# Whitepaper Técnico

## Uso Combinado de Hash y Estampa de Tiempo en Sistemas SGDEA y Preservación Digital

### Introducción

La garantía de integridad, autenticidad y trazabilidad temporal de los documentos electrónicos requiere la articulación de mecanismos técnicos complementarios. El uso conjunto de funciones hash y estampas de tiempo permite crear una arquitectura de confianza robusta, especialmente en sistemas de gestión documental electrónica (SGDEA), automatización de procesos (BPM) y preservación digital a largo plazo. Este whitepaper explora la implementación integrada de estas tecnologías en plataformas como DIGIFILE, alineadas con marcos como OAIS, MoReq y las mejores prácticas internacionales.

### 1. Integración Técnica: Flujo de Hash y Estampa de Tiempo

El proceso técnico para aplicar hash y estampa de tiempo en conjunto sigue típicamente estos pasos:

- Se genera el documento final (ej. resolución, certificado, acta).
- Se calcula un resumen hash con SHA-256 o superior.
- Este hash se envía a una TSA para obtener la estampa de tiempo (RFC 3161).
- La TSA retorna un archivo con sello digital (TSR) con la hora certificada.
- El sistema registra tanto el hash como la estampa en los metadatos del documento.
- Opcionalmente, se firma digitalmente el documento, que ya contiene hash y timestamp.

Este flujo técnico asegura integridad y evidencia temporal simultáneamente,

cumpliendo con estándares técnicos y jurídicos.

## 2. Aplicaciones en Plataformas SGDEA y BPM

La combinación hash + timestamp se implementa en:

- Expedientes electrónicos: para validar que un expediente cerrado no ha sido modificado.
- Flujos de aprobación BPM: documentos firmados son registrados con su hash y sello temporal.
- Transferencias documentales: el AIP incluye hash y timestamp para cada objeto digital.
- Auditorías internas: validación cruzada entre hash actual y hash original + estampa.
- Preservación digital: el AIP puede renovarse con nueva estampa al actualizar formato.
- Respaldo en litigios: permite demostrar no modificación desde una fecha específica.

## 3. Arquitectura de Implementación en DIGIFILE

DIGIFILE implementa esta combinación de la siguiente manera:

- Generación automática del hash en pasos definidos del BPM (ej. firma, cierre, exportación).
- Integración API con TSA para obtener estampas de tiempo certificadas (ej. GSE, Certicámara).
- Registro de hash y timestamp en campos protegidos en base de datos y metadatos PREMIS.
- Validación de integridad automatizada al acceder al documento.
- Historial de eventos hash/timestamp registrado por expediente o documento individual.
- Generación de bitácoras para preservación y control archivístico.

Esta arquitectura permite cumplir con requisitos de trazabilidad documental, interoperabilidad y confianza institucional.

## 4. Estándares y Buenas Prácticas

Recomendaciones para una implementación segura:

- Utilizar SHA-256 como mínimo estándar institucional.
- Usar TSA certificadas que cumplan RFC 3161 o eIDAS.
- Registrar los resultados en metadatos estructurados como PREMIS, METS o Dublin Core.
- Auditar periódicamente que los hashes no cambian y los timestamps siguen válidos.
- Asociar cada hash/timestamp con los eventos del flujo BPM.
- Renovar estampas de tiempo si el formato del documento se actualiza para preservación.

Estas prácticas aseguran cumplimiento con modelos como OAIS y MoReq.

## Conclusión

El uso combinado de funciones hash y estampas de tiempo es una estrategia técnica esencial para garantizar la integridad, la trazabilidad temporal y la validez a largo plazo de los documentos electrónicos. Plataformas como DIGIFILE incorporan esta combinación como parte de su arquitectura de confianza, permitiendo a las organizaciones públicas y privadas adoptar prácticas archivísticas modernas, seguras y legalmente válidas.