Modelo Para Tratamiento Forense de Incidentes Informáticos en la Nube

Bismark Francachs Castro
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
bfrancachs@gmail.com

***Resumen*—La Computación en Nube ha permitido que las organizaciones puedan extender sus servicios economizando en gastos de infraestructura y con el beneficio de dar acceso desde Internet a sus usuarios. Este fenómeno al potenciar el alcance de los usuarios a diferentes servicios, también ha generado el almacenamiento de información confidencial en equipos en la Nube, lo cual implica que información crítica queda almacenada en servidores de proveedores y podría verse comprometida o expuesta a delitos informáticos. Si se materializa un incidente informático, el mismo puede derivar en un proceso legal que implique el trabajo de operadores legales y peritos informáticos. En el presente trabajo se detallan los aspectos de la pericia forense en la nube, como los especialistas se enfrentan a nuevos retos en este entorno, las normas existentes y la situación de la forensia informática en Bolivia.**

Palabras clave—Computación en nube, Informática Forense, Investigación, Peritaje Informático, Incidente Informático.

I. INTRODUCCIÓN

La evolución de la tecnología en los últimos años ha permitido que las organizaciones implementen herramientas para automatizar diferentes procesos y tareas. El uso de Dispositivos Móviles, Aplicaciones Web y Sistemas Conectados a Internet, permite que la información esté disponible en tiempo real en cualquier parte del mundo. De esta manera la información se ha convertido en el activo más importante dentro y fuera de las organizaciones en el mundo. El uso de los sistemas también ha incrementado el volumen de información que se genera y almacena a diario, lo que implica que las organizaciones aumenten sus costos en adquisiciones de infraestructura tecnológica [1].

Bajo este contexto surge el Cloud Computing o Computación en Nube como una solución para ofrecer el servicio de almacenamiento, procesamiento y transmisión de información de forma rápida y segura desde servidores fuera de las organizaciones y como alternativa para disminuir costos e inversión en infraestructura [1].

La implementación de estas alternativas tecnológicas ha abierto nuevos desafíos de seguridad en las infraestructuras informáticas de las organizaciones permitiendo en algunos casos que se materialicen incidentes informáticos que interfieren con el servicio que prestan las mismas, además de exponer información confidencial de la organización, así como de clientes y usuarios que trabajan con estos servicios.

En 2020 el uso de la Computación en Nube ha sido una de las alternativas adoptadas por la fuerza para una mayoría de las organizaciones. Esto debido a la Pandemia de Covid-19. La pandemia ha obligado a las organizaciones a implementar recursos electrónicos para poder brindar servicios vía internet ante la emergencia que no permite que los usuarios puedan acceder a servicios de forma presencial [2]. En Bolivia también se han adoptado soluciones orientadas a la Nube sobre todo en el aspecto educativo, siendo Google la alternativa más utilizada, sobre todo en aspecto de almacenamiento [3].

Estas circunstancias influyen en que los operadores de justicia y especialistas en forensia deban ajustar sus conocimientos en el campo de la Computación en Nube, pasando por aspectos legales hasta aspectos técnicos.

De acuerdo con lo descrito en párrafos anteriores, es que se propone el presente trabajo de investigación, mismo que se enfoca en la elaboración de un modelo informático forense para tratamiento de incidentes en la Nube.

Para la investigación se ha identificado como problema la **ausencia de normas o leyes** para la pericia forense orientada a la Nube en Bolivia y se ha definido la siguiente hipótesis: El uso de un modelo esquematizado para informática forense orientado a la nube responde al **vacío técnico** en informática forense en Bolivia.

II. MARCO TEÓRICO

A. Metodología de la Investigación

La investigación es de tipo Propositiva, en la que se propondrá un modelo, esta investigación corresponde al nivel aplicativo de la línea de investigación. Dadas esta situación se debe desarrollar resultados correspondientes al nivel Explicativo, con el fin de evidenciar la relación causa-efecto de variables independiente y dependiente definidas en la hipótesis. [4].

Las técnicas a utilizar en la investigación son de tipo experimental y observacional, se utilizará información proveniente de bancos de datos existentes, se desarrollarán entrevistas no estructuradas, en especial a los **operadores de justicia y especialistas del área forense informática** [4].

B. Computación en la Nube

De acuerdo con la definición del Instituto Nacional de Normas y Tecnologías (NIST), la computación en Nube es un

Para referenciar este artículo (IEEE):
[N] B. Francachs, «Modelo Para Tratamiento Forense de Incidentes Informáticos en la Nube», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 22-25, 2020.

modelo que permite el acceso bajo demanda a redes ubicuas con el fin de compartir un conjunto configurable de recursos como ser Redes, Servidores, Almacenamiento, Aplicaciones y Servicios que se pueden proveer y liberar rápidamente con un mínimo esfuerzo de administración o interacción del proveedor de servicio. Se compone por cinco características que son [5]:

- Autoservicio bajo demanda.
- Acceso amplio a la red.
- Agrupamiento de recursos.
- Elasticidad rápida.
- Servicio medido.

El concepto de Nube no es algo que se haya acuñado de forma reciente, al contrario, en 1955 John McCarthy, el informático que acuño el término de Inteligencia Artificial propuso la teoría del tiempo compartido la cual consistía en compartir de forma concurrente los recursos computacionales como el tiempo de ejecución en CPU y el uso de la memoria entre muchos usuarios, dado que en ese tiempo solo se tenían 250 computadoras en el mundo [6].

En 1960 el Laboratorio Nacional de Física en 1960 introdujo el concepto de conmutación de paquetes que permitían descomponer información en paquetes más pequeños, permitiendo de esta manera que más usuarios utilicen la red. 6

En 1970 se creó el concepto de máquinas virtuales (VM) permitiendo que se desarrolle software como VMWare que hace posible ejecutar sistemas operativos en un entorno aislado al mismo tiempo [6].

No mucho tiempo después DARPA (Agencia de Proyectos de Investigación Avanzada de la Defensa) dio origen a las redes que se convertirían posteriormente en la Internet, que dieron acceso a la comunicación en el nivel que la conocemos actualmente [6].

En 1980 con la llegada de las computadoras personales permitieron una mayor expansión de la red, siendo que en 1996 George Favaloro y Sean O'Sullivan, ambos ejecutivos de Compaq Computer usaron por primera vez el término "Cloud Computing" llevándonos en este nuevo milenio a ver la implementación de la Computación en Nube a diferentes niveles pasando por servicio orientado a personas u organizaciones [6].

Fig. 1. Principales usos de la Computación en Nube [6]

Los servicios en la nube se agrupan de la siguiente manera:

- **Software as a Service (SaaS). –** En este esquema el software se aloja en los servidores de los proveedores y el acceso se realiza mediante el navegador web. Todo el mantenimiento soporte y disponibilidad es manejado por el proveedor [7].
- **Plataform as a Service (PaaS). –** En este servicio se ofrece acceso a un entorno en el cual el usuario puede crear y distribuir sus propias Aplicaciones [7].
- **Infraestructure as a Service (IaaS). –** En este servicio el proveedor proporciona el software y las Aplicaciones atraves de Internet, los usuarios acceden mediante la Web o API's del proveedor [7].

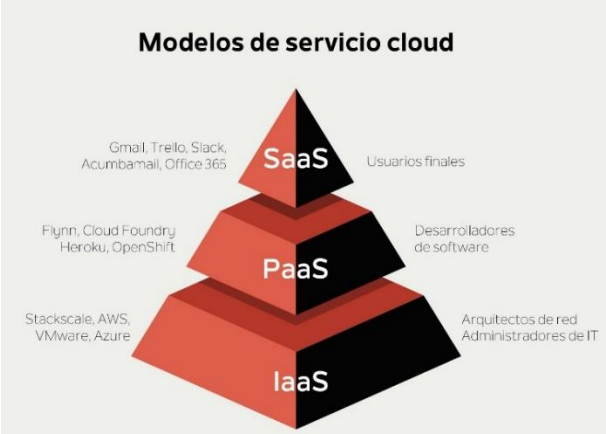

Fig. 2. Modelos de los servicios de la Nube [7]

C. *Incidentes Informáticos en la Nube*

Como ejemplo, se pueden citar la filtración de datos de Capital One en 2019 y la filtración de datos de Facebook también en 2019. En ambos casos los entornos afectados fueron en la Nube siendo que en el caso de Capital One se expuso de manera pública y sin autenticación información de Buckets S3 de Amazon Web Services (AWS), en la información expuesta se encontraba información sensible de clientes. En el caso de Facebook se expusieron registros de 540 millones de usuarios, incluidos datos personales, fotos y contraseñas, esto debido a que un grupo de desarrolladores dejo expuesta la base de datos almacenada en Amazon Web Services (AWS) [8].

D. *Informática Forense*

La Informática Forense son el conjunto de procesos científicos que permiten la colección, preservación, análisis, identificación, interpretación, validación y documentación de información obtenida en la escena de un incidente informático con el fin de presentar evidencia digital en un proceso legal [9].

El inicio de la Informática Forense se remonta al año 1984, cuando el FBI crea un programa conocido como el Programa de Medios Magnéticos que con el tiempo se convertirá en el CART (Computer Analysis and Response Team). o Equipo de Respuesta y Análisis Informático. El llamado padre de la Informática Forense Michael Anderson un agente de la División de Investigación Criminal (IRS) hasta 1990, fue el que trabajo inicialmente en el campo de la forensia digital fundando la compañía New Technologies Inc. Décadas después y hasta la actualidad los organismos policiales y militares siguen expandiendo las ciencias forenses digitales [10].

De la misma manera organizaciones del sector privado han logrado abrirse camino en la Informática Forense esto debido a la demanda que existe para realizar investigaciones forenses en las disputas de carácter civil. Y también contribuyendo con el desarrollo de Software Forense [10].

En la década de los noventas es cuando la Informática Forense es cimentada formalmente. En 1993 se lleva a cabo la primera Conferencia Internacional Sobre Evidencia Digital. En 1995 se forma la Organización Internacional de Evidencia Digital (IOCE). En 1997 los países miembros del G8 en Moscú

declaran que los funcionarios que hacen cumplir la ley deben estar capacitados para hacer frente a delitos de alta tecnología. De la misma manera en 1998 en el G8 se crean los principios internacionales, los procedimientos regessem relacionados a la evidencia digital. El mismo año la Interpol lleva a cabo el Forensi Science Symposium. En el año 2000 el FBI crea le primer laboratorio forense lo cual lleva en 2003 a que el trabajo forense en el FBI exceda los 6500 casos con un total de 782 terabytes de datos [10].

E. Análisis Forense Digital

El Análisis Forense Digital consiste en la aplicación de técnicas para extraer información de interés desde medios digitales como discos duros, memorias usb, memorias volátiles etc. para una investigación en procesos legales, esto sin alterar el estado de la información. Esto con la finalidad de analizar y encontrar patrones de comportamiento que revelen algún indicio de manipulación, alteración o eliminación de información crítica para una organización [11].

El primer paso en los procesos forenses y por lo tanto el más delicado es el de la adquisición, proceso en el cual el perito forense hace el levantamiento de una copia exacta de los medios a analizar, sin alterar la escena de investigación, esta adquisición de información se realiza en presencia de autoridades de la parte legal las cuales levantan un acta en la cual se detalla la escena en la cual se trabaja, los medios a analizar, las herramientas de adquisición de datos y el Hash obtenido en el proceso de recuperación y detalles de la cadena de custodia de los medios que se verificaran en el peritaje. El Hash servirá en el proceso forense para verificar y validar que la información adquirida y la analizada no ha sido alterada en ningún momento del análisis forense y ayudara a validar los hallazgos realizados como evidencia en un proceso legal [11].

El tener una copia exacta de los medios permite acceder a los sistemas de archivos y realizar la inspección de actividades de cuentas de usuario, documentos, programas, etc. De la misma manera mediante el uso de herramientas forenses se puede realizar búsquedas indexadas por palabras clave, recuperación de archivos borrados, revisar correos electrónicos, historiales de chat y navegación por internet inicios de sesión e interacciones de dispositivos [11].

F. Forensia en la Nube

En base a la perspectiva que se tiene sobre el análisis forense de una manera general, podemos indicar que la evolución a realizar análisis forense en los entornos de la Nube no es una trivialidad, e implica que tanto el perito informático como los operadores judiciales involucrados en la informática Forense deben adecuar su conocimiento para este fin, por lo que uno de los modelos a usar para esta circunstancia es el análisis de forense de redes [1].

A su vez el adaptar los procedimientos forenses informáticos y la legislación no siempre es lo más adecuada, ya que entornos virtualizados se deben aplicar otras técnicas como por ejemplo la toma de snapshots [1].

El hacer pericia forense digital orientada a la nube, aun implica muchos retos que van desde aspectos legales, técnicos u organizativos. En el documento de Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) se establecen 65 problemas en la aplicación de técnicas forenses en la nube, entre los que se pueden citar [1]:

- Arquitectura
- Colección
- Análisis
- Respuesta a Incidentes
- Retos Legales
- Estandarización

La forensia informática en la Nube es un subconjunto de la forensia informática en Redes, por lo que sigue las fases principales de esta, siendo que adapta sus técnicas al entorno en la Nube.

La Dra. Keyun Ruan y el Dr. Joe Carthy en su investigación proponen el modelo para la evaluación, el desarrollo y la mejora de la madurez del cloud forense *"Cloud Forensic Maturity Model"* CFMM el cual cuenta con dos partes relacionadas entre sí.

La primera *es Cloud Forensic Investigative Architecture* (CFIA), la cual es una arquitectura de referencia conceptual para investigaciones digitales en entornos de computación en la Nube. Y la segunda *Cloud Forensic Capability Matrix* (CFCM), consistente en una matriz de evaluación de las capacidades correspondientes a componentes del (CFIA).

G. Legislación y Estándares

En cuanto a legislación y estándares para la investigación y planteamiento del modelo se usarán los siguientes:

RFC 3227

Los RFC (Request For Comments) son documentos que recopilan propuestas de expertos en un área, con el fin de establecer pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo [12].

El RFC 3227 es un documento que recoge las directrices para la recuperación de evidencias y su almacenamiento en incidentes informáticos, y se puede usar como un estándar para la recopilación de información en incidentes de seguridad [12].

ISO/IEC 27037:2012

La norma ISO/IEC 27037:2012 es una norma que establece directrices para la identificación, recopilación, adquisición y preservación de evidencia digital [13].

III. Discusión

Según la investigación realizada y de forma preliminar, se puede evidenciar que en Bolivia no se cuenta con una legislación que norme la pericia forense informática.

De acuerdo con un artículo publicado en 2020 por el experto Guido Rosales de la empresa Yanapti, la pericia forense es un campo en el cual el país se encuentra atrasado. Esto puede deberse no solamente a la inexistencia de una legislación, sino también a que los delitos informáticos no cuentan con una legislación adecuada, siendo que solo se sancionan mediante el código penal los delitos de manipulación informática y alteración, acceso y uso indebido de datos informáticos. Esto implica vacíos técnicos y legales que pueden dejar delitos informáticos sin ser juzgados o llevar a resoluciones que no brinden una respuesta en el aspecto informático para víctimas de delitos como la porno venganza, grooming, etc. [14].

Fig. 3. Articulo G. Rosales sobre informática forense en Bolivia [14]

De la misma manera al no tener un estándar fijo, los procedimientos forenses en proceso legales pueden verse entorpecidos por el uso de herramientas que dejen sin validez los hallazgos de un delito.

Esto nos lleva a cuestionarnos del porque la forensia en Bolivia no avanza y como puede afectar este fenómeno a futuro a los incidentes informáticos.

Si hablamos de reglamentación en la Nube, la Autoridad de Supervisión del Sistema Financiero (ASFI), reglamenta en la Ley de Servicios Financieros las condiciones para la adquisición de servicios en la Nube por parte de instituciones reguladas en el Sistema Financiero y de Valores. No obstante, esta reglamentación no incluye aspectos para lidiar con controversias legales en caso de incidentes en un entorno de la Nube, dejando como recurso de respaldo a los acuerdos legales entre proveedores y organizaciones los aspectos de seguridad de acuerdo al servicio adquirido. Esto puede tornarse en un problema para equipos forenses en aspectos técnicos y legales dado que los servicios orientados a la Nube están alojados en servidores extranjeros y proveedor y contratante deben contar con sus equipos forenses. De esta manera si una empresa pequeña se ve afectada por un incidente y requiere una pericia forense digital, al no contar con el presupuesto para contratar a una empresa extranjera se verá en la necesidad de contratar una empresa local o recurrir al sistema judicial local para poder apoyarse en un proceso de esta índole.

El objetivo de la investigación es el planteamiento de un modelo informático forense orientado a la nube que apoye en la preservación de la escena, orientación en aspectos legales para el proceso forense, el análisis de la información obtenida y la presentación hallazgos de un incidente informático desde los siguientes pilares:

Diseño de un manual de procedimientos para la preservación de la escena y recolección de datos de un incidente informático en la nube basado en el documento RFC 3227 (Directrices para la recopilación de evidencias y su almacenamiento), la norma ISO/IEC 27037:2012 (Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital) y las normas UNE del gobierno español.

Establecer en el modelo los roles que deben intervenir en el proceso informático forense y los aspectos técnicos y legales que deben cumplir los mismos.

Esquematización de los pasos para el análisis forense de la escena del incidente informático en la nube basado en ISO/IEC: 27042:2015 (Guía para el Análisis e Interpretación de Evidencia Digital).

Categorización de las herramientas forenses a utilizar en el modelo para la obtención de información desde la Nube.

Elaboración de una plantilla para la presentación de hallazgos forenses en el Entorno de la Nube basado en la norma RFC 6283.

IV. Conclusiones

Basados en lo expuesto en este artículo, podemos ver que se debe investigar e implementar soluciones orientadas a los entornos en Nube, más aún en el contexto que se vive a nivel mundial con la pandemia de Covid-19 que ha obligado a organizaciones grandes y pequeñas a digitalizar sus operaciones, además de aprovechar el uso de tecnologías para brindar sus servicios de forma más rápida a los clientes.

El planteamiento de un modelo forense orientado a la Nube no solo puede ayudar en los procesos forenses informáticos, también puede servir como apoyo para la creación de reglamentos y leyes a nivel nacional que sean más de carácter proactivo que reactivo.

Referencias

[1] J. Oviedo Mercado, Explorando Cloud Forensics, Especialización en Seguridad Informática, 2015

[2] Y. Vásquez, Computación en la nube como estrategia en tiempos de cero contacto, https://andina.pe/agencia/noticia-la-computacion-la-nube-como-estrategia-tiempos-cero-contacto-807409.aspx, 2020

[3] G. Miranda, La Nube – Cloud Computing ,https://www.eldiario.net/noticias/2020/2020_09/nt200923/opinion.php?n=13&-la-nube-cloud-computing, 2020

[4] J. Supo, Portafolio de Aprendizaje Para la Docencia en Investigación Científica, 2017

[5] C. Primorac, Computación en Nube, 2014

[6] M Navarro-Pelayo, Historia de Cloud Computing, https://clinic-cloud.com/blog/breve-historia-la-nube-del-cloud-computing/

[7] B. Fernández, Gestión de Vulnerabilidades en Entornos Cloud, Catalunya, España, 2020

[8] A. Colmenares, D. Cruz, Importancia de la informática forense, 2013

[9] Artículo http://seginformaticacarolinavillamil.blogspot.com/p/el-campo-de-la-informatica-forense-se.html

[10] Artículo https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

[11] Artículo https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital/

[12] Artículo https://www.incibe-cert.es/blog/rfc3227

[13] Artículo G. Rosales, Informática Forense en Bolivia, https://yanapti.com/2020/informatica-forense-en-bolivia/, 2020

Breve CV del autor

Bismark Francachs Castro es Ingeniero de Sistemas por la Universidad de Aquino, Bolivia. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática de la UMSA.
Miembro del comité editorial-científico de la Revista PGI – Ciencia, Innovación y Tecnología en Informática (2019-2020).
Miembro del grupo de investigación GI-FORSAI UMSA. Ha trabajado como desarrollador en Banco Solidario S.A., La Boliviana Ciacruz Seguros Personales y en el Gobierno Autónomo Municipal de La Paz.
Email: bfrancachs@gmail.com. ORCID ID: https://orcid.org/0000-0002-2792-8808.