TAREA 03

REALIZACIÓN DE ANÁLISIS FORENSES EN CLOUD

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

Caso práctico
La empresa de María va a contratar servicios de cloud para poder almacenar determinados datos de la empresa, están barajando distintas ofertas de los proveedores.
Tienen la preocupación de llegado el caso de un Incidente de seguridad si serán capaces de poder realizar los análisis forenses correspondientes. También tienen la duda de qué pasará con esos datos y si serán accesibles.
Para ello solicitan la ayuda de María para internamente saber como deben de gestionar el contrato con el proveedor de servicios.

Apartado 1: Consideraciones de la Nube
Esta tarea es eminentemente teórica, para realizarla deberás repasar los conceptos previamente explicados e investigar sobre la protección de datos y regulaciones.

1. **Cuando una empresa contrata un servicio de cloud o nube, ¿qué consideraciones tiene que tener en cuenta y más teniendo en cuenta los aspectos de futuros forenses en este entorno?**

Al contratar un servicio en la nube (servicio Cloud), es fundamental que la empresa contemple una serie de aspectos tanto operativos como contractuales y legales que aseguren que, en caso de incidente de seguridad, se pueda realizar un análisis forense adecuado y se garantice el control y la integridad de la información.

Acuerdos contractuales
- Cláusula de incidentes de ciberseguridad, se debe definir la actuación ante un incidente, quiénes serán los responsables, qué responsabilidad tendrá cada uno, los tiempos de respuesta y cómo se coordinarán las acciones entre empresa y proveedor. Incluir penalizaciones en caso de incumplimiento de las obligaciones de seguridad y protección de datos.
- Acceso a los datos y evidencias, es fundamental que el proveedor asegure la colaboración en caso de incidente de ciberseguridad, garantizando el acceso a los datos y registros necesarios para realizar un análisis forense. Esto incluye disponer de la información histórica que permita rastrear actividades sospechosas o maliciosas.
- Cadena de custodia, definir los procedimientos de recolección de evidencias. El proveedor debe comprometerse a mantener la integridad de los datos, de modo que cualquier evidencia obtenida pueda ser admitida en procedimientos legales o investigaciones internas.

Auditorías y certificaciones
- Certificaciones de seguridad, preferir proveedores que cuenten con certificaciones reconocidas (ISO 27001), que demuestran un compromiso con la seguridad de la información y buenas prácticas en la gestión de seguridad y la preservación de la integridad de los datos.
- Auditorías, asegurar que se permita realizar auditorías de seguridad y forenses periódicas para verificar el cumplimiento de las políticas de seguridad y protección de datos implementadas, o que el proveedor proporcione informes detallados.

Consideraciones legales y control de datos
- Cumplimiento normativo, asegurar que el proveedor del servicio en la nube, cumpla las regulaciones aplicables tanto locales como internacionales (GDPR en Europa), que establece normas estrictas sobre la protección de datos personales.
- Ubicación de los datos, verificar donde se almacenarán los datos, ya que algunas regulaciones requieren que los datos se mantengan dentro de ciertas jurisdicciones.
- Encriptación, implementar medidas de encriptación tanto en el tránsito, como en reposo para proteger los datos sensibles.
- Gestión de accesos, implementar un sistema de gestión de identidades, autenticación multifactorial y control de accesos para asegurar que sólo personal autorizado pueda acceder a los datos.

Herramientas de seguridad
- Capacidades del proveedor, es importante que el proveedor cuente con mecanismos y herramientas que permitan la detección, recolección y análisis de incidentes. Asegurar que realice un monitoreo continuo y que vaya generando y almacenando logs detallados.

Recuperación ante desastres

- Respaldo de datos: asegurarse de que el proveedor tenga políticas de respaldo y recuperación que aseguren la integridad y disponibilidad de la información, de forma que se minimice la pérdida de datos y se facilite la reconstrucción de eventos posteriores a un incidente.

Al contratar un servicio en la nube, la empresa debe asegurarse de que el proveedor no solo ofrezca soluciones de almacenamiento, sino que también garantice un entorno preparado para realizar análisis forense de manera efectiva en caso de incidente. Esto implica definir algunos puntos importantes como quién es el responsable de cada aspecto, cómo se preservarán y se accederá a los datos y de qué forma se cumplirá con las regulaciones y normativas vigentes.

2. **¿Qué sucede si tenemos que hacer la investigación en un entorno o máquina que tenemos subcontratado a un proveedor que tiene los servicios en nube?**

Cuando se necesita realizar una investigación forense en un entorno con máquinas contratada a un proveedor de servicios en la nube, el proceso puede ser complejo y requiere una coordinación cuidadosa entre la empresa y el proveedor.
Primero, la empresa detecta un posible incidente de seguridad en su entorno de nube. Esto podría ser una brecha de datos, una actividad sospechosa o cualquier otra señal de que algo no está bien. Inmediatamente, se notifica al equipo de seguridad interno y al proveedor de servicios en la nube sobre el incidente para que ambos puedan comenzar a trabajar en conjunto.
A continuación, el equipo de seguridad de la empresa realiza un análisis preliminar para determinar la naturaleza y el alcance del incidente. Este análisis inicial es crucial para elaborar un plan de acción detallado para la investigación forense. En esta etapa, se identifican los datos y sistemas afectados y se decide qué evidencias serán necesarias para la investigación.
Una vez que se tiene un plan, la empresa se comunica con el proveedor para solicitar su colaboración. Aquí es donde los acuerdos contractuales juegan un papel crucial, ya que deben incluir cláusulas que obliguen al proveedor a colaborar y preservar las incidencias digitales.
El siguiente paso es la recolección de evidencias, el proveedor proporciona acceso a los datos y registros relevantes (logs de actividad, copias de seguridad y metadatos). Los investigadores forenses utilizan herramientas especializadas para recolectar y preservar estas evidencias, asegurando que se mantenga su integridad durante el proceso.
Una vez recolectadas las evidencias los forenses comienzan el análisis detallado, examinarán los datos en busca de cualquier actividad sospechosa. El análisis puede incluir la revisión de registros de actividad, la identificación de patrones inusuales y la reconstrucción de eventos para entender cómo ocurrió el incidente y cuál fue su impacto. Durante este proceso, es esencial cumplir con las regulaciones de protección de datos aplicables. Esto incluye respetar los derechos de privacidad y confidencialidad de los datos, además, se debe mantener una cadena de custodia rigurosa para asegurar que las evidencias sean admisibles en procedimientos legales.
Cuando se completa el análisis, se elabora un informe detallado con los hallazgos de la investigación. En el que se incluyen las evidencias recolectadas, el análisis realizado y las conclusiones sobre el incidente. También se proporcionan recomendaciones para mejorar la seguridad y prevenir futuros incidentes.
Finalmente la empresa y el proveedor implementan las medidas correctivas necesarias para mitigar el impacto del incidente y fortalecer la seguridad. Esto puede incluir la actualización de políticas de seguridad, la implementación de nuevas herramientas de monitoreo y la capacitación del personal. Además, se establece un monitoreo continuo para detectar y responder a posibles incidentes futuros.

3. **¿Qué obligaciones y responsabilidades tiene el cliente que contrata servicios de cloud a efectos de protección del dato?**

Cuando una empresa contrata servicios cloud, asume varias obligaciones y responsabilidades para garantizar la protección de los datos, a continuación nombraremos las más importantes:

Cumplimiento normativo y evaluación de resgos: el cliente debe asegurarse de que el proveedor de servicios en la nube cumpla con todas las regulaciones aplicables de protección de datos. Además, debe realizar una evaluación de riesgos para identificar posibles vulnerabilidades y amenazas de seguridad de los datos.

Contratos y acuerdos: es fundamental que el cliente establezca un contrato claro con el proveedor de servicio en la nube, en el que debe incluir cláusulas específicas sobre la protección de datos, la responsabilidad en caso de incidentes de seguridad y los procedimientos para la recolección de evidencias. También se deben definir las responsabilidades de ambas partes y cumplimiento normativo.

Medidas de seguridad: la empresa debe implementar medidas de seguridad adecuadas, como la encriptación de los datos en tránsito y en reposo, la gestión de identidades y accesos y la autenticación multifactorial. También es importante que el proveedor realice un monitoreo continuo y mantenga los logs detallados de las actividades.

Auditorías y supervisión: el cliente debe realizar auditorías periódicas para verificar que el proveedor cumpla con las políticas de seguridad y protección de los datos establecidas. Estas auditorías pueden ser realizadas por el propio cliente o por terceros.

Planes de respuesta a incidentes: esencial tener un plan de respuesta ante incidentes que incluya procedimientos claros para la detección, notificación y gestión de incidentes de seguridad. Además, el cliente debe proporcionar formación y concienciación sobre seguridad a sus empleados

Estos puntos resumen las principales obligaciones y responsabilidades del cliente al contratar servicios de cloud para garantizar la protección de los datos.

4. ¿Qué es un servicio transparente de cloud? ¿Qué consecuencias tiene un servicio opaco?

Un servicio transparente de Cloud es aquel en el que el proveedor ofrece una visibilidad clara y detallada sobre cómo se gestionan y protegen los datos. Esta transparencia es crucial para que los clientes puedan tener un control y conocimiento completo sobre el manejo de sus datos, facilitando el cumplimiento normativo y las medidas de seguridad implementadas y los procedimientos de acceso y auditoría. Esto incluye detalles sobre dónde se almacenan los datos, (proveedores locales, nube pública o nube privada), así como las políticas de encriptación, autenticación multifactorial y otras medidas de seguridad que protegen los datos. Además, los clientes pueden acceder a registros de auditoría y logs de actividad que les permite monitorear el uso y acceso a sus datos en tiempo real.
La transparencia en los servicios de cloud genera varios beneficios importantes. En primer lugar, aumenta la confianza entre el cliente y el proveedor, ya que el cliente sabe exactamente cómo se manejan y protegen sus datos. En segundo lugar, facilita el cumplimiento de regulaciones de protección de datos al proporcionar la información necesaria para demostrar que se están siguiendo las mejores prácticas. por último, permite identificar y mitigar rápidamente posibles vulnerabilidades y amenazas, ya que los clientes tienen acceso a la información detallada sobre la seguridad de sus datos. En resumen, un servicio transparente proporciona claridad y control sobre la gestión de los datos, lo que es esencial para la seguridad, el cumplimiento normativo y la confianza con el cliente.

Un servicio opaco de Cloud es aquel en el que el proveedor no proporciona suficiente información o visibilidad sobre cómo se gestionan y protegen los datos. Esta falta de transparencia puede tener varias consecuencias negativas para las empresas que utilizan estos servicios:

1. Riesgo de seguridad, la falta de transparencia puede ocultar vulnerabilidades y brechas de seguridad, lo que aumenta el riesgo de incidentes o pérdida de datos.
2. Cumplimiento normativo, sin una visibilidad clara es difícil asegurar que se cumplen todas las regulaciones de protección de datos, esto puede resultar en sanciones o multas.
3. Confianza y control, la opacidad puede deteriorar la confianza del cliente en el proveedor, ya que no tiene certeza sobre cómo se manejan y protegen los datos.
4. Costes ocultos, la falta de claridad en el costo y el uso de recursos, pueden llegar a gastos innecesarios y sobrecostos.
5. Dificultades en la auditoría, sin acceso a la información detallada, realizar auditorías se vuelven complicado, lo que puede comprometer la capacidad de la empresa para detectar y responder a incidentes.
6. Dependencia del proveedor, la falta de transparencia aumenta la dependencia del cliente en el proveedor, dificultando la migración a otros servicios o la implementación de medidas de seguridad adicionales.

En conclusión, la transparencia en los servicios de cloud es esencial para garantizar la seguridad, el cumplimiento normativo y la confianza del cliente. Un servicio transparente proporciona visibilidad clara sobre la gestión y protección de los datos, permitiendo a los clientes tener un control completo y facilitando

la identificación y mitigación de posibles vulnerabilidades. Por el contrario, un servicio opaco puede ocultar riesgos de seguridad, dificultar las auditorías y empeorar la confianza con el proveedor, aumentando la dependencia y complicando el cumplimiento de las regulaciones. Optar por un servicio transparente de Cloud es fundamental para asegurar la gestión efectiva y segura de los datos.

5. **¿Cómo puedo recuperar mis datos? ¿Y si son de carácter personal (art 20 RGPD)?**

Para recuperar tus datos en un servicio cloud, generalmente debes seguir los procedimientos establecidos por el proveedor del servicio. Esto puede incluir acceder a una interfaz de usuario donde puedes descargar tus datos o solicitar una copia a través del soporte técnico del proveedor. Es importante revisar los términos y condiciones del servicio para entender los pasos específicos y las políticas de recuperación de datos. Algunos proveedores también ofrecen herramientas de exportación que facilitan la descarga de grandes volúmenes de datos.

Si los datos son de carácter personal, el artículo 20 del Reglamento General de Protección de Datos (RGPD) establece el derecho a la portabilidad de los datos. Esto significa que tienes derecho a recibir los datos personales que has proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y a transmitir esos datos a otro responsable del tratamiento sin impedimentos. Este derecho se aplica cuando el tratamiento de los datos se basa en el consentimiento o en un contrato y se realiza por medios automatizados. Además, tienes derecho a que los datos personales se transmitan directamente de un responsable a otro cuando sea técnicamente posible. Este derecho facilita la transferencia de datos entre diferentes servicios y asegura que puedas mantener el control sobre tus datos personales, permitiéndote mover, copiar o transferir fácilmente tus datos de un entorno informático a otro de forma segura.

6. **¿Qué garantías debo pedir al proveedor de servicios de cloud para evitar tener problemas al hacer un forense en el entorno de cloud o nube?**

Para asegurarte de que puedes realizar un análisis forense efectivo en un entorno de Cloud, es fundamental pedir ciertas garantías al proyecto proveedor:

1. Acceso a datos y registros

Es crucial que el proveedor te garantice acceso a todos los datos y registros necesarios para realizar un análisis forense. Esto incluye logs de actividad, registros de acceso y cualquier información relevante. Sin este acceso sería muy difícil rastrear lo que ocurrió y quién estuvo involucrado, para ello, asegúrate de que el proveedor tenga políticas claras sobre cómo y cuándo puedes acceder a estos datos y que te proporcione las herramientas necesarias.

2. Preservación de evidencias e integridad de datos

Debes asegurarte de que el proveedor tenga políticas claras para la preservación de evidencias, esto significa que deben mantener los datos intactos y sin alteraciones desde el momento en el que se detecta un incidente hasta que se completa la investigación. La integridad de las evidencias es crucial para que sean admisibles en procedimientos legales.

3. Colaboración y soporte técnico,

el proveedor debe comprometerse a colaborar durante todo el proceso de investigación, esto incluye soporte técnico y acceso a expertos que puedan ayudarte a interpretar los datos y registros. La colaboración del proveedor es esencial para que la investigación sea efectiva y rápida, por lo que, hay que asegurarse de que el contrato incluya alguna cláusula que obligue al proveedor a colaborar.

4. Cumplimiento normativo y certificaciones de seguridad

Es importante que el proveedor cumpla con todas las regulaciones de protección de datos aplicables, esto asegura que los datos se manejen de forma segura y conforme la ley, lo cual es fundamental para evitar sanciones y problemas legales. Además, se debe pedir que el proveedor tenga certificaciones reconocidas, que demuestren su compromiso con la seguridad de la información.

5. Auditorías y monitoreo continuo

Debes asegurarte de que el proveedor permita realizar auditorías periódicas para verificar el cumplimiento de las políticas de seguridad y protección de datos. El proveedor debe realizar un monitoreo continuo de sus sistemas para detectar y responder rápidamente a cualquier actividad sospechosa. El acceso a informes de auditoría y monitoreo, permitirá tener una visión clara de cómo se están gestionando los datos y asegurar que se estén tomando las medidas adecuadas.

6. Planes de respuesta a incidentes

El proveedor debe tener un plan claro de respuesta ante incidentes que incluya procedimientos para la detección, notificación y gestión de incidentes de seguridad. Además, se pueden prevenir incidentes y preparar a los empleados para responder adecuadamente, ofreciendo formación y concienciación sobre seguridad.

Estas garantías aseguran un análisis forense efectivo en la nube, protegiendo los datos y cumpliendo con las regulaciones. Garantizan acceso a datos, preservación de evidencias, colaboración del proveedor, cumplimiento normativo, auditorías y planes de respuesta de incidentes. Esto fortalece la confianza y crea un entorno seguro para la gestión de la información

7. ¿Puedo pedir al proveedor que se convierta en el responsable de mis datos al tenerlos alojados en su nube?

Cuando contratas servicios de cloud, es importante entender cómo se distribuyen las responsabilidades entre el cliente y el proveedor de servicios en la nube. En general, no puedes transferir completamente la responsabilidad de tus datos al proveedor pero puedes pedirle que asuma ciertas responsabilidades específicas.

El modelo de responsabilidad compartida define claramente qué aspectos de la seguridad y la gestión de los datos son responsabilidad del proveedor y cuáles son responsabilidad del cliente. La mayoría de proveedores operan bajo este modelo.
El proveedor es responsable de la seguridad “de” la nube, incluyendo la protección de la infraestructura, la seguridad física y la seguridad de la plataforma y las aplicaciones (PaaS o SaaS). El cliente, es responsable de la seguridad “en” la nube, lo que incluye proteger la integridad, confidencialidad y disponibilidad de los datos, gestionar el control de acceso, cifrar los datos y mantener la configuración de seguridad.

Aunque no se puede transferir completamente la responsabilidad de los datos al proveedor, puedes pedirle que asuma ciertas responsabilidades adicionales como el monitoreo y las auditorías, para que el proveedor sea quien identifique y responda rápidamente a cualquier actividad sospechosa, confiar al proveedor el cumplimiento normativo, que se encargue de cumplir las regulaciones de protección de datos aplicables o incluso pedir al proveedor que ofrezca soporte técnico y colaboración en caso de un incidente de seguridad, incluyendo el acceso a los datos y registros necesarios para el análisis forense.
El proveedor de servicios de cloud puede actuar como encargado del tratamiento de los datos, pero la última responsabilidad la tiene el cliente. Esto significa que aunque el proveedor maneje y procese los datos, el cliente sigue siendo el responsable principal de asegurar que los datos se gestionen de acuerdo a las regulaciones. Sin embargo, es posible incluir cláusulas en el contrato que especifiquen las responsabilidades del proveedor en términos de protección y seguridad de los datos. Estas cláusulas pueden detallar las medidas de seguridad que el proveedor debe implementar, los procedimientos para la gestión de incidentes y las obligaciones en caso de investigación forense.

En resumen, aunque no se puede transferir completamente la responsabilidad de los datos al proveedor de servicios en la nube, puedes establecer acuerdos. Es fundamental entender el modelo de responsabilidad compartida y asegurarse de que el proveedor cumpla con sus obligaciones para proteger los datos del cliente y facilitar la gestión de la seguridad.