ANEXO TÉCNICO

Autor: Ing. Benjamín Abraham

Fecha: 13/12/2025

SISTEMA DE SELLADO TEMPORAL CRIPTOGRÁFICO Y VERIFICACIÓN DE DOCUMENTOS DIGITALES

Adaptado al proceso civil – República Argentina

(SHA-256 – OpenTimestamps – Blockchain pública)

I. OBJETO DEL ANEXO (FUERO CIVIL)

El presente anexo técnico se acompaña a fin de **brindar al Tribunal una explicación clara, completa y accesible** del funcionamiento y alcance de un **sistema de sellado temporal criptográfico de documentos digitales**, utilizado como **medio de soporte informativo de carácter técnico** dentro del presente proceso civil.

El objetivo del anexo es **facilitar la comprensión y valoración judicial** de la prueba documental digital ofrecida, conforme a los **principios de libertad probatoria, amplitud de medios de prueba y sana crítica racional** que rigen en el proceso civil argentino.

Este documento **no pretende atribuir efectos jurídicos automáticos**, ni sustituir la apreciación judicial, sino **poner a disposición del Tribunal información técnica objetiva**.

II. DOCUMENTO DIGITAL Y PROBLEMÁTICA PROBATORIA EN EL PROCESO CIVIL

En el ámbito del derecho civil contemporáneo, una parte significativa de los actos jurídicos, comunicaciones, contratos, informes y manifestaciones de voluntad **se instrumentan en formato digital**, lo cual genera particularidades probatorias relevantes.

A diferencia del documento en soporte papel, el documento digital:

- puede ser copiado sin límite,
- puede ser modificado sin dejar rastros visibles,
- carece de fecha cierta intrínseca confiable,
- depende de sistemas informáticos para su conservación y lectura.

En consecuencia, en el proceso civil surge con frecuencia la necesidad de **acreditar la preexistencia temporal de un documento digital** y **su inalterabilidad**, especialmente en conflictos contractuales, patrimoniales, societarios, de consumo o de responsabilidad civil.

III. DESCRIPCIÓN GENERAL DEL SISTEMA UTILIZADO

El sistema aquí descripto permite:

- **acreditar técnicamente que un documento digital existía en un momento determinado**,
- **demostrar que su contenido no fue modificado con posterioridad**,
- **permitir su verificación objetiva en cualquier momento del proceso**.

Todo ello se realiza:

- sin almacenar el documento,

- sin acceder a su contenido,
- sin generar copias,
- sin depender de una autoridad certificante privada o estatal.

IV. FUNDAMENTO TÉCNICO: FUNCIÓN HASH CRIPTOGRÁFICA (SHA-256)

IV.1. Concepto

El sistema utiliza una función hash criptográfica, específicamente el algoritmo **SHA-256**, que transforma un archivo digital en una **huella digital única**, representativa de su contenido.

Desde el punto de vista técnico-jurídico, el hash cumple una función equivalente a un **identificador objetivo del documento**.

IV.2. Relevancia probatoria del hash en el proceso civil

Las propiedades del hash permiten afirmar que:

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

Por ello, el hash funciona como un **sustituto técnico del documento**, útil para demostrar **identidad de contenido**, sin necesidad de exponer el contenido mismo.

V. LA FECHA CIERTA EN DOCUMENTOS DIGITALES

En el proceso civil, la **fecha cierta** reviste particular importancia (v.gr. contratos, comunicaciones, actos unilaterales, notificaciones).

Las fechas internas de un archivo digital:

- no dependen de terceros,
- pueden ser alteradas,
- no constituyen por sí mismas un elemento confiable.

El sistema aquí utilizado incorpora un **mecanismo externo, verificable e independiente**, que permite asociar el hash del documento a un momento temporal objetivable.

VI. SELLADO TEMPORAL DESCENTRALIZADO

VI.1. OpenTimestamps

El sistema emplea el protocolo **OpenTimestamps**, que permite realizar sellados temporales **sin intervención de una autoridad central**.

Este protocolo:

- no almacena documentos,
- no almacena datos personales,
- genera pruebas criptográficas verificables por terceros.

VI.2. Anclaje en blockchain pública

El sellado se ancla finalmente en la blockchain pública de **Bitcoin**, lo cual permite:

- asociar el hash a un bloque con fecha y hora verificables,
- garantizar la inmutabilidad del registro,
- permitir su verificación independiente.

VII. PROCEDIMIENTO TÉCNICO DE SELLADO (EXPLICADO)

El procedimiento utilizado consta de las siguientes etapas:

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

El documento **nunca se incorpora a la blockchain**, ni se transmite a terceros.

VIII. ARCHIVO DE PRUEBA (.OTS) COMO SOPORTE DOCUMENTAL

El archivo `.ots` constituye el **soporte técnico del sellado temporal** y puede ser acompañado al expediente como:

- respaldo documental,
- anexo informático,
- elemento a verificar pericialmente.

Contiene únicamente la información necesaria para verificar:

- la existencia temporal,
- la integridad del documento.

IX. PROCEDIMIENTO DE VERIFICACIÓN EN SEDE JUDICIAL

La verificación puede realizarse en cualquier etapa del proceso civil y consiste en:

1. Recalcular el hash del documento acompañado.
2. Compararlo con el hash sellado.
3. Verificar la cadena criptográfica.
4. Confirmar el anclaje en blockchain.

Este procedimiento es:

- objetivo,
- reproducible,
- independiente de la parte que lo produjo.

X. ALCANCE PROBATORIO EN EL PROCESO CIVIL

X.1. Lo que permite acreditar

Desde el punto de vista técnico, el sistema permite acreditar:

- la **preexistencia temporal** del documento,
- la **integridad del contenido**,
- la **inalterabilidad posterior**.

Ello resulta particularmente relevante en procesos civiles vinculados a:

- contratos,
- comunicaciones electrónicas,
- informes,
- presupuestos,
- intercambios previos al litigio.

X.2. Lo que no acredita

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

- autoría,
- consentimiento,
- voluntad negocial,
- validez jurídica del acto,
- identidad de las partes.

Su función es **complementaria** de la prueba documental, testimonial y pericial.

XI. VALORACIÓN JUDICIAL (PROCESO CIVIL)

El sistema debe ser valorado conforme a:

- las reglas de la sana crítica racional,
- el principio de apreciación integral de la prueba,
- la concordancia con otros elementos probatorios.

Puede operar como:

- indicio técnico,
- medio corroborante,
- soporte de pericia informática.

XII. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El sistema respeta principios relevantes en materia civil:

- confidencialidad contractual,
- protección de información sensible,

- minimización de datos.

No se almacenan documentos ni datos personales.

XIII. INDEPENDENCIA Y PERDURABILIDAD PROBATORIA

Una vez emitido el archivo `.ots`:

- no depende del proveedor,
- puede verificarse con software abierto,
- conserva su valor técnico en el tiempo.

XIV. CONCLUSIÓN (FUERO CIVIL)

El sistema descripto constituye un **medio técnico idóneo** para aportar al proceso civil **información objetiva sobre la existencia temporal e integridad de documentos digitales**, quedando su valoración sujeta al criterio del Tribunal conforme a derecho.