gao, L. He, X. Lu, C. Chang, K. Li, and K. Li, "Developing Energy-Aware Task Allocation Schemes in Cloud-Assisted Mobile Workflows," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 1266–1273.

[60] P. Garg and V. Sharma, "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function," *2014 Int. Conf. Issues Challenges Intell. Comput. Tech.*, pp. 334–339, Feb. 2014.

[61] J. George, C. A. Chen, R. Stoleru, G. G. Xie, T. Sookoor, and D. Bruno, "Hadoop MapReduce for Tactical Clouds," in *Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on*, 2014, pp. 320–326.

[62] J. Glowacka and M. Amanowicz, "Application of Dezert-Smarandache theory for tactical MANET security enhancement," in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–6.

[63] J. Glowacka, K. Parobczak, and M. Amanowicz, "On mechanism supporting situational awareness of a tactical ad-hoc network node," in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–8.

[64] D. Goyal and M. B. Krishna, "Secure framework for data access using Location based service in Mobile Cloud Computing," in *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1–6.

[65] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Secur. Priv. Mag.*, vol. 9, no. 2, pp. 50–57, Mar. 2011.

[66] N. Gupta and A. Agarwal, "Context aware Mobile Cloud Computing: Review," in *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*, 2015, pp. 1061–1065.

[67] M. Hauge, M. A. Brose, J. Sander, and J. Andersson, "Multi-Topology routing for QoS support in the CoNSIS convoy MANET," in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–8.

[68] K. Heurtefeux, N. Mohsin, and H. Menouar, “A hybrid platform for remote health monitoring: From concept to deployment,” in *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, 2015, pp. 1–2.

[69] D. B. Hoang and L. Chen, “Mobile Cloud for Assistive Healthcare (MoCAsH),” in *Proceedings of the 2010 IEEE Asia-Pacific Services Computing Conference*, 2010, pp. 325–332.

[70] D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, “Secure data processing framework for mobile cloud computing,” in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, 2011, pp. 614–618.

[71] D. Huang, T. Xing, and H. Wu, “Mobile cloud computing service models: A user-centric approach,” *IEEE Netw.*, vol. 27, no. 5, pp. 6–11, 2013.

[72] D. Huang, X. Zhang, M. Kang, and J. Luo, “MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication,” in *Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on*, 2010, pp. 27–34.

[73] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan, and Y. Zhang, “Software Defined Networking with Pseudonym Systems for Secure Vehicular Clouds,” *IEEE Access*, vol. 4, no. 99, pp. 3522–3534, 2016.

[74] P. P. Hung, T.-A. Bui, and E.-N. Huh, “A Thin-Thick Client Collaboration for Optimizing Task Scheduling in Mobile Cloud Computing,” in *2013 International Conference on IT Convergence and Security (ICITCS)*, 2013, pp. 1–4.

[75] S.-H. Hung, J.-P. Shieh, and Y.-W. Chen, “A profile-driven dynamic application offloading scheme for Android systems,” in *the 1st IEEE Global Conference on Consumer Electronics 2012*, 2012, pp. 540–541.

[76] M. Islam, A. Razzaque, and J. Islam, “A genetic algorithm for virtual machine migration in heterogeneous mobile cloud computing,” in *2016 International Conference on Networking Systems and Security (NSysS)*, 2016, pp. 1–6.

[77] M. L. Islam, N. Nurain, S. Shatabda, and M. S. Rahman, “FGPGA: An efficient genetic approach for producing feasible graph partitions,” in *2015 International Conference on Networking Systems and Security (NSysS)*, 2015, pp. 1–8.

[78] W. Itani, A. Kayssi, and A. Chehab, “Policy-based security channels for protecting network communication in mobile cloud computing,” in *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on*, 2011, pp. 450–456.

[79] D. Jana and D. Bandyopadhyay, “Controlled privacy in mobile cloud,” in *Recent Trends in Information Systems (ReTIS), 2015 IEEE 2nd International Conference on*, 2015, pp. 98–103.

[80] D. Jana and D. Bandyopadhyay, “Efficient management of privacy issues in mobile cloud environment,” in *Advance Computing Conference (IACC), 2015 IEEE International*, 2015, pp. 481–486.

[81] D. Jana and D. Bandyopadhyay, “Efficient management of security and privacy issues in mobile cloud environment,” in *2013 Annual IEEE India Conference (INDICON)*, 2013, pp. 1–6.

[82] D. Jana and D. Bandyopadhyay, “Management of security and privacy issues of application development in mobile cloud environment: A survey,” in *Recent Advances and Innovations in Engineering (ICRAIE), 2014*, 2014, pp. 1–6.

[83] D. Jana and D. Bandyopadhyay, “Management of identity and credentials in mobile cloud environment,” in *2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 2013, pp. 113–118.

[84] C. Jeyanthy, R. S. Shaji, and J. P. Jayan, “Symmetric key based cryptic scheme for mobile cloud storage,” in *Global Conference on Communication Technologies, GCCT 2015*, 2015, pp. 571–575.

[85] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, “SDSM: A secure data service mechanism in mobile cloud computing,” in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, 2011, pp. 1060–1065.

[86] Q. Jiang, J. Ma, and F. Wei, “On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services,” *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–4, 2016.

[87] Y. Jin, C. Tian, H. He, and F. Wang, “A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing,” in *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, 2015, pp. 172–179.

[88] J. Kang, X. Huang, R. Yu, Y. Zhang, and S. Gjessing, “Hierarchical mobile cloud with social grouping for secure pervasive healthcare,” in *2015 17th International Conference on E-health Networking, Application Services (HealthCom)*, 2015, pp. 609–614.

[89] G. Kantyka, T. Podlasek, P. Skarzynski, and T. Szymczyk, “The concept and realization of RSC (Remote Secure Controller) for control and management of services in dynamic enviroment,” in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–8.

[90] A. Khaldi, K. Karoui, N. Tanabene, and H. Ben Ghzala, “A Secure Cloud Computing Architecture Design,” in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on*, 2014, pp. 289–294.

[91] T. Kim, Y. Choi, S. Han, J. Y. Chung, J. Hyun, J. Li, and J. W. K. Hong, “Monitoring and detecting abnormal behavior in mobile cloud infrastructure,” in

Proceedings of the 2012 IEEE Network Operations and Management Symposium, NOMS 2012, 2012, pp. 1303–1310.

[92] A. Klein, C. Mannweiler, J. Schneider, and H. D. Schotten, "Access Schemes for Mobile Cloud Computing," in *2010 Eleventh International Conference on Mobile Data Management*, 2010, pp. 387–392.

[93] M. Klymash, M. Beshley, B. Strykhalyuk, T. Maksymyuk, M. Beshley, and T. Maksymyuk, "Research and development the methods of quality of service provision in Mobile Cloud systems," in *Communications and Networking (BlackSeaCom), 2014 IEEE International Black Sea Conference on*, 2014, pp. 160–164.

[94] I. Kounelis, J. Loschner, D. Shaw, and S. Scheer, "Security of service requests for cloud based m-commerce," in *MIPRO, 2012 Proceedings of the 35th International Convention*, 2012, pp. 1479–1483.

[95] D. Kovachev, Y. Cao, and R. Klamma, "Mobile Cloud Computing: A Comparison of Application Models," *Inf. Syst. J.*, vol. abs/1107.4, no. 4, pp. 14–23, 2011.

[96] D. Kovachev, D. Renzel, R. Klamma, and Y. Cao, "Mobile community cloud computing: Emerges and evolves," in *Proceedings - IEEE International Conference on Mobile Data Management*, 2010, pp. 393–395.

[97] K. Krenc, "Examination of combination rules for the purpose of information fusion in C2 systems: Application of Dezert-Smarandache Theory," in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–5.

[98] I. Krontiris and T. Dimitriou, "Privacy-respecting discovery of data providers in crowd-sensing applications," in *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*, 2013, pp. 249–257.

[99] G. Kulkarni, R. Shelke, P. B. N. Patil, V. Kulkarni, and S. Mohite, "Optimization in Mobile Cloud Computing for Cloud Based Health Application," in *2014 Fourth International Conference on Communication Systems and Network Technologies*, 2014, pp. 569–572.

[100] P. Kulkarni and R. Khanai, "Addressing mobile Cloud Computing security issues: A survey," in *Communications and Signal Processing (ICCSP), 2015 International Conference on*, 2015, pp. 1463–1467.

[101] G. Kumar, E. Jain, S. Goel, and V. K. Panchal, "Mobile Cloud Computing Architecture, Application Model, and Challenging Issues," in *Computational Intelligence and Communication Networks (CICN), 2014 International Conference on*, 2014, pp. 613–617.

[102] N. Kumar, R. Iqbal, S. Misra, J. J. P. C. Rodrigues, and M. S. Obaidat, "Bayesian Cooperative Coalition Game as-a-Service for RFID-Based Secure QoS Management in Mobile Cloud," *IEEE Trans. Emerg. Top. Comput.*, vol. PP, no. 99, p. 1, 2016.

[103] R. Kumar and S. Rajalakshmi, "Mobile Sensor Cloud Computing: Controlling and Securing Data Processing over Smart Environment through Mobile Sensor Cloud Computing (MSCC)," in *Computer Sciences and Applications (CSA), 2013 International Conference on*, 2013, pp. 687–694.

[104] S. Leblanc, "Are you safe with your temporary protective grounds? (Case study)," *Electr. Saf. Work. (ESW), 2014 IEEE IAS*, pp. 1–4, Feb. 2014.

[105] J. Lee and D. Hong, "Pervasive Forensic Analysis Based on Mobile Cloud Computing," in *2011 Third International Conference on Multimedia Information Networking and Security*, 2011, pp. 572–576.

[106] J. Lee and S. Un, "Digital forensics as a service: A case study of forensic indexed search," in *International Conference on ICT Convergence*, 2012, pp. 499–503.

[107] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. W. Phan, "Low Complexity Multi-Authority Attribute Based Encryption Scheme for Mobile Cloud Computing," in *Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on*, 2013, pp. 573–577.

[108] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage," *IEEE Trans. Emerg. Top. Comput.*, vol. 3, no. 1, pp. 127–138, Mar. 2015.

[109] S. Li and J. Gao, "Moving from Mobile Databases to Mobile Cloud Data Services," in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on*, 2015, pp. 235–236.

[110] Y. Li, J. Liu, Q. Li, and L. Xiao, "Mobile cloud offloading for malware detections with learning," in *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2015, vol. 2015–Augus, pp. 197–201.

[111] Z. Li, X. Zheng, and Y. Wei, "LSBA Based Security Verification in MCC," in *Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on*, 2009, pp. 1–4.

[112] H. Liang, D. Huang, L. X. Cai, X. Shen, and D. Peng, "Resource allocation for security services in mobile cloud computing," in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2011, pp. 191–195.

[113] L. Ling, W. Zhulin, and Y. Xiuhua, "Mobile Resource Reliability-Based Task Allocation for Mobile Cloud," in *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, 2015, pp. 1746–1750.

[114] C. Liu, R. Ranjan, J. Chen, P. S. Yu, B. Thuraisingham, and V. Varadharajan, "Message from the PriSecCSN2012 workshop chairs," in *Proceedings - 2nd International Conference on Cloud and Green Computing and 2nd International*

Conference on Social Computing and Its Applications, CGC/SCA 2012, 2012, pp. xxvii–xxvii.

[115] F. Liu, P. Shu, H. Jin, L. Ding, J. Yu, D. Niu, and B. Li, "Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications," *IEEE Wirel. Commun.*, vol. 20, no. 3, pp. 14–22, 2013.

[116] W. Liu, Z. Han, and Q. Wang, "An approach to the sensitive information protection for mobile code," in *Proceedings of the 1st International Symposium on Data, Privacy, and E-Commerce, ISDPE 2007*, 2007, pp. 289–291.

[117] F. Lobillo, Z. Becvar, M. A. Puente, P. Mach, F. Lo Presti, F. Gambetti, M. Goldhamer, J. Vidal, A. K. Widiawan, and E. Calvanesse, "An architecture for mobile computation offloading on cloud-enabled LTE small cells," in *Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE*, 2014, pp. 1–6.

[118] R. K. Lomotey and R. Deters, "Architectural Designs from Mobile Cloud Computing to Ubiquitous Cloud Computing - Survey," in *Services (SERVICES), 2014 IEEE World Congress on*, 2014, pp. 418–425.

[119] R. K. Lomotey and R. Deters, "Mobile-Based Medical Data Accessibility in mHealth," in *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on*, 2014, pp. 91–100.

[120] R. K. Lomotey, S. Jamal, and R. Deters, "SOPHRA: A Mobile Web Services Hosting Infrastructure in mHealth," in *Proceedings of the 2012 IEEE First International Conference on Mobile Services*, 2012, pp. 88–95.

[121] R. K. Lomotey and R. Deters, "Middleware-Enabled Mobile Framework in mHealth," in *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, 2013, pp. 1–8.

[122] P. Lubkowski, M. Bednarczyk, K. Maslanka, and M. Amanowicz, "QoS-aware end-to-end connectivity provision in a heterogenous military environment," in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–8.

[123] A. Luntovskyy and J. Spillner, "RAIC Integration for Network Storages on Mobile Devices," in *Proceedings of the 2013 Seventh International Conference on Next Generation Mobile Apps, Services and Technologies*, 2013, pp. 142–147.

[124] R. Ma, J. Li, H. Guan, M. Xia, and X. Liu, "EnDAS: Efficient Encrypted Data Search as a Mobile Cloud Service," *IEEE Trans. Emerg. Top. Comput.*, vol. 3, no. 3, pp. 372–383, Sep. 2015.

[125] T. Mavroeidakos, D. Kallergis, D. D. Vergados, and C. Douligeris, "Towards mobile cloud security performance: A cross-border approach," in *2016 23rd International Conference on Telecommunications (ICT)*, 2016, pp. 1–5.

[126] D. C. Mazur, J. A. Kay, and K. D. Mazur, "Intelligent Motor Control: Innovations in Process Optimization," *IEEE Ind. Appl. Mag.*, vol. 21, no. 2, pp. 30–37, 2015.

[127] A. R. Mohammad, K. Mohiuddin, M. Irfan, and M. Moizuddin, "Cloud the Mainstay: Growth of Social Networks in Mobile Environment," in *Cloud Ubiquitous Computing Emerging Technologies (CUBE), 2013 International Conference on*, 2013, pp. 14–19.

[128] I. Mouhib, E. O. Driss, and K. Zine-Dine, "Encryption as a service for securing data in mobile cloud computing," in *2015 15th International Conference on Intelligent Systems Design and Applications (ISDA)*, 2015, vol. 2016–June, pp. 546–550.

[129] N. Naik and P. Jenkins, "A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards," in *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2016, pp. 89–90.

[130] S. Neogy and S. Saha, "Developing a secure remote patient monitoring system," in *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*, 2015, pp. 1–4.

[131] M. Nkosi and F. Mekuria, "Improving the capacity, reliability life of mobile devices with Cloud Computing BT - 2011 IST-Africa Conference, IST 2011, May 11, 2011 - May 13, 2011," in *2011 IST-Africa Conference Proceedings, IST 2011*, 2011, pp. 1–9.

[132] F. Omri, S. Foufou, R. Hamila, and M. Jarraya, "Cloud-based mobile system for biometrics authentication," in *ITS Telecommunications (ITST), 2013 13th International Conference on*, 2013, pp. 325–330.

[133] A. Oredope, A. McConnell, C. Peoples, R. Singh, T. A. Gonsalves, K. Moessner, and G. P. Parr, "Cloud Services in Mobile Environments". The IU-ATC UK-India Mobile Cloud Proxy Function," in *Wireless Conference (EW), Proceedings of the 2013 19th European*, 2013, pp. 1–7.

[134] C. Oriaku, N. Alwan, and I. A. Lami, "The readiness of mobile operating systems for cloud computing services," in *2012 IV International Congress on Ultra Modern Telecommunications and Control Systems*, 2012, pp. 49–55.

[135] I.-S. Park, Y.-D. Lee, and J. Jeong, "Improved Identity Management Protocol for Secure Mobile Cloud Computing," in *2013 46th Hawaii International Conference on System Sciences*, 2013, pp. 4958–4965.

[136] J. W. Park, C. H. Yun, S. W. Rho, Y. W. Lee, and H. S. Jung, "Mobile cloud web-service for U-City," in *Proceedings - IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC 2011*, 2011, pp. 1061–1065.

[137] S. Park, J. N. Yoon, C. Kang, K. H. Kim, and T. Han, "TGVisor: A tiny hypervisor-based trusted geolocation framework for mobile cloud clients," in *Proceedings - 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015*, 2015, pp. 99–108.

[138] J. C. Pearson and D. A. Pandya, "Revitalizing and refurbishment of motor control centers AT NJI amp; BMC," in *Electrical Insulation Conference and Electrical Manufacturing Expo, 2005. Proceedings*, 2005, pp. 211–215.

[139] D. Popa, K. Boudaoud, M. Borda, and M. Cremene, "Mobile cloud applications and traceability," in *Proceedings - RoEduNet IEEE International Conference*, 2013, pp. 1–4.

[140] D. Popa, M. Cremene, M. Borda, and K. Boudaoud, "A security framework for mobile cloud applications," in *Roedunet International Conference (RoEduNet), 2013 11th*, 2013, pp. 1–4.

[141] Y. Qin, D. Huang, and X. Zhang, "VehiCloud: Cloud Computing Facilitating Routing in Vehicular Networks," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, 2012, pp. 1438–1445.

[142] S. S. Qureshi, T. Ahmad, K. Rafique, and Shuja-ul-islam, "Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues," in *Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on*, 2011, pp. 467–471.

[143] Ragini, P. Mehrotra, and S. Venkatesan, "An efficient model for privacy and security in Mobile Cloud Computing," in *2014 International Conference on Recent Trends in Information Technology*, 2014, pp. 1–6.

[144] M. Rahman and J. Gao, "A Reusable Automated Acceptance Testing Architecture for Microservices in Behavior-Driven Development," in *2015 IEEE Symposium on Service-Oriented System Engineering*, 2015, pp. 321–325.

[145] R. G. Ramani, S. S. Kumar, and S. G. Jacob, "Rootkit (malicious code) prediction through data mining methods and techniques," in *2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2013*, 2013, pp. 1–5.

[146] A. Reiter and T. Zefferer, "Paving the Way for Security in Cloud-Based Mobile Augmentation Systems," in *3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (IEEE Mobile Cloud 2015)*, 2015, pp. 89–98.

[147] S. Ruj, "Attribute based access control in clouds: A survey," in *2014 International Conference on Signal Processing and Communications (SPCOM)*, 2014, pp. 1–6.

[148] S. Saleem and N. Zhang, "A Risk-Aware Workload scheduler to support secure and efficient collaborative data transfer in mobile communities," in *Wireless On-*

demand Network Systems and Services (WONS), 2012 9th Annual Conference on, 2012, pp. 31–34.

[149] J. Samad, S. W. Loke, K. Reed, and Ieee, "Quantitative Risk Analysis for Mobile Cloud Computing: A Preliminary Approach and a Health Application Case Study," in *2013 12th Ieee International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 1378–1385.

[150] Z. Sanaei, S. Abolfazli, A. Gani, and M. Shiraz, "SAMI: Service-based arbitrated multi-tier infrastructure for Mobile Cloud Computing," in *2012 1st IEEE International Conference on Communications in China Workshops, ICCC 2012*, 2012, pp. 14–19.

[151] M. Sarvabhatla, M. Giri, and C. S. Vorugunti, "A robust ticket-based mutual authentication scheme for data security in cloud computing," in *2014 International Conference on Data Science & Engineering (ICDSE)*, 2014, pp. 62–67.

[152] M. Sarvabhatla and C. S. Vorugunti, "A robust mutual authentication scheme for data security in cloud architecture," in *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, 2015, pp. 1–6.

[153] M. Satyanarayanan, P. Bahl, R. Cáceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.

[154] R. Schutz, S. McLaughlin, T. Daeleman, M. Luoma, M. Peuhkuri, P. Carlen, and J. Haines, "Protected Core Networking (PCN): PCN QoS and SLA definition," in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–9.

[155] J. Seddar, H. Khalifa, V. Conan, and J. Leguay, "Exploiting cognitive radios in tactical point to multipoint communications," in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–5.

[156] H. Seifert, M. Franke, A. Diefenbach, and P. Sevenich, "SOA in the CoNSIS coalition environment: Extending the WS-I Basic Profile for using SOA in a tactical environment," in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–6.

[157] M. Sharma, A. Bansal, N. Hasteer, and A. Tuli, "Exploring challenges in mobile cloud computing: an overview," in *Confluence 2013: The Next Generation Information Technology Summit (4th International Conference)*, 2013, p. 9.13--9.13.

[158] R. Shiny, R. S. Shaji, and J. P. Jayan, "Signature based data auditing under mobile cloud system," in *2015 Global Conference on Communication Technologies (GCCT)*, 2015, pp. 565–570.

[159] P. Simon, N. Bret, and B. Ridard, “Enhancing the control of IP tactical networks via measurements,” in *Military Communications and Information Systems Conference (MCC), 2013*, 2013, pp. 1–5.

[160] S. Song, B.-Y. Choi, and D. Kim, “Selective encryption and component-oriented deduplication for mobile cloud data computing,” in *2016 International Conference on Computing, Networking and Communications (ICNC)*, 2016, pp. 1–5.

[161] P. Steinmetz, “Use of cross domain guards for CoNSIS network management,” in *Communications and Information Systems Conference (MCC), 2012 Military*, 2012, pp. 1–5.

[162] I. Stojmenovic and J. Voas, “HPCC 2011/FTDCS 2011 Keynotes,” in *High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on*, 2011, pp. xlviii–xlvix.

[163] W. T. Su, W. C. Liu, C. L. Chen, and T. P. Chen, “Cloud access control in multi-layer cloud networks,” in *Consumer Electronics - Taiwan (ICCE-TW), 2015 IEEE International Conference on*, 2015, pp. 364–365.

[164] C. Sun, J. Ren, X. Zheng, Y. Wei, and X. Zheng, “JVMTI-based model enforcement on java platform for model-carrying code,” in *Proceedings of the 4th International Conference on Ubiquitous Information Technologies and Applications, ICUT 2009*, 2009, pp. 1–5.

[165] S. Sung, C. Youn, E. Kong, and J. Ryou, “A distributed mobile cloud computing model for secure big data,” in *International Conference on Information Networking*, 2016, vol. 2016–March, pp. 312–316.

[166] H. Suo, Z. Liu, J. Wan, and K. Zhou, “Security and privacy in mobile cloud computing,” in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013, pp. 655–659.

[167] A. Taivalsaari and K. Systä, “Cloudberry: An HTML5 cloud phone platform for mobile devices,” *IEEE Softw.*, vol. 29, no. 4, pp. 40–45, 2012.

[168] Y. Tamura, Y. Nobukawa, and S. Yamada, “A Method of Reliability Assessment Based on Neural Network and Fault Data Clustering for Cloud with Big Data,” in *Information Science and Security (ICISS), 2015 2nd International Conference on*, 2015, pp. 1–4.

[169] L. Tang, L. Ouyang, and W. T. Tsai, “Multi-factor web API security for securing Mobile Cloud,” in *Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on*, 2015, pp. 2163–2168.

[170] L. Tawalbeh, Y. Haddad, O. Khamis, F. Aldosari, and E. Benkhelifa, “Efficient Software-Based Mobile Cloud Computing Framework,” in *Cloud Engineering (IC2E), 2015 IEEE International Conference on*, 2015, pp. 317–322.

[171] C. C. Teng, C. Green, R. Johnson, P. Jones, and C. Treasure, "Mobile ultrasound with DICOM and cloud connectivity," in *Proceedings - IEEE-EMBS International Conference on Biomedical and Health Informatics: Global Grand Challenge of Health Informatics, BHI 2012*, 2012, pp. 667–670.

[172] V. V. A. Thampi and R. K. Gopal, "A review on different encryption algorithms for a wellness tracking system," in *Global Conference on Communication Technologies, GCCT 2015*, 2015, pp. 817–822.

[173] H. Tout, C. Talhi, N. Kara, and A. Mourad, "Selective Mobile Cloud Offloading to Augment Multi-Persona Performance and Viability," *IEEE Trans. Cloud Comput.*, vol. PP, no. 99, p. 1, 2016.

[174] J. Tsai and N. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, Sep. 2015.

[175] S. Tu and Y. Huang, "Towards efficient and secure access control system for mobile cloud computing," *China Commun.*, vol. 12, no. 12, pp. 43–52, 2015.

[176] J. Wan, D. Zhang, S. Zhao, L. T. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 106–113, 2014.

[177] J. Wan, Z. Liu, K. Zhou, and R. Lu, "Mobile cloud computing: Application scenarios and service models," in *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, 2013, pp. 644–648.

[178] M. Wang, H. Li, J. Li, and G. Zhao, "UMCloud: A user-oriented security scheme for mobile cloud storage," in *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, 2015, pp. 1–6.

[179] P. Wang, L. Yang, G. W. Li, and X. Gao, "A Novel Substitution Judgment Method for Mobile Cloud Computing Application System Components," in *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, 2014, pp. 911–916.

[180] Y. Wang, Z. Zheng, and M. R. Lyu, "Entropy-Based Service Selection with Uncertain QoS for Mobile Cloud Computing," in *2015 IEEE Conference on Collaboration and Internet Computing (CIC)*, 2015, pp. 252–259.

[181] M. Whaiduzzaman and A. Gani, "Measuring security for cloud service provider: A Third Party approach," in *2013 International Conference on Electrical Information and Communication Technology, EICT 2013*, 2013, pp. 1–6.

[182] H. Woo, S. Han, E. Heo, J. Kim, and S. Shin, "A virtualized, programmable content delivery network," in *Proceedings - 2nd IEEE International Conference on Mobile*

Cloud Computing, Services, and Engineering, MobileCloud 2014, 2014, pp. 159–168.

[183] H. Wu, Q. Wang, and K. Wolter, "Methods of cloud-path selection for offloading in mobile cloud computing systems," in *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, 2012, pp. 443–448.

[184] T. Xing, H. Liang, D. Huang, and L. X. Cai, "Geographic-Based Service Request Scheduling Model for Mobile Cloud Computing," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 1446–1453.

[185] L. Xu, L. Li, V. Nagarajan, D. J. Huang, W. T. Tsai, and Ieee, "Secure Web Referral Services for Mobile Cloud Computing," in *2013 Ieee Seventh International Symposium on Service-Oriented System Engineering*, 2013, pp. 584–593.

[186] L. Xu, G. Li, C. Li, W. Sun, W. Chen, and Z. Wang, "Condroid: A Container-Based Virtualization Solution Adapted for Android Devices," in *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2015, pp. 81–88.

[187] K. Yamaji, M. Nakamura, Y. Nagai, T. Ito, and H. Sato, "Specifying a Trust Model for Academic Cloud Services," in *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2016, pp. 91–99.

[188] S. S. Yau and A. B. Buduru, "Intelligent Planning for Developing Mobile IoT Applications Using Cloud Systems," in *2014 IEEE International Conference on Mobile Services*, 2014, pp. 55–62.

[189] C. P. Young, Y. B. Lin, and C. C. Chia, "Software and hardware design of a multi-cipher cryptosystem," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2009, pp. 1–5.

[190] M. Yousif, "Toward #x0022; Hypergalactic-Scale #x0022; Computing," *IEEE Cloud Comput.*, vol. 2, no. 3, pp. 5–7, May 2015.

[191] M. S. M. Zahid, A. H. Abdullah, and E. Supriyanto, "Application of Mobile Cloud Computing in Care pathways," in *Humanitarian Technology Conference - (IHTC), 2014 IEEE Canada International*, 2014, pp. 1–5.

[192] P. Zhang, H. Sun, and Z. Yan, "Building up trusted identity management in mobile heterogeneous environment," in *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*, 2011, pp. 873–877.

[193] L. Zhiquan, C. Jialin, Z. Min, and F. Dengguo, "Efficiently Attribute-Based Access Control for Mobile Cloud Storage System," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*, 2014, pp. 292–299.

[194] X. Zhou, M. Sun, Y. Wang, and X. Wu, "A New QoE-Driven Video Cache Allocation Scheme for Mobile Cloud Server," in *Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), 2015 11th International Conference on*, 2015, no. Qshine, pp. 122–126.

[195] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in *Network and service management (cnsm), 2012 8th international conference and 2012 workshop on systems virtualiztion management (svm)*, 2012, pp. 37–45.

[196] S. Zickau, F. Beierle, and I. Denisow, "Securing Mobile Cloud Data with Personalized Attribute-based Meta Information," in *3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2015, pp. 205–210.

[197] Q. Zou, J. Wang, and X. Chen, "Secure Encrypted Image Search in Mobile Cloud Computing," *2015 10th Int. Conf. Broadband Wirel. Comput. Commun. Appl.*, pp. 572–575, 2015.

[198] "Program," in *Communications and Information Technology (ICCIT), 2013 Third International Conference on*, 2013, pp. 1–11.

[199] "IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications," *IEEE Std 1901.2-2013*, pp. 1–269, 2013.

[200] "Table of contents," in *Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on*, 2015, pp. 1–15.

[201] "[Title page i]," in *Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on*, 2013, pp. i–i.

[202] "Call for Papers - IEEE Transactions on Reliability Special Section on Trustworthy Computing," *IEEE Trans. Reliab.*, vol. 62, no. 1, p. 312, 2013.

[203] "Table of contents," in *Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on*, 2014, pp. 1–8.

[204] "[Copyright notice]," in *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, 2015, pp. 1–1.

[205] "[Title page]," in *Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on*, 2015, p. 1.

[206] "Table of contents," in *Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on*, 2013, pp. v–xiv.

[207] "CLOUD 2012: 2012 IEEE 5th International Conference on Cloud Computing [Cover art]," in *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*, 2012, pp. C4–C4.

Bibliografía ACM

[1] A. Agarwal, J. Govindaraj, N. Juneja, and V. Naik, "Feasibility study of on-device and in-the-cloud virtualization of mobiles," in *IBM Collaborative Academia Research Exchange*, 2013, pp. 1–4.

[2] H. S. Alqahtani and G. Kouadri-Mostefaou, "Multi-clouds Mobile Computing for the Secure Storage of Data," in *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, 2014, pp. 495–496.

[3] A. Baliga, X. Chen, B. Coskun, G. de los Reyes, S. Lee, S. Mathur, and J. E. Van der Merwe, "Vpmn," in *Proceedings of the second international workshop on Mobile cloud computing and services - MCS '11*, 2011, p. 7.

[4] F. Bancilhon and R. Ramakrishnan, "An amateur's introduction to recursive query processing strategies," in *Proceedings of the 1986 ACM SIGMOD international conference on Management of data*, 1986, vol. 15, no. 2, pp. 16–52.

[5] L. Bauer and F. Kerschbaum, "What are the most important challenges for access control in new computing domains, such as mobile, cloud and cyber-physical systems," in *Proceedings of the 19th ACM symposium on Access control models and technologies - SACMAT '14*, 2014, pp. 127–128.

[6] C. Chen, M. Won, R. Stoleru, and G. G. Xie, "Energy-efficient Fault-tolerant Data Storage & Processing in Dynamic Networks," in *Proceedings of the Fourteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2013, pp. 281–286.

[7] Y. Chen, T. Li, X. Wang, K. Chen, and X. Han, "Perplexed Messengers from the Cloud: Automated Security Analysis of Push-Messaging Integrations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2015, pp. 1260–1272.

[8] C.-Y. Chow and S. Shekhar, Eds., "MobiGIS '14: Proceedings of the Third ACM SIGSPATIAL International Workshop on Mobile Geographic Information Systems," 2014.

[9] G. Copeland and T. Keller, "A comparison of high-availability media recovery techniques," in *ACM SIGMOD Record*, 1989, vol. 18, no. 2, pp. 98–109.

[10] J. W. Coyne and N. C. Kluksdahl, "'Mainstreaming' Automated Information Systems Security Engineering (A Case Study in Security Run Amok)," in

Proceedings of the 2Nd ACM Conference on Computer and Communications Security, 1994, pp. 251–257.

[11] S. K. Dash, D. P. Mishra, R. Mishra, and S. Dash, "Privacy preserving K-Medoids clustering: an approach towards securing data in Mobile cloud architecture," *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*. ACM Press, New York, New York, USA, pp. 439–443, 2012.

[12] S. K. Dash, D. P. Mishra, R. Mishra, and S. Dash, "Privacy preserving K-Medoids clustering," in *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology - CCSEIT '12*, 2012, pp. 439–443.

[13] G. Di-Crescenzo, Y. Ishai, and R. Ostrovsky, "Universal Service-providers for Database Private Information Retrieval (Extended Abstract)," in *Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing*, 1998, pp. 91–100.

[14] G. Disterer and C. Kleiner, "Using Mobile Devices with BYOD," *Int. J. Web Portals*, vol. 5, no. December 2013, pp. 33–45, Jan. 2013.

[15] H. Eom, P. St Juste, R. Figueiredo, O. Tickoo, R. Illikkal, and R. Iyer, "Snarf," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC '12*, 2012, p. 29.

[16] P. Gilbert, B.-G. Chun, L. P. Cox, and J. Jung, "Vision: Automated Security Validation of Mobile Apps at App," in *Proceedings of the second international workshop on Mobile cloud computing and services - MCS '11*, 2011, p. 21.

[17] Y. Igarashi, K. Joshi, M. Hiltunen, and R. Schlichting, "Vision," in *Proceedings of the fifth international workshop on Mobile cloud computing & services - MCS '14*, 2014, pp. 35–39.

[18] M. H. Izadi and A. Drygajlo, "Embedding cylinder quality measures into minutia cylinder-code based latent fingerprint matching," in *Proceedings of the on Multimedia and security MM&Sec '12*, 2012, pp. 33–38.

[19] V. Jain, R. Kumar, and Z. Saquib, "An Approach Towards Digital Signatures for e-Governance in India," in *Proceedings of the 2015 2Nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, 2015, pp. 82–88.

[20] C. Jarabek, D. Barrera, and J. Aycock, "ThinAV: Truly Lightweight Mobile Cloud-based Anti-malware," in *Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12*, 2012, p. 209.

[21] R. Kravets, G. S. Tuncay, and H. Sundaram, "For Your Eyes Only," in *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services - MCS '15*, 2015, pp. 28–35.

[22] T. Li, X. Zhou, L. Xing, Y. Lee, M. Naveed, X. Wang, and X. Han, "Mayhem in the Push Clouds: Understanding and Mitigating Security Hazards in Mobile Push-Messaging Services," in *Proceedings of the 21st ACM SIGSAC Conference on Computer & Communications Security (CCS)*, 2014, pp. 1–12.

[23] R. K. Lomotey and R. Deters, "Using a cloud-centric middleware to enable mobile hosting of Web services: MHealth use case," *Pers. Ubiquitous Comput.*, vol. 18, no. 5, pp. 1085–1098, 2014.

[24] R. K. Lomotey and R. Deters, "Csb-Ucc," in *Proceedings of the Fifth International Conference on Management of Emergent Digital EcoSystems - MEDES '13*, 2013, pp. 100–107.

[25] J. C. S. Lui, "A peek into smartphones, cloud services and their security," in *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing - MCC '13*, 2013, p. 1.

[26] K. Mohiuddin, A. Islam, A. Alam, and A. Ali, "24X7X365: Mobile Cloud Access," in *Proceedings of the CUBE International Information Technology Conference on - CUBE '12*, 2012, p. 544.

[27] K. Nagin, D. Hadas, Z. Dubitzky, a Glikson, I. Loy, B. Rochwerger, and L. Schour, "Inter-cloud mobility of virtual machines," in *ACM International Conference Proceeding Series*, 2011, vol. 13, p. 3.

[28] R. Ostrovsky and V. Shoup, "Private information storage," in *Proceedings of the twenty-ninth annual ACM ...*, 1997, pp. 1–17.

[29] R. Ramakrishnan, F. Bancilhon, and A. Silberschatz, "Safety of Recursive Horn Clauses with Infinite Relations," in *Proceedings of the Sixth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, 1987, pp. 328–339.

[30] D. Schwab and L. Yang, "Entity Authentication in a Mobile-cloud Environment," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 2013, p. 42:1--42:4.

[31] R. Sekar, C. R. Ramakrishnan, I. V. Ramakrishnan, and S. A. Smolka, "Model-Carrying Code (MCC)," in *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*, 2001, p. 23.

[32] R. Sekar, V. N. Venkatakrishnan, S. Basu, S. Bhatkar, D. C. DuVarney, R. Sekar, V. N. Venkatakrishnan, S. Basu, S. Bhatkar, and D. C. DuVarney, "Model-carrying code," in *Proceedings of the nineteenth ACM symposium on Operating systems principles - SOSP '03*, 2003, vol. 37, no. 5, p. 15.

[33] S. Seneviratne, a Seneviratne, and P. Mohapatra, "Personal cloudlets for privacy and resource efficiency in mobile in-app advertising," in *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2013, pp. 33–39.

[34] X. Wang, Y. Yang, Y. Zeng, C. Tang, J. Shi, and K. Xu, "A Novel Hybrid Mobile Malware Detection System Integrating Anomaly Detection With Misuse Detection," in *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services*, 2015, pp. 15–22.

[35] Y. Xiao, P. Hui, P. Savolainen, and A. Ylä-Jääski, "CasCap: Cloud-assisted Context-aware Power Management for Mobile Devices," in *Proceedings of the Second International Workshop on Mobile Cloud Computing and Services*, 2011, pp. 13–18.

[36] L. Zhang, X. Ding, Z. Wan, M. Gu, and X.-Y. Li, "WiFace: A Secure Geosocial Networking System Using WiFi-based Multi-hop MANET," in *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, 2010, p. 3:1--3:8.

[37] Z. Zhou and D. Huang, "Efficient and Secure Data Storage Operations for Mobile Cloud Computing," in *Proceedings of the 8th International Conference on Network and Service Management*, 2012, pp. 37–45.

[38] Y. Zhu, D. Ma, D. Huang, and C. Hu, "Enabling secure location-based services in mobile cloud computing," in *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing - MCC '13*, 2013, p. 27.

[39] "MobileDeLi '14: Proceedings of the 2Nd International Workshop on Mobile Development Lifecycle," 2014.

[40] "MobiCom '15: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking," 2015.

[41] "MCC '13: Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing," 2013.

[42] "SACMAT '14: Proceedings of the 19th ACM Symposium on Access Control Models and Technologies," 2014.