Dificultades de Investigaciones Penales en Cloud Computing

Ariel Podestá[1], Martín Castellote[2], Bruno Constanzo[3], Julian Waimann[4], Juan Ignacio Iturriaga[5]

[1]Ingeniero en Informática, Docente e Investigador en Universidad FASTA, arielpodesta@gmail.com
[2]Ingeniero en Informática, Docente e Investigador en Universidad FASTA, castellotemartin@yahoo.com.ar
[3]Ingeniero en Informática, Investigador en Universidad FASTA, bconstanzo@ufasta.edu.ar
[4]Ingeniero en Informática, Investigador en Universidad FASTA, julianw@ufasta.edu.ar
[5]Ingeniero en Informática, Docente e Investigador en Universidad FASTA, Juan@ufasta.edu.ar

Abstract. En los últimos años se ha visto una migración de los sistemas informáticos clásicos a sistemas informáticos "en la nube". Ésta tendencia, llamada Cloud Computing, presenta una serie de características únicas, y nuevos problemas a enfrentar para la Informática Forense. En éste trabajo se analizan varios aspectos de los entornos Cloud Computing, los desafíos que presentan y algunas medidas a tomar en cuenta en su análisis.

Keywords: informática forense – cloud computing – Computación en la nube – Servicios en la nube – SaaS – PaaS – IaaP

1 Introducción

Dada la evolución y avance de la tecnología en la vida cotidiana del ser humano, hoy en día es cada vez más frecuente la presencia de la informática en controversias en donde la justicia debe intervenir para su resolución. Siendo así, en cada acto delictivo se ve involucrada una investigación que, llevada a cabo por personal especializado en informática forense[1], conduzca al esclarecimiento de la causa.

Hasta hace algunos años, en un caso convencional, el ámbito de la evidencia no excedía los límites de los dispositivos utilizados por el individuo implicado. Pero conforme pasa el tiempo, debido a la evolución de las intercomunicaciones, las redes y los sistemas informáticos, se hace cada vez más difícil encontrar un caso como el mencionado. Actualmente es poco factible el hallazgo de un equipo informático de uso común (notebook por ejemplo) que no haya tenido interacción alguna en esta red mundial denominada en Internet. La persona promedio tiene una actividad intensa en este espacio virtual utilizando diferentes servicios que le permiten consultar páginas web, enviar y recibir emails, pagar sus cuentas, comunicarse, almacenar archivos y muchas otras actividades. Este gran cúmulo de servicios brindados en forma paga o

1 Informática forense: Disciplina que se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

gratuitamente es lo que reconocemos, desde el punto de vista del usuario, como "*Cloud Computing*" o computación en la nube.
Esta gigantesca infraestructura de servicios informáticos toma partido en innumerables disciplinas y la informática forense no se ve exenta de ella.De esta manera, es pertinente, profundizar en el conocimiento de este nuevo paradigma, sus características y su principal impacto en una investigación forense digital.
Una de las principales problemáticas que presenta este contexto es determinar la distribución de responsabilidades entre los diferentes actores que intervienen en la provisión del servicio. Si hablamos de un servicio de casillas de email, por ejemplo, habrá un actor que provea la infraestructura física de la red (medios de transmisión, enrutadores, conmutadores, antenas, etc.), otro actor que disponga de los equipos servidores que brinden espacio de almacenamiento y tiempo de procesamiento, otro actor que utilizando los servicios de los anteriores monte una plataforma de software como servicio de emails; y así pueden seguirse generando diferentes actores según su contribución a esta prestación. De esta manera, frente a la necesidad de realizar una investigación en un entorno tal, la actividad se vuelve compleja requiriendo determinar el nivel de participación que cada actor tiene en cada caso.
Una vez identificada la distribución de responsabilidades, el problema subsiguiente que enfrenta una investigación informática es el alcance jurisdiccional con que se puede contar. En la gran mayoría de los casos solamente hay un apoyo legal a nivel de área o región dentro de un país. Pero lamentablemente en esta gran red, los recursos se encuentran distribuidos a nivel internacional. Esto significa que eventualmente si un investigador requiere datos de identidad de un usuario de una casilla de correo electrónico, posiblemente deba emitir un pedido a una entidad en otro país. Llegado el caso de que la entidad no se vea obligada legalmente a brindar la información solicitada, el investigador se enfrentaría con otra de las complicaciones que presenta este paradigma: dependencia del proveedor y su buena predisposición. Es sabido que cuando no existe una responsabilidad legal, todo proveedor de servicios estaría reticente a brindar información más allá de la estrictamente necesaria para el buen funcionamiento del suyo.
Estas y otras dificultades presentadas a continuación conforman un panorama ciertamente más complejo que el anterior, años atrás donde no existía esta gran red de servicios denominada *Cloud Computing*. Tenerlas presente es menester para todo investigador informático forense.

2 Marco de investigación y antecedentes

Este documento surge como uno de los productos del desarrollo de un proyecto de investigación que toma como punto de partida el conocimiento del fuerte vínculo entre la informática y el ser humano en el mundo actual, e intenta crear nuevas soluciones que aporten a la comunidad de profesionales enfocados a la informática forense. Dicho proyecto se denomina PURI o "Proceso Único de Recuperación de la Información", es llevado a cabo por un grupo de investigación de la Universidad F.A.S.T.A. y tuvo su comienzo en el año 2012.

A nivel general el proyecto PURI consiste en el estudio de métodos, técnicas y herramientas informáticas, cuya finalidad es la generación y formalización de un único proceso de recuperación de información digital que de soporte y oriente al informático forense a desempeñar su actividad lo más organizada, repetible y eficientemente posible, respetando las formalidades legales vigentes que apliquen.
Como uno de los objetivos secundarios de este proyecto se planteó la detección de "nichos carentes", entendidos como tareas de esta actividad que actualmente no se ven respaldadas por técnicas o herramientas que den soporte a las mismas. Durante los avances en este objetivo se hizo cada vez más evidente la necesidad el ahondar en entornos distribuidos.
El concepto de entorno distribuido, en informática, puede aplicarse a distintos contextos. En lo que atañe a una investigación forense podrían identificarse al menos tres modos de distribución de la información, según la infraestructura utilizada, que demandarían un procedimiento ciertamente distinto uno del otro, al momento de llevar a cabo un análisis de la misma.
Uno de esos casos se circunscribe a los límites de un solo equipo que utilizando RAID (arreglo redundante de discos independientes) distribuye su información en los mismos. Otro caso comprende una estructura más compleja que involucra a un cluster de servidores (conjunto de equipos servidor) en donde la distribución implica una red de datos entre los mismos. Por último, el entorno distribuido por excelencia hoy en día, que es el punto central de este informe, es innegablemente la Cloud Computing, donde ya no sólo los datos o el software pueden encontrarse distribuidos, sino que el hardware que soporta al sistema se encuentra descentralizado,
En PURI actualmente se trabaja en paralelo acerca estas tres situaciones de distribución de la información, pero el enfoque debe cambiar sustancialmente en una de ellas. Lidiar con la Cloud Computing en una investigación es un desafío significativamente más importante que los otros dos casos mencionados, y esto es así debido a numerosos factores que intervienen que exceden el aspecto técnico. Estos obstáculos es la temática a tratar a continuación en este paper.

3 Definición de *Cloud Computing* e introducción a la problemática

El Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST) [1] define Cloud Computing como un modelo para habilitar el acceso unívoco, por demanda, a un conjunto de recursos informáticos configurables provistos rápidamente y publicados con un mínimo esfuerzo de gestión o servicio del proveedor. Se clasifica en 3 modelos de servicios: Software como servicio (SaaS por sus siglas en inglés), Plataforma como servicio (PaaS) e Infraestructura como Servicio (IaaS). Este último, IaaS, es el más amplio, donde el usuario, o cliente, tiene control total sobre la aplicación, middleware y sistema operativo (SO); mientras que el proveedor del servicio controla el hypervisor, el software que maneja las máquinas virtuales. En PaaS el cliente tiene control limitado de programación en la capa de aplicación y middleware. Finalmente en el modelo SaaS el cliente solo tiene control limitado sobre la administración de la aplicación; mientras que el proveedor del servicio tiene control total sobre la administración y programación de la aplicación, middleware y SO.

Es necesario hacer la salvedad de que los modelos de servicio propuestos por el NIST en un caso real pueden combinarse, por ejemplo, supongamos el caso de un empresa X que desarrolla un sistema web para publicaciones de venta de productos que a su vez contrata otra empresa Y para realizar el hosting de su sistema. En este ejemplo se ven al menos 2 modelos de Cloud superpuestos: el primero sería un SaaS entre los usuarios que realizan publicaciones en el sistema y la empresa X, y a su vez se puede ver un modelo PaaS entre la empresa X y la Y. Por lo tanto, en esta situación, se encuentran como mínimo con 2 clientes y 2 proveedores, siendo uno de los casos más comunes. Sin embargo, para el desarrollo de este trabajo, en primer lugar se identificará la persona física o jurídica de la causa como el usuario o cliente de un servicio en la nube (sea SaaS, PaaS o IaaS) y como proveedor aquel que se encuentre en el nivel inmediato superior. Para clarificar el concepto, en el ejemplo anterior, si se está investigando a un usuario del sistema de publicaciones, esté sería "el cliente", la empresa X "el proveedor"; en cambio si se investiga la empresa X, esta misma sería "el cliente" y la empresa Y "el proveedor".
Ante una causa penal, cuando deba realizarse peritajes en sistemas de información en la nube, la característica principal, a diferencia de investigaciones en informática forense donde se dispone del o los dispositivos físicos (computadoras, discos, tarjetas de memoria, etc), es que no se tiene acceso directo al alojamiento de la información e inevitablemente la investigación dependerá de los datos que nos pueda brindar un tercero, justamente quien se definió como el proveedor del servicio. Por tal motivo las dificultades que se presentan no se limitan a un aspecto técnico, como puede ser desencriptar datos o buscar archivos borrados, sino que gran parte del problema consiste en acceder a la información por medios legales u organizacionales.
Más adelante bajo el título de "Dependencia del proveedor" se analizan en profundidad los motivos por los cuales es necesario contar con la participación del proveedor ante una investigación. Antes de ello es conveniente conocer las características principales de Cloud Computing, y de este modo comprender las ventajas que ofrece y como esto decanta en su uso masivo. Esta situación de "masividad", como se mencionó anteriormente en la introducción, provoca que no pueda pasarse por alto su estudio para el extender PURI[4].

4 Características de *Cloud Computing*

Los modelos de programación en la nube, comparados con modelos tradicionales, ofrecen principalmente la ventaja de combinar bajo costo y elasticidad, es decir que brindan los recursos especializados para una necesidad concreta y si la misma cambia pueden adaptarse rápidamente con un costo de implantación mínimo, más que económico para servicios pagos; por ejemplo en un servicio de almacenamiento de archivos en la nube (como Dropbox, o Sugar Sinc), se puede aumentar su capacidad sin ningún impacto en los archivos ya almacenados y en forma transparente al cliente. En servicios de IaaS, conveniente para la implantación de sistemas, el cliente puede solicitar mayor capacidad de procesamiento o ancho de banda, si hiciese falta y durante el tiempo necesario sin impacto sobre el sistema en producción.

La conveniencia en el uso de estos servicios es tal que en la última década se ha vuelto de uso masivo y sigue en aumento en todos los niveles de consumidores, desde el uso personal, hasta las empresas y gobiernos. Desde un SaaS, como Gmail, que permite a un empresa tercerizar su correo electrónico corporativo ahorrandose gastos en infraestructura y mantenimiento; al usuario corriente que permite acceso al correo desde múltiples plataformas. Hasda el caso de emprendedores autónomos, que no tienen posibilidad de invertir en una infraestructura propia, les resulta accesible montar su sistema en producción contratando PaaS o IaaS.

El NIST[1] define 5 características de la computación en la nube que nos pueden ayudar a comprender los motivos de su popularidad, y por ende la importancia de incluirla en el marco de un proceso de informática forense.

Autoservicio por demanda: el cliente unilateralmente es capaz de configurar las características del servicio como por ejemplo la hora del servidor o el espacio del almacenamiento sin interacción humana con el proveedor del servicio.

Acceso por redes de difusión: los recursos están disponibles en la red y pueden ser accedidos por medios normales que promueven el uso de plataformas heterogéneas como computadoras personales de escritorio, portátiles, puestos de trabajo, smart phones, tablets, smart tvs, etc.

Pooling de recursos: los recursos informáticos se encuentran reunidos por el proveedor permitiendo el acceso a varios consumidores por medio de plataformas multi-clientes, con diferentes recursos físicos y virtuales dinámicamente asignados y registrados acorde a la demanda del cliente. Existe un sentido de independencia tal que por lo general, el cliente, no posee ningún control o conocimiento de cuál es el recurso físico que se utiliza, o su ubicación geográfica, aunque en algunos servicio si se puede especificar la ubicación con un nivel alto de abstracción, como el país o la región.

Rápida elasticidad: Las capacidades del servicio pueden ser provistas y liberadas en forma elástica, por demanda y en muchos casos en forma automática que permite en escalar rápidamente los recursos. Para el cliente, las capacidades disponibles para el aprovisionamiento, a menudo, pueden parecer ilimitadas y provistas en cualquier momento.

Servicio medido: los sistemas de cloud se controlan automáticamente y permiten optimizar el uso de recursos mediante el aprovechamiento de la capacidad de medición en un cierto nivel de abstracción adecuado para el tipo de servicio, como el almacenamiento, procesamiento, ancho de banda, y las cuentas de usuario activas. El uso de recursos puede ser monitoreado, controlado y reportado, proporcionando transparencia tanto para el proveedor y el consumidor del servicio utilizado.

Del conocimiento de estas características se desprenden ciertos beneficios para los clientes de los servicios en la nube que resultan prácticos desde el simple uso personal hasta grandes proyectos empresariales. El uso personal de un sistema en la nube puede ser seducido por características como el *acceso por redes de difusión*, desde distintos dispositivos; mientras que para las empresas podría llegar a ser más atractiva una característica como la *rápida elasticidad,* es decir la posibilidad de poder utilizar recursos de hardware en forma “maleable” y tercerizados resulta una solución muy satisfactoria para el desarrollo y producción de un sistema, con posibilidad de crecimiento, sin la necesidad de una gran inversión inicial. En definitiva comprender la esencia de la computación en la nube, sus características, modelos y su versatilidad,

ayuda a vislumbrar la importancia de su estudio para la ciencia forense, teniendo como objetivo completar el desarrollo de un proceso unificado que contemple la investigación de la información en dichos sistemas.

5 Actores y sus roles en *Cloud Computing*

Cloud computing involucra personas y organizaciones quienes son los actores del sistema. Identificar los mismos es necesario, en principio para conocer el contexto en el que se trabaja y en segunda instancia, al aplicar y explicar conceptos, para saber inequívocamente a quién nos estamos refiriendo, en tal caso, y cual es su rol. Liu[5] identifica 5 actores principales en la nube: cliente (*consumer*), proveedor (*provider*), distribuidor (*carrier*), auditor (*auditor*) e intermediario (*broker*). Cada actor es una entidad, persona física o jurídica, que participa de alguna tracción o proceso y/o realiza alguna tarea sobre el sistema o servicio en la nube.

Cliente: Es quien utiliza el servicio y mantiene una relación de negocios con el proveedor. Un cliente, o usuario, de la nube recorre el catálogo de servicios de un proveedor, solicita el que le resulta conveniente, establece los contratos de servicios con el proveedor, y utiliza el servicio. El cliente es el actor principal en cloud computing.

Proveedor: Es el responsable por mantener el servicio. El proveedor es quien adquiere y administra la infraestructura necesaria para proveer el servicio en la nube y quien pone a disposición de los clientes, o consumidores, por medio de la red de acceso, generalmente Internet. Las actividades del proveedor principalmente serían: Implementación del servicio, dirección del servicio, administración del servicio, seguridad y privacidad.

Distribuidor: provee conectividad y transporte, el proveedor le requiere conexiones dedicadas y encriptadas para asegurar un nivel de consistencia acorde a las obligaciones contractuales con sus consumidores

Auditor: verifica la conformidad con estándares, evalúa servicios en términos de controles de seguridad, privacidad y performance

Intermediario: administra el uso, performance y distribución de los servicios, negocia relaciones entre proveedores y clientes. En ocasiones el cliente tiene relación con el intermediario sin conocer al proveedor.

6 Principal dificultad: Dependencia del proveedor

Entendiendo a la informática forense como “la ciencia de adquirir, obtener y preservar datos que han sido procesados electrónicamente y guardados en un medio computacional” [3], y teniendo en cuenta las características mencionadas de computación en la nube, hace prácticamente inconcebible esta actividad sin colaboración, principalmente del proveedor del servicio como parte del equipo forense, tanto para la identificación, adquisición y análisis de los datos. A continuación se describen los principales problemas que pueden afectar a esta actividad en este ambiente.

Problema 1: Identificar los servicios y los proveedores de los mismos

La cantidad en causas en las cuales es necesario recurrir a la informática forense en la nube es muy variada. Puede deberse desde un delito de acoso por medio de una red social, una estafa por medio de un sistema de ventas, o incluso una causa donde intervenga un dispositivo por el cual se acceden a múltiples servicios, por citar algunos ejemplos. En los primeros dos, puede estar claro un sistema a investigar, sin embargo en una investigación que recaiga en un dispositivo primero deben identificarse los múltiples servicios y luego identificar los diferentes proveedores de los mismos. De tal modo, es posible que en una investigación sea requerido involucrar varios proveedores no relacionados. Por lo tanto básicamente nos encontramos ante las siguientes situaciones:

Cuando la causa está vinculada directamente a un sistema en la nube: en este caso el sistema es esta plenamente identificado y se debe consultar al proveedor del mismo.

Cuando la causa vincula a un dispositivo y el mismo puede o no utilizar servicios de Cloud Computing: es posible que se tenga que recurrir primero a técnicas convencionales de informática forense buscando huellas en el uso de sistemas en la nube, por ejemplo, cookies, historiales del navegador o archivos de sistemas de alojamiento de archivos como una carpeta de dropbox. Una vez identificados los servicios, se deben identificar las cuentas utilizadas por el usuario como cliente, y por otra parte los proveedores vinculados a cada sistema.

Estos, especialmente en el segundo caso, son problemas adicionales a la investigación sobre un dispositivo, como el *file carving* sobre un disco rígido. La presencia de sistemas en la nube, agrega tiempo complejidad a la investigación ya que no toda la información en un medio físico el cual se tenga en posesión.

Problema 2: Imposibilidad de acceder a los medios físicos

Existen varios motivos por los cuales acceder directamente a los medios físicos donde se encuentra ubicada la información resulta extremadamente difícil o prácticamente imposible.

Subcontratación de servicios: en este caso el proveedor del servicio sea a su vez cliente de otro servicio de *Cloud*, y no disponga de servidor propio. Con lo cual el proveedor puede no conocer la ubicación física de los datos y habría que recurrir al proveedor de segundo nivel (el proveedor del proveedor).

Locación distribuida: los datos del sistema del servicio tiene locación distribuida, es decir que la información no se encuentren en un único servidor físico.

Recursos compartidos: es habitual que los recursos de los servicios de cloud sean compartidos por varios clientes, y estos completamente ajenos a la investigación con derechos sobre su información y el uso del sistema. Por tanto es posible que no se puedan retener tales recursos como evidencia, y las copias de información deban realizarse con el sistema en funcionamiento.

Por estos motivos, es recomendable, en este contexto no contemplar el acceso a medios físicos como un hecho, sino más bien derivar la tarea de recolección al proveedor del sistema. A su vez, sería deseable que el proveedor disponga de los medios para poder obtener y aislar los datos para poder ser presentados al resto del equipo forense.

Problema 3: Información de clientes no relacionados

La privacidad es un derecho, por lo cual solo personas autorizadas deben tener acceso al sistema. Como consecuencias de que los recursos sean compartidos, especialmente para el caso de locación de información, muchos clientes del servicio pueden tener su información en la misma locación (física o virtual), sea una base de datos u otro medio de almacenamiento de archivos. En el curso de una investigación esa información debe ser protegida y diferenciar claramente que pertenece a cada cliente y extraer como evidencia solo lo relacionado al cliente de la causa investigada. Esto también es una tarea que naturalmente recaería en el proveedor del servicio; puesto que aun teniendo acceso directo a los recursos, por parte de un investigador, podría ser complicado discriminar cuáles datos corresponden a cada cliente.

Problema 4: Interpretación del modelo de datos

Una vez adquiridos los datos, se debe disponer de algún medio de interpretación de los mismos. Nuevamente, recaería en el proveedor del servicio brindar la documentación necesaria para la correcta interpretación de los mismos, como por ejemplo modelos de datos, claves de encriptación, contexto semántico, conceptos del sistema, etc.

Dadas estas problemáticas en la informática forense en la nube, es posible notar que la participación y la dependencia del proveedor del servicio es crucial para el desarrollo de una investigación. De no contar con ello, adquirir, obtener y preservar los datos sería extremadamente difícil. Por ello es necesario que en los Términos y Condiciones del Servicio (SLA, por sus siglas en inglés) estén pactadas las obligaciones relacionadas con las disponibilidad y recuperación del acceso a la información. También es necesario contar con acuerdos que habiliten a peritos informáticos los medios solicitar a los proveedores dicha información. Estos acuerdos, idealmente, deberían ser internacionales ya que dado el alcance global de los servicios de cloud computing es posible que el cliente y el proveedor pertenezcan diferentes países.

Problema 5: Sincronización horaria

Debido al alcance global de *Cloud Computing*, un cliente podría estar utilizando servicio donde tanto los datos como los registros de sus acciones se encuentren en otro país, o continente, con una zona horaria distinta a él. Ante la presencia de un acto delictivo conocer la secuencia exacta de sucesos es crucial en la investigación. Sumado a esto se encuentra el solapamiento de los distintos modelos servicios debido a la tercerización de servicios (outsourcing en la nube). Como se mencionó anteriormente éste sería el caso de un proveedor de un servicio que subcontrata otro proveedor de servicios.

Este dinamismo, y versatilidad de casos puede hacer difícil para el investigador la tarea de interpretar las marcas de tiempo sin la colaboración del proveedor. Por lo tanto es fundamental que este informe la zona horaria asociada a las mismas. Más delicado es el problema, si se deben analizar registros de diferentes servicios, para el caso de investigaciones sobre un dispositivo por el cual se accedió a múltiples sistemas en la nube.

Lo más recomendable sería, si debe trabajarse con datos que tienen fechas y horas de distintas zonas horarias, compatibilizarlas por medio de un estándar, por ejemplo UTC. De todos modos, es posible que un dispositivo o un sistema con la hora mal configurada introduzca dificultades adicionales que deben resolverse.

7 Consideraciones para los términos y condiciones de uso de los servicios

Ante la necesidad de la colaboración de parte de los proveedores de servicios en la nube para el desarrollo de una investigación, es menester tener en cuenta que los mismos deberían incluir ciertos puntos en los términos y condiciones del servicio (SLA). Los clientes tiene el derecho de saber que sus datos está protegidos y bajo que circunstancias se permite el acceso a ello y por quienes.

Ruan [2] introduce un modelo de 3 dimisiones:organizacional, técnica y aspectos legales. La dimensión organizacional se relaciona con el equipo forense, su preparación, la interacción del proveedor del servicio y los usuarios con el equipo forense, entidades forenses externas y la ley aplicada. La dimensión técnica trata sobre técnicas para facilitar la investigación forense de los datos. Finalmente la legal trata sobre cuestiones vinculadas a la jurisdicción, propiedad de los datos, cadenas de custodia, notificaciones de eventos, cambios en el proveedor auditorías y cumplimiento de las normas. Basados esta dimensión legal propuesta, agregamos las siguientes items que deben considerarse para ser incluidos en los términos y condiciones del servicios (SLA) de Cloud Computing.

Jurisdicción: El proveedor debe aclarar las regulaciones legales vinculadas a la privacidad respecto de la jurisdicción. Si no está estipulada en las SLA dificultan la investigación. Este no es un tema menor ya que de las características intrínsecas de la computación en la nube es la transparencia en la locación. Así como en las redes sociales pueden conectar personas alrededor del mundo, también es posible contratar servicios en cualquier parte del mundo. como se mencionó anteriormente el cliente puede no conocer la localización geográfica de su información dentro del sistema o el proveedor.

Problemas con los datos de otros usuarios en la nube: En SaaS los clientes comparten el middleware, en PaaS el sistema operativo y hardware y en IaaS el Hypervisor y hardware. Ante un incidente es difícil recolectar solo los datos de un determinado cliente en cada nivel. El proveedor debe aplicar sobre los datos los filtros necesarios para entregar la información que involucra un solo cliente.

Propiedad de datos: refiere a la posesión y responsabilidad sobre los datos. La propiedad implica tanto poder como control. El control incluye acceder, crear, modificar, eliminar datos y todos los beneficios relacionados. Las SLA deben especificar quien es el dueño de los datos.

Cadena de custodia: La privacidad es un derecho, por lo tanto solo las partes autorizadas deben tener acceso a los datos del cliente. La obtención de los datos se debe realizar mediante técnicas forenses “en vivo”, ya naturalmente no se puede apagar el sistema Las SLA debe estipular que todos los datos serán extraídos y verificados por forenses competentes y entrenados y utilizando técnicas y herramientas apropiadas.

Notificación de eventos: Las SLA deben especificar un protocolo claro para la notificación de eventos que sucedieron en un instante de tiempo. De este modo una de las partes puede notificar a la otra sobre algún incidente crítico donde deba aplicarse la ley.

Cambios en proveedor de servicio de nube: Los clientes deben tener el derecho de poder cambiar de proveedor. Las SLA deben expresar en forma clara que el proveedor tiene la responsabilidad de retener datos del cliente para casos de investigación.
Auditorías: Tanto el cliente como el proveedor deben estar de acuerdo sobre las auditorías en las SLA. Relacionado a la característica de "Servicio Medido", sería posible disponer de historiales que registren todos los accesos al servicio..
Cumplimiento de las normas: cubre varias áreas como la ubicación de los datos, validez de los marcas de tiempo de la información, privacidad. Los clientes deberían conocer cuáles son las normas que se cumplir y los proveedores deben garantizar que cumple esas normas.

8 Casos particulares de solicitudes a proveedores

Si bien sería ideal que le proveedor forme parte del equipo forense, no siempre es posible. Algunos proveedores tienen implementados sistemas para colaborar con los investigadores forense. En general es necesario solicitar dicha información como funcionario público autorizado, asignado a una causa y las solicitudes deben realizarse por medio de una cuenta de correo electrónico gubernamental. A continuación, a modo de ejemplo, se explica como Facebook satisface esta necesidad.

Solicitudes de facebook en línea para aplicar la ley (Law Enforcement Online Requests)
La red social Facebook, aplica una serie de mecanismos para el acceso a la información disponibles para realizar una investigación. Estos mecanismos no están disponibles para cualquier persona, solo funcionarios policiales autorizados con una dirección de correo electrónico gubernamental válida pueden acceder y utilizar el sistema de solicitudes en línea para aplicar la ley.
Para obtener acceso, la persona autorizada deberá solicitar un *token* de seguridad cada vez que desee acceder a la herramienta. Dicho *token* se obtiene utilizando el correo electrónico emitido por el gobierno, de este modo se recibirá en la casilla, del mismo, un enlace que permite acceder al sistema. No se puede acceder al sistema si no se dispone de una dirección de correo gubernamental.
Una vez dentro del sistema, se pueden acceder al formulario para resguardo de la información del perfil, al Formulario para registros de *IP's* y a las preguntas frecuentes.
Las solicitudes de resguardo información demoran 90 días, a menos que se realice una solicitud de emergencia en cuyo caso será manejadas sin demoras. Las solicitudes de emergencia son aquellas de las cuales obtener la información en el menor tiempo posible depende la integridad física de una persona; riesgo de muerte o lesiones graves.
En cualquier caso las solicitudes deben estar acompañadas de documentación del caso. Se debe que adjuntar un oficio, lo más escueto posible, y en la medida de lo posible, firmado por un Juez de Garantía. Se realiza el oficio y se escanea para luego adjuntarlo. Es importante que la fecha de la firma del oficio concuerde concuerde con

la fecha en que se envía el formulario. La documentación puede estar en formato DOC, DOCX, PDF, JPG o PNG. Además se debe enviar el número de solicitud interna (IPP) y la cuenta del dueño del perfil a resguardar (la misma se puede obtener ingresando al contacto de Facebook). Para el caso de solicitudes de registros de *IP's*, se debe agregar el rango de fechas por las cuales se hace el pedido.

9 Conclusiones

En la actualidad es cada vez más raro encontrar dispositivos que no se conecten a Internet, y los sistemas Cloud son cada vez más utilizados. Incluso sin necesidad de un medio físico para el usuario, los sistemas SaaS pueden ser medios para cometer delitos. Ante ésta situación, la informática forense debe estudiar los entornos de Cloud Computing y sus particularidades deben contemplarse en un Proceso Unificado.

Al realizar un análisis forense sobre un sistema de Cloud Computing, se nos presentan problemáticas únicas que no encontramos al analizar otros dispositivos, y la principal barrera es la dependencia de los proveedores de servicios, ya que sin su ayuda, la adquisición y análisis de evidencia digital resulta impracticable. Éste problema no es una mera cuestión técnica, sino que involucra también cuestiones legales y organizacionales.

Conociendo, investigando y estudiando los entornos, en sus aspectos técnicos, legales y de organización, las problemáticas de Cloud Computing pueden resolverse. Esperamos que éste trabajo sea un disparador para otros trabajos, que puedan ayudar a validar y mejorar tanto éste, como los resultados de la investigación que seguimos desarrollando en el tema.

10 Agradecimientos

A los ingenieros Ana Di Iorio, Fernando Greco y Hugo Curti por compartir su experiencia y conocimiento. Al resto del Grupo de Investigación de Informática Forense, por su colaboración y trabajo constante. A La Universidad FASTA en general, y Mónica Pascual y Roberto Giordano Lerena en particular por impulsar y dar apoyo al Grupo de Investigación de Informática Forense.

Referencias

1. Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, Special Publication 800-145

2. K. Ruan, J. Carthy, M. Kechadi and M. Crosbie, Cloud forensics,in Advances in Digital Forensics VII, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 35-46, 2011.
3. Michael G. Noblett, Mark M. Pollitt, (2000) Recovering and Examining Computer Forensic Evidence, http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htmI
4. A. Di Iorio, R. Sansevero, M. Castellote, A. Podestá, F. Greco, B. Constanzo, J. Waimann "La recuperación de la información y la informática forense: Una propuesta de proceso unificado", CADI 2012
5. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D. (2011) 'NIST Cloud Computing Reference Architecture' National Institute of Standards and Technology, Special Publication 500-292
6. K. Ruan, J. Carthy (2012) Cloud Computing Reference Architecture and its Forensic Implications: A Preliminary Analysis
7. K. Ruan, J. James, J. Carthy, T. Kechadi (2012) KEY TERMS FOR SERVICE LEVEL AGREEMENTSTO SUPPORT CLOUD FORENSICS