Evidencia Digital en Entornos Cloud Native: Procedimientos forenses para arquitecturas distribuidas

Digital Evidence in Cloud Native Environments: Forensic procedures for distributed architectures

AUTOR:

Torres Ponce, Mariano Enrique
Abogado y Especialista en Derecho Informático

RESUMEN

La tecnología brinda nuevas soluciones y los profesionales deben adaptarse a estos cambios para poder hacer su trabajo eficientemente. El conocimiento adquirido se va volviendo obsoleto y nos presenta nuevos escenarios a resolver. La prueba digital cambia cuando los sistemas no están centralizados y son autosuficientes, sino que funcionan con contenedores que duran segundos y servicios repartidos por distintos países. Por esto podemos afirmar que recolectar evidencia digital se vuelve un desafío. Para entender cómo abordarlo, revisamos decenas de artículos recientes en Scopus, Web of Science e IEEE Xplore. Con ese material armamos una taxonomía de artefactos probatorios, ordenados por capa de infraestructura y duración. Propusimos métodos de captura que priorizan logs en JSON, trazas con OpenTelemetry y snapshots versionados en Git. El

objetivo no es repetir manuales, sino mostrar qué conviene documentar, cuándo y con qué nivel de detalle. Combinamos teoría con herramientas prácticas, vinculando los artefactos al modelo de servicio (IaaS, PaaS o SaaS) y a marcos como el Reglamento DORA en Europa o el NIST 800-207 en EE.UU. También diseñamos una matriz que reparte responsabilidades entre cliente y proveedor, e incluimos una plantilla de informe pericial adaptada a sistemas distribuidos. El aporte central: criterios claros y herramientas útiles para auditar incidentes sin depender de infraestructuras persistentes. Cerramos con una mirada a lo que viene: automatización forense con IA en la nube y los dilemas éticos que plantea.

ABSTRACT

Technology continuously generates new solutions, and professionals must adapt in order to perform their work efficiently. Acquired knowledge quickly becomes obsolete, giving rise to novel scenarios that demand new approaches. Digital evidence is transformed when systems are no longer centralized and persistent but instead rely on ephemeral containers and services distributed across multiple jurisdictions. Collecting such evidence therefore emerges as a significant challenge. To explore how this challenge can be addressed, we reviewed dozens of recent articles indexed in Scopus, Web of Science, and IEEE Xplore. Based on this material, we developed a taxonomy of evidentiary artifacts, organized by infrastructure layer and temporal persistence. We propose capture methods that prioritize JSON logs, OpenTelemetry traces, and versioned snapshots in Git. The aim is not to replicate procedural manuals but to highlight what should be documented, when, and with what degree of detail. We combine theoretical foundations with practical tools, linking artifacts to service models (IaaS, PaaS, SaaS) and to regulatory frameworks such as the DORA Regulation in Europe or NIST 800-207 in the United States. We also introduce a responsibility matrix between client and provider and include a forensic report template adapted to distributed systems. The central contribution is to provide clear criteria and practical tools for auditing incidents without relying on persistent infrastructures. We conclude by examining future perspectives, including forensic automation with cloud-based AI and the ethical dilemmas it raises.

PALABRAS CLAVE

Evidencia digital, cloud native, informática forense, Kubernetes, microservicios, cadena de custodia, Derecho de la informática, Gobernanza de Internet

KEYWORDS

Digital evidence, cloud native, digital forensics, Kubernetes, microservices, chain of custody, computer law, Internet governance

RESUMEN EJECUTIVO

Background: La transición a arquitecturas cloud native (basadas en contenedores efímeros, microservicios y despliegues automatizados) vuelve frágil la obtención de evidencia digital, ahora distribuida entre logs, métricas y trazas. Esto obliga a repensar observabilidad, sincronización temporal y cadena de custodia a la luz de marcos como DORA y NIST SP 800-207.

Gap: Las prácticas y herramientas forenses clásicas suponen soportes persistentes e infraestructuras centralizadas; faltan procedimientos operativos y formatos interoperables que preserven origen, contexto y cronología en entornos multi-proveedor y multi-jurisdicción, además de cláusulas contractuales que aseguren retención y exportabilidad probatoria sin romper el contexto.

Purpose: El trabajo busca ofrecer criterios y herramientas prácticas para la investigación de incidentes en entornos cloud native, mediante la construcción de una taxonomía de artefactos probatorios, el desarrollo de métodos de captura centrados en logs JSON, trazas OpenTelemetry y snapshots versionados, y la elaboración de una matriz de responsabilidades entre cliente y proveedor junto con una plantilla de informe pericial alineada a estándares y marcos regulatorios

Methodology: Revisión de decenas de trabajos (Scopus, Web of Science, IEEE Xplore); síntesis en una taxonomía por capa y vida útil; mapeo a IaaS/PaaS/SaaS y a estándares;

diseño de procedimientos de identificación, preservación, recolección y análisis para entornos efímeros; elaboración de checklist, matriz y plantilla pericial.

Results: Se obtuvo una taxonomía mínima de fuentes probatorias —logs estructurados, trazas distribuidas, métricas, artefactos de infraestructura como código y eventos de API/webhooks— junto con métodos de captura y requisitos de metadatos, sellado temporal e integridad. Se adaptaron procedimientos para entornos efímeros que priorizan la captura "en ejecución", el congelamiento del estado al declarar el incidente, la preservación de artefactos volátiles y la sincronización temporal auditable. Además, se desarrollaron instrumentos prácticos —matriz de responsabilidades en la nube, checklist de investigación y plantilla de informe pericial— alineados con estándares ISO/IEC 27037/27041/27042/27043 y marcos regulatorios como DORA, NIS2 y NIST. Finalmente, se identificaron tensiones operativas recurrentes entre privacidad y preservación, dependencia de terceros y costos de retención, así como desafíos jurisdiccionales en despliegues multi-región.

Conclusion: Los criterios clásicos no alcanzan en cloud native; investigar exige pensar en tiempo, automatización y portabilidad, con telemetría que conserve origen, secuencia y relaciones entre eventos, y con soporte legal-contractual explícito para retención y exportación. Se propone validar el enfoque con casos reales y fomentar una coordinación sostenida entre técnicos, peritos y reguladores para convertir principios en procedimientos auditables y replicables.

ÍNDICE

F.3. Consideraciones de multi-tenancy.

F.4. Documentación contractual.

G. Estándares y normas aplicables

G.1. Normas internacionales.

G.2. Marcos regulatorios europeos.

G.3. Estándares de industria.

G.4. Estándares emergentes cloud native.

H. Discusión crítica: preservación, dependencia y jurisdicción.

I. Conclusiones.

J. Bibliografía.

A. INTRODUCCIÓN

La evidencia digital atraviesa un cambio de época. Deja atrás el dominio de soportes previsibles y se produce en plataformas cloud native que automatizan despliegues, escalan en segundos y distribuyen datos entre regiones y proveedores. Este corrimiento obliga a revisar supuestos que parecían firmes: dónde reside la evidencia, quién la custodia en cada tramo, cómo se preserva su contexto y de qué modo se sostiene su validez cuando los sistemas se reconfiguran sin intervención humana (Palmer, 2001). La disciplina forense conserva sus principios; lo que cambió es el terreno donde se aplican y el ritmo al que muta.

El impacto no es solo técnico, sino que a medida que la infraestructura se describe con código y los planos de control gobiernan el estado, las huellas relevantes dejan de concentrarse en un único dispositivo y se reparten entre registros, métricas y trazas emitidas por servicios que nacen y mueren con rapidez. La cadena de custodia debe acompañar ese dinamismo de documentar origen y transformaciones, normalizar tiempos, calcular integridad en el momento de la captura y conservar metadatos suficientes para reconstruir una narrativa verificable del incidente. La automatización que aporta resiliencia también introduce riesgo probatorio si no se detiene a tiempo: puede corregir estados, rotar datos o eliminar artefactos efímeros antes de su preservación (Pichan, Lazarescu y Soh, 2015).

El campo jurídico acompaña la complejidad técnica. La residencia y la soberanía de datos dejan de ser accesorios y pasan a condicionar cada decisión de obtención y entrega y por tal motivo se necesitan acuerdos contractuales claros, plazos verificables y formatos interoperables para portar evidencia sin romper su contexto. A su vez, la cooperación entre equipos técnicos, áreas legales y reguladores se vuelve imprescindible para alinear retención, acceso y exportación con garantías de privacidad y con estándares que resistan la auditoría.

Este trabajo adopta una posición pragmática, no proponiendo reemplazar fundamentos clásicos, sino traducirlos a un ecosistema elástico y distribuido. Asumimos que la observabilidad, instrumentada con criterio, es en la actualidad la fuente primaria de artefactos probatorios y que la adquisición en ejecución, la portabilidad con metadatos mínimos y la sincronización temporal rigurosa son condiciones necesarias para sostener una narrativa técnica confiable. La validez no se asegura en un único paso, sino en una

cadena de decisiones documentadas que atraviesa diseño, operación y respuesta a incidentes. Con ese horizonte, el texto establece un lenguaje común para describir qué conservar, cómo preservarlo y con qué evidencias demostrar que el método fue adecuado a la naturaleza del entorno, sin anticipar desarrollos que se profundizan en el marco teórico.

B. MARCO TEÓRICO Y ESTADO DEL ARTE

Este capítulo ubica la prueba digital en cloud-native: conserva los principios clásicos de la disciplina, pero reinterpreta tácticas y fuentes para ecosistemas elásticos y distribuidos donde la evidencia cambia de lugar y de forma con mucha rapidez.

B.1. DE LOS FUNDAMENTOS CLÁSICOS A LO DISTRIBUIDO

La informática forense se construyó sobre un proceso nítido: identificar, preservar, analizar y presentar. Ese esquema ordenó el oficio durante décadas porque asumía persistencia, localización estable y control directo del soporte por parte del perito, desde la toma hasta el informe final (International Organization for Standardization, 2012). Ese piso no se pierde, pero hoy convive con plataformas compartidas, automatizadas y sujetas a ciclos de vida muy cortos.

Conviene entonces pensar la evidencia menos como objeto y más como estado con contexto. No alcanza con el archivo: importan la configuración efectiva, los metadatos de orquestación y relojes comparables que permitan leer una cronología consistente sin adivinar huecos ni interpolar supuestos (International Organization for Standardization, 2015). Esta mirada desplaza el foco del dispositivo aislado al ecosistema, y devuelve centralidad a la trazabilidad como condición para que el dato sea inteligible y defendible en un foro técnico o judicial.

B.2. QUÉ CAMBIA CON CLOUD NATIVE

Cloud-native no es un lugar, es una forma de construir y operar. Se apoya en contenedores, microservicios, automatización y observabilidad continua, con planos de control que materializan intención como estado del sistema en cada momento (Cloud Native Computing Foundation, 2024). En ese contexto, la evidencia aparece fragmentada y

veloz. Sin un modelo común de metadatos, la correlación se vuelve conjetura y la historia técnica pierde continuidad.

El orquestador y su plano de control pasan a ser fuente probatoria, y conviene entenderlo así desde el inicio. Manifiestos efectivos, eventos, reglas de scheduling y descripciones de recursos permiten reconstruir intención y ejecución más allá de lo que se ve en una sola instancia de servicio (Ruan, Carthy, Kechadi y Crosbie, 2011). La arquitectura de microservicios, por su parte, multiplica puntos de observación: la misma transacción puede atravesar decenas de componentes y regiones, de modo que las trazas distribuidas y los registros de API dejan de ser "complementarios" para convertirse en el hilo conductor del relato técnico (Newman, 2015).

B.3. IMPLICANCIAS PROBATORIAS Y MÉTODO

La volatilidad obliga a capturar en ejecución. Después, suele ser tarde. Por eso importan la instrumentación previa, la sincronización auditable de tiempo y el cómputo de integridad en el mismo punto de adquisición, porque ahí se juega la diferencia entre un relato verificable y una reconstrucción apoyada en supuestos. También conviene versionar y firmar manifiestos y parámetros de despliegue, para que la intención quede documentada y compare con lo efectivamente aplicado por el orquestador (Torres Ponce, 2020).

La cadena de custodia se vuelve transversal: cruza cuentas, regiones y servicios, pero debe conservar origen, contexto y verificaciones sin romper la coherencia temporal. Para distinguir qué rastro pertenece al incidente y qué al funcionamiento normal, la documentación del "estado efectivo" al momento del hecho es clave: límites de recursos, políticas de ciclo de vida, namespaces y eventos relevantes que expliquen por qué el sistema se comportó como se observó y no de otra manera.

B.4. MARCOS Y GUÍAS APLICABLES HOY

Los estándares de identificación, adquisición, preservación y análisis siguen siendo el ancla práctica. Orientan qué capturar, cuándo sellar y cómo preservar la relación dato-metadato en ambientes elásticos donde la topología cambia sin pedir permiso. A la vez, los enfoques de zero trust ordenan acceso y verificación en sistemas distribuidos, lo que impacta directo en la disponibilidad y el formato de la evidencia que se podrá registrar y auditar con éxito.

El ecosistema cloud native ofrece un vocabulario y una cartografía de responsabilidades que ayudan a diseñar procedimientos reproducibles en contextos de múltiples capas y proveedores (Cloud Native Computing Foundation, 2024). La literatura de microservicios, por su parte, recuerda que más piezas implican más interacciones y más puntos de falla controlada, de modo que la trazabilidad debe recorrer el flujo extremo a extremo y sobrevivir al escalado, a la recuperación automática y a los cambios continuos propios de producción. Ese es el ajuste metodológico que permite sostener investigaciones defendibles, sin resignar el rigor que la disciplina consolidó en su etapa clásica (Casey, 2011).

C. NUEVAS FUENTES DE EVIDENCIA DIGITAL

La transformación hacia arquitecturas cloud native cambia las fuentes de evidencia disponibles para la investigación forense. La información relevante ahora se encuentra dispersa en múltiples niveles de la infraestructura y en formatos que reflejan entornos distribuidos y efímeros. Logs estructurados, trazas, métricas, configuraciones declarativas y eventos de API ofrecen nuevas posibilidades probatorias, pero plantean retos de preservación, correlación y análisis que este capítulo examina en detalle.

C.1. LOGS ESTRUCTURADOS Y OBSERVABILIDAD

Los registros en cloud native se emiten como eventos JSON con campos timestamp, level, message, trace_id y span_id (Bray, 2017). Un servicio que procesa mil solicitudes por segundo genera un flujo continuo hacia agregadores como Fluentd o Vector, que normalizan esquemas antes de enviarlos a Elasticsearch con políticas de retención diferenciadas según severidad del log. El uso de formatos estandarizados como JSON favorece la correlación automatizada y aporta consistencia entre servicios y plataformas, lo que reduce ambigüedades al reconstruir hechos en sistemas heterogéneos. En ese marco, la observabilidad se apoya en tres fuentes que se complementan y ofrecen una lectura integral del comportamiento distribuido. Los registros documentan eventos discretos, las métricas describen tendencias a lo largo del tiempo y las trazas permiten seguir una transacción a través de componentes que cambian de estado con rapidez. La propagación uniforme de identificadores de contexto a lo largo de todo el recorrido es

decisiva para mantener una cronología comparable y una atribución precisa de acciones (World Wide Web Consortium, 2021).

La convergencia en especificaciones comunes consolidó este enfoque. OpenTelemetry se ha convertido en la referencia de instrumentación neutral, al definir modelos y puntos de recolección coherentes para aplicaciones y plataformas diversas. Su adopción facilita exportar evidencia técnica con metadatos mínimos y formatos interoperables, simplifica la comparación entre entornos y fortalece la validez probatoria de los artefactos observados (OpenTelemetry, 2024c).

C.2. TRAZAS DISTRIBUIDAS

Una traza distribuida captura el recorrido de una solicitud HTTP cuando atraviesa servicios de autenticación, bases de datos y cachés. El trace_id hexadecimal de 32 caracteres acompaña la solicitud desde el ingress hasta la respuesta final, mientras cada span registra latencia en microsegundos, código de estado y atributos del servicio que ejecutó esa porción del flujo (Jaeger Team, 2024). Esta aproximación permite observar de manera integral procesos que, en arquitecturas tradicionales, se encontraban ocultos tras los límites de cada aplicación.

Es así que, las trazas ofrecen un valor particular porque posibilitan la reconstrucción detallada de flujos de ejecución que resultan imposibles de inferir únicamente a partir de registros individuales. Una sola traza puede mostrar qué servicios intervinieron en una operación concreta, en qué momento ocurrieron transformaciones de datos y dónde se produjeron errores o anomalías (Zipkin Team, 2024). La granularidad de esta información proporciona una narrativa técnica que resulta especialmente útil para establecer responsabilidades en incidentes distribuidos.

Un aspecto clave de las trazas es la inclusión de span context, un mecanismo que permite correlacionar eventos entre servicios heterogéneos incluso cuando emplean sistemas de registro distintos o se ejecutan en regiones con zonas horarias diferentes. Esta correlación automática facilita la investigación de incidentes en entornos donde la evidencia se reparte entre decenas o centenares de servicios. El establecimiento de especificaciones abiertas y estandarizadas, como las impulsadas por iniciativas recientes, consolida la posibilidad de generar y analizar trazas con criterios comunes en múltiples plataformas (OpenTelemetry, 2024b).

C.3. MÉTRICAS DE SISTEMA Y APLICACIÓN

Las métricas en series temporales ofrecen una representación cuantitativa del comportamiento de sistemas distribuidos y constituyen una de las fuentes más valiosas para la detección temprana de incidentes (Prometheus Community, 2024). Al registrar valores numéricos con marcas temporales de alta precisión y etiquetas que permiten su clasificación, es posible observar patrones de uso que, bajo ciertas circunstancias, revelan indicios de actividad maliciosa.

Las métricas relacionadas con recursos básicos como CPU, memoria, red o almacenamiento pueden evidenciar intentos de denegación de servicio, actividades de minería de criptomonedas no autorizada o procesos de exfiltración de datos. De manera complementaria, las métricas de aplicación, que incluyen tasas de solicitudes, latencias de respuesta y proporción de errores, permiten identificar patrones de abuso de interfaces o conductas anómalas de usuarios.

Un aspecto relevante para la investigación forense es que los sistemas de monitoreo y alerta basados en métricas suelen generar registros con marcas temporales precisas. Estos pueden funcionar como disparadores tempranos que señalan el inicio de un incidente y ayudan a establecer cronologías con exactitud (Alertmanager Team, 2024). No obstante, la naturaleza agregada de las métricas implica que, aunque permiten detectar anomalías de manera eficaz, no siempre proporcionan el nivel de detalle necesario para un análisis probatorio completo. En consecuencia, las métricas deben considerarse un punto de partida valioso que orienta la investigación, pero necesitan complementarse con registros y trazas para lograr una reconstrucción integral de los hechos.

C.4. CONFIGURACIÓN COMO CÓDIGO INFRASTRUCTURE AS CODE (IaC)

La configuración como código constituye un cambio de paradigma en la gestión de infraestructuras, ya que reemplaza la administración manual por la definición declarativa en archivos versionados. A través de una buena cantidad de herramientas diseñadas para este fin, es posible describir de manera exacta recursos de cómputo, configuraciones de red y políticas de seguridad (HashiCorp, 2024). Esta práctica no solo optimiza la administración operativa, sino que introduce nuevas posibilidades y desafíos para la investigación forense. Desde el punto de vista probatorio, los archivos de configuración funcionan como snapshots que reflejan con precisión el estado de la infraestructura en un

momento determinado. Al estar integrados en sistemas de control de versiones, estos documentos conservan historiales completos de modificaciones que incluyen autoría, marcas temporales y comentarios asociados (Git Community, 2024). Este nivel de detalle proporciona un registro verificable de cambios que puede utilizarse para reconstruir con fidelidad la evolución de un entorno tecnológico.

El análisis de configuraciones como código permite identificar desde errores de diseño hasta modificaciones intencionales orientadas a introducir vulnerabilidades. Asimismo, la comparación de versiones sucesivas hace posible determinar qué cambios se aplicaron, cuándo ocurrieron y quién los ejecutó. En investigaciones relacionadas con incidentes internos, esta capacidad de rastreo resulta crítica para establecer responsabilidades y demostrar alteraciones no autorizadas (Ansible Community, 2024).

En suma, IaC convierte a la propia definición de la infraestructura en una fuente de evidencia digital, ampliando los espacios de análisis más allá de los registros de ejecución y consolidando un nuevo frente de observación para la informática forense en entornos cloud native.

C.5. EVENTOS DE API Y WEBHOOKS

Los entornos cloud native dependen intensivamente de interfaces de programación de aplicaciones para la interacción entre servicios y la gestión de recursos. Cada solicitud y respuesta registrada en un gateway de API contiene metadatos detallados, como encabezados, cargas útiles, códigos de estado e información de autenticación. Estos registros constituyen una fuente de evidencia que puede resultar determinante al momento de reconstruir la secuencia de actividades en un incidente.

La comunicación asincrónica basada en webhooks introduce otra dimensión probatoria que no podemos omitir. Estos mecanismos permiten que los servicios notifiquen eventos en tiempo real y generen huellas verificables de interacciones distribuidas. En muchos casos, los mensajes transmitidos incluyen firmas criptográficas que aportan garantías de integridad y de no repudio, lo que incrementa su valor como evidencia (IETF HTTP Working Group, 2024).

Los sistemas de autenticación y autorización modernos añaden un nivel adicional de información que también puede ser analizado en clave forense. Protocolos como OAuth 2.0 y OpenID Connect emplean tokens con estructuras normalizadas que contienen

afirmaciones sobre identidades y permisos. El examen de estos tokens puede revelar intentos de acceso no autorizado, escalación indebida de privilegios o patrones sospechosos de uso de credenciales (OAuth Working Group, 2012).

C.6. HERRAMIENTAS AUTOMATIZADAS DE FORENSE EN TIEMPO REAL

En entornos cloud native la adquisición forense en tiempo real resulta crítica cuando los recursos tienen vida breve y no dejan soportes persistentes. La práctica eficaz combina instrumentación de telemetría, sincronización de relojes para asegurar coherencia temporal, cálculo de valores de integridad en el momento de la captura y exportación de artefactos con metadatos suficientes para la cadena de custodia, entre ellos origen, responsable, parámetros de activación y contexto técnico. Este enfoque permite reconstruir acciones sobre contenedores y funciones de corta duración sin intervención tardía y con trazabilidad verificable. Para mitigar riesgos, los procedimientos deben congelar el estado al declarar incidente, documentar la configuración activa y evitar que automatismos de respuesta eliminen evidencias antes de su preservación. Con estos resguardos, la automatización reduce el tiempo entre detección y preservación y mejora la calidad probatoria en arquitecturas elásticas y distribuidas.

D. PROCEDIMIENTOS FORENSES ADAPTADOS

La expansión del cloud-native multiplicó y volvió más fugaces las fuentes de evidencia, esto junto a los logs aparecen trazas distribuidas, métricas, configuraciones declarativas y eventos de APIs con potencial probatorio. Esta heterogeneidad exige detectarlas a tiempo, preservarlas sin perder contexto y analizarlas con un método que entienda elasticidad y distribución, para sostener un peritaje viable y defendible en sistemas que cambian mientras se los observa.

D.1. IDENTIFICACIÓN EN ENTORNOS EFÍMEROS

La identificación de evidencia en entornos cloud native exige enfoques proactivos que no dependan de la persistencia de los recursos. En los sistemas tradicionales, los elementos probatorios podían localizarse en dispositivos estables, como discos duros o registros de sistemas que permanecían disponibles durante largos períodos de tiempo, en cambio, en

los entornos efímeros propios de arquitecturas modernas, los recursos aparecen y desaparecen con rapidez, lo que limita drásticamente la ventana temporal disponible para su detección y preservación (Zhang et al., 2020).

Un elemento central para afrontar este desafío es el uso de metadatos estructurados que acompañan a los recursos en ejecución. La asignación de etiquetas y anotaciones facilita la clasificación automática de componentes críticos, lo que permite priorizar su captura en caso de incidente. Esta práctica se vuelve esencial en sistemas donde los servicios generan elementos transitorios como volúmenes de almacenamiento, secretos o configuraciones dinámicas que, a pesar de ser indispensables para la operación, pueden ser eliminados sin intervención humana por procesos de recolección automática.

La investigación forense en este tipo de entornos depende de la capacidad de anticipar la desaparición de recursos relevantes. Para ello resulta necesario contar con políticas de observabilidad diseñadas de manera preventiva, de modo que los sistemas estén preparados para identificar dependencias temporales y registrar su existencia antes de que se eliminen. La identificación en contextos efímeros se transforma así en una tarea de detección temprana que, más que reaccionar a un incidente consumado, debe adelantarse al propio ciclo de vida de los recursos para asegurar la validez probatoria de la evidencia digital.

D.2. PRESERVACIÓN PROACTIVA Y REACTIVA

La preservación en entornos cloud native requiere combinar medidas que se preparan de antemano con acciones específicas al momento del incidente. En la fase proactiva el objetivo es que los datos críticos existan, sean localizables y conserven contexto cuando se los necesite. Esto implica definir políticas de retención que cubran ventanas reales de investigación, centralizar registros de aplicación, infraestructura y plano de control en un repositorio con inmutabilidad y auditoría, sincronizar relojes con referencia confiable y calcular integridad en el punto de adquisición. Resulta útil mantener instantáneas periódicas del estado de configuración y del inventario efectivo de recursos, junto con su historial de cambios, de modo que la reconstrucción de contexto no dependa de memoria ni de conjeturas. Cuando la plataforma usa infraestructura como código, la preservación incluye versiones firmadas y trazables de los manifiestos, las plantillas y los parámetros que describen el entorno que estaba vigente al momento del hecho.

La fase reactiva comienza previo al cambio, donde una vez detectado el incidente se congela el estado relevante para evitar que la automatización altere la evidencia. En la práctica se aconseja suspender escalados automáticos, detener tareas de autorrecuperación, aislar el servicio afectado sin borrar artefactos efímeros y hacer un cordón de seguridad con los nodos o espacios de nombres a fin de preservar su contenido. La captura debe prevalecer artefactos volátiles y de corta vida, incluidos registros de orquestación, trazas distribuidas, métricas con granularidad suficiente y copias puntuales de volúmenes y objetos, siempre con cálculo de integridad y sellos de tiempo normalizados. El procedimiento se documenta en runbooks con pasos verificables, responsables designados y criterios de reanudación controlada para que la continuidad operativa no erosione la cadena de custodia.

Este enfoque dual ordena la actuación técnica y facilita la validez probatoria. La anticipación asegura que coexistan datos completos con metadatos suficientes y la reacción inmediata evita que procesos automáticos borren o transformen rastros clave. La articulación de ambas dimensiones se apoya en principios reconocidos de identificación, adquisición y preservación y en prácticas de investigación de incidentes que exigen trazabilidad, coherencia temporal y cálculo de integridad en el momento de la captura. Con estos resguardos la prueba digital mantiene su fuerza aun frente a recursos efímeros y arquitecturas elásticas.

D.3. RECOLECCIÓN DISTRIBUIDA

La recolección de evidencia en entornos distribuidos plantea desafíos que van más allá de los que enfrentan los sistemas tradicionales. La necesidad de coordinar acciones entre múltiples plataformas, proveedores y jurisdicciones exige procedimientos meticulosos que aseguren tanto la completitud como la integridad de los datos obtenidos (Taylor et al., 2010).

Una de las estrategias más habituales consiste en utilizar herramientas de agregación de registros que centralizan información derivado de fuentes diversas. Sistemas como Elasticsearch, Fluentd y Kibana permiten consolidar eventos de manera unificada, lo que facilita el análisis posterior y reduce la dispersión de evidencias (Elastic, 2024). Sin embargo, esta centralización no elimina la necesidad de documentar cada etapa del proceso de recolección, ya que la trazabilidad resulta indispensable para garantizar la validez probatoria.

En muchos casos, la evidencia completa se encuentra distribuida entre múltiples interfaces de programación, bases de datos y servicios de almacenamiento que utilizan formatos y esquemas diferentes. El acceso a esta información está condicionado por limitaciones técnicas y contractuales, como políticas de control de tráfico o mecanismos de rate limiting que restringen la velocidad y el volumen de solicitudes (Splunk, 2024). Por ello, los investigadores deben diseñar cronogramas de recolección que contemplen estas restricciones al mismo tiempo que aseguren la preservación de la evidencia crítica.

En síntesis, la recolección distribuida demanda una planificación precisa, donde la integración tecnológica debe ir acompañada de protocolos claros de documentación y de un marco de coordinación que permita articular esfuerzos en contextos de varias jurisdiccionales con distintas leyes.

D.4. ANÁLISIS CORRELACIONADO

El análisis de evidencia en entornos cloud native exige capacidades avanzadas para correlacionar volúmenes masivos de datos distribuidos en múltiples capas de la arquitectura. Las plataformas de gestión de eventos y seguridad diseñadas para la nube ofrecen entornos especializados que permiten consolidar información procedente de distintas fuentes y aplicar procesos de correlación automatizados (Microsoft, 2024a). Esta capacidad resulta indispensable cuando los incidentes involucran múltiples servicios y regiones distribuidas, escenario en el cual un examen manual se vuelve técnicamente inviable.

El uso de técnicas de aprendizaje automático amplía estas posibilidades. Los algoritmos pueden identificar correlaciones sutiles en métricas, trazas y registros que anticipan comportamientos maliciosos o fallas críticas (Ab Rahman et al., 2016).

Sin embargo, la incorporación de mecanismos de inferencia automatizada introduce desafíos en el plano legal. La naturaleza opaca de algunos modelos, fenómeno conocido como "caja negra", dificulta explicar con claridad cómo se alcanzaron determinadas conclusiones. Como se ha señalado en el análisis de sistemas expertos y redes neuronales, existe una diferencia fundamental entre aquellos sistemas cuyas decisiones pueden justificarse mediante reglas explícitas y aquellos que operan mediante procesamiento distribuido donde "no hay manera de explicar la toma de decisiones que realiza el sistema" (Torres Ponce, 2019). Este aspecto puede debilitar el valor probatorio de los hallazgos si

no se acompaña de mecanismos de validación comprensibles y verificables que permitan a los operadores jurídicos entender el razonamiento subyacente.

Otro factor crítico es la consistencia temporal de las fuentes de evidencia. En sistemas distribuidos es frecuente la existencia de desajustes de reloj (clock drift) que generan inconsistencias en las marcas temporales. Este fenómeno debe ser corregido mediante protocolos de sincronización estandarizados, ya que una cronología imprecisa puede comprometer severamente la reconstrucción de eventos y generar interpretaciones erróneas sobre la secuencia real de los hechos (Mills, 1991).

El análisis y la correlación de evidencia en arquitecturas cloud native requieren integrar herramientas de agregación, técnicas de detección automatizada y protocolos de sincronización temporal. Esta integración debe asegurar tanto la solidez técnica como la validez jurídica de las conclusiones, considerando especialmente las limitaciones inherentes a los sistemas de inteligencia artificial en contextos donde la explicabilidad de las decisiones constituye un requisito fundamental para la admisibilidad probatoria.

E. COMPETENCIAS DEL PERITO DIGITAL CONTEMPORÁNEO

La transformación de la informática forense hacia entornos cloud native exige redefinir el perfil del perito digital. No basta con dominar técnicas tradicionales orientadas al análisis de dispositivos físicos o soportes estáticos; ahora se requiere un conjunto ampliado de conocimientos que abarca desde la gestión de arquitecturas distribuidas hasta saber cómo actuar en marcos normativos internacionales. El presente apartado tiene como propósito delinear las competencias clave que configuran al perito contemporáneo, agrupadas en dimensiones técnicas, analíticas, de seguridad y jurídicas.

E.1. COMPETENCIAS TÉCNICAS FUNDAMENTALES

El perfil del perito digital especializado en entornos cloud native requiere competencias técnicas que exceden de manera considerable las tradicionales. Una de las áreas esenciales de conocimiento es la tecnología de contenedores, que demanda familiaridad con motores como Docker, containerd o CRI-O. El dominio de estas herramientas permite analizar imágenes de contenedor, interpretar configuraciones de ejecución y extraer evidencia de entornos activos con garantías de integridad (Docker Security, 2024).

La comprensión de Kubernetes constituye otra competencia crítica, ya que este orquestador organiza el ciclo de vida de aplicaciones distribuidas. Para el perito resulta indispensable conocer en detalle el funcionamiento de pods, servicios, despliegues, controladores de ingreso, políticas de red y recursos personalizados. La investigación forense en este plano exige moverse con soltura entre distintos niveles de abstracción, desde los microservicios contenidos en un pod hasta la infraestructura que los soporta, con el fin de identificar, preservar y correlacionar la evidencia (Kubernetes SIG Security, 2024).

Las herramientas de gestión de infraestructura mediante código también se consolidan como una fuente probatoria de gran relevancia. Documentos declarativos producidos por Terraform, Ansible, Pulumi o CloudFormation describen con exactitud la infraestructura en momentos determinados, y su análisis permite reconstruir contextos operativos con detalle. Para el perito, la capacidad de interpretar estos archivos, comprender las dependencias entre recursos y rastrear modificaciones a través de sistemas de control de versiones constituye una competencia indispensable en la investigación de incidentes (HashiCorp Security, 2024).

Estas habilidades conforman un perfil profesional que ya no se limita a conocer técnicas de extracción en soportes estáticos, sino que exige un dominio integral de las plataformas que definen el ecosistema cloud native y que, al mismo tiempo, generan nuevas formas de evidencia digital.

E.2. OBSERVABILIDAD Y ANÁLISIS DE DATOS

La observabilidad se ha consolidado como una competencia transversal que integra dimensiones técnicas, analíticas y forenses. Para el perito digital, dominar este campo significa contar con la capacidad de examinar el comportamiento de sistemas distribuidos a través de múltiples fuentes de información. Herramientas como Prometheus, Grafana, Jaeger o Elasticsearch permiten capturar métricas, visualizar tendencias, reconstruir trazas distribuidas y analizar registros centralizados, ofreciendo una visión integral del entorno investigado (Observability Engineering, 2021).

En este ecosistema, OpenTelemetry se ha establecido como un marco unificador para la instrumentación de observabilidad. Su propuesta consiste en estandarizar la recolección y el intercambio de datos a través de interfaces consistentes que funcionan en diversos

lenguajes y plataformas. Comprender sus componentes principales, como spans, trazas, métricas y baggage, resulta esencial para interpretar la evidencia que se genera en sistemas modernos y para garantizar que pueda ser utilizada en procesos probatorios (OpenTelemetry, 2024a).

El trabajo del perito exige transformar la observación en hallazgos verificables y para ello debe saber formular consultas que respondan preguntas concretas. Con PromQL puede identificar un pico de tráfico en el minuto en que se produjo un acceso sospechoso. Con KQL es posible vincular intentos de autenticación fallida con direcciones de origen, y con sintaxis Lucene en Elasticsearch se pueden detectar secuencias de eventos que de otro modo quedarían ocultas en millones de registros. La fortaleza de la prueba radica en esta capacidad de correlación, siempre que se documenten sus límites cuando la sincronización temporal o los identificadores no sean consistentes (Prometheus, 2024).

En consecuencia, la observabilidad deja de ser únicamente una práctica de monitoreo operativo y se convierte en una herramienta central para la investigación digital, al proporcionar evidencias con un nivel de granularidad y correlación que difícilmente podrían obtenerse mediante técnicas tradicionales.

E.3. SEGURIDAD CLOUD Y MODELOS DE RESPONSABILIDAD

El análisis forense en entornos cloud native exige entender con precisión los modelos de responsabilidad compartida entre proveedor y cliente. Estos definen qué capas quedan bajo la administración del proveedor y cuáles permanecen bajo control del cliente, con impacto directo en la disponibilidad y el acceso a la evidencia. Las diferencias entre IaaS, PaaS y SaaS generan escenarios de recolección distintos, por lo que los procedimientos deben adaptarse a las responsabilidades y a los límites técnicos y contractuales de cada nivel (Cloud Security Alliance, 2020).

Aquí podemos ver que, los sistemas de gestión de identidades y accesos desempeñan un papel central. Soluciones de Identity and Access Management (IAM) generan registros de auditoría detallados que documentan procesos de autenticación y autorización. El perito debe ser capaz de interpretar políticas de acceso, analizar roles asignados y examinar los registros generados por intentos de inicio de sesión, ya que estas fuentes de información son decisivas en investigaciones relacionadas con el compromiso de credenciales (Amazon Web Services, 2024a).

La seguridad de red completa el cuadro probatorio en infraestructuras distribuidas. Conceptos como redes privadas virtuales, grupos de seguridad, listas de control de acceso y políticas en service mesh condicionan cómo circula el tráfico y qué se registra. Los registros de flujo de redes virtuales proveen evidencia comparable a capturas de paquetes, con menores costos de almacenamiento y mejor contexto para correlación temporal y por entidad (Google Cloud VPC, 2024).

Esto nos pone en la posición en la cual se puede ver que la capacidad probatoria no depende solo de controles técnicos; también del grado de madurez digital de la organización. Instrumentos de medición de madurez en transformación digital aplicados a gestión de personas muestran que prácticas, roles y responsabilidades influyen en la disponibilidad, calidad y gobernanza de los registros que sostienen la cadena de custodia. En investigaciones cloud native, mayor madurez se asocia con retenciones adecuadas, activación oportuna de legal hold y consistencia de metadatos a lo largo del ciclo de vida de la evidencia (Maliqueo Pérez y González Candia, 2020).

La comprensión de estos modelos y tecnologías no solo determina qué evidencia se encuentra disponible, sino también cómo debe preservarse e interpretarse para que resulte válida en procesos de investigación y eventualmente en contextos judiciales.

E.4. APIS Y MICROSERVICIOS

El análisis forense de arquitecturas basadas en APIs requiere un conocimiento profundo de los protocolos que estructuran la comunicación entre servicios. La comprensión de HTTP y HTTPS, junto con modelos de interacción como REST, GraphQL, gRPC o WebSocket, resulta indispensable para interpretar los registros que generan las pasarelas de API. Estos registros incluyen información sobre solicitudes, respuestas, autenticación y patrones de uso, y constituyen una fuente de evidencia capaz de revelar tanto intentos de acceso malicioso como abusos en la utilización legítima de los servicios (OWASP, 2023).

En el plano de la autenticación y la autorización, los sistemas modernos introducen nuevas complejidades que demandan competencias específicas. Protocolos como OAuth 2.0 y OpenID Connect utilizan tokens que contienen afirmaciones verificables sobre identidad y permisos. El análisis de estos elementos permite reconstruir flujos de autenticación, validar firmas criptográficas e interpretar los claims que describen el

alcance de los accesos concedidos. En consecuencia, los tokens no solo funcionan como mecanismos operativos de seguridad, sino también como evidencias que documentan con precisión actividades autorizadas en sistemas distribuidos (OAuth, 2022).

Las arquitecturas impulsadas por eventos incorporan además sistemas de mensajería que sostienen la comunicación asincrónica entre componentes. Plataformas como Apache Kafka o RabbitMQ gestionan grandes volúmenes de mensajes mediante patrones de publicación y suscripción, event sourcing y procesamiento basado en comandos y consultas. El conocimiento de estos modelos es fundamental para interpretar los rastros que dejan las interacciones asincrónicas, los cuales pueden ser decisivos para establecer secuencias de eventos en investigaciones forenses (Apache Kafka, 2024).

E.5. HERRAMIENTAS FORENSES ESPECIALIZADAS

El trabajo en entornos cloud native obliga a ampliar el conjunto de herramientas forenses más allá de las diseñadas para sistemas físicos o virtuales convencionales. Las arquitecturas basadas en contenedores y orquestadores exigen tecnologías capaces de operar en entornos distribuidos y efímeros sin comprometer la integridad probatoria.

Para la preservación de estado, Velero permite realizar copias de seguridad y restauración de clústeres completos de Kubernetes, incluyendo recursos de configuración y volúmenes persistentes. Esta capacidad resulta esencial para congelar un sistema en un momento determinado y facilitar la reconstrucción posterior de escenarios de investigación (Velero, 2024).

En detección en tiempo real, Falco monitorea llamadas al sistema en contenedores y en Kubernetes, generando alertas sobre conductas anómalas que pueden indicar compromisos de seguridad. La posibilidad de personalizar sus reglas lo convierte en un recurso adaptable a distintos contextos probatorios (Falco, 2024).

Herramientas como Sysdig ofrecen visibilidad profunda del comportamiento en tiempo de ejecución de contenedores. Abarcan procesos, conexiones de red y actividad en el sistema de archivos. Su valor radica en que pueden registrar evidencia sin necesidad de modificar las aplicaciones, lo que asegura que el proceso de investigación no altere la validez de los entornos observados (Sysdig, 2024).

Más allá de estos ejemplos, el ecosistema forense cloud native incluye instrumentos para orquestación (kubectl, Helm), observabilidad (Prometheus, Grafana, Jaeger, Elasticsearch), análisis de seguridad (Twistlock, Aqua Security) y forense especializado (KAPE, Volatility, Autopsy). La selección dependerá del modelo de servicio cloud, el tipo de incidente y las capacidades técnicas disponibles en cada contexto de investigación. Lo relevante es que estas herramientas deben ser capaces de observar sistemas vivos, dinámicos y distribuidos en los que la evidencia puede desaparecer en instantes.

E.6. COMPETENCIAS JURÍDICAS Y REGULATORIAS

El perito en cloud native necesita doble alfabetización, basada en los conocimientos técnica y respaldada por la sabiduría jurídica normativa. Cuando la evidencia se reparte entre regiones, debe identificar la base legal de cada recolección, respetar plazos de retención, garantizar derechos de acceso y supresión y documentar transferencias internacionales con su justificación. En Europa, alinearse con el RGPD; fuera de Europa, reconocer marcos locales equivalentes sobre finalidad, minimización y seguridad. No alcanza con saber "qué" guardar: hay que poder explicar "por qué" y "bajo qué norma".

El plano contractual define el terreno de juego. Términos del servicio, SLA y acuerdos de procesamiento deben asignar responsabilidades para identificar, adquirir, preservar, analizar y entregar. Conviene pactar activación de legal hold, plazos de acuse y de primera exportación, formatos verificables con metadatos mínimos, cifrado en tránsito y reposo, controles de integridad al ingreso y salida ordenada del servicio, además de portabilidad con campos obligatorios y una política clara de custodia de claves, idealmente con gestión del cliente cuando la norma lo admite. La idoneidad se acredita con formación en privacidad, evidencia digital y gobernanza de datos, más experiencia verificable en cadena de custodia y e-discovery; leer con ojo crítico informes de control como SOC 2 tipo II aporta insumos objetivos para evaluar al proveedor y traducir hallazgos en requisitos probatorios operables. En síntesis, se trata de una formación híbrida: integrar derecho y técnica para diseñar protocolos replicables, sostener trazabilidad en todo el ciclo de vida de la evidencia y asegurar que cada paso sea técnicamente sólido y jurídicamente válido.

F. CADENA DE CUSTODIA EN ENTORNOS DISTRIBUIDOS

La cadena de custodia es el eje que sostiene la validez de la evidencia: garantiza integridad, autenticidad y verificabilidad desde la captura hasta su presentación. En cloud native el panorama se vuelve más complejo porque la distribución geográfica, la replicación automática y la intervención de varios actores dejan cortos los mecanismos clásicos. La respuesta combina técnica y contrato, y conviene dejarla por escrito: sellos de tiempo y cómputos de integridad en origen, aislamiento de entornos compartidos con control de accesos y auditoría continua, además de reglas claras con el proveedor sobre quién conserva, cómo entrega, en qué formato y bajo qué jurisdicción. Así la evidencia viaja sin perder identidad.

F.1. PRINCIPIOS TRADICIONALES ADAPTADOS

La cadena de custodia en cloud-native exige traducir integridad, autenticidad y no repudio a infraestructuras distribuidas y multirregión. Hay que documentar sellos de tiempo normalizados, cómputos de integridad en el punto de adquisición, y la trazabilidad de actores y ubicaciones efectivas de cada réplica, de modo que cada traspaso conserve origen, contexto y verificaciones asociadas (International Organization for Standardization y International Electrotechnical Commission, 2012). La precisión temporal es crítica cuando el incidente se propaga entre zonas horarias y sistemas con relojes desalineados, por eso se necesita sincronización auditable, con registro de la fuente de tiempo y del desvío observado, y sellos expresados en un formato interoperable y estable a largo plazo (Klyne y Newman, 2002). También corresponde dejar explícita la residencia y la soberanía de datos, las obligaciones de retención y exportabilidad y las responsabilidades sobre custodia de claves. Con estas adaptaciones, los principios clásicos siguen operando y la prueba mantiene validez técnica y jurídica aun en plataformas elásticas y cambiantes.

F.2. MECANISMOS CRIPTOGRÁFICOS DE INTEGRIDAD

La integridad no se declama: se prueba. Cadenas de hash y estructuras tipo árbol permiten que cada registro dependa del anterior; si alguien toca un punto, se nota en toda la secuencia. Los ledgers inmutables llevan ese principio un paso más allá con verificación criptográfica y marcas temporales comprobables, útiles para custodias que deben resistir

auditorías serias en entornos distribuidos (Amazon Web Services, 2024b). La otra pata es la autenticidad: firmar en el momento de la adquisición con infraestructura de clave pública, registrar quién firma, con qué certificado y bajo qué política de sellado. Luego se valida, se archiva y se controla revocación. Con estos dos bloques de inmutabilidad verificable y firma digital, la evidencia conserva coherencia interna y origen trazable, sin depender del proveedor, pero aprovechando servicios que simplifican la operación en la nube (Microsoft, 2024b).

F.3. CONSIDERACIONES DE MULTI-TENANCY

El carácter multi-tenant de la nube pública introduce un riesgo específico para la cadena de custodia: varios clientes comparten infraestructura física y lógica y, si el aislamiento falla, la evidencia puede contaminarse. La documentación probatoria debe describir con precisión cómo se garantiza ese aislamiento en cada capa. Resulta indispensable consignar segmentación de red, separación de identidades y permisos, cifrado con llaves segregadas por inquilino y controles de acceso con registro auditable. Cuando existan mecanismos de aislamiento asistidos por hardware o entornos de ejecución protegidos, conviene dejar constancia del modo en que se activan y verifican.

Las capas de virtualización y de contenedores añaden complejidad porque intermedian la relación entre el evento y el artefacto recolectado. Para sostener la validez probatoria, el expediente debe incluir evidencias de verificación en cada transición. Se recomienda registrar la configuración efectiva del hypervisor o del orquestador, las políticas de scheduling, los límites de recursos y los espacios de nombres en uso en el momento del hecho. También es útil conservar pruebas de integridad y de origen que muestren que los componentes de la plataforma no modificaron el contenido capturado y que las transformaciones inevitables no alteraron el significado técnico de los datos.

La trazabilidad mejora cuando el proveedor entrega artefactos de aseguramiento que puedan incorporarse al expediente. Son especialmente valiosos los informes de auditoría de controles de seguridad, las descripciones de arquitectura de aislamiento, los resultados de pruebas de separación lógica y los registros de control de cambios del plano de administración. Si el servicio opera bajo marcos de certificación aplicables a entornos cloud, su referencia debe limitarse a aquello que efectivamente respalda el aislamiento y la preservación, evitando traslaciones automáticas de garantías generales a supuestos probatorios concretos.

Por último, conviene prever pruebas operativas periódicas que confirmen la separación entre inquilinos. Un plan razonable incluye ensayos de exportación y rehidratación de evidencia en un entorno alternativo, verificaciones cruzadas de metadatos que acrediten pertenencia a un único inquilino y controles negativos para descartar filtraciones entre espacios de nombres, cuentas o proyectos. Con estos resguardos, el multi-tenancy deja de ser un punto opaco y se integra como una condición controlada del proceso forense.

F.4. DOCUMENTACIÓN CONTRACTUAL

La cadena de custodia en entornos cloud native requiere soporte contractual explícito que complemente los controles técnicos. Los acuerdos deben fijar formatos de exportación y campos mínimos que acompañen cada artefacto, entre ellos sellos de tiempo con zona horaria normalizada, identificadores de solicitud o de traza, valores de integridad generados en adquisición y, cuando corresponda, firma digital verificable. La coherencia temporal se respalda con sellado conforme ISO 8601 o RFC 3339 y, para evidencias que lo requieran, con servicios de sellado de tiempo compatibles con RFC 3161. La autenticidad y la integridad se sostienen mediante funciones aceptadas como SHA-256 según NIST, registradas en el momento de la captura y conservadas a lo largo del ciclo de custodia.

Los contratos deben establecer niveles de servicio orientados a preservación y entrega. Resulta indispensable pactar plazos de acuse de recibo ante una orden de conservación, tiempos máximos para la primera exportación y mecanismos de reintentos cuando existan incidencias. La transferencia debe usar canales verificables con cifrado en tránsito y controles de integridad al ingreso, con constancia de recepción, persona responsable y entorno de destino. La identificación de puntos de contacto técnicos y legales no puede quedar en referencias genéricas. La ausencia de estos elementos erosiona la trazabilidad y debilita la prueba.

El modelo de responsabilidad compartida necesita quedar reflejado en la cadena de custodia. Conviene explicitar qué tareas asume el cliente y cuáles recaen en el proveedor en cada fase de identificación, adquisición, preservación, análisis y presentación, alineando el texto contractual con los principios de ISO/IEC 27037, 27041, 27042 y 27043. Esta delimitación permite asignar obligaciones, auditar su cumplimiento y determinar con claridad las consecuencias ante fallos de preservación o demoras de entrega.

Los procedimientos de legal hold en la nube requieren coordinación operativa para suspender rotaciones y borrados automáticos. El contrato debe prever la activación del legal hold, las señales que disparan la suspensión de políticas de ciclo de vida, los sistemas alcanzados y el modo de verificación de su aplicación. También debe documentar la salida del legal hold, los plazos de retención posterior y los requisitos para restituir políticas de eliminación sin pérdida inadvertida de contexto.

Cuando el servicio incluya telemetría, trazas y registros gestionados por el proveedor, es prudente acordar un modelo de portabilidad que preserve metadatos esenciales y permita rehidratar la evidencia en un entorno alternativo sin rupturas de contexto. El marco de acuerdos sobre niveles de servicio para la nube de ISO/IEC 19086 ofrece un lenguaje común para documentar estas obligaciones y reduce ambigüedades habituales en la interpretación de entregables. Con estas previsiones, el andamiaje contractual se integra con los controles técnicos y asegura una cadena de custodia verificable de punta a punta.

G. ESTÁNDARES Y NORMAS APLICABLES

La práctica forense en entornos cloud native no puede sostenerse únicamente en el desarrollo técnico, sino que requiere apoyarse en un entramado normativo y estandarizador que otorgue coherencia, legitimidad y validez jurídica a los procedimientos. Los estándares internacionales, los marcos regulatorios regionales, las guías emitidas por la industria y las propuestas emergentes específicas para arquitecturas cloud native conforman un cuerpo de referencia indispensable. Este apartado examina la evolución y aplicación de estos instrumentos, mostrando cómo aportan directrices que permiten adaptar los principios clásicos de la evidencia digital a un escenario caracterizado por la volatilidad de los recursos, la distribución global de datos y la necesidad de cooperación transfronteriza.

G.1. NORMAS INTERNACIONALES

Los marcos normativos internacionales son el punto de apoyo para estandarizar la práctica forense y deben leerse de manera consciente cuando el entorno es cloud native. Las normas ISO/IEC 27037 y 27042 siguen siendo la guía central para identificar, adquirir, preservar, analizar e interpretar evidencia digital. Nacieron en escenarios estables con

soportes persistentes, por eso su aplicación en recursos efímeros y distribuidos exige una traducción explícita. El perito debe documentar cómo lleva los principios de identificación y preservación a contenedores, funciones y planos de control y cómo asegura que cada artefacto conserva origen, contexto y tiempo comparable en sistemas que cambian de estado en minutos.

La consistencia del proceso se refuerza cuando la actuación técnica se alinea además con ISO/IEC 27041 y 27043. Allí se encuentran criterios para demostrar confiabilidad del proceso y para estructurar la investigación de incidentes. Esa lectura, combinada con un modelo de telemetría que mantenga trazabilidad entre registros, métricas y trazas, permite que la narrativa técnica sobreviva a la volatilidad propia de la nube. La coherencia temporal se garantiza con sellos de tiempo normalizados conforme ISO 8601 o RFC 3339 y, cuando corresponde, con sellado de tiempo conforme RFC 3161. La integridad se sostiene con funciones reconocidas como SHA-256 según lineamientos del NIST y con cálculo en el momento de la adquisición.

El andamiaje contractual también tiene estándar. La familia ISO/IEC 19086 sobre acuerdos de nivel de servicio en la nube aporta lenguaje común para fijar exportabilidad, tiempos de respuesta ante órdenes de conservación, campos mínimos de salida y responsabilidades sobre custodia de claves. Con ese marco se reducen ambigüedades en portabilidad y se ordena la entrega de evidencias con metadatos suficientes para reconstruir cadena de custodia.

En Europa, DORA exige que las entidades con servicios críticos conserven registros auditables y prueben su resiliencia operativa. NIS2 refuerza deberes de registro, notificación y cooperación entre operadores esenciales y autoridades competentes. Estas obligaciones se traducen en requisitos prácticos sobre retención, trazabilidad y disponibilidad de artefactos para investigación. En Estados Unidos, los lineamientos del NIST sobre gestión de registros y arquitectura de confianza cero, con especial referencia a SP 800-92 para logging y SP 800-207 para modelos de acceso, orientan qué capturar y cómo preservarlo en infraestructuras distribuidas.

Estas referencias permiten definir qué retener, durante cuánto tiempo y con qué metadatos asociados. La adaptación no consiste en crear reglas nuevas sino en hacer operables los principios existentes frente a recursos efímeros, multi-región y multi-tenant, dejando constancia de cada decisión para que el método pueda ser auditado y replicado. Con este

enfoque la prueba digital mantiene validez técnica y jurídica aun cuando la plataforma subyacente sea elástica y cambiante.

G.2. MARCOS REGULATORIOS EUROPEOS

El marco regulatorio europeo ha incorporado en los últimos años instrumentos orientados a reforzar la resiliencia digital. Entre ellos se destaca el Reglamento de Resiliencia Operacional Digital, conocido como DORA, que impone a las entidades financieras el mantenimiento de registros confiables y la capacidad de auditarlos en contextos de incidentes graves. Esta obligación se enlaza con la necesidad de contar con artefactos que permitan sostener investigaciones forenses en escenarios de ciberseguridad complejos. La relación entre resiliencia operativa y capacidad probatoria se vuelve así un eje central de la regulación (EBA, 2024).

De manera complementaria, la Directiva NIS2 amplía el alcance de las obligaciones de ciberseguridad para operadores de servicios esenciales y proveedores de infraestructuras críticas. Este marco impone requisitos de logging estandarizado y colaboración activa en investigaciones forenses, reconociendo que la trazabilidad de los eventos es un elemento fundamental para la respuesta coordinada frente a incidentes transfronterizos. Su aplicación refuerza la obligación de los actores clave de garantizar registros adecuados que puedan convertirse en evidencia válida (ETSI, 2024).

Por su parte, el Reglamento de Inteligencia Artificial introduce obligaciones de explicabilidad y trazabilidad en sistemas algorítmicos que inciden de manera directa en la práctica forense. La preservación de logs asociados a modelos y la documentación de decisiones automatizadas pasan a ser un requisito regulatorio, lo que modifica la forma en que se concibe la evidencia digital en infraestructuras cloud (European Commission, 2024).

DORA, NIS2 y el Reglamento de IA persiguen un objetivo común en materia probatoria. Todos buscan que existan registros suficientes y verificables que respalden la investigación de incidentes. Aunque los enfoques son distintos, el efecto práctico es claro. Estas obligaciones deben convertirse en retenciones efectivas de la información, en formatos íntegros que puedan exportarse y en cláusulas contractuales que garanticen la conservación de datos bajo legal hold con el proveedor.

G.3. ESTÁNDARES DE INDUSTRIA

Además de los marcos normativos internacionales y europeos, la industria ha desarrollado estándares específicos que guían la implementación práctica de controles de seguridad y preservación de evidencia en entornos cloud native. Uno de los más influyentes es el Cloud Controls Matrix de la Cloud Security Alliance, que ofrece un marco integral de controles diseñado para entornos de nube. Este documento no solo abarca aspectos generales de seguridad, sino que incluye apartados dedicados a logging, monitoreo y procedimientos de preservación de evidencia, convirtiéndose en una referencia fundamental para auditores y peritos digitales (CSA, 2024).

En el plano técnico, los Security Technical Implementation Guides elaborados por la Defense Information Systems Agency establecen requisitos detallados de configuración segura para plataformas de contenedores y orquestadores. Estos lineamientos ofrecen pautas específicas que, al aplicarse correctamente, reducen riesgos de alteración de evidencia y aseguran entornos más confiables para la práctica forense (DISA, 2024).

De manera complementaria, el Cybersecurity Framework del NIST, en su versión 2.0, incorpora perfiles especializados para entornos cloud. Estos perfiles permiten a las organizaciones mapear controles de seguridad con objetivos forenses, integrando prácticas de monitoreo, análisis y respuesta en un marco reconocido globalmente. La inclusión explícita de capacidades forenses dentro de este framework refleja la creciente importancia de la evidencia digital en la gestión de ciberseguridad.

Los estándares técnicos complementan los marcos normativos al ofrecer controles específicos para la captura, preservación y verificación de integridad. Su relevancia aumenta en entornos cloud native donde los despliegues son veloces, los recursos efímeros y las cadenas de suministro más complejas. La integración de estas guías con los requisitos legales aporta a los peritos y a las organizaciones un conjunto de prácticas comprobables que facilitan la admisibilidad de la evidencia.

G.4. ESTÁNDARES EMERGENTES CLOUD NATIVE

El desarrollo de estándares emergentes refleja el esfuerzo de la industria por responder a los desafíos específicos de los entornos cloud native, que trascienden las categorías contempladas en las normas tradicionales. La Cloud Native Computing Foundation ha

publicado documentos de referencia que ofrecen lineamientos concretos para la seguridad en arquitecturas basadas en Kubernetes y otros componentes cloud native. Entre ellos, el Whitepaper de Seguridad se destaca por incluir recomendaciones explícitas en materia de observabilidad forense, reconociendo que la visibilidad sistémica es un requisito indispensable para la preservación de evidencia (CNCF, 2024a).

De manera complementaria, el catálogo de controles de seguridad desarrollado por la misma fundación organiza de manera sistemática las medidas aplicables a distintos componentes del ecosistema cloud native. Este catálogo permite mapear controles técnicos directamente a requerimientos forenses, facilitando la integración de la seguridad con las prácticas de preservación y análisis de evidencia (CNCF, 2024b).

Otro aporte significativo es el marco Supply Chain Levels for Software Artifacts, que introduce un modelo de niveles progresivos de integridad para cadenas de suministro de software. La aplicación de este framework resulta esencial para la investigación de incidentes relacionados con compromisos en imágenes de contenedor, dado que establece métricas verificables que permiten rastrear la autenticidad y la trazabilidad de los artefactos desde su origen hasta su despliegue en producción (SLSA, 2024).

Por lo tanto, vemos que estos estándares emergentes complementan los marcos normativos y de la industria, y responden de manera directa a las particularidades del ecosistema cloud native, donde la rapidez de despliegue, la naturaleza efímera de los recursos y la complejidad de las cadenas de suministro demandan nuevas estrategias de control y aseguramiento probatorio.

H. DISCUSIÓN CRÍTICA: PRESERVACIÓN, DEPENDENCIA Y JURISDICCIÓN

Investigar en la nube exige más que listar herramientas o repetir normas. Cuando los sistemas se arman con contenedores que duran unos momentos, servicios repartidos y telemetría que aparece y desaparece, el peritaje se vuelve una práctica situada, una que decide qué retener y qué descartar sabiendo que cada movimiento impacta en derechos, en costos y en la posibilidad de sostener la prueba más adelante. La pregunta central deja de ser qué tecnología usar y pasa a ser cómo documentar, con criterio y a tiempo, decisiones que después van a tener que ser explicadas frente a alguien que no estuvo ahí.

El primer nudo aparece en la convivencia entre privacidad y preservación. Las reglas de minimización y de finalidad obligan a justificar con precisión qué se guarda y por cuánto, mientras que la reconstrucción de un incidente pide cronologías completas y metadatos consistentes para una cadena de custodia que se pueda verificar sin adivinar. El modo razonable de equilibrar esas demandas no es una receta única, sino una arquitectura de políticas que separa propósitos, segmenta datos sensibles, restringe accesos por rol y audita el uso efectivo; cuando se declara un incidente, conviene suspender las rotaciones automáticas, dejar asentada la decisión con sello de tiempo normalizado e identificar qué sistemas quedan alcanzados, y cuando termina la necesidad probatoria, restablecer las políticas con un cierre claro que explique qué se hizo y por qué. La portabilidad completa ese cuadro: mover evidencia entre proveedores sin perder contexto requiere acordar formatos de salida, conservar metadatos mínimos y asegurar coherencia temporal que luego permita rehidratar los artefactos en otro entorno sin abrir debates innecesarios sobre su autenticidad.

El segundo nudo es la dependencia de terceros. Un cambio unilateral en una API, una ventana de retención más corta o una condición contractual nueva pueden bloquear el acceso justo cuando más se lo necesita. Para reducir esa exposición, sirve pactar de antemano cláusulas de retención y mecanismos de e-discovery que se activen con el incidente, procedimientos de exportación verificables y tiempos de entrega definidos; sirve también sellar en la adquisición, conservar trazas de origen y de parámetros de exportación y usar modelos de telemetría que mantengan el vínculo entre datos y metadatos, de manera que el valor probatorio no se diluya en la mudanza. Los costos, además, no son un detalle: sin planificación, la factura empuja a purgar antes de tiempo, por eso ayudan las políticas diferenciadas por tipo de evidencia, las reducciones que no afectan el valor pericial y el almacenamiento inmutable con auditoría de accesos.

El tercer nudo es la adecuación de las herramientas. Mucho del instrumental forense nació para equipos únicos y discos con alta persistencia, y por eso tropieza cuando la escala, la diversidad y la fugacidad del dato son la regla y no la excepción; esta brecha ya fue advertida por los programas de evaluación de herramientas, que insisten en medir capacidad, fidelidad y trazabilidad en condiciones realistas de uso (National Institute of Standards and Technology, 2023). A la escala se suman el volumen y la variabilidad propios del big data, que empujan a rediseñar cómo se extrae, se procesa y se analiza evidencia cuando el contexto está distribuido y cambia todo el tiempo. Y, en paralelo,

aparece la necesidad de mirar flujos casi en tiempo real, porque hay señales que viven instantes y si no se capturan a la pasada se pierden sin remedio: ese enfoque de procesamiento en streaming, que ya es maduro en otras áreas, gana lugar en escenarios forenses donde adquirir sin interrumpir y dejar rastro de cada transformación se vuelve condición de admisibilidad, no un lujo metodológico. Si además se suma inteligencia artificial para filtrar o priorizar, hace falta algo más que rendimiento: hay que poder explicar modelos y decisiones, versionar lo que corre, registrar entradas y salidas, fijar umbrales y validar con muestras independientes, de modo que el apoyo automatizado complemente, en vez de reemplazar, el juicio pericial que finalmente se firma.

El cuarto nudo es jurisdiccional. Un mismo incidente deja rastros en varios países y no siempre las reglas conversan; por eso conviene decidir de entrada el foro que va a guiar el estándar probatorio, precisar la base legal de cada recolección, incluidas las transferencias internacionales y las garantías del interesado, y acordar con el proveedor un canal de entrega que conserve metadatos, respete zonas horarias normalizadas y preserve la integridad en tránsito y en recepción. Como los mecanismos clásicos de cooperación suelen ser más lentos que la vida útil de ciertos registros, la estrategia práctica combina preservación urgente en origen con solicitudes formales que lleguen a tiempo a los custodios, y alinea desde el inicio el formato de salida con lo que más tarde pedirá el tribunal.

El equilibrio no se logra con un checklist. Se necesita un diseño operativo que haga convivir lo técnico, lo legal y lo económico sin subordinar uno al otro.

Políticas de retención por finalidad, gobernanza clara de accesos, telemetría portable, sellos de tiempo e integridad estandarizados y una hoja de ruta jurisdiccional realista permiten investigar sin desproteger derechos. También ayudan a gestionar la dependencia de terceros como una variable que se controla, no como un punto ciego que se sufre.

Los informes que resultan de ese proceso no prometen infalibilidad, pero sí trazabilidad, contexto y razones suficientes para sostener la evidencia en entornos que cambian mientras se los está mirando.

I. CONCLUSIONES

Este trabajo deja claro que los criterios clásicos ya no alcanzan para los entornos cloud native, donde los recursos aparecen y desaparecen rápidamente, necesitamos pensar en términos de tiempo, automatización y portabilidad si queremos reconstruir lo que pasó con precisión. La observabilidad se vuelve clave, pero solo si capturamos los datos con contexto, orden y garantías desde el primer momento. No se trata de descartar de pleno lo que ya usamos, la esencia de lo que buscamos como elemento probatorio nos sirve como guía para poder adaptar las herramientas a sistemas que cambian rápido y reparten sus huellas por todos lados.

En la práctica, lo que más dificulta es la interoperabilidad, donde cada plataforma habla su propio idioma y no hay mínimos comunes, correlacionar eventos se vuelve frágil y reconstruir incidentes, impreciso. Por eso proponemos avanzar hacia modelos de telemetría que mantengan el origen, la secuencia y las relaciones entre eventos a lo largo de todo el ciclo de vida. Esa continuidad permite recuperar los datos en otros entornos sin perder el hilo, y comparar incidentes similares con más confianza.

También hace falta que el marco legal y contractual acompañe esta evolución técnica, dado que la validez de la prueba depende de que la retención, exportación y entrega estén bien definidas, siendo imprescindible definir los claramente cuales son los tiempos, campos obligatorios y roles asignados. La tensión entre privacidad y preservación no se resuelve sola; hay que tomar decisiones explícitas sobre base legal, alcance y registro de transferencias, para que la cadena de custodia sobreviva a escenarios complejos sin perder fuerza.

Lo que sigue es validar todo esto en la práctica, hay que probarlo con casos reales, medir qué se pierde, qué se conserva y qué se puede reconstruir. Proponemos repetir el protocolo en distintos servicios y regiones, con cronologías comparables y criterios definidos desde el inicio. Si los resultados muestran mejoras medibles, eso va a facilitar que las instituciones lo adopten y que se armonicen prácticas en el futuro.

La informática forense va a seguir siendo relevante si logramos que técnicos, peritos y reguladores trabajen juntos. Esa coordinación es lo que va a permitir convertir principios en procedimientos, y hablar un lenguaje común que conecte seguridad, registro y admisibilidad. Aunque la infraestructura cambie todo el tiempo, la disciplina puede seguir siendo eficaz si se adapta con criterio.

El análisis desarrollado en este trabajo muestra que las categorías clásicas de la informática forense resultan insuficientes cuando la evidencia proviene de entornos cloud native. Lo relevante no es repetir principios ya conocidos sino adaptarlos a recursos que aparecen y desaparecen en casi instantaneamente, a registros generados de manera distribuida y a infraestructuras sometidas a procesos de automatización constante. Este aporte se concreta en tres frentes: una taxonomía mínima de fuentes probatorias, un conjunto de procedimientos con plantilla pericial para guiar la recolección y preservación y un análisis de las obligaciones regulatorias que condicionan la validez de la prueba. Los próximos pasos deben centrarse en contrastar estas propuestas con estudios de caso y en medir de manera empírica qué pérdidas de contexto se producen según el modelo de servicio y la política de retención aplicada.

Los hallazgos permiten identificar tres grandes ejes de transformación. En primer lugar, el plano técnico: la preservación de logs estructurados, métricas, trazas distribuidas y configuraciones declarativas abre un campo probatorio más amplio, pero también más frágil. En segundo término, el plano jurídico: la dispersión multi-jurisdiccional de los datos obliga a replantear la cadena de custodia y a desarrollar marcos contractuales y regulatorios más ágiles y coordinados. Finalmente, el plano profesional: el rol del perito digital debe evolucionar hacia un perfil híbrido, capaz de integrar saberes de orquestación, seguridad cloud y observabilidad con competencias jurídicas y regulatorias.

Mirando hacia el futuro, emergen líneas de investigación y acción prioritarias: el diseño de herramientas forenses nativas de Kubernetes y microservicios; la incorporación de tecnologías de ledger distribuido para sostener cadenas de custodia inmutables; el desarrollo de sistemas de inteligencia artificial explicables que aporten correlaciones transparentes; y la armonización internacional de normas que equilibren preservación probatoria, privacidad y soberanía digital.

La informática forense en entornos cloud native se encuentra, en definitiva, ante un punto de inflexión histórico. La oportunidad reside en articular respuestas interdisciplinarias que fortalezcan la validez de la evidencia en un ecosistema tecnológico en permanente transformación. Este trabajo no pretende agotar el debate, sino abrir un camino de reflexión y propuesta que invite a la comunidad académica, técnica y jurídica a pensar de manera conjunta los cimientos de la forensia digital del futuro.

J. BIBLIOGRAFÍA

Ab Rahman, N. H., et al. (2016). Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing, 3*(1), 50–59.

Alertmanager Team. (2024). *Alertmanager documentation.* Prometheus.

Amazon Web Services. (2024a). *IAM documentation.*

Amazon Web Services. (2024b). *Amazon QLDB documentation.*

Apache Kafka. (2024). *Kafka documentation.*

Bray, T. (2017). *The JavaScript Object Notation (JSON) data interchange format (RFC 8259).* RFC Editor.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

Cloud Native Computing Foundation. (2024a). *Cloud native security whitepaper (v2).*

Cloud Native Computing Foundation. (2024b). *Security controls.*

Cloud Security Alliance. (2020). *Security guidance for critical areas of focus in cloud computing* (v4.0).

Cloud Security Alliance. (2024). *Cloud controls matrix (CCM v5).*

Defense Information Systems Agency. (2024). *Container platform STIG.*

Docker. (2024). *Docker security documentation.*

Elastic. (2024). *Elastic Stack documentation.*

European Banking Authority. (2024). *DORA technical standards.*

European Commission. (2024). *AI Act guidelines.*

European Telecommunications Standards Institute. (2024). *ETSI EN 319 401 v2.3.1: Trust services—General policy requirements for trust service providers.*

Falco. (2024). *Falco documentation.*

Git. (2024). *Git documentation.*

Google Cloud. (2024). *VPC flow logs.*

HashiCorp. (2024). *Terraform documentation.*

HashiCorp Security. (2024). *Terraform security best practices.*

International Organization for Standardization. (2012). *ISO/IEC 27037:2012: Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence.*

International Organization for Standardization. (2015). *ISO/IEC 27042:2015: Information technology—Security techniques—Guidelines for the analysis and*

interpretation of digital evidence.
IETF HTTP Working Group. (2024). *Webhooks security considerations* (Internet-Draft).
Jaeger Team. (2024). *Jaeger distributed tracing documentation.*
Klyne, G., & Newman, C. (2002). *Date and time on the Internet: Timestamps (RFC 3339).* RFC Editor.
Kubernetes SIG Security. (2024). *Kubernetes security overview.*
Maliqueo Pérez, C., & González Candia, J. C. (2020). Diseño y validación de un instrumento para medir el nivel de madurez en innovación y transformación digital en la gestión de personas. *Ciencia y Técnica Administrativa, 19*(3), 6.
Microsoft. (2024a). *Azure Sentinel documentation.*
Microsoft. (2024b). *Digital signatures in Azure.*
Mills, D. L. (1991). Internet time synchronization: The network time protocol. *IEEE Transactions on Communications, 39*(10), 1482–1493.
National Institute of Standards and Technology. (2020). *Zero trust architecture (SP 800-207).* U.S. Department of Commerce.
National Institute of Standards and Technology. (2023). *Computer Forensics Tool Testing Program (CFTT).*
Newman, S. (2015). *Building microservices.* O'Reilly Media.
OAuth Working Group. (2012). *The OAuth 2.0 authorization framework (RFC 6749).* IETF.
OAuth. (2022). *OAuth 2.1 draft.*
Observability Engineering. (2021). *Observability engineering.* O'Reilly Media.
OpenTelemetry. (2024a). *OpenTelemetry overview.*
OpenTelemetry. (2024b). *OpenTelemetry specification.* Cloud Native Computing Foundation.
OpenTelemetry. (2024c). *Tracing specification.* OpenTelemetry.
OWASP. (2023). *API security top 10.*
Palmer, G. (2001). *A road map for digital forensic research (DFRWS Technical Report DTR-T001-01 Final).* Digital Forensic Research Workshop.
Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation, 13,* 38–57.
Prometheus. (2024). *Querying Prometheus.*
Prometheus Community. (2024). *Prometheus documentation.*
Richardson, C. (2018). *Microservices patterns.* Manning Publications.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics. En G. Peterson & S. Shenoi (Eds.), *Advances in digital forensics VII* (pp. 35–46). Springer.

SLSA. (2024). *SLSA framework.*

Splunk. (2024). *Splunk Enterprise Security.*

Sysdig. (2024). *Sysdig documentation.*

Taylor, M., et al. (2010). Digital evidence in cloud computing systems. *Computer Law and Security Review, 26*(3), 304–308.

Torres Ponce, M. E. (2019). *Derechos y desafíos de la inteligencia artificial.* Revista Técnica Administrativa, 18(1), 1–10. Ciencia y Técnica Administrativa.

Torres Ponce, M. E. (2020). *Informática forense: El camino de la evidencia digital.* Revista Técnica Administrativa, 19, 1–10. Ciencia y Técnica Administrativa.

Velero. (2024). *Velero documentation: Backup and restore for Kubernetes workloads.* Cloud Native Computing Foundation.

World Wide Web Consortium. (2021). *Trace context (W3C Recommendation).*

Zipkin Team. (2024). *Zipkin documentation.*

Zhang, Y., et al. (2020). Ephemeral computing in cloud forensics. *Journal of Cloud Computing, 9*(1), 1–15.