GOBIERNO DE MÉXICO | CONAHCYT CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS | INFOTEC

BIBLIOTECA INFOTEC
VISTO BUENO DE TRABAJO TERMINAL

Maestría en Derecho de las Tecnologías de Información y Comunicación
(MDTIC)

Ciudad de México, a 12 de enero de 2024

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación:

"Forense digital: cadena de custodia en casos de almacenamiento en nube"

Desarrollado por el alumno: **Víctor Manuel Gómez Flores**, bajo la modalidad del **Diplomado en Derecho, TIC e Innovación del INFOTEC** cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Mtro. Carlos Josué Lavandeira Portillo
Director Adjunto de Innovación y Conocimiento

CJLP/jah

C.c.p. Felipe Alfonso Delgado Castillo.- Gerente de Capital Humano.- Para su conocimiento.
Víctor Manuel Gómez Flores.- Alumno de la Maestría en Derecho de las Tecnologías de Información y Comunicación.- Para su conocimiento.

MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“Forense Digital: Cadena de Custodia en casos de Almacenamiento en Nube”

Trabajo final del Diplomado
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Víctor Manuel Gómez Flores

Ciudad de México, noviembre, 2023.

CONACYT

INFOTEC POSGRADOS

Forense Digital: Cadena de Custodia en casos de Almacenamiento en Nube

Digital Forensics: Chain of Custody in Cloud Storage Cases

Victor Manuel Gomez Flores*

RESUMEN

EL SIGUIENTE ARTICULO TIENE COMO OBJETIVO BRINDAR AL LECTOR UNA GUÍA SOBRE LOS ELEMENTOS QUE DEBEN SER CONSIDERADOS DENTRO DE LA CADENA DE CUSTODIA EN CASOS DE FORENSE DIGITAL DE DATOS ALMACENADOS EN NUBE Y QUE SERÁ PARTE DE UN DICTAMEN PERICIAL PARA SER ENTREGADO A AUTORIDADES JUDICIALES O REGULATORIAS COMPETENTES EN MÉXICO.

LA RECOLECCIÓN DE PRUEBAS DIGITALES HA EVOLUCIONADO EN FUNCIÓN DE LOS DIVERSOS DISPOSITIVOS CONECTADOS A INTERNET Y DE LA ADOPCIÓN DE MÚLTIPLES TECNOLOGÍAS COMO LO SON LOS SISTEMAS DE CÓMPUTO BASADOS EN NUBE PÚBLICA Y PRIVADA QUE HAN INCREMENTADO SU POPULARIDAD EN DIVERSAS SOLUCIONES TECNOLÓGICAS; LAS SOLUCIONES DE ALMACENAMIENTO

ABSTRACT

The following article aims to provide the reader with a guide on the elements that should be considered in cases of digital forensics of data stored in the cloud and involving a chain of custody that will be part of an expert opinion to be delivered to competent judicial or regulatory authorities in Mexico.

The collection of digital evidence has evolved according to the various devices connected to the Internet and the adoption of multiple technologies such as computing systems based on public and private cloud that have increased their popularity in various technological solutions, cloud-based storage solutions present challenges for the area of digital forensics, due to the volatility of digital evidence, proving its existence and proper handling presents several challenges during the presentation of subject matter expert opinions.

Knowledge of the phases and the various elements of the chain of custody to be documented by professionals involved in the computer forensics field will help reduce errors and safeguard digital evidence, thus increasing the

* https://orcid.org/0009-0008-4833-1163

BASADAS EN NUBE PRESENTAN RETOS PARA EL ÁREA DE FORENSE DIGITAL, DEBIDO A LA VOLATILIDAD DE LA EVIDENCIA DIGITAL, DEMOSTRAR SU EXISTENCIA Y CORRECTO MANEJO PRESENTA DIVERSOS RETOS DURANTE LA PRESENTACIÓN DE DICTÁMENES PERICIALES.

EL CONOCIMIENTO DE LAS FASES Y LOS DIVERSOS ELEMENTOS A DOCUMENTAR DE LA CADENA DE CUSTODIA POR PARTE DE LOS PROFESIONALES INVOLUCRADOS EN EL ÁMBITO DE CÓMPUTO FORENSE AYUDARÁ A REDUCIR ERRORES Y A SALVAGUARDAR LA EVIDENCIA DIGITAL, INCREMENTANDO ASÍ LA POSIBILIDAD DE QUE LA EVIDENCIA SEA CONSIDERADA COMO LEGÍTIMA Y AUTÉNTICA ANTE LA AUTORIDAD EN PROCEDIMIENTOS JUDICIALES Y REGULATORIOS.

PALABRAS CLAVE: nube, forense digital, nube pública, DFIR, respuesta a incidentes, pericial, cadena de custodia

likelihood that the evidence will be considered legitimate and authentic before the authority in judicial and regulatory proceedings.

KEYWORDS: cloud, cloud computing, difr, incident response, digital forensics, chain of custody

1. Introducción

Los sistemas y aplicaciones basadas en nube presentan muchas ventajas sobre los sistemas tradicionales de cómputo, como compartición de recursos y rápida implementación de infraestructura en menos tiempo.

Estas ventajas permiten que diversos sistemas computacionales sean diseñados considerando al almacenamiento en la nube como parte de los componentes de la arquitectura que permitirán el funcionamiento del sistema con diferentes finalidades, el uso de nube extiende la posibilidad de nuevos funcionamientos como trabajo colaborativo o en tiempo real sin importar la ubicación geográfica de los usuarios.

Estas ventajas van de la mano con el tipo de almacenamiento, en los últimos años se ha incrementado el uso de la nube para esta finalidad, en diversas soluciones entre las que destacan el uso del protocolo de almacenamiento tipo S3 asíl como las soluciones de almacenamiento en frio para uso de históricos.

Este incremento de uso va de la mano con la necesidad de atender diversos incidentes de ciberseguridad que incluyen procesos legales que involucran al peritaje digital y estos siguen siendo un reto para el área de forense digital, principalmente porque no hay una evidencia física que manipular o resguardar, solo el acceso lógico a los datos.

El diseño de los componentes de la Nube computacional ocasiona que los elementos a ser considerados como evidencia digital sean volátiles, pues pueden desaparecer en cualquier momento, adicionalmente que el modelo de cómputo en la Nube está basado en recursos compartidos por diferentes usuarios o entidades, esto implica un reto, al demostrar que la evidencia presentada es auténtica e integra.

Relacionado a este punto tenemos a la cadena de custodia que es el proceso más importante y al mismo tiempo crítico durante la documentación de las pruebas en los procesos legales; el término “cadena de custodia” se refiere al *orden en el que se obtuvieron y gestionaron las pruebas durante la investigación de un caso en particular* (Longley, 2022), cuando un caso forense digital implica cadena de custodia es necesario determinar su inicio y fin, pues no hay documentos de cadena de custodia abiertos infinitamente (Houck, Crispino, & McAdam, 2017)

Una parte crítica del dictamen pericial radica en este documento, los elementos técnicos y documentales que son exigidos y que le dan validez ante un proceso legal o regulatorio se pueden cumplir con el formato propuesto más adelante, actualmente existen modelos que son sugeridos por el Estado en sus diferentes dependencias judiciales y legales, que han sido diseñados con los elementos de evidencia digital tradicional (discos duros, memorias USB, celulares, CD-ROMs, etcétera) pero que no es posible ajustar con facilidad ante casos que involucren almacenamiento en la nube, pues en estos casos el paradigma de acceso a la información y documentación de los metadatos de la nube cambia así́ como el número de responsables con acceso a la evidencia vía el proveedor de nube (*Cloud Service Provider*, CSP).

Hoy en día es posible dar una solución gracias a que existe una participación madura por parte de los proveedores de nube (*CSP*) que ofrecen diversos procesos y soluciones técnicas que permiten dar seguimiento y trazabilidad a los movimientos relacionados a la evidencia digital para garantizar la integridad y confidencialidad de los datos obtenidos.

2. Problemática actual

La cadena de custodia *permite demostrar la integridad, autenticidad, manejo y trazabilidad de una pieza de evidencia* (Devesh Banwani, 2021), así mismo este

documento es creado con un fin legal, pues las personas involucradas en custodiar evidencia puedan ser reconocidas como testigos o responsables de la misma durante un proceso legal en caso necesario, por esta razón se sugiere crear una cadena de custodia de la evidencia digital sin importar si el caso tendrá repercusiones legales o regulatorias en México.

Los sistemas de cómputo en la nube presentan diferentes retos durante la copia y presentación de la evidencia digital. En la presentación de evidencia digital de elementos tradicionales (laptops, celulares, dispositivos de almacenamiento, etcétera) usualmente se identifica a una persona como responsable del equipo de cómputo, sin embargo, en los ambientes de nube los recursos de cómputo son compartidos y separados por reglas lógicas.

Lo anterior es parte del paradigma tradicional de acceso físico a la evidencia digital el cual está sustentando en el formato de cadena de custodia, presentado el 17 de junio de 2016 *"Cadena de Custodia – Guía Nacional"* (Secretariado Ejecutivo Mexico, 2015) y presentado en el Diario Oficial de la Federación (Diario Oficial de la Federación ACUERDO A/009/15, 2015) ,en donde se expidió el *Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales* (PODER JUDICIAL DE LA FEDERACIÓN CONSEJO DE LA JUDICATURA FEDERAL, 2016)

En el desarrollo de peritajes para cómputo en la nube no existe un acceso físico a los centros de datos con la finalidad de acceder la evidencia como sucedería en un entorno tradicional, la negativa al acceso físico está documentada en los términos y condiciones de diversos proveedores de cómputo en la nube, como Amazon[1], Google[2] y Microsoft-Azure[3] ,es importante recalcar que los sistemas de cómputo en

[1] https://aws.amazon.com/compliance/data-center/controls/
[2] https://cloud.google.com/security/compliance
[3] https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

la Nube se rigen bajo *los paradigmas de la elasticidad y escalabilidad* (W. Liu, 2012),por esta razón la información alojada en la nube es almacenada en diversos equipos y regiones, por lo que pensar en una copia física tradicional es poco práctico.

Los sistemas en la nube comparten recursos físicos con diversos sistemas y plataformas, por lo que la seguridad es administrada con diversos controles lógicos en diferentes capas. Es posible documentar estos controles y realizar una analogía con la copia de información utilizada en métodos tradicionales enfocados al mundo físico.

Lo anterior presenta retos y oportunidades, que nos obligan a pensar nuevos mecanismos que permitan documentar los procesos de forense digital en los sistemas de almacenamiento en la nube y así actualizar el proceso de cadena de custodia adaptado al paradigma computacional de la nube.

El proceso de cadena de custodia enfocado a computo en la nube es clave, ya que este proceso es fundamental para dar certeza científica y jurídica de que la *evidencia ha sido gestionada de una manera adecuada y garantizar la calidad e integridad de la prueba* (Vazquez, 2022).

Los procesos de copia, aseguramiento y preservación de la información contenida en sistemas de almacenamiento en la nube dependerán de diversos factores y están diseñados al tipo de nube y al proveedor de esta, sin embargo, lo que se busca es *garantizar que la información fue recolectada y documentada de manera adecuada para preservar los principios del manejo de evidencia digital* (Ieong, 2006).

Se busca que tras el aseguramiento de la evidencia se realicé una explicación clara y sin exceso de jerga técnica que permita a jueces y autoridades judiciales entender la validez de la prueba sin abrumarse por términos técnicos que demeriten la claridad legal de la prueba y puedan ser utilizados en contra del equipo que ofrece la prueba como ha sucedido en famosos casos como *ART+COM vs Google* (United States Court of Appeals, Federal Circuit., 2017) y *Google vs Oracle* (Carlisle, 2021) dónde el exceso de datos técnicos favoreció al equipo legal contrario.

2.2 Casos típicos de peritaje en cómputo en la nube:

Aunque usualmente no existen casos idénticos en el rubro legal o del peritaje en Informática, podemos hablar de diversos tipos de casos relacionados al almacenamiento de información en la nube que pueden ser atendidos con un peritaje adecuado:

- Compromiso (ciberataque) de instancia de almacenamiento en la nube.
- Publicación no autorizada de información privada en entornos de nube.
- Malas prácticas en la configuración de sistemas de almacenamiento en la nube.

3. Bases teóricas

Para el desarrollo del modelo de peritaje para sistemas de almacenamiento en la nube, se consideraron diversos documentos que darán las bases legales en el entorno México):

1. Manual de Prueba Pericial, Carmen Vázquez, Suprema Corte de Justicia de la Nación, 2022

2. DOF – Sobre Guía de Cadena de Custodia junio 2017
3. Evidencia científica, Suprema Corte de Justicia de la Nación, 2022
4. Documentación de cadena de custodia del sector tecnológico:
    a. ISO 22095:2020*, Chain of custody, General terminology, and models*
    b. Norma Mexicana NMX-I-289-NYCE-2016, Tecnologías De La Información-Metodología De Análisis Forense De Datos Y Guías De Ejecución
    c. CISA Insights: *Chain Of Custody And Critical Infrastructure Systems* (CISA, s.f.)
5. Recursos técnicos de los proveedores de nube (*CSP*) más representativos:
    a. Microsoft: *Computer forensics chain of custody in Azure* (Microsoft Azure, 2023)
    b. Amazon AWS: *Digital Evidence Archive on AWS* (Archivo de pruebas digitales en AWS , 2023)
    c. Google GCP: *Cloud Audit Logs* (Descripción general de los registros de auditoría de Cloud, 2023)
6. Guías, casos y procedimientos del gobierno de Estados Unidos, (Departamento de Justicia):
    a. Guiding Principles on Cloud Computing in Law Enforcement, (International Assoc of Chiefs of Police, 2015)
    b. *CloudAct* (Criminal Division - US Deparment of Justice , 2023)

4. Metodología

Para el proyecto de investigación que se presenta, se empleó un método deductivo y de análisis, el cual tomó en consideración la información pública disponible en los portales de documentación de los principales proveedores de servicios de Nube Pública como: Amazon AWS, Google Cloud Storage y Microsoft Azure Storage con

la finalidad de analizar las políticas y controles de privacidad que estos brindan, dicha información se organizará a través de esquemas de control que permitan su comparación y revisión pormenorizada, con la finalidad de identificar elementos comunes y divergentes.

Estos elementos que son revisados desde un trabajo de gabinete contrastando con los elementos focalizados de la normativa mexicana como:

1. El Código Penal Federal.
2. El Código Nacional de Procedimientos Penales.
3. La Guía Nacional de Cadena de Custodia.
4. El Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.
5. La Norma Mexicana NMX-I-289-NYCE-2016, referente análisis forense digital.

De la misma forma, fueron revisados expedientes y las resoluciones de autoridades jurisdiccionales, criterios de la Suprema Corte de Justicia de la Nación y sentencias obtenidas a través de solicitudes públicas de información, referentes a casos de extracción de datos en medios digitales y dictámenes forenses digitales públicos.

Es conveniente efectuar el análisis de casos concretos cuya relevancia mediática ha contribuido a conocer qué actores y activos digitales estuvieron involucrados, así como las determinaciones de las autoridades. La revisión de notas de prensa también es parte del análisis realizado, ya que permitió ubicar datos de contexto y seguimiento de acciones que carecen de publicidad, para lo cual se efectuó la selección de un caso particular y la disección de los elementos técnicos normativos intervinientes.

Esto tiene como objetivo ubicar qué elementos son requeridos normativamente en la valoración de pruebas periciales en el contexto digital.

A través de un ejercicio de selección, fue posible ubicar los elementos mínimos indispensables que un dictamen pericial (incluido la cadena de custodia) debe contener para aportar elementos técnicos y jurídicos relevantes ante las autoridades ministeriales y judiciales en el proceso de una investigación relacionada con delitos cometidos en el contexto digital en la nube.

Finalmente, se incluyen recomendaciones basadas en las mejores prácticas internacionales en forense digital, acudiendo a la revisión de marcos de referencia técnica y jurídica en escenarios internacionales.

5. Propuesta de solución del problema

Como hemos mencionado con anterioridad, la computación en la nube ofrece diversas posibilidades por los múltiples servicios y modalidades de contratación (dicha oferta crece exponencialmente debido al ajuste que cada *proveedor de servicios de nube (CSP)* (DiMaria, 2020) realiza en términos de competencia del mercado, la facilidad de uso durante la implementación y el rápido crecimiento ha permitido *que muchas organizaciones sean víctimas de ataques por su alta exposición a Internet* (Culafi, 2023).

5.1 El reto del forense digital en ambientes de Nube vs el computo tradicional

Los entornos de cómputo en la nube dificultan el acceso a diversos componentes de evidencia, pues para una adquisición completa en muchas ocasiones se requiere cooperación del proveedor de servicios de nube, por la segregación de privilegios, debido a que normalmente los entornos de nube son compartidos con otros clientes y separados por reglas lógicas así como la posibilidad de “congelar” la evidencia, mediante la creación de imágenes forenses digitales, que solo son posibles con el acceso completo al entorno de nube del sistema analizado.

En los entornos de nube es necesario recalcar que existen diversas arquitecturas y modelos de servicio: *IaaS, PaaS, SaaS y CaaS* cada uno posee diversos retos al momento de realizar investigaciones forenses, siendo los entornos *SaaS* los de mayor demanda en la cooperación con el proveedor (por ejemplo, para obtener alguna bitácora del sistema operativo).

En los ambientes de cómputo físico es posible realizar un apagado y aislamiento absoluto de equipos, en el caso de nube no es posible realizarlo tan fácil, debido a

que la nube es sinónimo de multi arrendatarios, donde varios clientes comparten grandes porciones de infraestructura.

Dicho de otra manera, en el ambiente de cómputo en la nube está solo proporciona datos de manera lógica y en el ambiente computacional físico tradicional proporciona acceso a diversos componentes de Hardware y a los datos que se almacenan en el mismo.

5.2 El papel de los proveedores de cómputo en la nube como facilitadores del cómputo forense.

Es posible realizar una adaptación al “nuevo mundo” del cómputo en la nube y afrontar los retos del forense digital. Como se menciona, el almacenamiento en nube es sinónimo de solo datos, y al mismo tiempo estos pueden ser increíblemente volátiles, pues el almacenamiento en nube no ofrece persistencia real de los datos, es decir un dato puede estar almacenado en varios lugares y tras el borrado o modificación es difícil rescatar la información de la infraestructura de hardware.

Afortunadamente hay diversos modos de mitigar estas carencias de persistencia y alta volatilidad, y que son controles compatibles con la mayoría de los proveedores de nube, como por ejemplo el acceso a bitácoras de seguridad del proveedor (CSP) y la posibilidad de crear copias exactas de la información contenida en la nube para su posterior descarga y análisis.

Es posible que el proveedor (CSP) proporcione acceso a estás bitácoras a través de una base de datos de sincronización continua (no modificable), accesible por *API (Application Program Interface)* (Wikipedia, 2023), está base de datos funciona como una bitácora de navegación marítima o área que contiene los detalles de

modificación de las estructuras de datos, cambios en la red o registros en el sistema operativo y de la propia nube, todo cambio realizado se verá reflejado en está bitácora y no es posible realizar una modificación a la misma.

Otro aspecto importante durante a adaptar como se ha mencionado es la cadena de custodia, este componente es crítico para la creación de todo dictamen pericial, en un ambiente de cómputo tradicional es trivial mantener un histórico de acceso a la evidencia y gestión de esta, en el caso de la nube se tiene una dependencia absoluta del proveedor y del administrador técnico de la misma.

Este entorno de multi responsabilidad puede dar pie a corrupción durante el caso al permitir confabular entre diversos actores del caso, por lo que documentar como se realizó el acceso y que mecanismos del proveedor fueron utilizados (como el acceso a las bitácoras de seguridad de la nube vía *API*) para evitar que terceros puedan corromper la evidencia.

En resumen, en la nube, no hay infraestructura física accesible, sólo acceso lógico, datos por analizar, proteger y recolectar con ayuda del propio proveedor (CSP) y el acceso a bitácoras de la nube mediante *API* para garantizar una mayor cobertura de evidencia y esto hace que mantener la cadena de custodia sea un reto mayor.

5.3 La cadena de custodia, como punto central en el éxito del dictamen forense.

La preparación de un dictamen forense digital involucra múltiples procesos (Mansilla Moya & Mansilla Moya, 2022) donde destaca la administración de la evidencia, para asegurar la integridad de la información recopilada, al dar certeza sobre quién

accedió a los datos de un caso específico y la forma en que fue utilizada durante el proceso de análisis.

Ante las autoridades judiciales y entidades regulatorias, los peritos tienen que garantizar que las pruebas que aportadas son válidas durante su ciclo de vida que va desde el levantamiento/copia, el análisis, almacenamiento, resguardo, trazabilidad y control de acceso a las mismas (restringido solo a los autorizados).

Todo este proceso queda registrado en el formato de cadena de custodia, que debe cumplir con los elementos anteriores para poder considerar a la evidencia como válida y auténtica ante autoridades judiciales o regulatorias.

De acuerdo con el artículo 227 del Código Nacional de Procedimientos Penales, la cadena de custodia se define como: *"La cadena de custodia es el sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo, hasta que la autoridad competente ordene su conclusión.*

Con el fin de corroborar los elementos materiales probatorios y la evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, empaque y traslado; lugares y fechas de permanencia y los cambios que en cada custodia se hayan realizado; igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos." (CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES, 2023).

En México se encuentra documentada bajo el formato de Guía Nacional de Cadena de Custodia (SEGOB, 2015) y reconocida como parte clave dentro de la

presentación de pruebas (Vazquez, 2022) así como en diversas tesis de la SCJN *(XXVII.1o.5 P (10ª))* (Gaceta del Semanario Judicial de la Federación, 2018) y en diversos criterios de la *SCJN* (Criterios del Poder Judicial de la Federación : en materia de protección de datos personales y otros conceptos relacionados, 2018) dónde se reconoce la importancia de un correcto manejo de evidencia digital.

Estos apuntes nos permiten ratificar la sólida documentación que existe sobre el proceso de cadena de custodia en el ambiente de criminalística tradicional, revisemos entonces su adaptación al ambiente de cómputo en la nube.

5.4 La cadena de custodia con aplicación a ambientes en cómputo en la Nube

En entornos de nube, el uso de la cadena de custodia implica una mayor complejidad, por diversos factores mencionados inicialmente, destacando el número de involucrados que podrían tener acceso a las evidencias en sistemas productivos: usuarios, administradores técnicos, y el propio proveedor de la nube (*CSP*); todos tienen acceso a los datos en mayor o menor medida dependiendo su rol. Al igual que las investigaciones digitales tradicionales, el objetivo final es conservar copias inalteradas de los datos y garantizar su integridad mediante algoritmos de integridad *Hash*.

La documentación de la cadena de custodia tiene que adaptarse a las estructuras de cómputo en la nube. En una investigación tradicional, existen elementos físicos probatorios (como discos duros, memorias USB, teléfonos, etcétera) y los datos que residen en estos medios. En cambio, en los entornos de almacenamiento en nube sólo hay datos que formaran la evidencia final y metadatos de esta, lo que incrementa el reto en la gestión documental de la cadena de custodia.

La propuesta de solución radica en el modelo de multi responsabilidades durante la creación de la cadena de custodia, la recolección y documentación de diversos metadatos del ambiente de nube y el uso de algoritmos Hash para garantizar la inalterabilidad de los datos recolectados durante todo el proceso del caso o incidente atendido.

Se busca que durante el dictamen final el formato de cadena de custodia cumpla con los lineamientos de las tesis de la SCJN (previamente citadas) y el Formato Nacional de Cadena de Custodia.

5.5 Propuesta de elementos en cadena de custodia para ambientes en nube

Elementos por incluir (metadatos):

- **Contexto del sistema:**
    - **Descripción de las estructuras de almacenamiento del sistema** incluyendo tipo de datos que se están almacenando (datos personales, salud, financieros, secreto industrial, públicos, etcétera) *para determinar el impacto del incidente* (Suprema Corte de Justicia de la Nación, 2018).
    - **Dirección(es) IP origen:** Los ambientes de nube tienden a tener diferente comportamiento tras acceder desde diversos países o lugares de red, se documentará que dirección IP fue utilizada para la prueba.
    - **Nombre del patrocinador del servicio:** Quién es el responsable de financiar el servicio de nube.
    - **Administradores técnicos:** Nombre completo y especificar el esquema de permisos y detalle técnico dentro de la nube.

- **Cuenta de super-usuario:** Especificar que cuenta(s) o *API tokens* fueron utilizados para realizar la extracción de los datos.
- **Metodología utilizada:** Indicar los procedimientos para generar la copia forense del archivo, (cada fabricante de nube tiene su propio procedimiento bien definido)
    - **Azure:** Azure Blob Storage.
    - **Amazon AWS:** Control de versiones S3, AWS CloudTrail.
    - **Google GCP:** Bitácoras de auditoría en el entorno GCP de almacenamiento y gestión de identidades (IAM).
- **Nombre del archivo:** Especificar cual era el nombre público y nombre interno (en las estructuras de la nube) del archivo.
- **Ruta del archivo:** Indicar la ruta absoluta del archivo dentro de la estructura del proveedor de nube.
- **Registro SHA256:** Resultado de la firma hash de cada elemento almacenado durante el caso o las imágenes forenses resultades.
- **Tamaño del archivo(s).**
- **Fecha de inicio y fin de adquisición de la evidencia**
- **Registro documental de la existencia en Internet**: En sistemas de almacenamiento públicos (expuestos a internet), demostrar que esa evidencia existía y era públicamente accesible. Esto se puede llevar a cabo utilizando los sitios como Archive.org y Archive.is o soluciones comerciales parecidas (como AXIOM evidence.com).
- **Ubicaciones geográficas:** El almacenamiento en nube no posee una característica de persistencia real, esto sumando a temas regulatorios obliga a documentar las regiones geográficas donde está siendo almacenada la

información, el modelo de negocio de la nube se basa en el acceso desde diferentes regiones, de ahí su importancia documental.

- **Personal responsable de la copia:** Indicar quienes resguardarán la información recolectada y el medio de almacenamiento.
- **Número de evidencia:** Número secuencial que permita identificar la evidencia.

6. Discusión de la propuesta

En los últimos años, los procesos y componentes de ciberseguridad en la nube han madurado significativamente, los proveedores de servicios de nube (*CSP, Cloud Service Provider)* han invertido en nuevas tecnologías para mejorar la seguridad de sus plataformas incluyendo módulos como:

- Implementación de tecnologías de cifrado para proteger datos en tránsito (red) y en reposo (almacenamiento).
- Automatización: Que permiten que la construcción de arquitecturas con componentes establecidos por él CSP sea ágil y con características de seguridad por defecto.
- Nuevos procesos y servicios: Muchos procesos tenían que ser diseñados por los clientes de las plataformas de nube, actualmente los CSP ofrecen diversas soluciones y procesos previamente construidos que ayudan a que los clientes seleccionen y adapten a sus necesidades (como *Playbooks* y procesos con flujos predeterminados).

En los últimos años, las técnicas de forense digital con aplicación al cómputo en la nube han experimentado una serie de mejoras importantes, impulsadas por el

aumento de la adopción de la nube en múltiples sistemas, los ciberataques a sistemas de cómputo y requisitos de reguladores de diferentes sectores.

Algunas de las mejoras más importantes incluyen: El desarrollo de nuevas herramientas y técnicas dentro del campo forense digital estás permiten a los investigadores forenses/peritos realizar análisis más completos y precisos de las evidencias digitales en la nube, así como una importante colaboración por parte de los proveedores (CSP) que permite a los forenses, peritos y autoridades obtener acceso a datos y recursos que de otro modo serían inaccesibles ahora se pueden extraer datos de múltiples servicios en la nube, incluidos *Microsoft Azure , Amazon Web Services (AWS) y Google Cloud Platform (GCP)* y realizar análisis más complejos de estos identificando comportamientos y tendencias que antes tomarían meses o no eran plausibles.

Sin embargo, a pesar de estos avances, el forense digital aplicado al cómputo en la nube sigue siendo un campo con muchos retos por delante, para fines de nuestra propuesta el más importante es comprobar la existencia de los datos dentro de las plataformas de Nube, pues la volatilidad de la evidencia y los múltiples participantes dificultan la tarea de la prueba digital.

La propuesta sugerida radica en cumplir con los lineamientos de una cadena de custodia típica enfocada al entorno digital, donde se debe garantizar que el manejo de la evidencia ha sido adecuado y que no haya alteraciones en la misma y más allá de un simple formato a modo histórico, sino que además incluya los elementos algorítmicos necesarios para garantizar la integridad de la información (el uso del algoritmo SHA256 en cada imagen generada)

Investigaciones previas en el tema (Nasreldin, El-Hennawy, Aslan3, & El-Hennawy, 2015) sugieren mecanismos de extracción de datos utilizando un modelo cliente

servidor (Prayudi & SN, 2015), donde un operador es el encargado de realizar la copia de la información así como ejecutar algoritmos de integridad sobre la evidencia adquirida y documentar manualmente todos los elementos de la infraestructura de nube involucrada en la investigación, sin embargo, en la actualidad los CSP han adaptado sus procesos y catálogo de servicios en función de las diversas necesidades en ciberseguridad y forense digital, está evolución se puede comprobar en diversas resoluciones positivas del departamento de justicia de Estados Unidos (justice.gov), por lo que la propuesta incluye la documentación de estos procesos en el lado del CSP, desde la extracción hasta la comprobación de integridad con algoritmos y una segunda comprobación por parte del perito en sus instalaciones.

6.1 Antecedentes en México: Modelos de cadena de custodia y regulación asociada.

La propuesta incluye los 3 componentes legislativos principales relativos al tema de cadena de custodia, empezando por el código nacional de procedimientos penales dentro de su *Título III (Etapa de Investigación) y Capítulo III (Técnicas de Investigación)* (DOF 25-04-2023, 2023) en donde se define los elementos de la cadena de custodia, el personal que puede ser responsable en ella, así como los elementos indispensables en la cadena de custodia: Identificación, recolección, preservación, embalaje y traslado (cubierto en los artículos 227 y 228 respectivamente) así como el acuerdo A/009/15 (SEGOB - Diario Oficial de la Federación, 2015) , donde es especificado los sujetos legales y la delimitación de sus funciones y finalmente *el "Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales"* (SEGOB - Diario Oficial de la Federación, 2016)

6.2 Otras propuestas analizadas

Existen diversos trabajos enfocados a la *nueva cadena de custodia con el uso de tecnologías de bloque en nube pública* (Chopade, Khan, Shaikh, & R. Pawar, 2019), donde en términos generales *se documenta la existencia de componentes de la nube en un cadena de bloques* (D. Tosh, Liang, Kamhoua, & Njilla, 2019), haciendo que está cadena de custodia sea no repudiable, sin embargo, en estas propuestas se protege la cadena de custodia de una manera digital y no se incluye al proveedor *(CSP)* como parte del proceso de extracción de evidencia y no se consideran los elementos legales para ser incluida como evidencia solida ante tribunales y reguladores.

El papel de los proveedores de nube (CSP) ha permitido que muchas de las propuestas pasadas sean innecesarias, pues al existir la posibilidad de acceder a una base de datos no modificable vía API o por un portal del proveedor, dicha base puede incluir toda la información de acceso de lectura y escritura dentro de la instancia, es decir los datos del sistema o solución analizada, con esto el investigador forense digital requiere el acceso a esta base de datos para continuar su labor de análisis de la misma, y posteriormente realizar la copia de la evidencia mientras documenta todo en el proceso.

6.3 Elementos de fortaleza de la propuesta sugerida

Cómo se ha comentado previamente, en los entornos de nube no existe un acceso directo a la información sin ser auxiliado por un proveedor de servicios (CSP) y sin importar el tipo de modelo que este ofreciendo esta nube (IaaS, PaaS, SaaS y CaaS), por lo que existen elementos de suma importancia para qué la cadena de custodia sea considerada como válida y como una prueba de evidencia sólida, siguiendo elementos de integridad y trazabilidad de la información, apego a los elementos legales Mexicanos, la documentación de metadatos de la infraestructura

de nube con el soporte del CSP y el listado de las recomendaciones generales en el tratamiento de evidencia en nube computacional

6.4 Posibles impedimentos de la propuesta

La documentación de los metadatos propuestos dentro de la cadena de custodia dependerá principalmente del acceso a la instancia dentro de la nube donde radique el sistema a analizar, para garantizar un mayor acceso se requiere la cooperación del proveedor de nube (CSP) dicha cooperación dependerá principalmente de dos factores:

1. ¿Quién es responsable de la instancia? Si este es un cliente directo con el que el investigador forense esté colaborando será más simple acceder a los recursos necesarios, si este no es el caso, por ejemplo, al documentar un sistema de un tercero, los metadatos documentados serán menores y se deberá incrementar el número de evidencias a documentar para crear un dictamen pericial sólido.
2. Localización de la instancia en países restringidos al investigador forense: De la mano al punto anterior algunos proveedores restringen el acceso a instancias de nube que se encuentran dentro de países con *políticas restrictivas de privacidad o acceso a la información* (Eustice, s.f.)
3. Modelos de nube CaaS: Las instancias computacionales basadas en contenedores presentan un reto importante pues su infraestructura de alta disponibilidad es gran medida volátil debido a que los servidores y sistemas operativos de cada contenedor se crean y destruyen con alta velocidad según las necesidades de elasticidad del sistema, por lo que existe una baja probabilidad de obtener evidencia de los datos generador dentro de cada servidor y la única posibilidad de probar la existencia de datos será utilizando la documentación de la bitácoras inmutables del proveedor de nube (CSP).

7. Conclusión

El proceso de cadena de custodia es fundamental durante el proceso del desarrollo del dictamen pericial, la correcta ejecución y documentación es clave para asegurar la calidad del documento, mientras más datos sean documentados se permitirá preservar la volatilidad de la evidencia, este es el punto más sobresaliente hablando en términos de análisis al almacenamiento en nube computacional.

Actualmente los proveedores de nube (CSP) desarrollan un papel fundamental en el desarrollo de la cadena de custodia, debido a que proporcionan mecanismos técnicos que permiten realizar una extracción de evidencia y su correcta documentación de los metadatos resultantes, garantizando la integridad de la información y permitiendo que los datos sean resguardados, protegiéndolos así de las características de volatilidad propias de los sistemas computacionales en nube, adicionalmente proveen bitácoras inmutables con múltiple información valiosa para la cadena de custodia, como lo es eventos de auditoría y uso de la nube, su lectura es accesible mediante API, lo que garantiza trazabilidad.

La nube computacional, y su proceso de documentación como primer respondiente es un aspecto nuevo para equipos técnicos de sistemas y equipos legales, por lo que un trabajo de concientización a estas áreas es importante para su correcto entendimiento e interpretación de las analogías con el mundo digital físico tradicional.

En México no existen muchos casos públicos documentados del tipo legales-técnico esto se debe a que no hay una transparencia real de los casos juzgados que involucran un tema digital vs los casos juzgados que se pueden analizar en sitios como justice.gov del gobierno estadunidense.

8. Bibliografía

CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES. (25 de 04 de 2023). *DOF 25-04-2023*. Obtenido de https://www.diputados.gob.mx/: https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf

Carlisle, M. (6 de Abril de 2021). *How Google's Big Supreme Court Victory Could Change Software Forever*. Obtenido de Time.com: https://time.com/5952718/google-oracle-supreme-court/

CISA. (s.f.). *CHAIN OF CUSTODY AND CRITICAL INFRASTRUCTURE SYSTEMS*. Obtenido de CISA.gov: https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf

Longley, R. (13 de Julio de 2022). *Chain of Custody*. Obtenido de https://www.thoughtco.com/: https://www.thoughtco.com/chain-of-custody-4589132

Chopade, M., Khan, S., Shaikh, U., & R. Pawar. (2019). Digital Forensics: Maintaining Chain of Custody Using Blockchain," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud. *IEEE International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 744-747.

Criminal Division - US Deparment of Justice . (Octubre de 2023). Obtenido de CLOUD Act Resources: https://www.justice.gov/criminal/cloud-act-resources

Culafi, A. (18 de Abril de 2023). *Mandiant: 63% of breaches were discovered externally in 2022*. Obtenido de TechTarget: https://www.techtarget.com/searchsecurity/news/365535068/Mandiant-63-of-breaches-were-discovered-externally-in-2022

Archivo de pruebas digitales en AWS . (Octubre de 2023). Obtenido de Amazon AWS: https://aws.amazon.com/solutions/implementations/digital-evidence-archive-on-aws/

D. Tosh, S. S., Liang, X., Kamhoua, C., & Njilla, L. L. (2019). Data Provenance in the Cloud: A Blockchain-Based Approach," in IEEE Consumer Electronics Magazine. *IEEE Consumer Electronics Magazine*, 38-44.

Descripción general de los registros de auditoría de Cloud. (12 de Octubre de 2023). Obtenido de Google Cloud: https://cloud.google.com/logging/docs/audit

Devesh Banwani, Y. K. (2021). Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody. *OpenAccess, 10*(3).

Diario Oficial de la Federación ACUERDO A/009/15. (30 de 01 de 2015). Obtenido de ACUERDO A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia: https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5381699

DiMaria, J. (30 de Abril de 2020). Obtenido de https://cloudsecurityalliance.org/blog/2020/04/30/what-is-a-cloud-service-provider/

Eustice, J. C. (s.f.). *Understand the intersection between data privacy laws and cloud computing* . Obtenido de Legal Thomson Reuters: https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing

Gaceta del Semanario Judicial de la Federación. (09 de Febrero de 2018). *Tesis: XXVII.1o.5 P (10a.)*. Obtenido de SCJN - Tesis Aislada: https://bj.scjn.gob.mx/doc/tesis/ovZrMHYBN_4klb4HhIIN/%22Computadoras%22

Houck, M., Crispino, F., & McAdam, T. (2017). *The Science of Crime Scenes, 2nd ed.* Cambridge, MA, USA: Scholarly Press.

Ieong, R. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 29-36.

International Assoc of Chiefs of Police. (2015). *Guiding Principles on Cloud Computing in Law Enforcement*. Obtenido de US - Office of Justice Programs: https://www.ojp.gov/ncjrs/virtual-library/abstracts/guiding-principles-cloud-computing-law-enforcement

Mansilla Moya, M. M., & Mansilla Moya, M. (30 de 09 de 2022). Cadena de Custodia 2.0. *Revista Mexicana De Ciencias Penales*, 47-62.

Microsoft Azure. (2023). *Computer forensics chain of custody in Azure*. Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/azure/architecture/example-scenario/forensics/

Nasreldin, M. M., El-Hennawy, M., Aslan3, H. K., & El-Hennawy, A. (2015). Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing. *IJCSI International Journal of Computer Science Issues,*, 153-160.

PODER JUDICIAL DE LA FEDERACIÓN CONSEJO DE LA JUDICATURA FEDERAL. (Junio de 2016). *CONSEJO DE LA JUDICATURA FEDERAL.* Obtenido de LINEAMIENTOS PARA LA OBTENCIÓN Y TRATAMIENTO DE LOS RECURSOS INFORMÁTICOS Y/O EVIDENCIAS DIGITALES: https://www.cjf.gob.mx/resources/index/infoRelevante/2016/pdf/LINEAMIENTOS_OBTENCION_TRATAMIENTO_RECURSOSINFORMATICOS.pdf

Prayudi, Y., & SN, A. (03 de 2015). Digital Chain of Custody: State of the Art. *International Journal of Computer Applications*.

Secretariado Ejecutivo Mexico. (28 de Octubre de 2015). *Cadena de Custodia Guia Nacional.* Obtenido de Secretariado Ejecutivo Mexico: https://www.secretariadoejecutivo.gob.mx/docs/pdfs/normateca/protocolos/VF10GuaNacionalCadenadeustodia28-10-2015.pdf

SEGOB - Diario Oficial de la Federación. (02 de 12 de 2015). *ACUERDO A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia.* Obtenido de SEGOB DOF: 12/02/2015:

https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015#gsc.tab=0

SEGOB - Diario Oficial de la Federación. (17 de 06 de 2016). *ACUERDO General del Pleno del Consejo de la Judicatura Federal, por el que se expide el Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales.* Obtenido de SEGOB - DOF 17/06/2016: https://www.dof.gob.mx/nota_detalle.php?codigo=5441707&fecha=17/06/2016#gsc.tab=0

SEGOB. (26 de 11 de 2015). *EXTRACTO de la Guía Nacional de Cadena de Custodia.* Obtenido de SEGOB Diario Oficial de la Federación: https://www.dof.gob.mx/nota_detalle.php?codigo=5417232&fecha=26/11/2015#gsc.tab=0

Suprema Corte de Justicia de la Nación. (2018). *Criterios del Poder Judicial de la Federación : en materia de protección de datos personales y otros conceptos relacionados.* Ciudad de mexico, Mexico.

United States Court of Appeals, Federal Circuit. (20 de Octubre de 2017). *United States Court of Appeals, Federal Circuit.* Obtenido de United States Court of Appeals: https://caselaw.findlaw.com/court/us-federal-circuit/1878050.html

Vazquez, C. (2022). *Manual de Prueba Pericial.* Suprema Corte de Justicia de la Nación. Obtenido de Vázquez, C. (2022). Manual de Prueba Pericial, p. 285. https://www.scjn.gob.mx/derechos-humanos/sites/default/files/Publicaciones/archivos/2022-04/MANUAL%20DE%20PRUEBA%20PERICIAL_DIGITAL.pdf

W. Liu. (2012). Research on cloud computing security problem and strategy. *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 10.1109*, 1216-1219.

Wikipedia. (15 de Noviembre de 2023). *https://en.wikipedia.org/wiki/API*. Obtenido de Wikipedia: https://en.wikipedia.org/wiki/API