CLOUD AUDIT & FORENSICS

Análisis de retos y estrategias de Auditoría y Análisis Forense en entornos Cloud

Una iniciativa de:

isms forum spain

CSAES cloud security SPAIN alliance℠

CLOUD AUDIT & FORENSICS

Coordinador

Pablo Castaño Delgado (IT Auditor, Sareb)

Con la participación de los siguientes profesionales

Beatriz Blanco Arenas (IT Audit Manager, Amadeus IT Group)

Iván Robles del Amo (Sales Engineering Manager, Prosegur Ciberseguridad).

Antonio Sanz Alcober (Threat Intelligence, Incident Response & Forensic Senior Analyst, S2 Grupo).

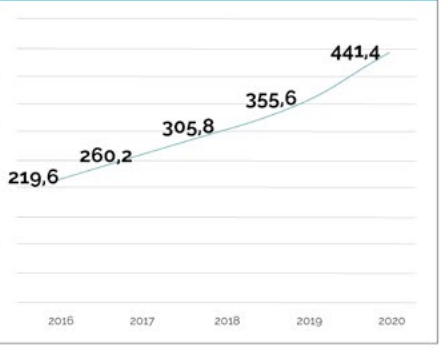
ÍNDICE

1 INTRODUCCIÓN

1.1. Introducción.

La adopción de servicios en la nube, que sirven de soporte a las actividades y operativa de negocio, sigue en aumento. A pesar de no ocupar los primeros puestos en la lista de tecnologías emergentes desde hace algunos años, sigue generando gran cantidad de debate en torno a ella, tanto por su potencial para la innovación, como por los retos que presenta.

Previsión de ganancias de servicios de nube pública a nivel mundial (en billones de dólares)					
Servicio cloud	2016	2017	2018	2019	2020
Business Process as a Service	39,6	42,2	45,8	49,5	53,6
Platform as a Service	9,0	11,4	14,2	17,3	20,8
Software as a Service	48,2	58,6	71,2	84,8	99,7
Gestión y seguridad Cloud	7,1	8,7	10,3	12,0	13,9
Infrastructure as a Services	24,4	34,7	45,8	58,4	72,4
Publicidad Cloud	90,3	104,5	118,5	133,6	151,1
Mercado total	**219,6**	**260,2**	**305,8**	**355,6**	**441,4**

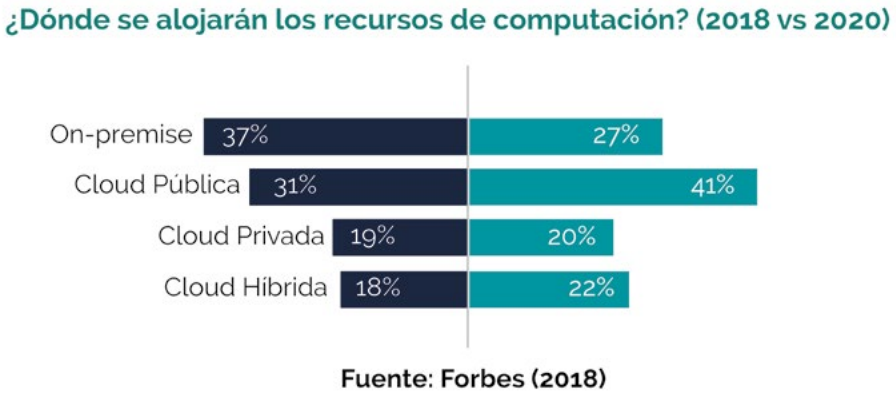


Fuente: Gartner (Octubre 2017)

Nos encontramos ante una tecnología en auge y que, sin embargo, sigue provocando recelo por la falta de control y supervisión que parece imponer su adopción. Si bien el tipo de servicios que se ofrece utilizando modelos basados en la nube aumenta, la supervisión de las organizaciones sobre éstos no madura a una velocidad suficiente.

Fuente: Gartner (2009)

Muchas empresas siguen considerando que las tecnologías cloud limitan su control y visibilidad sobre los sistemas y la información que soportan. Al mismo tiempo, éstos parecen estar más expuestos a ciberataques y otros riesgos por el simple hecho de compartir recursos accesibles a través de Internet.



Fuente: Forbes (2018)

Como puede verse en el gráfico anterior, parece improbable que el uso de los servicios en la nube decrezca, más aún si tenemos en cuenta su coste competitivo y su versatilidad. Por ello, es imprescindible que se articulen en torno a ellos los medios y estrategias necesarios para que su adopción se produzca de forma segura, garantizando un gobierno y control efectivos de los mismos por parte de las empresas.

1.2. Supervisión del servicio Cloud.

Existen multitud de estrategias destinadas a reducir el riesgo derivado del uso de recursos tecnológicos y de comunicaciones en entornos tradicionales. A pesar de que el uso de servicios en la nube es relativamente reciente, los sistemas subyacentes utilizados para prestarlos no dejan de ser muy similares a los utilizados en otros entornos, y por tanto existe cierta predisposición a adoptar las estrategias que se llevan usando durante décadas.

Encontramos que lo realmente desafiante a la hora de lograr adoptar servicios en la nube con un nivel suficiente de control y gobierno de TI, no radica tanto en lo particular de su infraestructura, como en los nuevos modelos de interacción surgidos a partir de la "externalización" de recursos, que en este caso son desplegados por un proveedor de servicios en la nube (CSP) y al que se concede acceso parcial al cliente. Por ello, muchas de las técnicas y estrategias comúnmente utilizadas para llevar a cabo actividades de supervisión se vuelven ineficaces o incompletas a la hora de aplicarlas en entornos en la nube.

Lograr un nivel de supervisión adecuado en este contexto resulta una tarea compleja, habiendo multitud de retos a los que debemos enfrentarnos, entre los que destacan las limitaciones legales y contractuales, las restricciones de acceso a los recursos de un tercero o los riesgos específicos asociados a este modelo de servicio, entre otros.

A lo largo de este documento, se presentará una estrategia de supervisión en la nube, tanto para las actividades auditoría como de análisis forense, que considerará las particularidades de los entornos en la nube, y propondrá un nuevo enfoque para las fases dentro de cada actividad que se deban adaptar al entorno a supervisar.

1.3. Objetivos.

Dada la importancia que los servicios en la nube han adquirido en las organizaciones, se hace necesario articular una estrategia propia para su supervisión, que considere desde su inicio las características y complejidad inherente a este tipo de entornos.

Así pues, el trabajo de investigación descrito en el presente documento se centra en el desarrollo de una estrategia de supervisión de servicios en la nube, que se orquestará en torno a las actividades de auditoría y análisis forense.

Por un lado, porque se considera necesario incluir los servicios en la nube dentro del alcance de la función de aseguramiento desarrollada por los departamentos de Auditoría Interna de las organizaciones. Por otro lado, porque las organizaciones que hagan uso de servicios en la nube deben ser capaces de articular una estrategia reactiva orientada a la mejora continua del control del servicio y una reducción progresiva de los niveles de riesgo asociados, a partir de la ejecución de análisis forenses tras la ocurrencia de incidentes que afecten a estos servicios.

1.4. Contexto / Entorno de referencia

1.4.1. Principales modelos de servicios en la nube

Como en cualquier otro ámbito de TI, la auditoría de servicios en cloud requiere comprender la infraestructura tecnológica en cuestión, identificar los riesgos, evaluar los controles de mitigación y auditar los elementos de riesgo. La comprensión y la evaluación de los riesgos, y por lo tanto su análisis, variará en función del modelo de servicio al que nos enfrentemos, pues cada cual presenta unas particularidades que hacen que su supervisión difiera en determinados puntos y confluya en otros tantos.

A modo de resumen, los diferentes tipos de servicio de cloud se pueden agrupar en las siguientes categorías de servicios: de Infraestructura, Plataforma y Software (IaaS, PaaS y SaaS, respectivamente).

1.4.1.1. Infrastructure as a Service (IaaS)

En este modelo, el proveedor del servicio cloud (CSP) ofrece una infraestructura de recursos TI como un servicio (típicamente un entorno de virtualización de plataforma), facilitando procesamiento, energía, almacenamiento, redes y otros recursos básicos para que el cliente pueda implementar y ejecutar cualquier aplicación sobre ellos. El usuario controla los sistemas operativos, el middleware, el almacenamiento y las aplicaciones. Esta configuración permite un sencillo escalado según las necesidades del cliente.

Los servicios de tipo IaaS permiten reemplazar o complementar la infraestructura interna y por lo tanto, los factores clave a considerar en un proveedor de IaaS son: el rendimiento flexible, la escalabilidad, la disponibilidad y la seguridad.

Dentro de IaaS pueden considerarse los siguientes elementos y sus riesgos asociados:

- Conectividad. En cuanto al acceso fiable a Internet y a los sistemas y tecnologías relacionados. Los riesgos asociados serían la disponibilidad / tiempo de inactividad y la velocidad de acceso.

- Servicios y gestión de red. Se refieren no solo a proporcionar capacidades de red, sino también a administrarla, supervisarla y proporcionar un acceso eficiente a través de aspectos como el balanceo de carga. Los riesgos relacionados son: disponibilidad, transmisiones seguras y nivel de acceso.

- Servicios y gestión de computación. Son aquellos servicios sobre recursos tales como núcleo, procesadores, memoria y administración del sistema operativo. El principal riesgo asociado es la disponibilidad.

- Almacenamiento de datos. Los principales riesgos en este ámbito incluyen: la seguridad de los datos, la recuperación, y la disponibilidad.

- Seguridad. Comprende seguridad física y lógica. Entre otros riesgos se contemplaría la seguridad frente al acceso no autorizado por intrusos malintencionados y empleados deshonestos del proveedor de IaaS.

1.4.1.2. Platform as a Service (PaaS)

En la plataforma como servicio, la capacidad proporcionada al cliente es el despliegue de todos los elementos necesarios para la construcción y puesta en marcha de aplicaciones y servicios web completamente accesibles en Internet. El consumidor no interviene en la capa de infraestructura de la nube, pero gestiona las aplicaciones allí alojadas, y posee la capacidad de controlar su entorno y configuración.

El objetivo principal de este modelo es proteger los datos. Esto es especialmente importante en el caso concreto del almacenamiento como servicio. Un elemento importante que considerar dentro de PaaS es la planificación de una respuesta frente a una interrupción de servicio del proveedor de cloud. Esta debe otorgar la capacidad de balancear la carga entre los proveedores para garantizar la conmutación de los servicios en caso de una interrupción. Otra consideración clave debe ser la capacidad de cifrar los datos mientras están almacenados en una plataforma de terceros y estar al tanto de los problemas regulatorios que puedan aplicarse a la disponibilidad de datos en diferentes ubicaciones geográficas.

PaaS facilita la implementación de aplicaciones, al tiempo que limita o reduce el coste y la complejidad que implica comprar y gestionar las capas subyacentes de hardware y software.

1.4.1.3. Software as a Service (SaaS)

En un servicio SaaS, el cliente puede utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura cloud, pudiendo acceder a ellas desde distintos dispositivos e interfaces, evitando la necesidad de instalar y ejecutar la aplicación en los equipos del cliente, lo que simplifica el mantenimiento y el soporte. En este tipo de servicio, para el cliente, la infraestructura subyacente es transparente, por lo que no será consciente de los elementos de red, servidores, sistemas operativos o almacenamiento, salvo quizás por algunos parámetros de configuración de la aplicación específicos del usuario. Por lo tanto, el usuario utiliza el personal de TI del proveedor para el mantenimiento de los servidores, y no requiere de personal técnico específico que cubra esta función.

Es importante considerar el modelo de procesos de negocio del cliente, lo que implica la necesidad de alinear la estructura organizacional y la integración de los sistemas existentes.

Ejemplos de riesgos asociados con SaaS incluyen: un posible desajuste del proceso de negocio con respecto a la aplicación, conectividad inadecuada entre las aplicaciones y los datos, incompatibilidad con los sistemas ya existentes o una supervisión inadecuada de los procesos y eventos del SaaS, siendo el SLA un objetivo clave de auditoría. También existe el riesgo de un adecuado control de costes y la realización de estimaciones imprecisas, por lo que el aspecto de medición de costes / facturación de SaaS debe tenerse en cuenta también.

Además de los anteriores, existen otros modelos basados en combinaciones de éstos o centrados en funcionalidades específicas. A continuación, se exponen algunos ejemplos de dichos modelos de servicio.

1.4.1.4. Big Data as a Service (BDaaS)

BDaaS hace referencia a servicios que ofrecen análisis de conjuntos de datos grandes o complejos utilizando los servicios alojados en la nube. Servicios similares incluyen el uso de SaaS o IaaS, donde se utilizan opciones específicas de Big Data como servicio para ayudar a las empresas a gestionar los datos. El objetivo de BDaaS es liberar recursos de la organización aprovechando las habilidades de análisis predictivo de un proveedor externo para administrar y evaluar grandes conjuntos de datos. Estas configuraciones contribuyen a ofrecer servicios ágiles con buen rendimiento, aunque las empresas no tienen control sobre muchos de los sistemas por los que transitan sus datos.

La capacidad de crear clusters Hadoop altamente escalables en los centros de datos de los proveedores cloud para el procesamiento batch, permite a las organizaciones ahorrar costes, evitando alojar servidores locales que usarían sólo esporádicamente.

Una de las ventajas de BDaaS es la ubicación de los recursos de almacenamiento de datos en cloud en combinación con el análisis, de modo que los datos, ya sean "fríos" (a los que ya no se accede) o "calientes" (a los que se accede con frecuencia) se almacenan cerca del lugar donde se manipularán para su análisis. Esto puede contribuir a reducir el esfuerzo necesario para mover los datos en un programa o plataforma de análisis.

1.4.1.5. Disaster Recovery as a Service (DRaaS)

DRaaS es un modelo de servicio que se basa en el uso de tecnologías cloud como solución de restauración en caso de desastre. Consiste en disponer de todo el entorno informático crítico virtualizado, de forma latente (idle).

El coste del servicio se basa en mantener snapshots virtuales de los servidores físicos o virtuales, y por la réplica de los datos desde el data center primario al secundario. Además, se paga por la infraestructura como servicio (IaaS) solo en caso de desastre, cuando las máquinas virtuales (snapshots de los servidores del data center primario) son utilizadas como sustitutas de las originales, lo que reduce los costes notablemente en comparación con duplicar un data center. La virtualización además contribuye a reducir los tiempos de recuperación (RTO), y la automatización del proceso agiliza la respuesta. Puede ser muy útil para pequeñas y medianas empresas que no tienen capacidad para disponer, configurar y/o probar un DRP adecuadamente.

Entre otros riesgos, los posibles tiempos de latencia en función de la distancia a la que se encuentre el proveedor de cloud pueden tener asimismo un impacto significativo en la respuesta, como también la dependencia de los servicios de red involucrados. Otro riesgo podría estar en la migración de vuelta de los datos al servidor primario para restaurar el servicio. Los requerimientos y expectativas sobre el servicio DRaaS deben quedar documentadas en un SLA, por lo que su monitorización es muy importante.

1.4.1.6. Backup as a Service (BaaS)

En este modelo la organización decide que ficheros guardará en el sistema de almacenamiento del proveedor cloud para su back up. El proveedor solo se responsabiliza de la consistencia de los datos y de restaurar las copias en caso necesario. El cliente establece los parámetros asociados a la ejecución de las copias, como son: frecuencia, ventanas, RPOs y RTOs.

1.4.1.7. Security as a service (SECaaS)

Se trata de un modelo de servicio en el que el proveedor integra sus servicios de seguridad en una infraestructura corporativa en base a una suscripción y facilita un mayor abanico de servicios de seguridad integrados de lo que podría permitirse una organización por si misma por el mismo precio. Está inspirado en SaaS, aplicado a la seguridad de la información y no requiere tener hardware propio en el cliente, por lo que se reducen los costes. Algunos ejemplos de los servicios que incluyen son: autenticación, antimalware, antispyware, detección de intrusión, pentesting y gestión de eventos de seguridad.

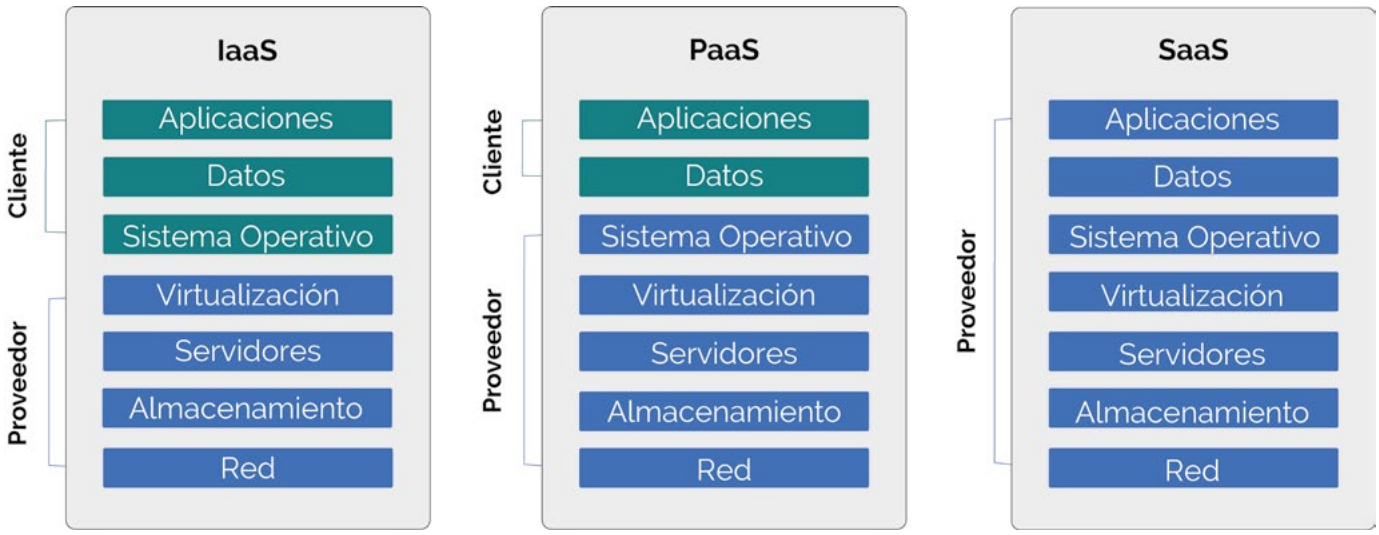
1.4.2. Comparativa de los modelos de servicio

Basándonos en las definiciones del apartado anterior, podemos concluir que la capacidad de supervisar los servicios descritos disminuye a medida que ascendemos en las capas de control de dichos servicios por parte del proveedor cloud. Esto es, cuanto mayor control tenga el proveedor sobre la infraestructura, más difícil resultará para el cliente supervisar dichos servicios. De este modo, la capacidad de supervisión intrínseca sobre el modelo SaaS resultaría a priori menor que la que podría tenerse sobre un PaaS y esta a su vez será inferior a la que se pueda tener sobre un modelo IaaS.

Dado que en un modelo SaaS el cliente hace uso de las aplicaciones que el proveedor cloud pone a su disposición sobre plataformas e infraestructuras transparentes al usuario, resulta complejo para el cliente supervisar dichos servicios, sobre los que en principio no tiene visibilidad. Por ello, en caso de que el cliente requiriese supervisar dichos servicios, sería necesario analizar la posibilidad de establecer controles alternativos sobre el servicio prestado y la tecnología subyacente a otros niveles.

En el otro extremo, el modelo IaaS permite al cliente tener un mayor control y por lo tanto conocimiento sobre la infraestructura subyacente, y esto permite asimismo establecer parámetros de supervisión y monitorización de acuerdo a las necesidades o exigencias del propio cliente. No obstante, sigue habiendo capas sobre las que el usuario del servicio cloud no tiene esa visibilidad y cabe considerar también la posible necesidad de supervisarlas.

A alto nivel, se muestran en esta introducción algunas de las principales diferencias que presentan dichos modelos en cuanto a la capacidad de supervisarlos:



1.4.2.1. Gestión de Identidades y Accesos (IAM)

En cualquiera de los tres modelos estándar de servicio es un área de gestión crítica (más compleja cuanto más cerca esté de la infraestructura), y requerirá diferentes grados de monitorización.

1.4.2.2. Gestión de Licencias

Abarcan desde las licencias de las aplicaciones, a las de bases de datos y servidores. A priori, en el modelo SaaS el coste de la licencia resulta transparente para el usuario ya que viene embebido en la contratación del servicio. No obstante, será necesario supervisar que el proveedor haya establecido los controles apropiados para no incurrir en posibles incumplimientos por uso ilegal de software. Cuanto más nos acerquemos a la infraestructura, más control habrá sobre las licencias. El modelo PaaS, como situación intermedia, puede resultar particularmente complejo en lo que respecta a dicha supervisión de licencias.

1.4.2.3. Gestión de amenazas y vulnerabilidades

En los modelos PaaS e IaaS dependerá en gran medida de la gestión de parches, a veces realizada por el cliente, a veces por el proveedor. En modelos SaaS cabe considerar controles como revisión de código seguro, threat modelling, etc.

1.4.2.4. Cumplimiento regulatorio

Aplicará en mayor o menor medida en función de los datos que se manejen, por lo que la elección del modelo de servicio en este caso es crítica en función de la sensibilidad de la información tratada. Si por cumplimiento regulatorio o legal se exigen una serie de controles a distintos niveles, que un determinado modelo de servicio no garantiza, está en manos de cliente tomar la decisión más adecuada sobre el modelo de servicio elegido, el proveedor más apropiado e incluso en última instancia, la decisión de migrar o no cierta información a la nube.

1.4.2.5. Disponibilidad

Dependiendo de la criticidad de la información que tengamos alojada en cloud, los controles sobre su disponibilidad serán más o menos relevantes. Por ejemplo, no es lo mismo un servicio SaaS para la gestión de cuentas de correo corporativas que para compartir archivos de forma puntual con agentes externos a la compañía. En cualquier caso, llegada la necesidad de supervisar dicha disponibilidad, de nuevo la visibilidad sobre un SaaS será inferior que la que se pueda tener sobre un IaaS y en cualquier caso, el conocimiento sobre sus políticas de continuidad y la monitorización de los SLAs establecidos, ayudarán a medir en cierto modo el estado de este parámetro.

1.4.2.6. Operaciones de seguridad

Desde el punto de vista de un proveedor, un SOC ayudaría en la monitorización y gestión de amenazas de seguridad y el cliente podría apoyarse en él para tener información fiable y actualizada sobre la situación de sus datos. Independientemente de la existencia o no de un SOC, el cliente tendrá sus propias políticas y estándares en los que basarse para requerir, al igual que ocurría en el caso del cumplimiento, que se establezcan ciertos controles a determinados niveles. Cuanto más sensible sea la información manejada, mayores serán los controles de seguridad requeridos.

1.4.2.7. Desarrollo de aplicaciones

El proceso de supervisión de esta área puede complicarse especialmente en modelos PaaS si no se han establecido de antemano los criterios adecuados ni las reglas de compromiso que decidirán los roles y responsabilidades de cada parte, y por ende los controles que se habrán de implementar según las circunstancias.

AUDITORÍA DE SERVICIOS EN LA NUBE

2

2.1. Introducción

El uso de cloud introduce unas nuevas variables y desafíos que generalmente no son de aplicación en un proceso de auditoría convencional. Esto obliga a los auditores a adaptarse a los cambios y abordar los riesgos de este nuevo entorno, con la misma eficiencia y precisión que en cualquier otra auditoría.

Este capítulo tratará de analizar los retos que surgen al enfrentar la supervisión de entornos cloud, cuál podría ser la estrategia para abordar este tipo de auditorías, así como qué fases del proceso sería conveniente desarrollar.

A continuación, se listan algunos de los desafíos a los que los auditores de deben enfrentarse durante el proceso de análisis de servicios en la nube:

2.2. Retos de la auditoría de entornos cloud.

A continuación, se exponen los principales retos a la hora de auditar servicios en la nube, derivados de la adquisición del servicio, como alternativa a la adquisición de la tecnología necesaria para el despliegue de sistemas tradicionales internamente; así como por las características específicas de los entornos cloud:

2.2.1. Derecho a auditar al CSP.

La auditoría de servicios cloud implica la supervisión de un proveedor, por lo que, al tratarse de un tercero, no siempre se tiene el derecho a auditarles. Para ello, esta actividad deberá quedar estipulada por contrato (cláusula right to audit). Adicionalmente, este hecho puede complicarse en cuanto a que las negociaciones de cambios de clausulado en los contratos con algunos proveedores de cloud no siempre resultan todo lo flexible que cabría esperar. En ocasiones, en lugar de ofrecer la posibilidad de auditar el servicio, los proveedores conceden acceso a certificaciones tipo ISO 27001 o SOC/ISAE, e incluso a sus informes de auditoría.

2.2.2. Comunicación con el CSP.

En función del tamaño del proveedor o de la relación de confianza con el mismo, puede ser complejo encontrar un punto único de contacto que pueda ayudar al auditor en el proceso de la auditoría, tanto para la recopilación de evidencias, como para la resolución de dudas sobre las mismas. En muchos casos, las dificultades de comunicación podrían derivar en una limitación al alcance.

2.2.3. Acceso restringido a las evidencias.

Aunque el proveedor conceda derecho a auditar el servicio cloud, fundamentado en un principio de confidencialidad con sus otros clientes, pueden existir reticencia por su parte para facilitar el acceso a determinadas evidencias, que podrían ser necesarias para la auditoría (Ej. acceso a información criptográfica, logs de accesos, listados de administradores, evidencias de restauración de backups, resultados de DRPs/BCPs, etc.).

2.2.4. Dificultad para auditar entornos multi-cliente (multi-tenant).

En los entornos cloud, la capacidad para compartir la infraestructura que soporta el servicio entre distintos clientes supone un beneficio por la reducción de costes asociada. No obstante, los riesgos de seguridad se ven incrementados, así como la complejidad del acceso a información sobre el proveedor o el servicio con fines de auditoría.

2.2.5. Dispersión geográfica.

El uso de servicios cloud puede suponer que la información esté dispersa en diferentes países, con sus propias regulaciones y legislaciones locales, lo que supone que el acceso del cliente ya no está sujeto únicamente a sus propios requerimientos internos y locales, sino que podría depender además de otras jurisdicciones. Esto se hace especialmente relevante en el ámbito de la privacidad y seguridad de los datos, por lo que, en un proceso de auditoría, es indispensable conocer la ubicación geográfica de la información.

2.2.6. Elementos virtuales.

Los entornos cloud hacen uso de tecnologías virtuales y entornos volátiles. El nivel de abstracción introducida por estas tecnologías dificulta el proceso de auditoría, y puede obligar a adaptar el alcance de las actuaciones.

2.2.7. Estándares y regulaciones no adaptadas a cloud.

Salvo por algunas excepciones, como la CCM (Cloud Control Matrix), y algún otro marco específico de seguridad, los estándares y regulaciones aplicables a los entornos tradicionales no están siempre adaptados a cloud. Esto requiere un esfuerzo por parte de los auditores, quienes deben identificar los marcos aplicables según el objetivo de la auditoría y adaptarlos, detectando los posibles gaps, para poder adecuarlos a sus necesidades específicas.

2.2.8. Limitación en la monitorización de costes.

En algunos proveedores, la monitorización periódica de los costes se puede realizar con cierto detalle a través de las herramientas que estos ponen a disposición del cliente, pero no siempre existe dicha opción o en ocasiones la información facilitada no contiene un detalle suficiente para poder trazar de forma precisa el coste frente al uso del servicio, lo que puede dificultar el análisis por parte de un auditor.

2.2.9. Planificación y gestión de la capacidad.

Si bien en entornos SaaS este puede ser un punto menos preocupante para el cliente porque queda fuera de su alcance, en entornos PaaS e IaaS se requiere de un mayor control por parte del usuario del servicio para garantizar que la escalabilidad resulte eficiente. Por lo tanto, la falta de gestión y planificación de la capacidad en cloud por parte del cliente, puede resultar en un reto importante durante la ejecución de auditorías.

2.2.10. SLAs, monitorización del rendimiento y disponibilidad.

Los contratos con proveedores cloud deben abordar las obligaciones a las que queda sujeto el proveedor en lo relativo al nivel del servicio provisto (SLA). Para que este tipo de cláusulas contractuales puedan aplicarse adecuadamente es necesario que el proceso de monitorización de los indicadores correspondientes funcione adecuadamente. Como en cualquier auditoría de un servicio prestado por un tercero, se hace complejo auditar este aspecto, por la dificultad para acceder a las evidencias del incumplimiento.

2.2.11. Desarrollo de software.

Este reto se vuelve especialmente relevante en el caso de las auditorías sobre el desarrollo de software en modelos tipo SaaS, ya que el cliente dispone de poco control sobre ellos. En modelos PaaS la complejidad radica en manejar diferentes entornos en cloud (desarrollo, test, calidad, preproducción, producción, etc.), con la posibilidad de que existan sobre ellos distintos niveles de responsabilidad por parte del cliente o el proveedor. Si estas responsabilidades no están claramente definidas por contrato, sin duda será un reto para el auditor definir cómo abordar los controles de su revisión.

2.2.12. Eliminación de información.

Aunque los contratos con proveedores cloud estipulen que la información del cliente será eliminada tras la finalización del contrato, o bien bajo petición expresa del cliente, es una tarea compleja para un auditor tener garantías de que dicha información se ha eliminado de manera efectiva de sus sistemas. La replicación en diferentes servidores, que además pueden estar distribuidos geográficamente, o en sistemas de almacenamiento compartidos, dificulta la obtención de evidencias fehacientes sobre los controles aplicados para garantizar la eliminación, o sobre la propia eliminación.

2.2.13. Falta de concienciación del Comité de Auditoría o del Consejo.

Si de por sí resulta complejo el proceso de auditar entornos "virtuales", alojados en la infraestructura de un proveedor, con la complejidad que su gestión y control puede suponer a nivel interno, el auditor se puede encontrar además limitado por la falta de concienciación de las principales partes interesadas sobre la necesidad de supervisar los servicios cloud y su gestión interna.

2.3. Estrategia de auditoría de entornos cloud.

La estrategia de auditoría en entornos cloud debe permitir identificar las necesidades de aseguramiento de la organización, en lo relativo a los servicios cloud adquiridos, considerando aspectos internos y externos.

2.3.1. Inputs para la elaboración de la estrategia de gobierno.

De entre todos los enfoques que se pueden seguir a la hora de planificar, diseñar y ejecutar auditorías, el que ofrece un mayor nivel de madurez es el enfoque basado en riesgos, puesto que permite identificar y tratar los riesgos a los que está expuesta la organización, de forma que ésta vaya mejorando de forma progresiva.

Otro enfoque muy ampliamente utilizado es el basado en cumplimiento, de forma que se determinen aquellos requerimientos legales a los que está sujeta la organización y se asegure el cumplimiento con estos a lo largo del tiempo. En realidad, puesto que uno de los riesgos más obvios para la organización es el de incumplimiento, esta aproximación ya estaría incluida en el enfoque basado en riesgos. En cambio, en el enfoque basado en cumplimiento, no se tienen en cuenta las características de la organización para plantear las auditorías, por lo que el soporte al negocio es menor.

Considerando lo anterior, el primer elemento que se considerará a la hora de definir una estrategia de auditoría eficiente para ofrecer aseguramiento sobre los servicios en la nube usados por la organización serán los riesgos a los que ésta se ve expuesta por el uso de dichos servicios.

2.3.1.1. Riesgos para la organización derivados del uso de servicios en la nube.

A continuación, se incluyen algunos de los principales riesgos asociados al uso de servicios en la nube. La identificación de riesgos cloud asociados al servicio adquirido es una actividad que debe desarrollar cada organización, puesto que sus características, así como las de los servicios adquiridos y uso de los mismos, determinará en gran medida los riesgos a los que se está expuesto.

2.3.1.1.1. Brechas / Fugas de datos.

Al igual que los entornos tradicionales, las tecnologías cloud pueden verse afectadas por las amenazas clásicas presentes en aplicaciones, sistemas y redes. El matiz en este caso estriba en el alto volumen de datos almacenados en los servidores de la nube y la mayor dificultad para establecer controles de acceso, lo que implica que, en caso de producirse una brecha de datos, el impacto sería significativamente más alto.

El nivel de impacto vendría dado por el carácter y sensibilidad de los datos expuestos, como por ejemplo aquellos relacionados con la salud, propiedad intelectual o propiedad industrial.

Asimismo, el daño económico, derivado de las potenciales sanciones que podría imponer un regulador o autoridad de control; así como el daño reputacional, que podría afectar a la imagen de marca durante años; hace que el análisis de este tipo de riesgos sea muy importante para cualquier organización.

2.3.1.1.2. Inadecuada gestión de identidades, accesos y credenciales.

La asignación de permisos y la definición de identidades conllevan un esfuerzo y dificultad que en muchos casos implica que se cometan errores, otorgándose permisos y accesos a información y sistemas a usuarios que no deberían tenerlos. Conocida es la situación de riesgo que se produce cuando alguno de los usuarios de la organización cambia de puesto o de departamento, siendo una prueba básica de auditoría verificar que los permisos de acceso se han actualizado correctamente.

Igualmente, los mecanismos de asignación de contraseñas o los propios sistemas de autenticación, cuando no disponen de controles para robustecerlas y evitar que un usuario ilegítimo acceda a donde no debe, son amenazas que preocupan diariamente a los responsables de seguridad de cualquier organización.

Por otro lado, han de valorarse los riesgos que implica federar las identidades con un proveedor de cloud frente a la centralización de las mismas en un repositorio único. En el caso de optar por el cloud, el auditor debe analizar si la organización ha revisado los controles de seguridad que dicho proveedor ofrece para proteger la plataforma de identidad.

2.3.1.1.3. Vendor Lock-in.

Los servicios cloud están diseñados para que el cliente pueda abstraerse de la tecnología y acceder de forma sencilla y rápida a unas necesidades tecnológicas específicas. Sin embargo, derivado en parte de esta abstracción, así como de la localización de los datos en un entorno controlado por un tercero, se puede llegar a producir una situación de bloqueo en la que el cliente no sea capaz de migrar el servicio cloud a la infraestructura de otro proveedor.

Esto suele deberse a la incompatibilidad surgida entre la tecnología desplegada por dos proveedores distintos, o por restricciones en el acceso a los datos depositados en la nube. Asimismo, esta situación también puede estar causada por una mala negociación de las cláusulas del contrato con el proveedor del servicio cloud.

2.3.1.1.4. Pérdida de control sobre la administración.

En ocasiones, el cliente de servicio cloud no solo contrata un servicio en la nube, sino que además delega su administración, voluntariamente o no, en el propio proveedor del servicio.

Esta práctica entraña un riesgo, debido al perfil de acceso que adquiere el proveedor sobre los datos del cliente. Por otro lado, no poder acceder a funcionalidades para las que se requiere acceso privilegiado al entorno podría suponer una administración del entorno cloud desalineada con las necesidades, políticas, estándares y procedimientos internos de la organización.

Aunque pudiera parecer que solo los modelos IaaS están expuestos a este riesgo, puesto que en los modelos PaaS y SaaS la mayor parte de la infraestructura está controlada por el proveedor, es importante que el cliente pueda controlar y administrar las funcionalidades críticas de las capas bajo su control, cuando éstas no impacten en la infraestructura subyacente.

2.3.1.1.5. API e interfaces inseguras.

Cualquier proveedor de servicios en nube ofrece actualmente funciones vía APIs, así como interfaces para facilitar la administración que el cliente haga de los servicios, tanto a nivel de aprovisionamiento, como de gestión y seguimiento de los mismos.

La seguridad y disponibilidad de los servicios en la nube dependen de la seguridad de la API en lo que, a autenticación, control de acceso, cifrado y supervisión de éstas se refiere. Cuantos más servicios y usuarios dependan de la API, mayor riesgo existe, puesto que también aumenta el número de credenciales para acceder a los servicios. Las interfaces y APIs débiles provocan un aumento de riesgo, dado que son la parte más expuesta del sistema, al ser accesibles desde Internet.

2.3.1.1.6. Explotación de vulnerabilidades en el sistema.

Las vulnerabilidades del sistema y otros errores explotables asociados al software y los protocolos de red se han convertido en un problema más acentuado en los entornos cloud, debido al hecho que conlleva compartir infraestructura, aplicaciones y sistemas, creando una mayor superficie de ataque.

2.3.1.1.7. Secuestro y apropiación indebida de cuentas.

En los últimos tiempos, el secuestro de cuentas, vía phishing principalmente, ha estado a la orden del día en numerosas organizaciones. En el caso de la nube, el atacante que se apropie de una cuenta puede, no solo acceder a datos, sino espiar las actividades y manipular transacciones, así como llegar a utilizar la infraestructura / aplicación en la nube para actividades ilícitas.

2.3.1.1.8. Ataques internos.

Un gran número de ataques en las organizaciones están provocados por usuarios internos que hacen un uso malintencionado de los recursos. Empleados o socios descontentos, así como usuarios del sistema que han sido despedidos de la compañía, pero a los que no se les han retirado los derechos de acceso, pueden utilizar sus privilegios de acceso para dañar la compañía.

Entre los ataques que puede desencadenar un empleado interno en un entorno de nube se encuentran desde el robo o la manipulación de información, hasta la destrucción de la infraestructura virtualizada.

2.3.1.1.9. Amenazas Persistentes Avanzadas –APT-.

Este tipo de amenazas también son conocidas como "parasitarias", debido a que suelen basarse en accesos a un punto origen, desde el cual, de manera sigilosa y prolongada llevan a cabo ataques muy elaborados.

Las APT son difíciles de detectar. Los mecanismos más habituales de infección del sistema se basan en ataques de ingeniería social, unidades USB que incluyen software malicioso, redes comprometidas de terceros, etc. Dado que uno de los objetivos de las APTs son equipos fuertemente bastionados, suelen hacer uso de la falta de concienciación y formación de los usuarios de la infraestructura para evadir los controles perimetrales.

2.3.1.1.10 Incumplimiento regulatorio.

En los entornos en la nube existe una mayor complejidad a la hora de establecer la responsabilidad frente a las obligaciones legales, así como las jurisdicciones aplicables. Ante esta mayor complejidad, una falta de diligencia puede conllevar el incumplimiento involuntario de algún requerimiento legal, lo que puede acarrear sanciones económicas, especialmente graves en el caso de aquellas impuestas por incumplimientos del RGPD.

2.3.1.1.11. Abuso y uso malintencionado de los servicios cloud.

Tanto los usuarios internos malintencionados, como aquellos usuarios que hayan conseguido vulnerar los controles de seguridad, pueden hacer un uso indebido del servicio cloud, pudiendo acarrear esto impactos económicos, derivados del uso excesivo del servicio por sus capacidades de uso bajo demanda; reputacionales, en caso de que el uso indebido tenga exposición hacia terceros; o incluso regulatorios.

2.3.1.1.12. Denegación de Servicio.

Las arquitecturas que soportan los servicios en la nube no son invulnerables a los ataques de denegación de servicios. Aunque pueden utilizar sus capacidades inherentes y las herramientas desplegadas en la infraestructura subyacente para reducir el impacto, existe un riesgo incrementado de pérdida de disponibilidad del servicio.

Aunque la forma más conocida de pérdida de servicio son los ataques DoS y DDoS, utilizando éstos últimos el uso de máquinas distribuidas para incrementar la potencia del ataque; existe un sinfín de causas que pueden provocar una denegación del servicio, desde un cambio incorrecto de la configuración de red, hasta un incidente en la infraestructura o en el ISP.

2.3.1.1.13. Infección por ransomware.

Los ficheros cargados en la nube siguen siendo vulnerables a infecciones por ransomware. En caso de que exista sincronización entre los ficheros en la nube y en local, una infección por ransomware podría transferirse desde la nube a los recursos de almacenamiento internos de la organización.

2.3.1.1.14. Falta de alineamiento con las expectativas de las partes clave o con los objetivos de negocio.

Este riesgo, lejos de ser exclusivo de los servicios en la nube, es quizás el único intrínseco a cualquier tipo de tecnología. En el caso de las tecnologías y servicios cloud, la falta de alineamiento con el negocio se produce como resultado de una falta de control y planificación, y provoca una reducción o incluso eliminación de los beneficios obtenidos como resultado de la inversión en servicios cloud.

2.3.1.1.15. Pérdida de visibilidad sobre la infraestructura.

Los peligros asociados a las ShadowIT son muy diversos, desde la falta de protección de la infraestructura, hasta la exposición no controlada de información sensible para la organización.

2.3.1.2. Soporte a Negocio.

Además de los riesgos para la organización, existen determinados aspectos, tanto de carácter interno a ésta, como externos, que también es importante considerar para la planificación estratégica de las auditorías, y que están estrechamente relacionados con las necesidades y expectativas de Negocio.

Según la Norma 2010 – Planificación, del Instituto de Auditores Internos, se deben considerar los siguientes aspectos a fin de priorizar correctamente las actividades de un Plan de Auditoría:

2.3.1.2.1. Análisis de riesgos.

El Plan de Auditoría debe fundamentarse en una evaluación de riesgos formal, que debería ser actualizada al menos anualmente. Esto permitirá ajustar los trabajos de auditoría al contexto de riesgo, tanto interno como externo, y favorecer el soporte a negocio, lo que redundará en un mayor aporte de valor a la organización. Por ello, una vez identificados los principales riesgos a los que se ve expuesta la organización a causa de la adopción de servicios en la nube (véase apartado 2.3.1.1), dichos riesgos deberán evaluarse para determinar la criticidad de los mismos, y permitir así su priorización.

2.3.1.2.2. Expectativas de las partes interesadas.

Es fundamental que el Plan de Auditoría se diseñe de tal forma que las actuaciones den respuesta a las principales inquietudes y preocupaciones de los miembros clave de la organización, como la alta dirección, el Consejo y en particular, el Comité de Auditoría. Considerando las opiniones de estos grupos, junto con sus necesidades y expectativas, se favorecerá el alineamiento de los trabajos con la consecución de los objetivos de la organización. Sin embargo, puede ocurrir que, asociado al servicio en la nube adquirido, se identifiquen partes interesadas adicionales, o que cambie la relevancia de alguna de las existentes.

2.3.1.2.3. Soporte a negocio y función de asesoramiento.

Además de responder a las inquietudes de actores como la alta dirección y el Consejo, es importante que la función de auditoría se desarrolle considerando también las necesidades y preocupaciones de otras áreas clave de la organización, posicionadas en la primera y segunda líneas de defensa. En el caso de las Auditorías de TI, es necesario que el Plan de Auditoría haya sido consensuado al menos con las áreas de Negocio responsables del servicio en cloud, incluyendo aquellas encargadas de la tecnología, las operaciones, la ciberseguridad y el cumplimiento (y eventualmente, también con el área de Compras y el departamento Legal, entre otros). De esta manera, sus expectativas podrán considerarse en la definición del Plan, sin que ello llegue a perjudicar la independencia en el desarrollo de la función.

2.3.1.3. Experiencias previas.

Junto con estos aspectos formales, hay otros de tipo más operativo, que dependen de las experiencias previas, tanto de la propia organización, como del entorno, y que es fundamental analizar para el desarrollo del Plan de Auditoría:

2.3.1.3.1. Incidentes y brechas de seguridad ocurridas.

Considerando la función de Auditoría Interna como la tercera línea de defensa de una organización, es importante que, para la planificación de las auditorías, se tengan en cuenta todas las incidencias y brechas de seguridad ocurridas en la Organización que puedan afectar a los entornos cloud.

Las características particulares de esta tecnología requieren considerar, no solo aquellas brechas e incidentes que afecten directamente a ésta, sino cualquier otro incidente que pudiera provocar impacto en los servicios cloud, como por ejemplo aquellos sufridos por el proveedor del servicio.

2.3.1.3.2. Riesgos identificados en auditorías previas.

La elaboración del Plan de Auditoría debe tener en cuenta aquellos riesgos identificados en auditorías previas sobre los que sea necesario realizar un trabajo adicional de análisis. Esto, en el caso de las auditorías en la nube, permitirá, una vez ejecutadas auditorías de alto nivel, como las de cumplimiento, ciberseguridad, etc., dirigir de forma más precisa aquellas auditorías de tipo más técnico que se desarrollen a continuación de las primeras.

2.3.1.3.3. Experiencias de terceros.

Puesto que en muchos casos los servicios cloud son compartidos y están expuestos a Internet, es conveniente considerar, no solo la experiencia recabada por la propia organización, sino cualquier brecha o incidente sufrido por un tercero que afecte a un servicio contratado por la organización o a cualquiera de las tecnologías utilizadas para proveerlo. Esta exploración de fuentes externas, para las que es muy recomendable apoyarse en técnicas de ciberinteligencia, puede realizarse a varios niveles. Por ejemplo:

I. Conviene identificar brechas sufridas por un proveedor cloud concreto, analizando aquellas causas asociadas al propio proveedor, como una mala gestión de las contraseñas de administración, servicios indebidamente expuestos, etc.

II. También es recomendable investigar qué brechas ha sufrido un servicio cloud particular, dado que en dicho caso existe una alta probabilidad de que los clientes que hacen uso de ese servicio se hayan visto expuestos.

III. Es necesario investigar las vulnerabilidades detectadas sobre las tecnologías que dan soporte al servicio cloud, puesto que serán una vía de entrada a posibles atacantes.

2.3.1.4. Cambios relevantes.

Otro input relevante a considerar son los cambios relevantes ocurridos sobre la organización, que puedan generar cierto impacto sobre la tecnología cloud.

2.3.1.4.1. Cambios legislativos o regulatorios.

Uno de los aspectos más relevantes que deben requerir la inclusión de actividades de supervisión específicas en un Plan de Auditoría, destinadas a ofrecer aseguramiento en entornos cloud, es la entrada en vigor de nueva legislación, o cambios en la legislación existente que afecten a

los servicios contratados en la nube. Este aspecto puede ser especialmente complejo de analizar en el caso de las tecnologías en la nube dado que los datos pueden estar geográficamente dispersos, y el control sobre la infraestructura de TI no está en manos del propietario de dichos datos. Por tanto, en el diseño del Plan de Auditoría, el primer aspecto a considerar es la necesidad de garantizar que los servicios cloud adquiridos se adaptan a los cambios en la legislación aplicable.

2.3.1.4.2. Cambios organizativos de tipo tecnológico.

No solo los riesgos identificados o materializados deben influir en el planteamiento del Plan de Auditoría de una organización. Los cambios en su estructura también deben considerarse, para que la función de auditoría se alinee con las necesidades y expectativas de negocio. Por ello, no es recomendable iniciar la supervisión únicamente cuando los cambios ya se han producido, sino antes, durante y después de que éstos ocurran. Hay diversos cambios que pueden darse en una organización y que es recomendable considerar:

I. **Migraciones:** La adopción de servicios en la nube exige, en muchos casos, la transferencia de información que hasta el momento se localizaba en el dominio de control de la organización, hacia un sistema de almacenamiento fuera de los límites de ésta. Adicionalmente, un cambio de proveedor también puede suponer una migración de datos, así como un cambio en el modelo de despliegue, de una nube privada a una pública, o viceversa. En cualquiera de estos escenarios, la función de auditoría debe asegurar la integridad y disponibilidad de la información durante todo el proceso, así como su confidencialidad. Por ello, es conveniente que se supervise el proceso previo a la migración, así como la migración en sí misma y el proceso de post-migración. En este caso, en lugar de plantear una auditoría centrada en el servicio, o en la infraestructura de TI que da soporte a éste, lo fundamental es revisar la información que va a ser transferida, así como el propio proceso de transferencia y su gestión.

II. **Cambios de proveedor cloud:** Un cambio de proveedor, más allá de la migración de información asociada, requiere una revisión en profundidad que debería producirse al menos desde un punto de vista de gobierno, para evaluar si dicho proveedor cloud posee suficientes medidas para el control y supervisión del servicio adquirido y de la información albergada en sus sistemas, así como para garantizar que no se produce una pérdida de derechos de supervisión sobre el nuevo proveedor con respecto al anterior.

2.3.1.4.3. Evolución de la tecnología.

La tecnología está sujeta a cambios de forma permanente, que se van acelerando con el paso del tiempo. La capacidad de gestionar el cambio, en este caso el tecnológico, es una habilidad fundamental en las organizaciones actuales y futuras que se acentúa con el proceso de transformación digital. La función de aseguramiento llevada a cabo por auditoría interna debe adaptarse a estos cambios, y ayudar a que la organización se mantenga estable en un entorno tecnológico cada vez más cambiante.

I. **Nuevos servicios:** La creación de nuevos modelos de servicios en la nube lleva implícita la aparición, junto con nuevas funcionalidades y ventajas operativas y técnicas, de nuevos riesgos que deben ser tenidos en cuenta. Dichos riesgos variarán en función del tipo de información gestionada, del servicio en sí, y el soporte de éste a los procesos de negocio.

II. **Nuevas tecnologías (protocolos, plataformas, etc.):** La incesante evolución tecnológica, desde la creación de plataformas completamente disruptivas, hasta la actualización de protocolos obsoletos o vulnerables, exige a las organizaciones tomar conciencia del riesgo al que se exponen, evaluándolo de forma periódica. Los servicios en la nube, al estar expuestos en su mayoría a través de Internet, poseen diversos puntos en los que una vulnerabilidad podría ser explotada para acceder a la información de la organización o degradar el servicio. La función de aseguramiento llevada a cabo por el área de Auditoría Interna es doble en este aspecto. Por un lado, permite identificar cualquier riesgo explotable, de forma que la evolución tecnológica lleve siempre asociada la adopción de medidas específicas para tratar los riesgos asociados a ésta. Por otro lado, es fundamental que ayude a detectar cualquier riesgo ya materializado derivado de la adopción de una nueva tecnología, dado que la experiencia común adquirida por el mercado será menor cuanto más reciente sea dicha tecnología. En este sentido, se hace patente la necesidad de que los equipos de auditoría se mantengan al día en cuanto a las evoluciones tecnológicas en entor-

2.3.1.4.4. Uso cambiante de la tecnología cloud en la organización.

Deben considerarse, no solo aquellos cambios tecnológicos u operativos que impacten sobre los servicios cloud contratados, sino también el rumbo estratégico de la organización auditada en relación con el uso de las tecnologías cloud. Aunque no es una tecnología excesivamente reciente, no hay un criterio claro en cuanto a si la adquisición de servicios cloud es recomendable o no. En la mayoría de los casos, depende de la organización y del servicio adquirido. Por ello, existe la posibilidad de que se produzcan cambios estratégicos en ese sentido, y es vital que los

trabajos de auditoría interna les den soporte y sean los suficientemente flexibles para adaptarse a los cambios estratégicos.

2.3.2. Tipologías de auditoría del entorno cloud.

El equipo de auditores internos, especialmente aquellos destinados a ofrecer aseguramiento sobre sistemas de información, debe centrar sus esfuerzos alrededor de los pilares fundamentales sobre los que se sustenta la relación entre la organización y el servicio.

De esta forma, se plantean una serie de tipologías básicas de auditorías que pueden realizarse sobre el servicio en la nube. Se presentan a continuación las más básicas, aunque podrían diseñarse otras a partir de combinaciones y variaciones de éstas.

I. Análisis de procesos de TI o de negocio soportados por el servicio en la nube.
II. Revisión de los procesos internos para la gestión del servicio cloud.
III. Verificación del cumplimiento regulatorio (en función del tipo de datos gestionados, así como de la normativa o regulación sectorial aplicable).
IV. Auditoría de la operación del servicio cloud.
V. Revisión de la gestión de proveedores de TI/cloud.
VI. Análisis del gobierno de TI y de ciberseguridad del servicio cloud.
VII. Revisión de ciberseguridad del servicio cloud (Ej. revisión de Controles Generales de IT -ITGCs- o pentesting).
VIII. Análisis de la gestión de datos en la nube.

2.3.3. Análisis de recursos para la realización de auditorías.

Una vez que se han considerado aquellos elementos que pueden motivar la supervisión de un aspecto específico y se han identificado las tipologías básicas de auditoría, es necesario identificar los recursos de los que se disponen para la realización del trabajo.

2.3.3.1. Cobertura contractual.

2.3.3.1.1 Clausulado.

Las arquitecturas de TI tradicionales, en las que todos los recursos se despliegan in house, ofrecen diversas ventajas de cara a la realización de auditorías, siendo una de las principales la mayor capacidad y autonomía para analizar los recursos y servicios de TI.

A la hora de analizar servicios en la nube, deben considerarse dos alternativas principales. Aquellos servicios cloud que se encuentran controlados en mayor o menor medida por la organización usufructuaria de los mismos (nube privada, nube híbrida, etc.), y aquellos cuya capacidad de control escapa en gran medida de los usuarios del servicio (nube pública).

Mientras que con aquellos servicios cloud bajo el control del cliente, la capacidad de auditarlos no está limitada - al menos en lo relativo a la parte alojada por la propia organización - las compañías proveedoras de servicios cloud suelen imponer restricciones a sus usuarios para supervisar el servicio suministrado o los recursos TI utilizados para dar soporte a dicho servicio.

En este contexto, se vuelve necesario definir de forma explícita los derechos del usuario de servicios cloud en lo relativo a la auditoría del servicio, así como las obligaciones del proveedor a la hora de facilitar información.

Pese a que la negociación de las cláusulas en los contratos con determinados proveedores de cloud suele resultar en ocasiones no tan flexible como convendría al cliente, en general hay varias cláusulas que sería recomendable encontrar en un contrato para lograr una óptima supervisión del servicio cloud y los recursos de TI.

I. Visibilidad del usuario sobre los recursos TI del proveedor: Es recomendable reflejar la necesidad de definir un procedimiento o mecanismo por el que el usuario de los servicios cloud pueda obtener información sobre los recursos utilizados por el proveedor para ofrecerle el servicio cloud. En general, a medida que un servicio cloud ofrece mayor acceso a la infraestructura, la visibilidad sobre ésta será mayor. Así, un servicio SaaS ofrecerá el mayor nivel de opacidad, mientras que un servicio de tipo IaaS incluso permitiría al cliente la instalación de sus propias herramientas de recopilación y supervisión, incrementando la visibilidad y capacidad para auditar de forma independiente al proveedor.

II. Capacidad para supervisar los recursos usados para la provisión del servicio: Además de obtener visibilidad sobre recursos de TI, sería recomendable que el usuario incluyese en el contrato la posibilidad de auditar el servicio suministrado y los recursos TI desplegados para tal fin. Por lo tanto, disponer de una cláusula de derecho de auditoría (right-to-audit) facilitaría mucho el proceso de supervisión. Es importante que se indique sobre qué elementos se podrá realizar la auditoría, entre los que podrían incluirse: registros generados asociados al uso del servicio cloud por parte del proveedor, políticas y procedimientos, facturas, información sobre proveedores subcontratados para la provisión del servicio, recursos hardware / software utilizados para la provisión del servicio así como los registros generados por éstos,

utilizados para la provisión del servicio así como los registros generados por éstos, certificaciones obtenidas por el proveedor relevantes para la auditoría, así como los informes asociados a éstas, etc. Un caso particularmente sensible es el de los servicios multi-tenant (principalmente utilizados en entornos SaaS), donde el proveedor debe dejar claros los límites de auditabilidad, las responsabilidades de los clientes y las consecuencias que el impacto de sus auditorías podría tener sobre los restantes servicios del tenant compartido.

III. Periodo de almacenamiento de logs o registros: El proveedor de servicios cloud generará información o registros a partir de la actividad realizada por el usuario sobre la infraestructura, o por el propio funcionamiento de dicha infraestructura. Además de ponerlos a disposición del usuario en caso de que desee llevar a cabo una auditoría, es importante definir durante cuánto tiempo se compromete el proveedor a conservar esta información. El periodo de retención definido debe tenerse en cuenta a la hora de programar las auditorías, para garantizar que la información que se incorporará como evidencia permanece disponible. La retención de esta información debería garantizarse durante todo el tiempo que dure la relación contractual, y por un periodo pre-definido tras la finalización de ésta.

IV. Disponibilidad de recursos del proveedor para el desarrollo de la auditoría: Además de la información, el usuario podría querer requerir al proveedor cloud su participación en las posibles auditorías que éste lleve a cabo. Para no impactar significativamente en el desarrollo de la actividad normal del proveedor cloud, éste puede limitar el número de auditorías por año o número de horas que dedicará a dar soporte al cliente para la ejecución de auditorías. También existe la posibilidad de que el proveedor incluya una tarificación para este servicio.

V. Tiempos de notificación: Es importante establecer el tiempo máximo disponible para que el proveedor responda a las solicitudes del usuario del servicio, que generalmente variará según el tipo de información solicitada.

VI. Desarrollo del proceso de auditoría: Las reglas que deben seguirse a la hora de ejecutar la auditoría también suelen relejarse a nivel contractual. Es habitual que el proveedor restrinja la dedicación a su horario de oficina, y que requiera que la auditoría en ningún caso impacte sobre su operativa habitual. Asimismo, el cliente puede solicitar el acceso en remoto a la información, para no requerir el desplazamiento a las oficinas del proveedor, así como acceso a sistemas, instalaciones, etc.

VII. Responsabilidad: Para que, tras la finalización del trabajo de auditoría y emisión del informe y conclusiones, ésta sea efectiva, debe incluirse en el clausulado las obligaciones del proveedor en caso de que durante el proceso se identifiquen riesgos que deban ser tratados por éste. La responsabilidad del proveedor puede establecerse de diferentes maneras, bien asociando la identificación de riesgos significativos a la rescisión legítima del contrato, penalizaciones mediante SLAs, etc.

VIII. Extensión del derecho de auditoría: Por último, puede requerirse que el derecho a auditar se extienda, no solo al proveedor de servicios cloud, sino a cualquier tercero que éste contrate para aprovisionar total o parcialmente el servicio.

Aunque los puntos anteriores incluyen los elementos que podrían tratar de negociarse en la firma de un contrato de servicios cloud para garantizar su adecuada supervisión, el número y detalle de dichos elementos podría variar sustancialmente dependiendo del proveedor y de la capacidad negociadora del cliente. A este respecto, un mayor número de cláusulas y de detalle en el contrato, beneficiará generalmente las labores posteriores de supervisión del servicio cloud, pero hay que tener en cuenta que, en caso de que el proveedor acceda a incluir todas o alguna de las cláusulas descritas, esto podría encarecer el precio del servicio y sin duda impactaría en el proceso de selección y adquisición del proveedor.

2.3.3.1.2. Alineamiento con la Política de Seguridad del cliente de cloud.

A pesar de que el elemento más relevante a incluir en un contrato de provisión de servicios en la nube de cara a las tareas de auditoría son las cláusulas de derecho de auditoría, la labor de la auditoría se complica si el servicio prestado no está alineado con la Política de Seguridad de la Información del usuario del servicio.

El principal impacto de dicha falta de alineamiento vendría dado por la complejidad que supondría para el cliente exigir al proveedor la adopción de ciertas medidas para la subsanación de los riesgos identificados.

Un alineamiento del proveedor cloud con la Política de Seguridad del cliente garantiza un entendimiento común en lo relativo a la seguridad de la información, y establece las bases para mejorar la seguridad del servicio cloud cuando así se requiera. Una posible forma de lograr dicho alineamiento sería a través de la adhesión del proveedor a la Política de Seguridad del cliente a través de un anexo al contrato.

2.3.3.2. Aspectos formales.

2.3.3.2.1. Marcos de controles de seguridad aplicables a cloud.

A diferencia de la actividad de análisis forense, que se basa en un procedimiento a seguir, la ejecución de auditorías requiere además una base sobre la que evaluar.

Para ello, se pueden utilizar distintos marcos de control que ofrecen una guía útil sobre la que planificar el trabajo, lo que facilita la adopción de un enfoque estandarizado y riguroso.

A continuación, se exponen algunos de los principales marcos de control de los que se puede seleccionar un conjunto de controles relacionados con seguridad:

Marco de control	Descripción	Nº de controles	Dominios de control
CSA CCM[1]	Orientados desde una perspectiva tanto de proveedor de servicios Cloud como de cliente de los mismos.	98	1. Cumplimiento 2. Gobierno del dato 3. Seguridad en las instalaciones 4. Recursos Humanos 5. Seguridad de la Información 6. Legal 7. Gestión de las Operaciones 8. Gestión de versiones 9. Resiliencia 10. Gestión de Riesgos 11. Arquitectura de seguridad
ISO 27002	Cubre aspectos generales de seguridad de la información, sin hacer hincapié en la seguridad Cloud	113	1. Políticas de seguridad de la información 2. Organización de la seguridad de la información 3. Seguridad relativa a los recursos humanos 4. Gestión de activos 5. Control de acceso 6. Criptografía 7. Seguridad física y del entorno 8. Seguridad de las comunicaciones 10. Adquisición, desarrollo y mantenimiento de sistemas 11. Relación con proveedores 12. Gestión de incidentes de seguridad de la información 13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio 14. Cumplimiento

3 CCM (Cloud Controls Matrix) facilita un marco de controles que proporciona una comprensión detallada de los conceptos y principios de seguridad en cloud, que están alineados con la Guía de la CSA en sus 13 dominios.

ISO 27017	**Adaptación de la ISO 27002 junto con nuevos controles específicos para la Nube**	44	Esta norma proporciona una guía sobre 37 controles basados en la ISO/IEC 27002 que se han adaptado al entorno Cloud, y presenta adicionalmente siete nuevos controles particulares de Cloud, que no están duplicados en la 27002.
NIST SP 800-144	**Mejores prácticas de seguridad y privacidad para servicios en la nube públicos**	N/A	Aunque no ofrece una relación de controles en sí, identifica los aspectos clave a considerar a la hora de gestionar servicios Cloud contratados, por lo que puede servir como base para auditar el gobierno de servicios Cloud de la organización.

2.3.3.2.2. Regulación aplicable.

Si bien los marcos de referencia explicados en el punto anterior se centran fundamentalmente en aspectos de seguridad, pueden existir otros marcos a tener en cuenta de cara a la selección de controles para la auditoría. Entre otros, podría ser necesario considerar la RGPD (o legislaciones locales sobre privacidad, en caso de haberlas), PCI-DSS, ENS, SOX, PSD-2, etc.

De este modo, si se opta por realizar una auditoría de cumplimiento, existe legislación diversa a la que hay que dar cumplimiento, pudiendo variar según la localización geográfica del usuario del servicio, el proveedor, y de los datos.

2.3.3.2.3. Políticas, Estándares y Procedimientos internos aplicables a servicios cloud.

La selección de controles debe asegurar además el análisis de lo dispuesto en las Políticas, Estándares y Procedimientos internos a la organización, cuando éstos sean aplicables al alcance auditado. Para ello existen dos alternativas:

a. Establecer un mapeo entre los controles seleccionados y los requisitos de seguridad definidos por la organización, para comprobar que éstos últimos quedan cubiertos, seleccionando un mayor número de controles en caso contrario.

b. Construir los objetivos de control a partir de los requisitos definidos por la organización en su documentación interna sobre seguridad, seleccionando aquellos controles aplicables dado el alcance seleccionado. En este caso, los controles definidos para satisfacer los requisitos internos pueden complementarse con controles incluidos en alguno de los marcos de control para complementar la auditoría.

2.3.3.2.4. Certificaciones.

Las certificaciones deben considerarse como un elemento más al que el proveedor de servicios cloud puede dar acceso, en caso de que esté en posesión de ellas, para garantizar su cumplimiento con el estándar que promueva cada certificación.

Aunque la posesión de certificaciones puede suplir hasta cierto punto la falta de acceso a información para la realización de auditorías, no pueden sustituir a la ejecución de una auditoría por dos motivos:

a. El alcance de una certificación puede no estar alineado con las necesidades de un cliente concreto, por lo que no puede considerarse como una respuesta incondicional para obtener el aseguramiento.

b. Incluso aunque el alcance de la certificación abarque de forma completa el ámbito requerido por el cliente, generalmente ofrecerá un punto de vista muy general, a partir del cual no suele ser posible revisar aspectos concretos.

De mayor a menor opacidad, se encuentran en un primer nivel aquellos proveedores que únicamente ofrecen acceso al certificado. A partir de esta información, el cliente únicamente podrá comprobar que el proveedor efectivamente está en posesión del certificado, y el alcance que comprende éste. A este nivel, el aseguramiento alcanzado es muy general, y las garantías ofrecidas son bastante limitadas.

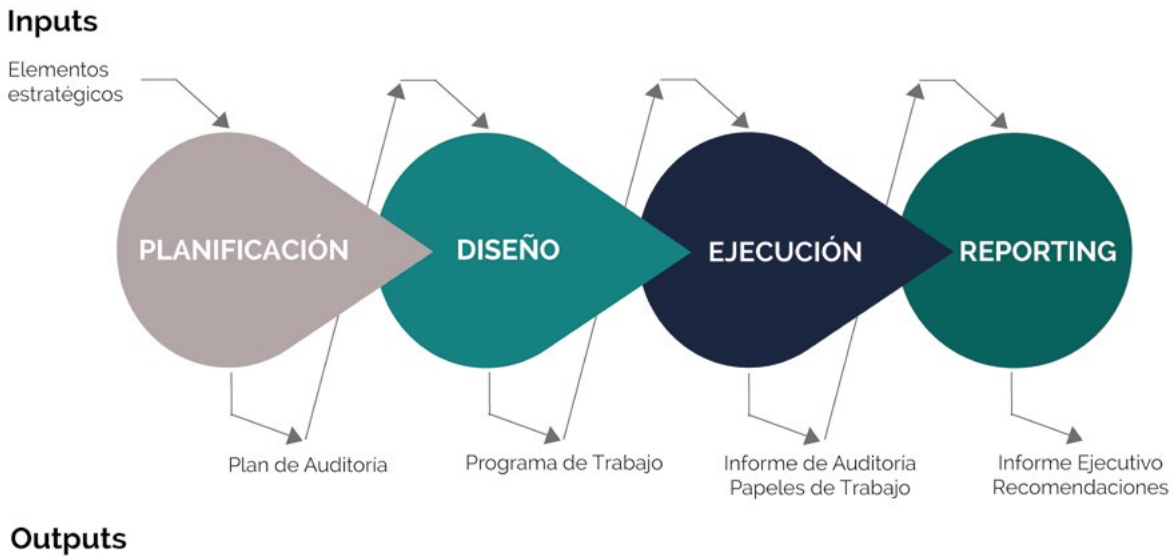
En segundo lugar, el proveedor puede ofrecer también acceso al informe de auditoría elaborado por el auditor independiente para la obtención del certificado. En este caso, además de la información incluida en el certificado, el cliente puede consultar con mayor detalle los aspectos analizados y las conclusiones relevantes del auditor, entre las que se incluyen los incumplimientos identificados. Dependiendo de la certificación, el nivel de detalle del informe podría variar sustancialmente, pero al menos la información anteriormente indicada debe estar incluida.

Por último, además de todo lo anterior, el proveedor podría facilitar la información analizada por el auditor para la obtención de la certificación. Esta opción no suele ser habitual, puesto que esta información tiene un carácter confidencial y el proveedor podría incurrir en un incumplimiento de su propia Política de Seguridad en caso de relevación a terceros. Una alternativa ofrecida por algunos proveedores es la posibilidad de consultar la documentación de forma presencial y supervisada.

En este último caso, aunque el alcance de la revisión queda limitado al de la certificación revisada, el equipo de auditoría del cliente de servicios cloud podrá adquirir un entendimiento suficiente sobre el estado del proveedor con respecto a los elementos cubiertos.

2.4. Fases relevantes de la auditoría de entornos cloud.

La auditoría de servicios cloud deberá seguir los procedimientos y mejores prácticas definidos en las Normas Internacionales de Auditoría Interna. Por ello, las fases no deberían diferir de aquellas utilizadas habitualmente. En este caso, la adaptación al servicio cloud se produce a partir de las consideraciones necesarias que deben tenerse en cada una de las fases.



2.4.1. Definición del Plan de Auditoría.

A partir de todos los aspectos considerados en el punto previo, incluyendo los riesgos a los que está expuesta la organización, los condicionantes a nivel interno y externo a ésta, así como las tipologías habituales de auditoría que se pueden llevar a cabo, debe diseñarse un Plan de Auditoría, que generalmente comprenderá aquellas auditorías a ejecutar durante el siguiente año. En dicho Plan de Auditoría, se deberán incluir auditorías de servicios cloud en función de la estrategia definida por la organización, de forma que éstas se integren con el resto de las auditorías de IT a desarrollar por la organización.

Esta fase no debería sufrir grandes modificaciones para que la auditoría de servicios cloud se integrara en la función de aseguramiento de la organización, más allá de los aspectos particulares que deberán considerarse para determinar qué auditorías cloud es necesario ejecutar.

2.4.2. Diseño de la auditoría.

2.4.2.1. Selección del alcance.

A la hora de seleccionar el alcance que deben cubrir las auditorías de servicios cloud, debe prestarse atención al grado de madurez de la organización en relación con la supervisión de estos servicios. Una buena aproximación consistiría en utilizar una estrategia top-down, que empiece analizando cuestiones de gobierno y cumplimiento, continuando con el análisis de los procesos de TI involucrados en la utilización, gestión y la provisión del servicio, para finalizar con el análisis pormenorizado de un aspecto específico o que cubran una amplia gama de aspectos de índole operativa y técnica.

Esta estrategia a la hora de seleccionar el alcance debe complementarse de forma que los riesgos de mayor criticidad, identificados de forma inicial, queden adecuadamente cubiertos. Una opción para combinar estos dos aspectos consiste en comenzar realizando actuaciones que revisen un mayor número de aspectos de gobierno y cumplimiento, en el que se cubran aspectos operativos y técnicos de forma puntual. A medida que se vaya adquiriendo mayor madurez y los riesgos identificados se vayan tratando, podrán irse espaciando las revisiones que cubran aspectos de alto nivel, aumentando así la cobertura de aspectos puntuales, o de naturaleza más técnica.

No cubrir aspectos relativos al cumplimiento desde un inicio podría suponer que se escape la detección de situaciones por las que la organización podría enfrentarse a sanciones, ocasionando además un impacto reputacional. Asimismo, iniciar la supervisión de servicios cloud sin analizar la gestión que a nivel corporativo se hace de este servicio y de los aspectos relevantes relacionados, podría suponer el tratamiento de riesgos de menor impacto frente a aquellos de tipo estructural, o con mayor un impacto o alcance.

A continuación, se exponen algunos indicadores que deberían motivar una auditoría que evalúe aspectos asociados al servicio en la nube contratado, y ejemplos de cómo podría enfocarse el alcance de las actuaciones destinadas a cubrirlos:

Indicador 1: No existe un programa de Cumplimiento Corporativo (o equivalente) o éste no cubre aspectos relativos a servicios cloud.

Tratamiento: Evaluar si la empresa dispone de procesos capaces de identificar eficientemente la legislación aplicable a la tecnología cloud, y el impacto de dicha tecnología en ésta. Asimismo, es conveniente analizar si el servicio cloud, o el uso de éste, entraña algún tipo de incumplimiento o infracción con respecto a la legislación o regulación aplicable.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. Existencia de políticas y procedimientos escritos en las que se expresen, de forma clara, las expectativas de la organización con respecto al cumplimiento de obligaciones legales que se deriven de la adopción de servicios en la nube, así como los procedimientos concretos requeridos para alcanzar los objetivos de cumplimiento definidos.

II. Definición de una estructura de roles y responsabilidades que permita garantizar el cumplimiento de las obligaciones legales asociadas al uso de la nube. Para ello, debe analizarse tanto la capacidad de cada rol para cumplir con sus responsabilidades, y la formación y sensibilización de dichos roles con respecto al uso de servicios cloud y sus riesgos asociados.

III. Localización geográfica de los datos propiedad de la organización utilizados por el servicio cloud e identificación del tratamiento que el proveedor hará de los mismos.

IV. Identificación de la existencia de datos de carácter personal tratados o almacenados en plataformas cloud, así como de las medidas de seguridad implementadas tanto por el proveedor como por el propio cliente para proteger estos datos.

V. En base a los datos identificados en el punto anterior, consideración de los marcos legislativos aplicables y de regulación o normativa sectorial a fin de definir un programa de trabajo que dé cobertura a las necesidades de cumplimiento específicas de la entidad para el servicio gestionado.

VI. Análisis de la cobertura contractual relativa al cumplimiento de compromisos legales por parte del proveedor y del cliente, como por ejemplo el uso que se hará de los datos o la capacidad para articular una gestión de incidencias conjunta y eficaz.

VII. Existen los medios necesarios para que los distintos miembros de la organización puedan actuar de forma proactiva a la hora de asegurar el cumplimiento de las obligaciones legales adquiridas con la contratación de servicios cloud. Por un lado, debe existir una línea de reporte que cubra a todos los actores involucrados (no solo empleados internos, sino personal del proveedor). Asimismo, deben llevarse a cabo labores de monitorización y revisión de riesgos. Como resultado de estas actividades, debe analizarse si la organización actúa para remediar aquellas situaciones que pudieran poner en riesgo a la organización desde un punto de vista legal.

Indicador 2: Se aprecian deficiencias claras en la gestión de servicios cloud desde una perspectiva corporativa, como la existencia de servicios cloud adquiridos por empleados para el desarrollo de sus funciones sin el conocimiento de la organización (Shadow IT).

Tratamiento: El enfoque abarca una deficiencia corporativa que afecta también a entornos tradicionales, no cloud, por lo que se puede tratar de centrar el análisis en el modelo de gobierno de cloud corporativo, así como en los procesos destinados a garantizar el cumplimiento con dicho modelo de gobierno.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. La definición formal de procesos TI incluye descripciones sobre cómo aprovechar y operar con los servicios cloud adquiridos.

II. Existe una arquitectura de referencia que integra tecnologías en la nube, y existe un plan de adaptación en caso de que dicha arquitectura no se corresponda con la arquitectura corporativa en uso.

III. vEn los procesos de TI definidos, así como en los procedimientos que involucren servicios cloud, se aportan directrices claras sobre cómo maximizar el valor obtenido de dicho servicio y aprovechar sus principales ventajas (ahorro de costes, elasticidad, movilidad, etc.).

IV. Existen procesos para registrar, monitorizar y analizar el desempeño del servicio cloud y la seguridad asociada a éste.

V. Existe un plan de gestión cloud que contempla todas las fases del ciclo de vida del servicio cloud, desde la identificación de necesidades, evaluación de proveedores, adopción, hasta la migración de los datos y la finalización de un servicio en la nube (por cambio de proveedor o cambio de modelo de provisión del servicio).

VI. Existe alineamiento entre la estrategia general de TI y la estrategia de uso de cloud, y estás aportan valor a la estrategia de negocio.

VII. El modelo de gobierno TI tiene en cuenta los principales riesgos asociados al uso de las tecnologías en la nube y define controles que los mitigan hasta un nivel aceptable, considerando el nivel de exposición y riesgo particular de la organización (mediante la realización de un análisis de riesgos que considere los servicios cloud adquiridas y las tecnologías concretas de las que éstos hacen uso).

VIII. El modelo de gobierno cloud se fundamenta en estándares ampliamente aceptados por la industria (ITIL, COBIT, COSO, ISO 27000, etc.).

IX. El gobierno de las tecnologías cloud (de forma aislada o como una particularidad del modelo de gobierno IT), considera el contexto tanto interno como externo de la organización

Indicador 3: Aunque el uso de las tecnologías cloud está extendido entre la organización, no hay una directriz corporativa clara sobre cómo o para qué debería usarse, o simplemente los planes de negocio no se integran con esta tecnología, siendo ésta ampliamente usada.

Tratamiento: Analizar la estrategia de adopción y uso de las tecnologías cloud, para verificar que los objetivos a alcanzar permiten maximizar el soporte a negocio y que el plan para alcanzarlos es adecuado.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. Como parte de la estrategia cloud, se han definido objetivos adecuados, en cuanto a la capacidad de éstos para dar soporte a las necesidades de negocio, como en lo relativo a su seguimiento (objetivos SMART).

II. Se ha hecho una correcta identificación del estado actual de la organización en cuanto a sus recursos tecnológicos, y se ha evaluado la viabilidad de éstos.

III. La estrategia cloud definida se fundamenta en una evaluación de alternativas, en lo relativo a proveedores, modelos de servicio y modelos de despliegue, de forma que se opte por aquellos que mejor se adecúan, tras un análisis formal de los mismos, a los objetivos marcados.

IV. La estrategia cloud se fundamenta en el modelo de gobierno cloud definido y en el entorno regulatorio, de forma que se garantice el cumplimiento con la legislación aplicable y con los requerimientos de gobierno del dato.

V. Se han considerado las expectativas de las partes involucradas, incluyendo a los empleados de la organización, y existe un plan de adaptación / formación específica para cada grupo.

VI. Se ha evaluado el impacto en la gestión y en la operativa de los procesos de TI asociado a la adopción de servicios cloud, y el coste-beneficio de éste se considera aceptable.

VII. Se han tenido en cuenta las características de la tecnología cloud a la hora de decidir qué servicios adoptar y a qué procesos darán soporte éstos, de manera que no se introduzca un riesgo no asumible (ej. Requisitos de disponibilidad, control sobre la localización física de los datos, etc.).

Indicador 4: Existe un aumento de los incidentes de ciberseguridad sufridos que afectan al servicio cloud o que están provocados directa o indirectamente por éste.

Tratamiento: Debe evaluarse la capacidad de respuesta ante incidentes de la organización y comprobar que las tecnologías cloud son consideradas e integradas en las distintas fases del ciclo de vida de gestión de incidentes.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. Los procesos de TI y procedimientos definidos para la gestión de incidentes están adaptados al uso que la organización hace de las tecnologías cloud.

II. El proveedor de servicios cloud da visibilidad sobre los incidentes de seguridad sufridos, especialmente cuando éstos afectan al servicio adquirido por la organización.

III. Tanto durante un incidente, como después de que éste se haya resuelto y como resultado de la investigación posterior, el proveedor de servicios cloud pone a disposición de la organización información suficiente como para poder entender el alcance e impacto del incidente sufrido, y para tomar las medidas oportunas (desde el lado del cliente), para evitar que vuelva a suceder de nuevo.

Indicador 5: Existe cierto desconocimiento sobre el tipo de uso que se está haciendo de los servicios en la nube contratados por la organización, y por tanto se desconoce la importancia de los datos almacenados en la nube o la gestión que se está haciendo de éstos.

Tratamiento: Realizar una evaluación del gobierno del dato en la nube, de forma que se analicen medidas concretas para la gestión y gobierno de los datos en la nube.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. El diccionario de datos corporativo identifica qué datos están alojados en la nube, y cada tipología de dato posee un valor asociado establecido a partir de criterios objetivos.

II. Localización de los datos datos a lo largo de todo su ciclo de vida, desde que éstos se crean, hasta que se destruyen, incluyendo cualquier gestión o copia que se realice de los mismos.

III. El riesgo asociado al almacenamiento y gestión de datos en la nube se ha evaluado utilizando una metodología ampliamente aceptada.

IV. Existe control sobre el acceso a los datos, según su nivel de clasificación, incluyendo perfiles de acceso y medidas de seguridad destinadas a prevenir el acceso no autorizado a los mismos.

V. Las medidas de seguridad implementadas para proteger los datos con un mismo nivel de criticidad, implementadas en el contexto de la organización, así como en el contexto en la nube, garantizan un nivel de protección uniforme, en línea con la criticidad de dichos datos.

VI. Entre las medidas de seguridad definidas para la protección de los datos almacenados o tratados en la nube tienen en cuenta los distintos riesgos asociados al uso de la nube, incluyendo el riesgo de indisponibilidad, pérdida de confidencialidad, etc.

VII. Se controlan las copias de un mismo dato a lo largo de la organización y el servicio cloud, de manera que se no generen redundancias innecesarias o distintas instancias temporales de un mismo dato.

VIII. Se han definido roles para el gobierno y la gestión de los datos, y entre sus responsabilidades definidas se incluyen aspectos específicos para garantizar su adecuada gestión cuando éstos se encuentran en un contexto cloud.

Indicador 6: No existen procesos específicos o éstos no se encuentran bien definidos, destinados a la gestión del servicio en la nube, cuando esta labor recae sobre el cliente de dicho servicio.

Tratamiento: Debe evaluarse la gestión operativa del servicio cloud, lo cual debe consistir en la evaluación de los procesos de TI específicos para la operación del servicio, tanto a nivel de diseño como de aplicación.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. Existen procesos para definir las características básicas del servicio, y dicha definición se realiza de forma sistematizada, incluyendo análisis de requerimientos operativos, planificación de capacidad, definición de configuraciones, etc.

II. Existen procesos de gestión del servicio en la nube, incluyendo:

a. Administración del sistema operativo virtualizado.
b. Administración de la configuración de red.
c. Administración de las capacidades de almacenamiento.
d. Administración de las copias de seguridad.
e. Administración de la configuración de seguridad.

III. Existen procesos de gestión de cambios en la nube, y éstos consideran las capacidades de elasticidad y de escalado particulares del servicio adquirido.

IV. Existen procesos de monitorización y revisión del servicio suministrado, los distintos componentes administrados por el cliente, y la capacidad.

V. Existen procesos de respuesta a incidentes de forma que los operadores puedan identificar, contener, tratar e investigar los incidentes ocurridos sobre el servicio.

Indicador 7: Existe cierto desconocimiento sobre los mecanismos de protección del propio servicio cloud y de los recursos tratados en la nube.

Tratamiento: Evaluar el nivel de ciberseguridad del servicio cloud adquirido, pudiendo adoptar un enfoque desde un punto de gobierno o más técnico.

Ejemplos de aspectos clave a incluir en una revisión de este tipo:

I. En función del modelo de servicio contratado, identificar claramente los roles y responsabilidades internos y externos, y enfocar el análisis de la seguridad, tanto desde el punto de vista del servicio ofrecido por el proveedor, como desde el punto de vista interno en cuanto a las operaciones gestionadas por el propio cliente.

II. Existen procedimientos formalizados que cubren la ciberseguridad en los servicios cloud adquiridos.

III. Existen objetivos de ciberseguridad que contemplan los servicios cloud contratados.

IV. Se ha realizado una evaluación de riesgos considerando las tecnologías cloud, los datos albergados en éstas, y las amenazas particulares de este tipo de tecnologías.

V. En línea con la Política de Seguridad interna, verificar los controles destinados a salvaguardar el servicio y los datos almacenados en la nube o gestionados por éste, incluyendo:

a. Controles para prevenir divulgación no autorizada de información.
b. Prevención de pérdidas de información (desde un punto de vista de la disponibilidad).
c. Gestión de identidades y control de acceso.
d. Generación y gestión segura de credenciales de acceso.
e. Seguridad de la red y las interfaces de comunicación utilizadas.
f. Vulnerabilidades técnicas asociadas al software utilizado para desplegar el servicio cloud.
g. Control del proveedor de servicios cloud.
h. Prevención de uso no autorizado del servicio
i. Monitorización y revisión del servicio y la actividad de los usuarios en éste (incluyendo administradores).
j. Continuidad del servicio (a nivel técnico y por vendor lock-in).

2.4.2.2. Selección de los controles del Programa de Trabajo.

Como en cualquier otro tipo de auditoría, la selección de controles a analizar se basará principalmente en un marco de control ampliamente aceptado por la industria que garantice una base de trabajo probada y fiable.

No obstante, no existe un único marco de control del que puedan obtenerse todos los controles para auditar servicios en la nube, dado que como ya se ha indicado, su elección dependerá del alcance y objetivos de la auditoría, así como de los siguientes factores:

2.4.2.2.1. Modelo de servicio y tipo de despliegue.

Aunque la tecnología utilizada para desplegar servicios en la nube no tiene por qué variar independientemente de si se adquiere el servicio mediante contratación de un proveedor (cloud pública) o a través del despliegue in-house (cloud privada), los controles utilizados para auditar deben tener esto en cuenta porque existirán particularidades asociadas a la gestión del servicio.

Un servicio de cloud público puede auditarse seleccionando por ejemplo un marco de control específico para servicios en la nube (ej. CCM), dado que el modelo de despliegue estará fuertemente influenciado por las características de esta tecnología (elasticidad, control parcial sobre la infraestructura, despliegue de datos en una infraestructura contratada, etc).

Si la nube a auditar es de tipo privado, igualmente podría utilizarse la CCM como base, o bien un marco de control más generalista y complementarlo con ciertos aspectos cloud puntuales (ej. Controles relativos a la capa del hipervisor).

2.4.2.2.2. Objetivo de la auditoría.

Si el enfoque de nuestra auditoría está orientado hacia la seguridad, marcos de referencia como la ISO 27017 o NIST SP 800-144 (véase el apartado 2.3.3.2), pueden ser buenos puntos de partida. De igual modo, pueden definirse matrices de controles alineados con la Política de Seguridad corporativa.

En caso de ser necesario un cumplimiento con certificaciones o regulaciones específicas (PCI-DSS, PSD-2, ENS, SOX, o incluso controles generales de TI), los objetivos de control aplicables al entorno cloud deberán asimismo tenerse en cuenta. Cabe destacar que la CSA ha desarrollado un mapeo de la CCM (Cloud Controls Matrix) con la mayoría de estos estándares y normativas, por lo que se podría utilizar como base muy útil para identificar de un vistazo cuáles son los controles que podemos aprovechar de la CCM y cuales no quedan cubiertos.

2.4.2.2.3. Entidad auditada.

Dependiendo de si la auditoría va a centrarse sobre el proveedor, sobre la propia organización, o sobre ambos, el conjunto de controles TI a revisar puede verse afectado.

A la hora de auditar la provisión del servicio cloud, lo que centraría la actuación sobre el proveedor, los controles seleccionados deben cubrir el control que la organización establece sobre dicho proveedor, y los procesos de gestión y supervisión tanto del propio proveedor como del servicio. Otro aspecto clave que debería cubrirse con la selección de controles para evaluar el proveedor, es el cumplimiento de éste con las obligaciones legales y contractuales.

Sin embargo, al auditar la organización, los controles seleccionados pueden ser de tipologías más diversas. Pueden seleccionarse controles generales de TI para aquellos aspectos específicos que estén bajo el control de la organización. Asimismo, pueden seleccionarse controles que evalúen aspectos de alto nivel, como el alineamiento con las necesidades de negocio, el gobierno, etc. Aunque el alcance en el caso de auditar la organización aumenta, los controles deben volverse más generalistas, dado que la evaluación no solo debería centrarse en el servicio, sino en todos los aspectos sobre el que éste impacta.

En caso de que la auditoría posea un enfoque más amplio y se audite tanto el servicio provisto como el uso de la organización del mismo, bastará con optar por un enfoque combinado.

2.4.2.2.4. Nivel de madurez.

Como punto de partida, el equipo de auditoría debe extraer los controles a utilizar para la evaluación del servicio cloud a partir de aquellos requerimientos a los que la organización se vea obligada por su actividad, el uso que haga del servicio, o la información que se almacene en la nube. Así, una selección básica de controles debería permitir evaluar el cumplimiento con requerimientos legales y regulatorios.

En un segundo nivel de madurez, un marco de control ofrece un buen punto de partida para la ampliación de la selección de controles que se revisarán durante una auditoría. Un marco de controles TI reducirá el foco sobre el análisis del cumplimiento regulatorio y profundizará en aspectos TI más específicos, como el gobierno TI o la protección de los recursos de TI.

No obstante, a medida que la organización va adquiriendo madurez en la gestión y evaluación del servicio cloud, la utilización de un marco de control puede no ser suficiente, dado que éstos no están adaptados a las necesidades particulares de cada organización. En el tercer nivel de

madurez, los controles procedentes de marcos de control deben complementarse con controles específicamente diseñados para evaluar el cumplimiento con los requisitos definidos por la organización, bien sea a nivel contractual, o en su cuerpo normativo de ciberseguridad y gobierno de TI.

2.4.2.2.5. Capacidad de supervisión sobre el proveedor.

Aquellas auditorías centradas en el proveedor de servicios cloud deben considerar la capacidad para obtener información de éste, así como las obligaciones de éste para con la organización.

Aunque este hecho no determinará qué marco de control concreto utilizar, podrá reducir los controles que es viable evaluar. En este sentido, será lo estipulado en el contrato de provisión del servicio lo que determinará los dominios de control que podrán evaluarse. Las posibilidades son muy variadas, desde una visibilidad casi nula, no pudiendo siquiera evaluar el cumplimiento del proveedor con sus obligaciones legales, a la evaluación de controles de TI sobre la infraestructura subyacente al servicio cloud. En última instancia, cabrá la posibilidad de evaluar las certificaciones e informes de auditoría que el proveedor estime oportuno facilitarnos.

2.4.3. Ejecución del trabajo de campo.

2.4.3.1. Recopilación de evidencias.

La capacidad de opinar por parte del equipo de auditoría, una vez seleccionado el alcance a cubrir, se verá afectada en gran medida por las evidencias obtenidas y la información que se pueda extraer de las mismas.

Hay diversos factores que afectan a la cantidad y detalle de las evidencias que podrán obtenerse durante la ejecución de una auditoría.

I. Como ya se ha tratado anteriormente a lo largo de este documento, las cláusulas incluidas en el contrato afectarán enormemente al desarrollo de la auditoría. Puede acordarse con el proveedor el envío de informes del servicio, reportes de incidencias, informes de auditoría llevados a cabo por el proveedor, etc.

II. El modelo de servicio también es un factor clave a la hora de obtener evidencias. En un modelo SaaS, las evidencias accesibles por la organización son esencialmente internas, relativas a aquellos aspectos observables por la misma, sin que llegue a obtenerse demasiada información sobre la infraestructura que soporta el servicio, pero sí sobre el acceso a ésta. Sin embargo, un modelo IaaS, permitirá la obtención de evidencias más ricas sobre dicha infraestructura y su funcionamiento.

III. El modelo de despliegue es otro factor determinante. Una nube privada desplegada por la propia organización ofrece un acceso mucho mayor a evidencias que un despliegue público.

IV. A medida que la madurez de la organización en relación con el uso de servicios cloud aumenta, así como el gobierno cloud mejora, habrá una mayor cantidad de evidencias disponibles como fruto del control que la organización ejerce sobre el servicio.

Una vez considerados estos factores, es importante que la organización evalúe la cantidad y tipología de evidencias disponibles para analizar durante la actuación. En la medida en la que el número de evidencias aumente, y éstas contengan información más relevante o detallada, la organización podrá realizar auditorías de tipo más técnico.

Asimismo, debe evaluarse, dependiendo de cómo se haya obtenido cada evidencia, el nivel de fiabilidad de ésta. Aunque una evidencia no se haya manipulado de manera malintencionada, sigue existiendo la posibilidad de que ésta no sea relevante o que el proceso de obtención no haya sido apropiado.

En caso de que la organización no tenga a su disposición evidencias suficientemente robustas, deberá tratar de obtener evidencias complementarias, y limitar su análisis y conclusiones para que éstas no se vean comprometidas a posteriori.

Es importante que la organización lleve a cabo auditorías en las que exista un alineamiento entre el alcance y las evidencias a su disposición. De otro modo, las conclusiones obtenidas corren el riesgo de no ofrecer una visión precisa, lo que reducirá el aseguramiento provisto a la organización.

2.4.3.2. Análisis de las evidencias y obtención de conclusiones preliminares.

Estas actividades se realizarán como parte del proceso de auditoría de servicios cloud de la misma manera que para cualquier otro tipo de auditoria de TI, y siempre de conformidad con lo estipulado en las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna.

2.4.4. Reporting y seguimiento.

Como en cualquier otra auditoría, el trabajo de auditoría y las conclusiones obtenidas en el proceso, culminarán con la elaboración de un informe de auditoría.

Llegados a este punto, este tipo de auditorías poseen ciertas particularidades que deben tenerse en cuenta.

2.4.4.1. A quién reportar.

Idealmente, además de compartirse las conclusiones con las áreas de la organización afectadas, así como con los roles clave (miembros de la Dirección, Comité de Auditoría, etc.), es conveniente informar al propio proveedor de las conclusiones alcanzadas cuando se haya identificado algún riesgo relevante.

El reporting al proveedor puede llevarse a cabo de distintas maneras, que dependerán, una vez más, de lo acordado contractualmente. Existe la posibilidad de elaborar un informe ad hoc que solo contenga las conclusiones que afecten al proveedor, de forma que no se le comuniquen aspectos internos a la organización.

En caso de que no exista tal posibilidad, es posible tratar los riesgos materializados identificados durante la auditoría en las sesiones conjuntas de gestión de incidencias, en caso de que exista esta herramienta conjunta de gestión de riesgos.

2.4.4.2. Qué reportar.

Es fundamental que la comunicación se realice de forma discrecional. A nivel interno, deben comunicarse de forma completa las conclusiones obtenidas durante la auditoría, especialmente a las áreas auditadas y a los miembros clave de la organización. El reporte debe permitir entender de forma clara el riesgo identificado y permitir su tratamiento por parte de las áreas, a través de planes de acción concretos, accionables y acordados. Asimismo, debe dar un suficiente nivel de aseguramiento y permitir la toma de decisiones con un conocimiento preciso sobre el estado de la organización a los miembros de la Dirección y del Comité.

Por otro lado, únicamente se debe informar al proveedor cloud de aquellos aspectos que le afecten directamente. Asimismo, deberían resaltarse los riesgos más relevantes.

Las oportunidades de mejora y recomendaciones menores, que tengan impacto sobre aspectos formales, pero sin mayor incidencia a nivel operativo o técnico, pueden exponerse únicamente a nivel interno, dado que será más difícil defenderlas de cara al proveedor, y podría desviar el foco de aquellos aspectos de mayor relevancia.

2.4.4.3. Canales de reporting.

A nivel interno, el reporting debe realizarse mediante la emisión del informe de auditoría y la comunicación de éste a los roles clave involucrados en la auditoría.

A nivel externo, existen diversas opciones ya identificadas en puntos previos, entre los que se incluyen, de más a menos conveniencia:

I. Distribución de la versión adaptada al proveedor cloud del informe de auditoría.
II. Reporte de los riesgos detectados por los canales definidos por el proveedor para tal fin.
III. Tratamiento de los riesgos materializados detectados como una incidencia.
IV. Renegociación de las cláusulas del contrato para cubrir los riesgos detectados.

2.4.4.4. Seguimiento continuo.

A fin de alcanzar un modelo maduro de mejora continua, todos los riesgos identificados como parte del proceso de auditoría deben ser tratados.

Internamente, las recomendaciones emitidas deben tratarse como en cualquier otro tipo de auditoría. Mientras tanto, externamente no suele existir una obligación por parte del proveedor en relación con el tratamiento de los riesgos identificados, aunque esto puede estipularse contractualmente. Conviene diferenciar aquellos aspectos que deben ser tratados pero que aún no han provocado un impacto, de aquellos que sí, siendo más frecuente que los proveedores definan canales de comunicación y gestión (conjunta o unilateral) de las incidencias sufridas.

El tipo de tratamiento y nivel de compromiso del proveedor con los riesgos identificados puede variar enormemente. En última instancia, en caso de que el proveedor no ofrezca ningún mecanismo de gestión para la resolución de los riesgos identificados, el tratamiento deberá realizarse enteramente por el cliente mediante la renegociación del contrato o con el cambio de proveedor, si así lo estima conveniente en base al balance coste-beneficio frente a los riesgos.

ANÁLISIS FORENSE DE SERVICIOS EN LA NUBE

3

3.1. Introducción.

Como la segunda de las actividades de supervisión, se encuentra el análisis forense. A diferencia de la ejecución de auditorías, que debe realizarse de forma continua como medio para identificar y tratar riesgos, el análisis forense es una actividad que se orienta más hacia la investigación de un incidente. En ambos casos, existe un componente muy relevante de remediación de los riesgos detectados.

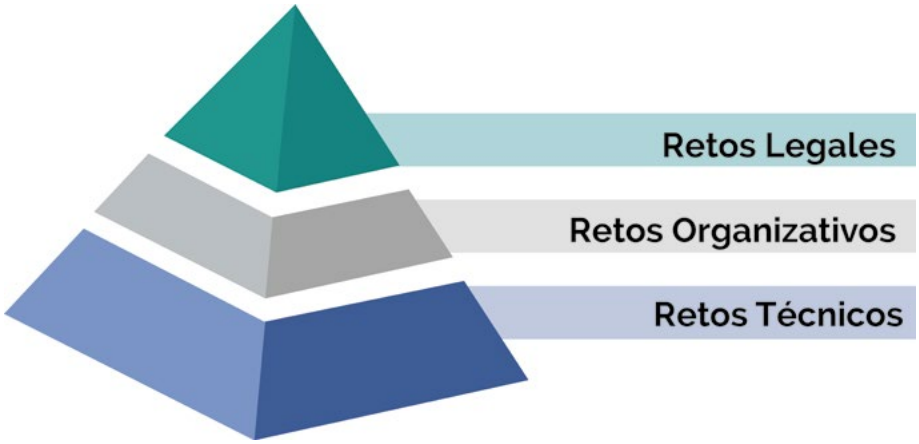
Las actividades de análisis forense están fuertemente procedimentadas, y existe un gran volumen de documentación que cubre todas las fases del proceso. Esto se debe principalmente a que, fruto de una investigación, existe la posibilidad de que se tomen acciones legales. Por ello, para que cualquier proceso posterior que se inicie como resultado de la ejecución de análisis forense no se vea invalidado, es imprescindible desarrollar esta actividad con las máximas garantías, contando en todo momento con el soporte legal oportuno, y de forma que la evidencia y el posterior análisis no se vean comprometidos.

En las siguientes secciones se aporta mayor nivel de detalle sobre la estrategia y las consideraciones particulares que es necesario tener en cuenta en cada una de las fases que se ven modificadas al tratar con entornos en la nube. Es por esto que no se incluye una explicación pormenorizada de todas las fases necesarias para el desarrollo de un análisis forense, sino de aquellas que se ven afectadas por las características y requerimientos de los entornos en la nube.

Antes de profundizar más en esta actividad, es importante destacar que lo expuesto a continuación hace referencia a entornos de nube pública o híbrida. En el caso de los despliegues de nube privada, dado la realización de un análisis forense será en gran medida similar a como se llevaría a cabo en un entorno tradicional. Únicamente sería necesario considerar las necesidades especiales para la adquisición de evidencias impuesta por la existencia de una capa de virtualización.

3.2. Retos del análisis forense en cloud.

A diferencia de la auditoría en la nube, que posee un mayor margen de adaptación según las condiciones y características del entorno en la nube a auditar, los procesos de análisis forense son muy dependientes de los datos, y requieren un tratamiento muy específico de los mismos.



Aunque las fases del análisis forense en la nube sean muy similares sobre el papel al análisis tradicional, en la práctica existen una serie de condicionantes que es importante conocer y gestionar, de forma que aparecen una serie de retos a nivel legal, organizativo y técnico. A continuación, se identifican los principales retos dentro de cada tipología:

3.2.1. Retos Legales.

3.2.1.1. Requerimientos legales asociados a la obtención de evidencias.

La fácil movilidad y dispersión de los datos almacenados en la nube complica la adquisición de las evidencias, debido a que existe diversa legislación aplicable, pudiendo llegar a producirse un cambio de jurisdicción entre el cliente de servicios en la nube, el proveedor de servicios, e incluso el CPD en el que se almacenan los datos.

3.2.1.2. Falta de cooperación del CSP.

Por lo general, cualquier aspecto que no esté apropiadamente regulado a nivel contractual, no podrá ser reclamado al proveedor. Esto incluye cualquier participación del mismo en la preparación del entorno o en la provisión de evidencias forenses. En el caso de proveedores de bulletproof servers, que ponen pocas o ninguna restricción al tipo de información a cargar en la nube, la falta de cooperación puede ser incluso mayor.

3.2.1.3. Mantenimiento de la cadena de custodia.

El mantenimiento de la cadena de custodia se complica cuando los recursos están en la nube, dado que aumenta el número de actores que intervienen en su adquisición y preservación, y existen por tanto más puntos en los que la evidencia forense puede verse comprometida en caso de no adoptar las medidas oportunas.

3.2.2. Retos Organizativos.

3.2.2.1. Falta de gobierno de datos.

No establecer responsabilidades claras sobre la propiedad de los datos dentro de la organización es un riesgo para la organización. Sin embargo, cuando estos datos están localizados en la nube el riesgo es aún mayor, puesto que se aumenta la dificultad para identificarlos y localizarlos.

3.2.2.2. Falta de procedimientos.

Como ya se ha comentado, la realización de análisis forense es una actividad que debe seguir procedimientos rigurosos, claramente definidos y basados en estándares. En el caso de la nube, los riesgos del proceso son aún mayores, debido entre otros factores a la deslocalización de los datos, la volatilidad del entorno, y la mayor dificultad para establecer una cadena de custodia. Sin embargo, no se cuentan con procedimientos específicos para el análisis forense en cloud.

3.2.2.3. Falta de aspectos forenses en el contrato y los SLAs.

Es muy poco frecuente que el proveedor de servicios en la nube incluya cláusulas o SLAs a nivel contractual en relación con su participación en actividades de análisis forense llevadas a cabo por el cliente cuando éstas involucren al servicio contratado. Sin embargo, en la mayoría de los casos la colaboración del CSP es vital a lo largo del proceso de adquisición de evidencias.

3.2.2.4. Cadena de trabajo extendida.

En un proceso forense tradicional, existen distintos perfiles dentro de la organización que deben colaborar a lo largo del proceso. En el caso del análisis forense en cloud, estos perfiles no siempre pertenecen a la misma organización, provocando que la colaboración entre ellos se vuelva más difícil.

3.2.3. Retos Técnicos.

3.2.3.1. Problemas en la identificación de las evidencias.

En muchos casos el inicio del proceso de análisis forense se ve complicado por la dificultad de identificar qué evidencias deben ser adquiridas, con retos como la localización distribuida y la volatilidad introducida por los sistemas de virtualización, que dificultan la localización física, e incluso lógica, dentro de la infraestructura del proveedor de servicios en la nube.

3.2.3.2. Arquitecturas en la nube.

Dependiendo del modelo de despliegue utilizado, el acceso y adquisición de información se complica. A medida que aumenta el nivel de abstracción, siendo el más bajo el de los servicios IaaS, y el más alto el de los SaaS, las capacidades del usuario del servicio para interactuar con la infraestructura se reducen, incrementándose así las dificultades para el desarrollo de las primeras etapas del análisis forense.

3.2.3.3. Uso de tecnologías serverless.

El uso de servicios cloud de tipo serverless, en los que el usuario carga el código en la nube y la infraestructura se adapta de forma totalmente dinámica a las necesidades de éste, introduce uno de los niveles más altos de abstracción en la nube. Aunque estos servicios ofrecen grandes ventajas a los usuarios, dificultan en gran medida la localización y extracción de la información que se utilizará como evidencia forense.

3.2.3.4. Volatilidad de los datos.

Como ya se ha comentado anteriormente, la volatilidad de la información complica la obtención de evidencias forenses. En un entorno en el que la información se almacena en discos virtualizados, las posibilidades de que un dato se pierda permanentemente son mayores que en los sistemas de almacenamiento físico.

3.2.3.5. Múltiples formatos de logs y plataformas.

A la hora de recopilar y centralizar la información para su posterior análisis, ya sea como parte de un proceso de monitorización o de análisis forense, uno de los mayores retos es la diversidad de formatos y plataformas en los que los logs se generan. Por la variedad de despliegues y servicios ofrecidos en la nube, este reto se vuelve aún mayor cuando el análisis forense involucra servicios en la nube.

3.2.3.6. Validación de las evidencias adquiridas.

A lo largo de todo el proceso de adquisición y tratamiento de evidencias forenses, dos de los requisitos más importantes son mantener la cadena de custodia, y llevar a cabo un tratamiento que evite que la evidencia se corrompa. Por las características de los entornos en la nube, así como por la falta de adaptación de las herramientas forenses a éstos, este proceso no siempre es posible, lo que implica que en ocasiones no sea posible adquirir una evidencia determinada sin que el propio proceso la corrompa, como por ejemplo al capturar imágenes de memoria de una máquina en la nube.

3.2.3.7. Herramientas insuficientes.

Como se deduce del punto anterior, el hecho de que las herramientas forenses no estén diseñadas para trabajar en la nube genera algunas dificultades añadidas durante el proceso, de forma que las vuelve en algunos casos inservibles, haciendo que en otros el proceso sea mucho más complejo.

3.2.3.8. Recuperación de datos borrados.

En muchos análisis forenses la recuperación de datos borrados de los soportes es clave. En los entornos en la nube los datos tienen una alta movilidad y volatilidad, lo que complica sobremanera la recuperación de estos datos.

3.2.3.9. Grandes cantidades de datos implicados.

Por la capacidad de los entornos cloud de escalar dinámicamente para adaptarse a los requerimientos del servicio, es posible encontrar despliegues de gran tamaño con decenas de servidores y cantidades ingentes de información, lo que complica tanto la adquisición de las evidencias forenses como el análisis posterior.

3.2.3.10. Velocidades de transferencia lentas.

Aún con la disponibilidad actual de conexiones de alta velocidad, los volúmenes de información a transferir en un análisis forense en cloud son tan altos que pueden ralentizar de forma significativa su adquisición, incrementando los tiempos de ejecución del análisis forense.

3.2.3.11. Sincronización temporal de fuentes de información.

Cuando una investigación requiere de una correlación entre distintas fuentes de información (o entre distintos proveedores de servicios en la nube), un requerimiento fundamental es que pueda establecerse una secuencia temporal de eventos. Sin embargo, dado que las máquinas no están controladas por la misma organización, las probabilidades de que los tiempos de todas las máquinas involucradas estén correctamente sincronizados es menor.

3.2.3.12. Falta de conocimiento especializado.

Por la relativamente reciente adopción de las tecnologías cloud en el mundo empresarial, existe una falta generalizada de técnicos con conocimientos de análisis forense especializado en entornos en la nube.

3.3. Estrategias de Análisis Forense en Cloud.

Contar con una estrategia de análisis forense adecuada es fundamental para asegurar la disponibilidad de los recursos y capacidades necesarios para, una vez ocurrido el incidente, conseguir identificar las causas, el alcance y el impacto real causado por el mismo. Esto requiere contar con medios humanos, técnicos y organizativos que permitan desarrollar las actividades de análisis forense de manera eficiente y precisa.

Disponer de los recursos necesario permitirá realizar los trabajos de análisis forense con la debida diligencia, de forma que se satisfagan las expectativas y necesidades de las partes interesadas de la organización, y se dé cumplimiento a todos los requerimientos legales aplicables, encabezados por el RGPD y la directiva NIS.

Las fases del análisis forense siguen siendo las mismas que en el análisis tradicional. Sin embargo, las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos) imponen una serie de requerimientos que obligan adaptar las actividades realizadas, especialmente durante las primeras fases del proceso.

Estos requerimientos específicos a los entornos cloud y la relación con los proveedores asociados impactarán más significativamente sobre las fases previas al análisis forense, en las que la interacción con el entorno a analizar es mayor. Por último, las fases de reporting y posteriores también podrán verse afectadas, en este caso a causa de la relación entre el cliente de los servicios en la nube y el proveedor.

3.3.1. Requerimientos mínimos para el análisis forense en cloud.

Una adecuada estrategia de análisis forense, y por extensión una que involucre servicios cloud, se basa en los siguientes aspectos fundamentales:

3.3.1.1. Planificación.

Los medios materiales y los procedimientos deben estar correctamente definidos para agilizar todo el proceso de análisis forense. Dichos procedimientos, así como los recursos previstos en éstos, deben contemplar de forma específica la ejecución de las actividades descritas en entornos en la nube.

3.3.1.2. Conocimiento del entorno.

Tanto en la fase de adquisición como en la de análisis, tener conocimiento de cómo está desplegado y configurado el entorno (red, sistemas, seguridad, aplicaciones, etc.) ayuda enormemente a la realización del análisis forense. Por las características especiales de los entornos en la nube, es importante que el equipo encargado del análisis disponga formación específica que le permita entender el funcionamiento y características de éstos.

3.3.1.3. Cumplimiento legal.

El análisis forense está fuertemente ligado a procedimientos legales. La observación y cumplimiento escrupuloso de dichos procedimientos. Si bien no hay una variación sustancial a la hora de determinar la legislación aplicable a la actividad forense en cloud, hay que considerar que en estos entornos hay un mayor número de actores involucrados, por lo que es necesario prever las implicaciones y obligaciones legales de cada uno de ellos.

3.3.1.4. Rigurosidad.

Un buen análisis forense debe realizarse de forma metódica y sistemática, teniendo en cuenta todas las posibilidades y aceptándolas o descartándolas en función de las evidencias que se van encontrando a lo largo del análisis. A causa de las dificultades durante las fases de adquisición y preservación de las evidencias, extraer conclusiones válidas a partir de éstas requiere un esfuerzo mayor.

3.3.1.5. Eficiencia.

En muchos casos un análisis forense está limitado por los recursos, tanto de personal como de tiempo. Adaptar los recursos disponibles para satisfacer los objetivos es fundamental. Esto es aún más importante cuando los recursos no siempre son internos a la organización, debido a la involucración del proveedor cloud.

3.3.2. Dimensiones del análisis forense en cloud.

A la hora de articular adecuadamente una correcta estrategia de análisis forense, deben tenerse en cuenta tres dimensiones fundamentales:

3.3.2.1. Dimensión Regulatoria.

Desde un punto de vista legal, hay que tener en consideración diversos aspectos relacionados tanto con el proveedor como con el cliente.

Por un lado, es necesario identificar toda la legislación relevante a la que deba darse cumplimiento durante la ejecución del análisis forense, empezando por aquella aplicable al cliente de servicios cloud, pero también analizando cualquier aspecto relevante sobre el proveedor.

Además, es necesario considerar los acuerdos y SLAs incluidos en el contrato entre proveedor y cliente. La inclusión de determinadas cláusulas o penalizaciones influirá significativamente en la estrategia de análisis forense, afectando a elementos fundamentales como el tipo de información que se podrá recopilar, la colaboración del proveedor a la hora de investigar un incidente, etc.

Por último, existen determinados aspectos derivados de las características de los servicios en la nube, como la existencia de entornos multi-cliente o la distribución de los datos, que deben considerarse a la hora de definir una estrategia de análisis forense en cloud.

3.3.2.2. Dimensión Organizativa.

A nivel organizativo, la estrategia de análisis forense debe centrarse en garantizar la disponibilidad de recursos a lo largo del proceso.

Los recursos no solo se limitan a aquellos de tipo económico. También es necesario definir estructuras de roles y responsabilidades, así como aquellos procedimientos necesarios para garantizar la correcta ejecución de los análisis.

Como en cualquier otro proceso interno a la organización, esto requiere la involucración de la dirección y de los órganos de gestión afectados por el proceso.

Para lograr un correcto alineamiento, así como un adecuado soporte de la actividad, la estrategia debe partir de la concienciación a las partes interesadas clave, de forma que éstas dispongan de la información suficiente como para permitir la adecuada toma de decisiones en materia de análisis forense en cloud.

Otro de los objetivos más relevantes de la estrategia de análisis forense a nivel organizativo, además de garantizar los medios necesarios para su realización, consiste en lograr que la comunicación entre proveedor y cliente sea lo más fluida posible y no dificulte la realización del análisis forense.

3.3.2.3. Dimensión Técnica.

Desde un punto de vista técnico, hay tres características del servicio en la nube que influyen significativamente a la hora de definir la estrategia.

3.3.2.3.1. Modelos de servicio.

Dependiendo de su el servicio es de tipo IaaS, PaaS o SaaS, habrá enormes variaciones en la capacidad para modificar configuraciones, desplegar herramientas u obtener evidencias. Para que la estrategia sea realista y permita cubrir los objetivos definidos, deberán tenerse en cuenta estos aspectos y las limitaciones impuestas por ellos.

3.3.2.3.2. Modelos de despliegue.

Este punto es crítico a la hora de definir la estrategia. En caso de que el despliegue sea de tipo nube privada, podrá optarse por un enfoque mucho más tradicional, dado que el proceso solo deberá adaptarse a la nube para considerar la capa de virtualización utilizada. En cambio, si el despliegue es público o híbrido, habrá que considerar otro gran número de factores, como la interconexión entre el proveedor y el cliente, la información accesible por el cliente, y otras características inherentes de la nube como la existencia de entornos multi-cliente.

3.3.2.3.3. Características técnicas del entorno.

La tecnología utilizada tanto para ofrecer el servicio (infraestructura virtualizada), como para soportarlo (capa del hipervisor e inferiores), pueden introducir modificaciones en la estrategia. Entre los aspectos técnicos a considerar para la elaboración de la estrategia se encuentran el sistema

operativo instalado, la solución de virtualización utilizada, los métodos de acceso al entorno por parte del cliente o las tecnologías de almacenamiento. A este respecto, no solo hay que tener en cuenta la solución tecnológica utilizada, sino también la versión desplegada.

3.3.3. Objetivos del análisis forense en cloud.

La estrategia, a partir de las dimensiones en las que se articula, debe permitir satisfacer los objetivos definidos por la organización en materia de análisis forense. Aunque los objetivos deben adaptarse a cada organización, así como al uso de los servicios en la nube que ésta haga y las características del mismo, existe una serie de objetivos mínimos que deberían tenerse en cuenta durante la definición de la estrategia:

#	Dimensión	Objetivo
1	**Regulatoria**	Dar cumplimiento a todos los requerimientos legales relativos al servicio en la Nube y a la realización de análisis forenses.
2	**Regulatoria**	Adaptar el análisis realizado de forma que no se vea limitado su resultado o conclusiones como consecuencia de la relación entre el proveedor de servicios Cloud y el cliente.
3	**Organizativa**	Concienciar a la organización en lo relativo a la importancia de análisis forense en Cloud, lo que se traduce en una adecuada asignación de recursos.
4	**Organizativa**	Lograr alineamiento entre las expectativas de la organización en lo relativo al proceso de análisis forense y los recursos asignados para su desarrollo.
5	**Organizativa**	Permitir, una vez concluido el análisis forense, que puedan tomarse las decisiones oportunas para tratar los aspectos identificados durante el mismo.
6	**Técnica**	Preparar el entorno Cloud antes de la ocurrencia de un evento que requiera una investigación forense, de forma que pueda obtenerse información relevante y útil durante el proceso.
7	**Técnica**	Garantizar la adecuación de los procesos y herramientos utilizados para el análisis forense son adecuados para la extracción, preservación y análisis de información relevante, válida, precisa y útil de los entornos en la Nube, considerando las tecnologías utilizadas en ellos.
8	**Técnica**	Diseñar el proceso de análisis forense de forma que absorba la complejidad introducida por la distribución de las evidencias en diversos entornos y tecnologías, y en general todas aquellas particularidades del entorno en la Nube analizado.
9	**Técnica**	Realizar la adquisición y análisis de evidencias de forma que éstas no queden invalidadas a causa del uso de entornos virtualizados para la provisión de servicios en la nube.

3.4. Fases relevantes del Análisis forense en cloud.

Con respecto a la ejecución de un análisis forense en cloud, hay fases que cobran una importancia mucho mayor frente a su realización sobre un entorno tradicional, como la de preparación; mientras que otras que se vuelven más complejas, como la de reporting.

Adicionalmente, durante la ejecución del trabajo, se vuelve necesario adoptar técnicas y herramientas específicas para poder ejecutar el resto de las fases de forma correcta.

3.4.1. Preparación del entorno.

Cuando un analista forense debe acceder a un sistema para su análisis, una de las primeras actividades a ejecutar consiste en tratar de conservar el sistema inalterado mediante técnicas de aislamiento, para que las evidencias no se volatilicen. Esto se consigue obteniendo copias inalteradas de la información del sistema, mediante el uso de herramientas de análisis forense.

En los entornos en la nube, la capacidad para instalar o hacer uso de software de terceros, se reduce considerablemente, así como los mecanismos para adquirir evidencias sin alterarlas durante el proceso. Además, la descarga rápida de grandes volúmenes de información no siempre es posible. Asimismo, tampoco es posible aislar completamente un entorno cloud, dado que en tal caso el investigador forense tampoco tendría acceso a éste.

Esto implica que, para poder realizar un análisis forense satisfactorio de un entorno cloud, es necesario haberlo preparado antes (el concepto Cloud Forensics Readiness se asocia a esta preparación previa para el análisis forense), lo que convierte al análisis forense en cloud en una actividad proactiva, que se anticipa a la ocurrencia del incidente a investigar.

Aunque existen diversos marcos para la preparación del entorno cloud para el análisis forense, en general existen tres dimensiones que es necesario considerar: regulatoria, organizativa y técnica.

3.4.1.1. Aspectos regulatorios.

En un primer nivel, es necesario identificar la legislación aplicable a la ejecución del análisis forense en la nube, que dependerá tanto del marco jurídico al que están sujetos el proveedor y el cliente según su localización, como de las actividades que se deseen desarrollar.

3.4.1.1.1. Marco Legal.

En España, el marco legal que ampara y regular el ejercicio de la actividad forense incluye, entre otras:

I. Constitución Española: Regula aspectos clave que aseguran las garantías mínimas del proceso penal, así como en relación con la intimidad de las personas y la protección de los datos.

II. Código Penal: No hay que olvidar que un análisis forense puede desembocar en un proceso judicial, por lo que es importante considerar las actividades delictivas reflejadas en el Código Penal.

III. Ley de Enjuiciamiento Civil: Al igual que en el caso anterior, se encarga de regular y ofrecer un marco legal para el proceso posterior tras la realización del análisis.

IV. RGPD: Regula el tratamiento de los datos de carácter personal, lo que impacta sobre la información utilizada durante el análisis, cuando ésta involucre a personas físicas.

V. Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico: El ámbito de aplicación de esta Ley son los servicios provistos a través de Internet, como el comercio electrónico, la contratación en línea, etc.

Como es habitual al hablar de servicios cloud, asociado al hecho de que el servicio sea ofrecido por un proveedor, es necesario acudir a las cláusulas definidas en el contrato para saber cuál es el compromiso del proveedor a la hora de facilitar una investigación forense llevada a cabo por el cliente. Además, es importante que se hayan definido las responsabilidades de cada una de las partes a la hora de desarrollar el análisis forense.

3.4.1.1.2. Cláusulas contractuales.

Con respecto a qué elementos deberían estar presentes en el contrato con el proveedor de servicios en la nube para regular el desarrollo de análisis forenses, como mínimo deberían acordarse los siguientes aspectos:

I. Capacidad para recopilar información: En el contrato con el proveedor, en caso de que éste autorice la recopilación de información de sus sistemas, es importante que se especifique cuál será la finalidad de la recolección, que puede ir desde la simple remediación hasta el inicio de un procedimiento judicial; así como la naturaleza de los datos que serán recopilados. También es importante considerar si será necesario que el proveedor facilite aquella información que el cliente no esté en disposición de extraer del entorno en la nube, especialmente en aquellos modelos en los que el acceso a la información esté restringido (SaaS y PaaS). En caso de que el proveedor deba facilitar información al cliente, será recomendable definir los medios para realizarlo y los tiempos máximos en los que deberá suministrarse.

II. Jurisdicción aplicable: En un entorno en el que la información puede estar distribuida a lo largo de diferentes países, y en el que cliente y proveedor no tienen por qué estar localizados en el mismo país, se vuelve especialmente relevante definir qué jurisdicción aplicará al proceso de análisis forense, así como a cualquier acción posterior que se derive de éste. No hay una respuesta clara en relación con esta cuestión, aunque generalmente se aplicar la jurisdicción según la localización de la sede central del proveedor en la nube.

III. Obligación de comunicación: Generalmente, los proveedores no conceden acceso libre a la información sobre la infraestructura utilizada para soportar el servicio. Por ello, es importante dejar claro a nivel contractual las circunstancias en las que el proveedor deberá facilitar información al cliente. Generalmente, para que esta obligación entre en vigor, el cliente deberá notificarle la ocurrencia de un incidente. Por ello, no se trata de una medida proactiva, no ofreciendo ninguna capacidad de detección adicional.

IV. Períodos de retención: Por lo general, la mayoría de las compañías poseen políticas y procedimientos que determinan durante cuánto tiempo se conservará la información extraída de su infraestructura (generalmente logs). Es una buena práctica que en el contrato se acuerde que, en caso de que haya una investigación en curso notificada al proveedor, éste garantice la conservación de cualquier evidencia durante el tiempo que dure dicha investigación, incluso si éste es superior al definido por el proveedor en circunstancias normales.

3.4.1.2. Aspectos organizacionales.

Se entenderán por aspectos organizacionales todos aquellos elementos relevantes para el correcto desarrollo de la actividad forense en un entorno cloud que dependan de la organización, y que sean independientes de la tecnología o sistema que deba analizarse.

Como para cualquier otra actividad, contar con el apoyo de la organización, especialmente de los miembros de la Dirección, y con recursos suficientes son aspectos básicos para garantizar el correcto desarrollo de la actividad forense. Entre los aspectos organizacionales más relevantes a considerar se encuentran los siguientes:

3.4.1.2.1. Apoyo de la Dirección

Con respecto a la realización de análisis forense, el apoyo de la Dirección implica en primer lugar contar con los recursos necesarios. Esta asignación de recursos se verá influenciada en gran medida por la cultura y concienciación de la organización. Por ello, es importante que el área responsable de la realización de los análisis forenses sea capaz de transmitir a la Dirección la importancia de poder contar con esta capacidad de supervisión del servicio, siempre desde una perspectiva de coste-beneficio. Contar con el apoyo de la Dirección ayudará a asegurar la predisposición de la organización, y condicionará al resto de aspectos.

3.4.1.2.2. Estrategia de preparación del entorno.

El desarrollo de un análisis forense no es una actividad que pueda dejarse a la improvisación. Es de vital importancia haber definido una estrategia a nivel interno que garantice que, en caso de ser necesaria la realización de un análisis forense, la organización y el entorno en la nube estarán preparados. Esta estrategia debe involucrar aspectos directamente relacionadas con el servicio cloud y las tecnologías asociadas, así como otros puramente organizacionales, incluyendo estructuras de responsabilidades, procedimientos claramente definidos y adaptados, etc.

3.4.1.2.3. Gobierno del análisis forense.

Como ya se comentaba en el punto anterior, contar con una estructura clara de roles y responsabilidades a la hora de realizar análisis forenses es un aspecto clave. Dichas responsabilidades deben estar ligadas directamente a cada una de las actividades definidas en los procedimientos que se utilicen para desarrollar esta actividad, y deben ser asignadas a empleados que tengan las capacidades necesarias, por las funciones de su puesto, para garantizar el correcto desempeño de la actividad forense. En el caso de los entornos cloud, las responsabilidades deberían extenderse además al proveedor del servicio, quedando éstas reflejadas a nivel contractual.

3.4.1.2.4. Procedimientos de actuación.

Deben definirse y documentarse, de forma previa a la realización del análisis forense en cloud, todas las actividades que será necesario desarrollar durante el proceso, con un nivel de detalle suficiente como para que se garantice la correcta ejecución de las mismas. La definición debe comprender aspectos tanto procedimentales como técnicos, para que queden reflejadas no solo qué actividades desarrollar, sino también cómo ejecutarlas sobre los entornos cloud usados por la organización.

3.4.1.2.5. Formación y concienciación.

En los entornos en la nube, debido a que la capacidad de supervisión por parte de la organización que los contrata se ve reducida, es de especial relevancia que todos los usuarios que interactúan con el servicio estén adecuadamente formados y concienciados, de forma que sepan detectar un incidente y que comprendan la importancia de notificarlo. Además, deberán saber cómo reaccionar debidamente para no comprometer el análisis forense posterior, en caso de considerarse necesario. Aunque el análisis forense debe dejarse en manos del personal cualificado para su ejecución, es importante contar con la colaboración y buen hacer del resto de usuarios para que las evidencias no se degraden o corrompan. Además, es importante que el personal no solo esté formado, sino que entienda la importancia del proceso, y la utilidad de la información que ofrece a posteriori.

3.4.1.3. Aspectos Técnicos.

Desde un punto de vista técnico, la preparación del entorno cloud para la realización de análisis forenses, requiere garantizar que éste genera la información necesaria para llevar a cabo el análisis posterior, y que dicha información es adecuadamente gestionada y protegida.

A diferencia de los anteriores, estos aspectos son muy dependientes del modelo de servicio cloud. En un modelo SaaS o PaaS, apenas habrá información que se pueda recopilar sin la intervención del proveedor. En cambio, los modelos IaaS, ofrecen mayores posibilidades a la hora de configurar distintos elementos relativos a la adquisición de información que podría usarse como evidencias forenses.

Para ello, en primer lugar, será necesario realizar configuraciones y desplegar herramientas suficientes como para obtener la información requerida, incluyendo:

3.4.1.3.1. Configuración de logs y captura de eventos.

Los sistemas más utilizados, como Linux, Windows o z/OS, poseen configuraciones que permiten definir los logs a recopilar. De la misma manera que en un entorno on premise, un entorno IaaS puede ser configurado para generar registros de auditoría. Hasta llegar a la capa de Sistema Operativo, será el cliente el que pueda y deba configurar la generación de logs que mejor considere para el análisis de la actividad. En cambio, a partir de la capa del hipervisor, solo el proveedor podrá configurar los logs a generar.

El primer paso para una correcta configuración del registro de eventos es identificar qué sistemas y aplicaciones pueden generar logs, y qué eventos debe recopilarse en cada uno de ellos. Para determinar sobre qué eventos deben generarse registros es conveniente utilizar un enfoque multinivel.

3.4.1.3.1.1. Nivel de cumplimiento.

Los requisitos impuestos a nivel legal o regulatorio en cuanto a la adquisición y preservación de logs debe ser el primer nivel que considerar, debido a las posibles consecuencias en caso de incumplimiento.

Existe diversa regulación dedicada a promover un uso responsable de los datos en la organización y a garantizar un adecuado nivel de ciberseguridad. No todas estipulan qué información debe ser recopilada, en ocasiones simplemente se regula cómo deben protegerse los registros.

Sin embargo, es necesario identificar si, a nivel regulatorio o contractual, se deben generar y almacenar registros concretos.

Estas consideraciones pueden ser bloqueantes a la hora de adoptar una solución en la nube si el tipo de información a almacenar y las capacidades de registro ofrecidas por el proveedor (para modelos SaaS y PaaS), son incompatibles entre sí. En este caso, si no existe forma alguna de obtener la información requerida en caso de incidente, debe desistirse del uso del servicio en la nube, u optarse por un despliegue de nube privada.

3.4.1.3.1.2. Nivel de procesos de negocio.

Deberán identificarse todas las actividades realizadas por la empresa en el entorno cloud, así como el nivel de supervisión requerido para cada una de ellas. Las mayores necesidades de supervisión vendrán impuestas por la criticidad de la actividad para el negocio, como por la existencia de SLAs comprometidos.

Al hablar de SLAs comprometidos, hay que considerar en primera instancia aquellos comprometidos por el cliente del servicio con un tercero. No obstante, también es importante adquirir la capacidad para medir todos aquellos SLAs comprometidos por el proveedor del servicio con el cliente, dado que será importante contar con evidencias suficientes a la hora de reclamar compensaciones en caso de incumplimiento.

El registro de estas actividades y de información relevante sobre las mismas, además de aportar información relevante durante una investigación forense, podrá usarse tanto para tomar decisiones orientadas a la optimización y reingeniería de los procesos, como para identificar cualquier necesidad futura en relación con el servicio cloud adquirido, como el cambio de funcionalidades adquiridas o la capacidad de las máquinas en uso.

3.4.1.3.1.3. Nivel operacional.

Cualquier aspecto que tenga un impacto a nivel operativo debe ser registrado, de forma que se adquiera visibilidad sobre el funcionamiento de los sistemas y aplicaciones desplegados en el entorno en la nube.

Hay cuatro categorías de eventos a registrar en este nivel:

I. Incidencias que afecten a un componente específico desplegado en la nube: Aunque a priori no es posible determinar si un incidente está causado por un mal funcionamiento de la aplicación o por una amenaza materializada, en ambos casos deberá ser registrada. Solo un análisis posterior permitirá determinar dentro que cuál de las dos tipologías se enmarca la incidencia. Se entiende por incidencia, como mínimo, cualquier cambio imprevisto en el funcionamiento de un componente que afecte a la experiencia de los usuarios de forma negativa.

II. Paradas, inicios y reinicios de un componente: Una aplicación que se reinicia frecuentemente, que no es capaz de iniciarse, o que se para de manera inesperada, puede estar sufriendo una incidencia que debe ser investigada, aunque no en todos los casos será necesario realizar un análisis forense.

III. Cambios de configuración: Cualquier cambio de configuración sobre un componente desplegado en la nube puede afectar de forma diversa a su funcionamiento. Podría impactar sobre la actividad de los usuarios, pero también sobre la capacidad de la aplicación para interactuar con otros componentes del sistema o sobre la capacidad de supervisión. En ocasiones, los roles encargados de llevar a cabo estos

cambios no tienen visibilidad sobre posibles causas adversas ocasionadas por dicho cambio, y suelen ser los usuarios del servicio los que reporten la incidencia ocasionada por el cambio. En otros casos, un cambio en la configuración estará provocado por la actividad en el sistema de un usuario malicioso. Si no se recopila la información sobre los cambios de configuración, identificar la causa de un funcionamiento anómalo se volvería una actividad mucho más compleja.

IV. Información en memoria: Además de los registros almacenados en el sistema, otra fuente de información relevante durante cualquier análisis forense, y por tanto también cuando éste se realiza sobre un entorno en cloud, es la información almacenada en la memoria.

■ *3.4.1.3.1.4. Nivel de seguridad.*

Dentro de la información que debe recopilarse en un entorno cloud sobre eventos de seguridad, podemos diferenciar dos grandes grupos:

I. Información generada por las herramientas de seguridad: Existe gran número de herramientas de seguridad que pueden desplegarse en un entorno en la nube, tales como anti-malware, firewalls, herramientas IPS/IDS, analizadores de protocolos, etc. Todas ellas generan información sobre su actividad y eventos detectados que es conveniente monitorizar y analizar de forma periódica. Además, está información suele ser fácil de exportar y es de gran utilidad durante una investigación forense.

II. Información sobre la actividad de usuarios relativa a aspectos de seguridad: En este segundo grupo se encuentra la información generada en el proceso de identificación, autenticación y autorización de usuarios. Entre los eventos de seguridad a recopilar dentro de este grupo se encuentran: intentos de inicio de sesión (exitosos y fallidos) y cierres de sesión, cambios de contraseña o de los permisos asociados al usuario, intentos de acceso a recursos para los que no se dispone de autorización, y cualquier actividad llevada a cabo por una cuenta privilegiada.

Para que se pueda investigar cualquier evento relevante ocurrido sobre la infraestructura que da soporte al servicio en la nube o que forma parte del propio servicio, es importante que se habilite la generación de logs en cada capa y en cada aplicación que se encuentre desplegada en el entorno en la nube. Además, debe definirse la cantidad de información a incorporar en cada log, lo que se conoce como nivel de verbosidad.

Aunque pudiera parecer que un mayor número de logs con un mayor nivel de verbosidad es siempre la mejor opción, hay que tener en cuenta que los entornos en la nube pueden llegar a ser accedidos por un alto volumen de usuarios y generan un mayor volumen de información de registro. Por tanto, la organización deberá contar con las capacidades necesarias para analizar los logs generados. Además, volumen de los registros excesivo saturará con mayor rapidez los recursos destinados para su almacenamiento, por lo que habrá que considerar esta circunstancia a la hora de definir dónde se almacenarán.

Una posible solución a este problema es el uso de utilidades SIEM, dado que las capacidades de correlación de logs permiten una supervisión más eficiente de logs cuando el volumen de éstos es muy elevado.

Aunque los registros de auditoría no son la única fuente de información que se utiliza durante un análisis forense, sí que es una de las que más trabajo previo requiere. En las siguientes secciones se verá que, además de esta fuente de información, también será necesario obtener otro tipo de información, como las imágenes de memoria.

3.4.2. Identificación y adquisición de las evidencias.

Durante la fase de identificación y adquisición se realiza la captura de las evidencias seleccionadas en la fase de identificación. En el caso de los modelos de servicio de tipo PaaS y SaaS, debido al mayor nivel de abstracción de éstos, deberá requerirse la participación del proveedor cloud para la extracción de las evidencias.

En el caso de los modelos IaaS, el cliente posee una mayor libertad para extraer las evidencias del entorno en la nube, debiéndose considerar lo expuesto a continuación.

3.4.2.1. Identificación de evidencias a recopilar.

A la hora de determinar qué evidencias recopilar, es fundamental tener en cuenta las posibles fuentes de evidencias en entornos en la nube y del evento que se quiere investigar. En el caso de las evidencias accesibles, habrá que diferenciar entre aquellas accesibles por el cliente, y las que deberán ser suministradas por el proveedor de servicios cloud:

Fuente	Accesibilidad	Tipos
Usuarios	Cliente	1. Logs de herramientas de seguridad instaladas en los equipos de los usuarios finales. 2. Información de navegación y logs almacenados en los navegadores web. 3. Logs de acceso a la máquina. 4. Caché de aplicaciones.
Red	Cliente	1. Logs de acceso a la red. 2. Registro de transacciones, incluyendo información de cabeceras y contenidos de los mensajes enviados.
Infraestructura	Proveedor (SaaS y PaaS) o Cliente (IaaS)	1. Logs de las herramientas de seguridad instaladas en el entorno. 2. Registros de acceso. 3. Registros de actividad en el sistema. 4. Logs de red generados. 5. Imágenes de memoria. 6. Snapshots del sistema virtualizado (Cliente o Proveedor dependiendo de si se ofrece la funcionalidad con el servicio). 7. Registros de acceso al hipervisor (solo Proveedor). 8. Registros de actividad en el hipervisor, incluyendo cambios de configuración (solo Proveedor). 9. Logs de acceso a la infraestructura sobre la que se despliegan los hipervisores (solo Proveedor)

3.4.2.2. Orden de volatilidad.

La primera decisión que debe tomarse es la priorización sobre los datos a adquirir. El análisis forense define el orden de volatilidad como la facilidad de un dato en un sistema de sufrir una acción que conlleve a su modificación, lo que ayuda a establecer su prioridad de adquisición desde un punto de vista forense. El orden de adquisición impuesto por la volatilidad de la memoria es el siguiente:

I. Memoria RAM del sistema.
II. Estado del sistema.

a. Conexiones de red abiertas (extraer antes de aislar el sistema).
b. Listado de ficheros abiertos.
c. Información sobre procesos en ejecución.

III. Memoria persistente del sistema.

Aunque el nivel de volatilidad de la memoria RAM y el estado del sistema es muy similar en los entornos cloud frente al resto de entornos, la memoria persistente es por lo general mucho más volátil en la nube, a causa de la virtualización del sistema.

3.4.2.3. Orden de adquisición.

Se plantea entonces una adquisición de evidencias en cuatro niveles:

I. Memoria RAM.
II. Datos de triaje.
III. Metadatos del cliente en el proveedor de servicios en la nube.
IV. Disco duro del sistema.

3.4.2.4. Extracción de las evidencias.

La adquisición de evidencias puede realizarse de dos formas, dependiendo de si las herramientas empleadas permiten o no el acceso remoto a la memoria del sistema a analizar.

En el caso de las herramientas de adquisición remota, éstas tienen la capacidad de acceder al sistema en la nube utilizando un agende desplegado o mediante una conexión remota, y realizan la adquisición completa de todas las evidencias forenses. La ventaja de estas herramientas es la mayor independencia del proveedor usado, así como la facilidad y rapidez en la adquisición.

Con respecto a aquellas herramientas de adquisición que no permiten el acceso remoto, debe obtenerse una imagen del sistema. La opción más recomendable es la realización de una captura del sistema (snapshot), estando esta funcionalidad disponible en muchos modelos IaaS. Esta opción ofrece mayores garantías de integridad de las evidencias adquiridas y generalmente no provoca modificaciones en la información dentro del sistema. En caso de que no sea posible obtener una snapshot, existen métodos alternativos que implican la creación de discos virtuales secundarios montados en modo solo lectura en los que se vuelque toda la información.

La adquisición en local es más costosa que mediante el uso de herramientas de adquisición remota. Sin embargo, también tiene sus ventajas. En primer lugar, permite una mayor compatibilidad con herramientas de análisis forense tradicionales, puesto que éstas se ejecutarán como una imagen de memoria similar a aquellas obtenidas en entornos tradicionales. En segundo lugar, permiten copiar las evidencias adquiridas con mayor facilidad, al no depender de una conexión directa con el entorno analizado.

3.4.2.5. Carga de las evidencias en el sistema local.

Una vez que se haya generado la evidencia forense, y en caso de que no se haya hecho uso de una herramienta de adquisición en remoto, deberán importarse a un sistema local en el que se pueda realizar el análisis sin las restricciones de los entornos en la nube.

La importación de las evidencias a un sistema local ofrece mayores garantías de disponibilidad e integridad de la información recopilada, de cara a un futuro análisis.
Para que las evidencias recopiladas en un entorno en la nube no se vean comprometidas, hay que garantizar lo siguiente:

3.4.2.5.1. Marcas de tiempo (timestamps).

Las marcas de tiempo (timestamps) incluidas en cada evento registrado deben permitir establecer una secuencia temporal de eventos. Por ello, cualquier sistema que recopile logs debe tener su reloj interno sincronizando con el sistema que se encargará de su almacenamiento y análisis. Una buena práctica es utilizar una fuente externa de sincronización.

3.4.2.5.2. Protocolo de transferencia.

El protocolo utilizado para el envío de los logs y las imágenes de memoria debe garantizar su integridad, confidencialidad, y que éstos alcanzan el destino. Para ello, el uso de protocolos de cifrado, checksums o hashes, y de comunicación síncrona es una buena opción para asegurar que los registros se transmiten correctamente y que no son alterados.

3.4.2.5.3. Sistema de compresión.

Dado el alto volumen de información que puede llegar a generarse en un sistema en la nube sobre distintos eventos, debe optarse por una solución que permita el envío comprimido de los registros, para no impactar significativamente sobre el ancho de banda. En un entorno ideal, no debería enviarse información de registro por el mismo canal utilizado para el resto del tráfico hacia o desde el entorno en la nube, especialmente en el caso del tráfico utilizado por los usuarios.

3.4.2.6. Alternativas para PaaS y SaaS.

Dentro de los modelos PaaS y SaaS, existen algunas herramientas capaces de obtener información directamente de los servicios, siempre que el cliente disponga de las credenciales adecuadas (véase Anexo I para consultar el listado de herramientas).

Estas herramientas funcionan con muchos de los servicios SaaS o PaaS más populares, pero son muy dependientes de éstos.

Además, existen limitaciones en cuanto a la información que podrán recopilar, por lo que deberá analizarse si la información que ponen a disposición del usuario es de utilidad para el análisis forense.

3.4.2.7. Cadena de custodia.

Garantizar la cadena de custodia de las evidencias es un requisito imprescindible para asegurar su validez durante un proceso judicial. Esto implica asegurar la integridad de la evidencia, de forma que se garantice que ésta no ha sido alterada desde el momento de su adquisición. Aunque no todas las investigaciones forenses desembocan en acciones legales, no es posible anticipar los cursos de acción que se derivarán de la investigación, por lo que todas las evidencias adquiridas y utilizadas deben ser admisibles en un proceso judicial.

En un entorno cloud, dado que la información accesible por parte del usuario sin recurrir al proveedor es de tipo volátil, y se encuentra en formato digital, asegurar la cadena de custodia implica garantizar que la información recopilada no ha sido alterada. De la misma manera, toda copia física que se realice de la información en formato digital deberá preservar también su integridad. Para lograr esto último, y desde un punto de vista puramente centrado en la integridad física del soporte, existen diversos contenedores y sistemas de precinto para garantizar que un dispositivo físico se mantiene íntegro.

En lo relativo al aseguramiento de la integridad y no manipulación de la información en formato digital, la nube introduce desafíos adicionales. El primer reto lo introduce la figura del proveedor del servicio. En caso de que éste deba intervenir en la adquisición o extracción de la evidencia forense del entorno en la nube, existe un punto potencial de fallo en la cadena de custodia por la falta de control del cliente sobre los procesos seguidos y el personal involucrado. En general, la parte del proceso llevada a cabo por el proveedor suele ser muy opaca, lo que vuelve difícil asegurar que se ha realizado con la suficiente diligencia. Por otro lado, en caso de que deba obtenerse una copia de un disco físico, el hecho de que la infraestructura esté compartida por distintos clientes impone diversas restricciones a nivel legal.

Por tanto, para evitar estos problemas, debe intentar obtenerse la mayor cantidad posible de información sin tener que recurrir al proveedor, extrayéndola directamente de aquellas capas controladas por el cliente.

Además, es muy recomendable que tanto la identificación como la adquisición de las evidencias forenses se realicen en presencia de un notario que de fe de las acciones realizadas. Para facilitar la labor del notario, es recomendable disponer de un documento previo en el que se expliquen, de forma sencilla y comprensible por personal no técnico, las acciones a realizar para facilitar la comprensión del notario y garantizar que éste pueda realizar su trabajo de la forma más eficiente posible.

Otra estrategia propuesta para paliar el problema derivado de la interacción del proveedor con las evidencias es la generación de registros duplicados de actividad en una infraestructura local, que puedan ser protegidos de acuerdo a los requerimientos del cliente del servicio.

En cualquier caso, una buena forma de garantizar la cadena de custodia de las evidencias forenses es la utilización de técnicas de hashing y cifrado. De esta manera se garantiza la integridad de la información adquirida, aún cuando el proveedor deba intervenir en el proceso.

Por último, al igual que ocurre en los entornos tradicionales, mantener un registro con todos los pasos seguidos y actividades ejecutadas durante la realización del análisis, así como el personal involucrado, desde las fases iniciales, supone una práctica obligatoria para garantizar la validez del proceso y dar aseguramiento, aunque éste no sea completo, sobre la preservación de la cadena de custodia.

3.4.3. Preservación.

Una vez identificadas y adquiridas las evidencias, la cadena de custodia debe seguir manteniéndose, así como la integridad de las mismas.

Adicionalmente, es crítico garantizar que únicamente las personas autorizadas pueden acceder a las evidencias adquiridas. En caso de que las evidencias adquiridas residan en la nube, esto puede lograrse mediante el uso de una interfaz segura de acceso, habilitada solo para el personal encargado de la investigación. En el caso de que las evidencias residan en local, siendo esta opción por la que debería optarse siempre que fuera posible, basta con implementar mecanismos de identificación, autenticación y autorización sobre el sistema en el que se almacenen las evidencias.

Una vez que la información es enviada a un servidor bajo el control de la organización, deben tomarse las siguientes consideraciones para asegurar la validez del proceso posterior de análisis:

I. En caso de que se haga uso de un sistema de gestión de logs, bien sea un SIEM, o cualquier otra utilidad que permita su acceso y visualización, debe seleccionarse y configurarse teniendo en cuenta los sistemas que generarán los registros. Es importante considerar esto de cara a garantizar que no habrá problemas con el formato en el que dichos registros se generan.

II. Cuando el volumen de registros de auditoría generado en un sistema es alto, así como cuando deban recopilarse logs de diversas fuentes, es importante que éstos sean procesados antes de proceder a su análisis. El objetivo de procesar los logs de forma previa al análisis es poder contextualizar la información, darle un formato común, agruparla cuando así se considere necesario, y poder eliminar toda aquella información de la que no se podrá extraer conocimiento para cubrir el objetivo del análisis forense.

III. Asegurar que el sistema de almacenamiento de las evidencias permite adaptarse de forma dinámica al volumen de informado generado, o bien existe un proceso periódico de análisis de la capacidad, lo que debe poder evitar que el sistema se quede sin espacio disponible.

IV. La información debe ser fácilmente accesibles y recuperable, de forma que todos los usuarios que dispongan del perfil de acceso necesario puedan consultarla de forma ágil.

V. Hay que asegurar que las evidencias estarán disponibles a lo largo del tiempo, para garantizar que, ante un evento que deba ser investigado, se podrá realizar un análisis forense válido. La opción más habitual para conseguir esto es realizar copias de seguridad de las evidencias adquiridas, y almacenarlas de manera segura. Además, no solo debe garantizarse que la información esté disponible, sino también que será recuperable en cualquier momento.

VI. Las evidencias no deben ser accesibles por cualquier empleado. Los roles y responsabilidades definidos para la realización de análisis forense deben reforzarse mediante la aplicación de medidas técnicas de seguridad que garanticen que solo el personal que deba tener acceso a los registros y capturas de memoria puede consultarlos, aplicando para ello controles de identificación, autenticación y autorización.

VII. Independientemente de dónde se almacenen o de quién acceda a las evidencias, éstas deben conservar su integridad en todo momento. Aunque su consulta pueda realizarse sin restricciones por parte del personal debidamente autorizado, debe evitarse cualquier modificación o eliminación de la información. Es fundamental que se conserve inalterada desde el mismo momento en el que es extraída del sistema origen. Esto incluye al almacenamiento una vez recopilada, pero también cualquier instante posterior a su generación, aunque ésta aún resida en el sistema origen.

El acceso a las evidencias, tanto si se trata de logs de auditoría o de imágenes de memoria, como un evento relevante más, también debe ser registrado. Aunque las evidencias no deben poderse modificar o eliminar, es importante saber quién las ha consultado, para dejar traza de todo el proceso de análisis forense, cuando su acceso sea legítimo; o para detectar posibles abusos de privilegios, cuando no lo sea.

Una práctica muy recomendable es el almacenamiento de las copias realizadas a partir de las evidencias originales en una localización distinta a la original. Asimismo, siempre que se vaya a trabajar una evidencia, deberá generarse una copia de ésta, de forma que se conserve la evidencia original junto a la procesada. De esta forma se evitan posibles problemas generados por errores en la manipulación de éstas, como por ejemplo al montar una imagen de memoria en modo lectura y escritura, pudiendo producirse borrado accidental de datos.

Adicionalmente, la realización de copias también ofrece protección frente a pérdidas de disponibilidad, como por ejemplo en caso de que se pierda la conectividad con el servidor remoto en el que se almacenan las evidencias.

3.4.4. Análisis.

El análisis de evidencias, una vez que éstas son recopiladas, no debería diferir sustancialmente entre entornos tradicionales y entornos en la nube. Sin embargo, debido a las mayores dificultades para adquirir las evidencias y los retos introducidos en el proceso por los entornos en la nube, suele optarse por un modelo de aproximación al análisis que permita optimizar el proceso.

3.4.4.1. Fases para lograr un análisis forense en cloud eficiente.

Puede usarse un enfoque multinivel que comprenderá las siguientes fases de análisis:

3.4.4.1.1. Inspección inicial / Triaje.

El triaje es la fase inicial, y por tanto más superficial y rápida, dentro de la etapa de análisis.

Durante el proceso de triaje, el objetivo principal es categorizar el tipo de incidente reportado, atendiendo a su impacto sobre la organización y las partes interesadas; y determinar si requerirá la ejecución de un análisis posterior o no.

Normalmente, esta fase del análisis se realiza sobre el entorno afectado, y con una cantidad de información mucho menor a la que se utilizará en caso de que se considere necesario incrementar el nivel de análisis.

Además de identificar la necesidad de un análisis forense posterior, durante la fase de triaje se identificará el nivel inicial de profundidad que requerirá dicho análisis, y la mejor fuente para cada una de las evidencias forenses necesarias durante el análisis posterior.

3.4.4.1.2. Análisis forense preliminar.

El objetivo de esta fase es adquirir la información necesaria para plantear el enfoque del análisis forense en profundidad, de forma que se adquiera un entendimiento superficial del evento a investigar.

Durante esta fase, en caso de que el triaje haya permitido concluir que es necesario un análisis posterior, se iniciará una recopilación inicial de información. A diferencia de la fase de triaje, en esta se realiza un primer análisis mediante el uso de herramientas forenses, que generalmente se ejecutan con un alto nivel de automatismo y cuya finalidad última no es determinar de forma precisa las causas u origen del evento, sino detectar algún indicio de dicho evento.

Como resultado de la ejecución de las primeras herramientas, se identificarán las primeras evidencias del evento a investigar. En caso de que, tras toda la recopilación de información inicial, no se detecte ningún indicio que haya sospechar de la ocurrencia de un evento que requiera investigación, podrá concluirse el análisis en esta fase.

Aunque llegados a este punto puede optarse por no seguir con la fase de análisis, puesto que existe la posibilidad de que el evento se haya producido pero la información recopilada inicialmente no haya permitido su detección, siempre es recomendable seguir investigando hasta obtener una evidencia clara de que se trata de un falso positivo.

3.4.4.1.3. Análisis forense en profundidad.

Una vez que el análisis entra en esta fase, existe la certeza, o al menos un indicio, de la necesidad de un análisis forense en profundidad, a causa de la ocurrencia de un evento adverso. Por tanto, debe realizarse un análisis completo, similar al que se lleva a cabo en cualquier otro entorno, para analizar la situación, incluyendo el curso de acción, las razones, los causantes o culpables y las consecuencias.

Es importante considerar que, al igual que en otro tipo de entornos, existen herramientas específicas que facilitan este proceso. Sin embargo, en el caso de la nube, el número de herramientas específicas disponibles es más reducido. Además, al igual que ocurre con entornos on premise, estas herramientas son muy dependientes de la solución cloud utilizada.

Las herramientas especialmente diseñadas para ser usadas en entornos cloud están generalmente pensadas para facilitar la adquisición de datos, puesto que el análisis de los mismos siempre debería realizarse en un entorno controlado por la organización.

En el Anexo I se incluye un cuadro resumen con algunas de las herramientas utilizadas para la realización de análisis forense en la nube.

Debido a las particularidades de este tipo de análisis, están surgiendo cada vez más servicios de FaaS o DFaaS (Forensics-as-a-Service o Digital-Forensics-as-a-Service, respectivamente). Estos servicios permiten la centralización de todas las evidencias en un sistema de almacenamiento centralizado, y ofrecen distintas interfaces de conexión para que los investigadores forenses puedan acceder a los datos y analizarlos. A pesar de su nombre, los servicios FaaS no se encargan tanto de la investigación sino de ofrecer un entorno accesible y seguro para los investigadores, facilitando el trabajo colaborativo.

En algunos modelos de DFaaS, se ofrece a los usuarios un conjunto de herramientas forenses ya cargado en el entorno, de forma que no solo puedan acceder a los datos de forma centralizada, sino que el servicio también les facilite las herramientas para tratarlos y analizarlos.

3.4.5. Reporte.

Una vez concluida la investigación forense, toda la información relevante generada durante el proceso debe presentarse a la audiencia objetivo.

Esta fase no se diferencia sustancialmente en un enfoque en la nube, aunque sí hay determinadas consideraciones que deben tenerse en cuenta:

I. Además del público objetivo habitual, también debe tenerse en cuenta al proveedor de servicios en la nube como un destinatario más del informe.

II. Las conclusiones emitidas deberán considerar con especial cuidado las evidencias utilizadas para el análisis. En caso de que, por las características de los entornos en la nube, no haya sido posible obtener una evidencia lo suficientemente robusta, o no existan evidencias adicionales que la respalden, deberá evitarse concluir, o hacerlo con rotundidad, si no se dispone del soporte suficiente.

III. Las conclusiones emitidas como parte de la investigación deben diferenciarse claramente según su destinatario. En el caso de aquellas conclusiones que afecten de manera directa al proveedor en la nube, hay que tener en cuenta que, a menos que se especifique lo contrario a nivel contractual, éste no está obligado a aplicar ninguna medida de remediación.

IV. En caso de que, como resultado del análisis realizado, se considere necesario iniciar acciones legales, habrá que tener presente que muchos proveedores tecnológicos incluyen cláusulas en el contrato que imponen ciertas condiciones o restricciones en caso de iniciarse estas acciones. En ocasiones, se exige al cliente poner en conocimiento del proveedor cualquier acción legal que vaya a acometerse. En otros casos, también se estipula que el proveedor tendrá capacidad de negociación durante el juicio, con el objetivo de intentar llegar a un acuerdo.

V. Debe segregarse la información que vaya a transmitirse al proveedor, de forma que éste solo sea provisto con aquella información que le resulte relevante, y que afecte a la parte de la infraestructura gestionada por éste. De esta manera, se garantiza que la información confidencial del cliente no sea divulgada.

4. CONCLUSIONES Y PRÓXIMOS PASOS

4.1. Conclusiones.

A partir del trabajo realizado, ha sido posible alcanzar una serie de conclusiones que se enumeran a continuación:

I. Para ambas actividades, la fase de preparación, necesaria antes de realizar las actividades de auditoría y análisis forense, cobra mayor relevancia, debiendo contar un soporte robusto a nivel legal, contractual, organizativo y técnico.

II. Cualquier actividad en la que deba participar el proveedor, incluyendo las de análisis forense y auditoría en la nube, debe estar perfectamente definida a nivel contractual, de manera que existan cláusulas que indiquen el alcance de las actividades y las responsabilidades de cada una de las partes.

III. La no inclusión de cláusulas que den soporte a las actividades de auditoría y análisis forense en cloud en el contrato con el proveedor en ningún caso debe suponer la no realización de estas actividades. Aunque es fundamental que toda actividad de supervisión realizada esté soportada a nivel contractual, existe un amplio margen para adaptar la estrategia de ejecución de forma que se obtenga un aseguramiento mínimo en relación con el servicio en la nube en uso.

IV. Aunque llevar a cabo actividades de supervisión sobre el servicio en la nube es necesario, esta actividad debe enfocarse considerando la relación coste-beneficio. Dependiendo del uso que se haga del servicio, el proceso soportado dentro de la organización, así como los datos gestionados, el nivel de riesgo de la empresa asociado al uso del servicio cloud contratado variará. Por ello, las actividades de supervisión, y el coste de su ejecución, deben estar justificadas por dicho nivel de riesgo.

V. Para que las actividades de supervisión aporten el máximo aseguramiento a la organización, es necesario que la organización disponga de un modelo de gobierno en cloud, que permita alinear estas actividades con los objetivos corporativos y las necesidades de las partes interesadas.

VI. A lo largo de todas las fases en las que se dividen las actividades de auditoría y análisis forense, debe tenerse muy presente al proveedor de servicios en la nube, involucrándole en el proceso cuando así se pueda y adaptándose a la relación establecida a nivel contractual; así como a las características particulares de este tipo de entornos.

VII. Muy en línea con el punto anterior, destaca la fuerte dependencia, a la hora de plantear las actividades de supervisión sobre los servicios en la nube, de la tecnología utilizada, el modelo de servicio y el modelo de despliegue. Estos aspectos pueden modificar radicalmente el enfoque a utilizar. Mientras que un modelo de nube privada no requerirá modificaciones sustanciales a la hora de realizar auditorías o análisis forenses con respecto a un enfoque tradicional, un servicio SaaS sobre una nube pública introducirá fuertes restricciones, y limitará enormemente la capacidad de supervisión.

VIII. El modelo de servicio afecta considerablemente al alcance de las actividades a desarrollar. En el caso de la auditoría en la nube, la capacidad de supervisión del proveedor se ve limitada, pero aún sigue siendo posible centrar el análisis en otros aspectos que permitan dar aseguramiento. En cambio, en el caso del análisis forense, las fases de preparación del entorno y adquisición de evidencias pueden verse casi completamente reducidas en modelos de tipos SaaS o PaaS, generándose una dependencia del proveedor difícil de evitar.

IX. La supervisión de servicios en la nube no requiere de forma obligatoria el uso de procedimientos muy distintos a los usados en otro tipo de entornos. En general, el mayor cambio se produce a la hora de plantear la estrategia de supervisión, así como por la necesidad de tener en consideración aspectos relevantes asociados a las tecnologías cloud.

X. A pesar de que los servicios en la nube llevan siendo usados de forma extensa desde la década de los 2000, aún no hay un nivel de madurez suficiente en lo relativo a la supervisión y control de éstos. Sigue siendo difícil encontrar documentación que permita adquirir el conocimiento necesario para garantizar una correcta supervisión. La mayoría de las referencias suelen centrarse en aspectos muy específicos de las actividades de auditoría o análisis forense.

XI. Con respecto a la realización de análisis forenses en cloud, el número de herramientas específicamente diseñadas para trabajar en entornos cloud es muy reducido. Aunque en muchos casos es posible utilizar herramientas de uso más generalista, ciertas partes del proceso no están adecuadamente soportadas por las herramientas adecuadas. Esto se debe en gran medida a la mayor diversidad de entornos en la nube, lo que dificulta el desarrollo de herramienta que puedan integrarse con la mayoría de las soluciones cloud disponibles.

XII. En relación con la auditoría de servicios cloud, no puede tratarse como una actividad puntual. Los servicios cloud deben integrarse en los planes de supervisión de los clientes de servicios cloud, y abordarse con un enfoque multinivel que ofrezca aseguramiento sobre los distintos aspectos relevantes del servicio, incluyendo, pero no limitándose a, cumplimiento regulatorio, gobierno y ciberseguridad.

XIII. Identificar la jurisdicción y regulación aplicable es fundamental para la ejecución de las actividades de supervisión descritas, para ello, se vuelve fundamental identificar la localización tanto del proveedor, como de los datos almacenados en la nube.

XIV. Si bien desde la perspectiva del proveedor en la nube la realización de actividades de supervisión no se ve sustancialmente modificada con respecto a actividades de supervisión generales, no ocurre así con el cliente. En este segundo caso, es importante llevar a cabo supervisión tanto a nivel interno, incluyendo aspectos bajo la responsabilidad de la propia organización; como a nivel externo, para garantizar que el proveedor da cumplimiento a las cláusulas definidas a nivel contractual.

XV. Las actividades de supervisión descritas en este documento, por sí mismas, no garantizan el tratamiento de los riesgos asociados a los servicios en la nube. Para ello, dichas actividades deben integrarse en un ciclo de gestión continua en el que participen tanto el cliente de servicios en la nube como el proveedor de los mismos. En este sentido, es especialmente importante que la información obtenida a partir de estas actividades se use, entre otras cosas, para alimentar un proceso de gestión de incidencias.

XVI. La información de reporte generada como resultado de ambas actividades de supervisión debe ser dirigida a la audiencia objetivo. En este caso, se introduce la figura del proveedor de servicios en la nube, al que idealmente deberían comunicársele únicamente aquellos hallazgos identificados de los que sea responsable. Por ello, es necesario definir dos niveles de reporte: uno a nivel interno, en el que se incluyan las conclusiones relevantes para las partes interesadas; y otro externo, incluyendo exclusivamente

la información que involucre al proveedor y no suponga una divulgación de información confidencial del cliente.

XVII. Cualquier respuesta o acción que deba tomarse una vez finalizada la actividad de supervisión, especialmente cuanto ésta comprenda acciones legales, deberá respetar las condiciones y restricciones definidas a nivel contractual, dado que en muchos casos se incluyen cláusulas que condicionan el proceso a seguir.

4.2. Próximos pasos.

El enfoque utilizado en el presente documento pretende ofrecer una primera aproximación a dos actividades fundamentales de supervisión de los servicios en la nube, como son la auditoría y el análisis forense.

Aunque existe diversa documentación en la que se cubren determinados aspectos de estas dos actividades y su enfoque a un entorno cloud, no es tan frecuente encontrar información que aporte una visión global sobre los aspectos más relevantes que deben contemplarse a la hora de abordar estas actividades, con un nivel de detalle suficiente.

Es por esto por lo que el documento no profundiza en aspectos concretos sobre determinadas fases o herramientas de análisis. Por ello, a partir de lo expuesto en este documento, existen diversas vías de investigación que sería interesante cubrir, siendo los siguientes algunos ejemplos de ellas:

I. Realizar un análisis más en profundidad de toda la legislación aplicable a las actividades de supervisión en la nube, incluyendo las principales jurisdicciones aplicables.

II. Definir un mayor nivel de detalle qué controles utilizar para ejecutar cada una de las auditorías propuestas.

III. Definir los requisitos y funcionalidades necesarias para el desarrollo de herramientas de análisis forense de forma que éstas estén adaptadas a los entornos en la nube y satisfagan los objetivos de cada una de las fases.

IV. Definir un mapa de riesgos completo para cada uno de los modelos de servicios y de despliegue, de forma que pueda asociarse un alcance concreto y un conjunto de controles para cubrir cada uno de los riesgos.

V. Profundizar en todos los elementos necesarios para garantizar un adecuado gobierno de los servicios en la nube, con un enfoque holístico que permita cubrir aspectos legales, operativos, tecnológicos, de ciberseguridad, etc.

VI. Analizar cómo las nuevas tecnologías podrían facilitar las labores de supervisión en la nube, especialmente aquellas que facilitan o dan soporte en el análisis de grandes volúmenes de información.

VII. Identificar nuevas tendencias o avances aplicables a las actividades de auditoría y análisis forense que permitan llevar a cabo este tipo de supervisión de forma más eficiente.

VIII. Una vez descritas con suficiente nivel de detalle las dos actividades de supervisión cubiertas en este documento, y con el objetivo de obtener un mayor aporte de valor, debe analizarse la mejor forma para integrarlas en un proceso de respuesta ante incidentes.

ANEXOS

ANEXO I. Listado de herramientas forense en cloud.

En el presente Anexo se se incluye un cuadro de resumen con algunas de las herramientas utilizadas habitualmente para la realización de análisis forense en cloud. Su presencia dentro de la lista no responde a ningún criterio particular, salvo que se han identificado a lo largo de la investigación realizada. Asimismo, el orden en el que se presentan no responde a ningún criterio ni comparación entre ambas, sino que se basa en la priorización de las herramientas específicas para entornos cloud, y una ordenación alfabética como segundo criterio.

Herramienta	Funcionalidad	Específica para entornos Cloud
Cellebrite UFED Cloud Analyzer	Esta aplicación permite la adquisición de evidencias a partir del análisis de la información en dominios públicos, redes sociales, mensajería instantánea y sistemas de almacenamiento en la Nube.	Sí
CloudTrail	Servicio que ofrece capacidades forenses para sistemas Cloud AWS, permitiendo consultar las llamadas a la API y las órdenes ejectuadas desde la consola de administración.	Sí
FROST	Herramienta de adquisición de evidencias forenses diseñadas para el servicio de IaaS de OpenStack, lo que permite la adquisición de discos virtuales, la gestión de los logs de las APIS y del firewal.	Sí
Magnet Axiom Cloud	Esta herramienta permite acceder y recopilar evidencias de servicios Cloud tales como Facebook, Office 365, Google apps, iCloud, Instagram, Twitter, Youtube, Outlook o Dropbox. Su finalidad es facilitar la adquisición de evidencias y mejorar la cadena de custodia.	Sí
MetaSpike, Forensic Email Collector	Facilita la adquisición de emails de servidores Exchange e IMAP, incluyendo Office 365 y Gmail.	Sí
OWADE	Permite la adquisición de diversa información contenida en discos duros sobre los que se encuentre instalado un sistema operativo Windows, incluyendo información sobre navegación en navegadores e información en la nube.	Sí
Belkasoft RAM Capturer	Permite la extracción completa de la memoria volátil de un sistema, pudiendo evadir determinados sistemas de protección de tipo anti-debugging y anti-dumping.	No
BrimorLab BambiRaptor	Utilizada para la extracción automática de memoria volátil de sistemas Windows, *nix y OSX.	No
CyLR	Esta herramienta se utiliza para la recopilación de artefactos forenses en remoto a través de una conexión segura (SFTP) con un impacto mínimo en el sistema origen, al no recurrir a la API de Windows.	No
Encase	Suite completa de análisis forense que ofrece diversas funcionalidades centradas en la adquisición de evidencias forenses y su posterior análisis.	No
Encase Endpoint Investigator	Sonda que puede ser desplegada en servidores en la Nube y que facilita la visualización y recopilación de información para investigaciones forenses de diversa índole.	No

FTK Imager	Herramienta de previsualización y generación de imágenes de memoria. Adicionalmente, también permite acceder a las evidencias recopiladas en modo solo lectura y crear hashes para garantizar la integridad de la evidencia.	No
FTK Remote Agent	Utilizada para la adquisición remota de imágenes de sistema operativo. Sin embargo, dado que su propia ejecución modifica la información del sistema, podría invalidar la evidencia en caso de que sea necesario recurrir a un proceso judicial.	No
F-Response	Esta aplicación permite acceso directo de solo lectura a memoria en remoto, incluyendo discos duros, memoria volátil y a sistemas de almacenamiento en Cloud.	No
LIME	Herramienta utilizada para la adquisición de imágnes de memoria en sistemas Linux.	No
Sleuth Kit	Permite la adquisición de imágenes de sistema (Windows y Linux), y ofrece diversas herramientas para el análisis de los datos capturados, tales como análisis de metadatos u ordenación temporal de todos los ficheros modificados en el sistema.	No
Sport	Se trata de una herramienta de análisis de red que facilita la captura y el análisis de paquetes TCP/IP enviados a través de la red.	No
SPEKTOR	Herramienta que facilita el desarrollo de actividades de triaje forense, ayudando a preservar y a examinar la información del sistema.	No
WinpMem	Compatible con sistemas operativos Windows, Linux y OSX, ofrece la posibilidad de adquirir imágenes de memoria.	No
Wireshark	Analizador de protocolos, con una funcionalidad muy similar a Sport, y que ofrece una perspectiva multi-nivel de los paquetes capturados en la red.	No
X-Ways	Aplicación utilizada para el análisis forense de entornos Windows que permite la adquisición y análisis de imágenes forenses tanto de disco duro como de memoria lógica utilizada por los procesos en ejecución.	No

REFERENCIAS

(2017). Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna. The Institute of Internal Auditors. (Accesible en https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Spanish.pdf)

R. Mogull, J Arlen, A. Lane, G. Peterson, M. Rothman y D. Mortman. (2017). CSA Security Guidance Version 4.

T. W.Singleton. (2010). IT Audits of Cloud and SaaS. (Accesible en https://www.isaca.org/Journal/archives/2010/Volume-3/Pages/IT-Audits-of-Cloud-and-Saas.aspx)

Interoute. ¿Qué es IaaS? (Accesible en https://www.interoute.es/what-iaas)

Interoute. ¿Qué es PaaS? (Accesible en https://www.interoute.es/what-paas)

Interoute. ¿Qué es SaaS? (Accesible en https://www.interoute.es/what-saas)

G. Allouche. (2013) Big Data as a Service has Arrived. (Accesible en https://www.socpub.com/articles/big-data-as-a-service-has-arrived-5805)

N. Mishra. (2011). Advantages of Disaster Recovery as a Service. (Accesible en https://www.datacenterknowledge.com/archives/2011/10/25/advantages-of-disaster-recovery-as-a-service)

Wetcom. DRaaS o Disaster Recovery as a Service, la nueva tendencia en recuperación de desastres. (Accesible en http://www.wetcom.com.ar/content/draas-o-disaster-recovery-as-a-service-la-nueva-tendencia-en-recuperacion-de-desastres/)

Fulcrum Inquiry. (2013). Detailed Audit Provisions Save Headaches. (Accesible en https://www.fulcrum.com/detailed-audit-provisions/)

G. L. Greene. Using the Right to Audit Clause to Detect Procurement Fraud. (Accesible en https://www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives/right-to-audit-clause.html)

Association of Certified Fraud Examiners. (2012). Sample Right-toAudit Clause. (Accesible en https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/sample-documents/sample-right-to-audit-clause.pdf)

Chartered Institute of Internal Auditors. (2017). Cloud Computing.

A. Aplin. The Cloud and the EU GDPR: Six Steps to Compliance. (Accesible en https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance)

The Open Group. Cloud Computing Governance Framework – Cloud Computing Governance Processes. (Accesible en http://www.opengroup.org/cloud/gov_snapshot/p7.htm)

R. S. Hartunian. (2018). The Eight Key Elements of Effective Compliance Programs. (Accesible en https://www.manatt.com/Insights/Newsletters/Health-Update/The-Eight-Key-Elements-of-Effective-Compliance-Pro)

Sungardas. 7 key elements of a successful cloud strategy. (Accesible en https://www.sungardas.com/globalassets/_multimedia/document-file/sungardas-7-key-elements-of-a-successful-cloud-strategy-white-paper.pdf)

Salesforce. 12 Benefits of Cloud Computing. (Accesible en https://www.salesforce.com/hub/technology/benefits-of-cloud/)

B. Reijnders. (2017). Master Thesis - A comparison of governance models for cloud computing. (Accesible en http://arno.uvt.nl/show.cgi?fid=144876)

D. Shackleford. (2018). RSA Conference2018: Incident Response in the Cloud. (Accesible en https://www.rsaconference.com/writable/presentations/file_upload/air-w14-incident-response-in-the-cloud.pdf)

The Institute of Internal Auditors. Cloud Computing – Key Risks and Management's Role. (Accesible en https://chapters.theiia.org/raleigh-durham/Events/Documents/Cloud%20Training%20-%20IIA.pdf)

REFERENCIAS

T. Morrow. (2018). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. (Accesible en https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html)

J. Jablonski. 12 Steps Guide for Data Governance in a Cloud-First World. (Accesible en https://www.cloudtp.com/doppler/12-step-guide-data-governance-cloud-first-world/)

C. K. Leong. (2014). Cloud Operating Model Transformation. (Accesible en https://infocus.dellemc.com/choong_kengleong/cloud-operating-model-transformation/)

B. Violino. (2018). The dirty dozen: 12 top cloud security threats for 2018. (Accesible en https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html)

A. Alenezi, R. Khalid Hussein, R. J. Wlaters, y G. B. Wills. (2017). A Framework For Cloud Forensi Readiness in Organizations. University of Southampton.

J. Jeffers. Computer Forensics: Forensic Issues With Virtual Systems. (Accesible en https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/forensic-issues-with-virtual-systems/#gref)

L. De Marco, F. Ferruci y M-Tahar Kechadi. (2014). Reference Architecture for a Cloud Forensic Readiness System. (Accesible en https://www.insight-centre.org/sites/default/files/publications/icst-transactions-2014.pdf)

C. Gervilla Rivas. (2014). Trabajo de Final de Master – Metodología para un Análisis Forense. (Accesible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf)

D. Willson. (2014). Legal Issues of Cloud Forensics. (Accesible en http://www.mcrinc.com/Documents/Newsletters/201402_Legal_Issues_of_Cloud_Forensics.pdf)

V. R. Kebande y H.S. Venter. (2015). Adding Event Reconstruction to a Cloud Forensic Readiness Model. University of Pretoria. (Accesible en http://icsa.cs.up.ac.za/issa/2015/Proceedings/Full/8_Paper.pdf)

S. Naaz y F. Ahmad Siddiqui. (2016). Comparative Study of Cloud Forensics Tools. Faculty of Engineering and Technology Jamia Hamdard. (Accesible en https://www.caeaccess.org/archives/volume5/number3/naaz-2016-cae-652258.pdf)

Sumo Logic. (2018). Collet Logs for Google Cloud Storage. (Accesible en https://help.sumologic.com/07Sumo-Logic-Apps/06Google/Google_Cloud_Storage/Collect_Logs_for_Google_Cloud_Storage)

P. Ramarao. (2017). Best Cloud Storage Services With Read Only Access. (Accesible en https://www.cloudwards.net/best-cloud-storage-services-with-read-only-access/)

G. Sadowski. (2010). Using logs for forensics after a data breach. (Accesible en https://www.networkworld.com/article/2193990/tech-primers/using-logs-for-forensics-after-a-data-breach.html)

A. Fortuna. (2017). Windows event logs in forensic analysis. (Accesible en https://www.andreafortuna.org/dfir/windows-event-logs-in-forensic-analysis/)
R. Marty. (2011). Cloud Application Logging for Forensics. (Accesible en https://pixlcloud.com/applicationlogging.pdf)

S. Alqahtany, N. Clarke, S. Furnell y C. Reich. A Forensic Acquisition and Analysis System for IaaS. (Accesible en https://core.ac.uk/download/pdf/74389545.pdf)

J. Dykstra y A. Sherman. (2013). Design and Implementation of FROST – Digital Forensic Tools for the OpenStack Cloud Computing Platform. (Accesible en https://www.dfrws.org/sites/default/files/session-files/pres-design_and_implementation_of_frost-_digital_forensic_tools_for_the_openstack_cloud_computing_platform.pdf)

R. B. van Baar, H. M. A. van Beek y E van Eijk. (2014). Digital Forensics as a Service: A game changer. (Accesible en https://www.researchgate.net/publication/261762759_Digital_Forensics_as_a_Service_A_game_changer)

Y. Wen, X. Man, K. Le y W. Shi. (2013). Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and Processing Using Cloud. (Accesible en http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.9583&rep=rep1&type=pdf)

S. Almulla, Y. Iraqi y A. Jones. (2013). Cloud forensics: A research perspective. (Accesible en https://www.researchgate.net/publication/255723934_Cloud_forensics_A_research_perspective)

K. Ruan, J. Carthy, T. Kechadi y M. Crosbie. (2011). Cloud forensics: An overview. (Accesible en https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview)

REFERENCIAS

S. Mrdovic, A. Huseinovic y E. Zajko. (2009). Combining static and live digital forensic analysis in virtual environment. (Accesible en https://www.researchgate.net/publication/224087812_Combining_static_and_live_digital_forensic_analysis_in_virtual_environment)

K. Kent, S. Chevalier, T. Grance y H. Dang. (2006). Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. (Accesible en https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf)

D. A Orr y P. White. (2018). Current State of Forensic Acquisition for IaaS Services. (Accesible en https://juniperpublishers.com/jfsci/pdf/JFSCI.MS.ID.555778.pdf)

M. M. Nasreldin, M. El-Hennawy, H. K. Aslan y A. El-Hennawy. (2015). Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing. (Accesible en https://www.ijcsi.org/papers/IJCSI-12-1-1-153-160.pdf)

SHI Staff. (2017). How to negotiate a better software audit clause. SAM/IT Asset Management Software. (Accesible en https://blog.shi.com/software/negotiate-better-software-audit-clause/)

S. Simou, C. Kalloniatis, S. Gritzalis y H. Mouratidis. (2016). A survey on cloud forensics challenges and solutions. (Accesible en https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1688)

M. Taylor, J. Haggerty, D. Gresty y R. Hegarty. (2010). Digital evidence in cloud computing systems. (Accesible en http://users.cis.fiu.edu/~fortega/df/research/Cloud%20Forensics%20II/Referenced%20Material/12%20-%20Digital%20evidence%20in%20cloud%20computing%20systems.pdf)

J. James, A. F. Shosha y P. Gladyshev. (2012). Digital Forensic Investigation and Cloud Computing. (Accesible en https://www.researchgate.net/publication/259497217_Digital_Forensic_Investigation_and_Cloud_Computing)

E. Casey, M. Ferraro y L. Nguyen. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. (Accesible en https://www.researchgate.net/publication/26819089_Investigation_Delayed_Is_Justice_Denied_Proposals_for_Expediting_Forensic_Examinations_of_Digital_Evidence)

C. Liu, A. Singhal y D. Wijesekera. Identifying Evidence for Implementing a Cloud Forensic Analysis Framework. Department of Computer Science George Mason University.

M. Rafique y M. N. A. Khan. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools.

S. Simou, C. Kalloniatis y E. Kavakli. (2014). Cloud Forensics Solutions: A review.

S. Park, Y. Kim, G. Park, O. Na y H. Chang. (2018). Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment.

Trabajo colectivo de los asistentes a la Digital Forensic Research Conference. (2001). A Road Map for Digital Forensic Research. (Accesible en http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf)

J. Dykstra, L. Gowen, R. Jackson, O. Scot Reemelin, E. F. Rojas, K Ruan, M. Salim, K. E. Stavinoha,

L. P. Taylor y K. R. Zatyko. (2014). NIST Cloud Computing Forensic Science Challenges. National Institute of Standards and Technology. (Accesible en https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf)

isms forum spain

CSAES cloud security SPAIN alliance℠

www.ismsforum.es