Documentación técnica

Autor: Ing. Benjamín Abraham

Fecha: 13/12/2025

Uso del sistema de sellado temporal criptográfico en el ámbito penal

(SHA-256 · OpenTimestamps · Blockchain pública)

1. Introducción

En el ámbito del derecho penal, la **evidencia digital** ocupa un rol cada vez más relevante. Comunicaciones electrónicas, documentos digitales, registros informáticos, informes técnicos y archivos multimedia forman parte habitual de investigaciones penales y procesos judiciales.

La particularidad de este tipo de evidencia es que:

- puede ser copiada sin límite,
- puede ser modificada sin dejar huellas visibles,
- puede ser cuestionada en cuanto a su fecha de creación o alteración.

El sistema de sellado temporal criptográfico aquí descripto fue diseñado para **aportar un soporte técnico objetivo** que permita **demostrar la existencia temporal e integridad de archivos digitales**, sin sustituir la función judicial ni la actividad pericial.

2. Finalidad del sistema en contextos penales

El sistema permite:

- respaldar técnicamente la **preexistencia de un archivo digital**,
- demostrar que un contenido **no fue modificado** desde un determinado momento,
- preservar evidencia digital **sin alterar el archivo original**,
- facilitar posteriores verificaciones periciales.

Su función es **preventiva, conservativa y corroborativa**, no probatoria automática.

3. Naturaleza del sistema

El sistema implementa un mecanismo de:

- sellado temporal criptográfico,
- basado en funciones hash,
- con anclaje en registros distribuidos públicos (blockchain).

No se trata de un sistema de:

- vigilancia,
- interceptación,
- monitoreo,
- ni obtención de prueba.

El usuario **conserva en todo momento el control del archivo original**.

4. Fundamento técnico: función hash criptográfica (SHA-256)

4.1 ¿Qué es un hash?

Una función hash criptográfica transforma un archivo digital en una **huella digital única**, de longitud fija, representativa de su contenido.

El sistema utiliza el algoritmo **SHA-256**, estándar internacional ampliamente aceptado en contextos forenses e informáticos.

4.2 Relevancia en materia penal

Desde el punto de vista técnico:

- el mismo archivo genera siempre el mismo hash,
- cualquier modificación genera un hash completamente distinto,
- no es posible reconstruir el archivo a partir del hash.

Esto permite utilizar el hash como **identificador objetivo del contenido**, sin necesidad de exponerlo.

5. El problema de la fecha en evidencia digital penal

En investigaciones penales, la **dimensión temporal** resulta crítica:

- secuencia de hechos,
- anterioridad o posterioridad de conductas,
- conservación de evidencia,
- cadena de custodia.

Las fechas internas de los archivos digitales:

- dependen del dispositivo,
- pueden ser alteradas,
- no constituyen por sí solas una referencia confiable.

Por ello, el sistema incorpora un **mecanismo externo, independiente y verificable** de sellado temporal.

6. Sellado temporal descentralizado

6.1 Protocolo OpenTimestamps

El sistema utiliza el protocolo **OpenTimestamps**, diseñado para asociar datos a un momento temporal sin necesidad de confiar en una autoridad central.

Características relevantes:

- no almacena documentos,
- no almacena información legible,
- permite verificación independiente,

- utiliza pruebas criptográficas encadenadas.

6.2 Anclaje en blockchain pública

El sellado se ancla en la blockchain pública de **Bitcoin**, aprovechando su carácter:

- público,
- distribuido,
- resistente a alteraciones,
- verificable en el tiempo.

Una vez anclado, el registro **no puede ser modificado sin alterar la blockchain completa**, lo cual resulta técnicamente inviable.

7. Procedimiento técnico de sellado

El procedimiento consta de las siguientes etapas:

1. Selección del archivo digital.
2. Cálculo local del hash SHA-256.
3. Generación de una prueba criptográfica.
4. Anclaje del hash en blockchain.
5. Emisión de un archivo de prueba `.ots`.

El archivo original:

- no se sube,
- no se almacena,
- no se comparte,
- no se modifica.

8. Archivo de prueba (.ots)

El archivo `.ots` constituye el **comprobante técnico del sellado temporal**.

Contiene:

- la cadena de pruebas criptográficas,
- la referencia al anclaje en blockchain,
- la información necesaria para su verificación futura.

No contiene:

- el documento original,
- datos personales,
- información sobre el contenido.

9. Verificación técnica y pericial

La verificación puede realizarse en cualquier momento posterior, incluso por terceros independientes, y consiste en:

- recalcular el hash del archivo,
- compararlo con el hash sellado,
- verificar la prueba OpenTimestamps,
- confirmar el anclaje en blockchain.

Este proceso es:

- objetivo,
- reproducible,
- auditable,
- compatible con pericias informáticas.

10. Alcance del sistema en el proceso penal

10.1 Qué puede aportar técnicamente

El sistema puede aportar información técnica objetiva respecto de:

- existencia temporal de un archivo,
- integridad del contenido,
- inalterabilidad posterior,
- preservación temprana de evidencia digital.

Resulta especialmente útil en:

- denuncias penales,
- investigaciones preliminares,
- conservación de evidencia,
- respaldo previo a allanamientos o secuestros digitales.

10.2 Qué no acredita el sistema

El sistema **no acredita por sí mismo**:

- autoría penal,
- intencionalidad,
- veracidad del contenido,
- identidad del sujeto,
- licitud u origen del archivo.

Su función es **complementaria** y siempre sujeta a valoración judicial.

11. Cadena de custodia digital

El sistema puede integrarse como **herramienta auxiliar** dentro de una cadena de custodia digital, al permitir:

- fijar un estado inicial del archivo,

- demostrar que no fue alterado,
- facilitar su control pericial posterior.

No sustituye los protocolos formales de custodia.

12. Seguridad y confidencialidad

- No se almacenan archivos.
- No se procesan datos personales.
- No se crea base de evidencia.
- El sistema trabaja exclusivamente con huellas criptográficas.

Esto reduce riesgos de:

- filtraciones,
- contaminación de prueba,
- exposición indebida de información sensible.

13. Independencia y perdurabilidad

Una vez generado el archivo `.ots`:

- no depende de la plataforma,
- puede verificarse con herramientas abiertas,
- mantiene su validez técnica en el tiempo.

Esto resulta especialmente relevante en procesos penales de larga duración.

14. Consideración final

El sistema de sellado temporal criptográfico constituye una **herramienta técnica de apoyo** para la preservación y verificación de evidencia digital en el ámbito penal, aportando **información objetiva sobre la existencia temporal e integridad de archivos**, sin sustituir la función jurisdiccional ni la actividad pericial.