# Whitepaper Técnico

## Fundamentos Criptográficos del Hash y su Aplicación en la Gestión Documental Electrónica

### Introducción

En el contexto de la gestión documental electrónica y la transformación digital institucional, garantizar la integridad de los documentos es una necesidad crítica. Una de las herramientas más robustas y ampliamente aceptadas para cumplir con este propósito es la función criptográfica de hash. Este whitepaper explica a profundidad qué es un hash, cómo se calcula, sus propiedades matemáticas y su aplicación práctica en sistemas como los SGDEA, BPM y plataformas de preservación digital como DIGIFILE.

### 1. Definición y Propiedades de una Función Hash

Una función hash criptográfica es un algoritmo matemático que toma una entrada (un archivo, texto o dato digital) y produce una cadena de longitud fija (hash o resumen) que representa de manera única dicha entrada. Las funciones hash usadas en entornos documentales deben cumplir las siguientes propiedades:

- Determinismo: El mismo archivo siempre genera el mismo hash.
- Unicidad (no colisión): Archivos distintos no deben generar el mismo hash.
- Irreversibilidad: No se puede reconstruir el archivo original a partir del hash.
- Sensibilidad:
- Cambios mínimos en el archivo generan hashes totalmente distintos.

- Eficiencia: Rápido de calcular incluso para archivos grandes.

## 2. Principales Algoritmos de Hash Criptográfico

Entre los algoritmos más utilizados para calcular hashes se encuentran:

- SHA-1 (Secure Hash Algorithm 1): Genera un hash de 160 bits. Actualmente considerado inseguro para entornos críticos.
- SHA-256 (Secure Hash Algorithm 2):** Genera un hash de 256 bits. Es el estándar actual más recomendado en gestión documental y firma electrónica.
- SHA-512: Genera un hash más largo y seguro, usado en entornos de alta seguridad.
- SHA-3: Última generación de algoritmos aprobados por NIST, con un enfoque distinto (Keccak).

Ejemplo práctico:
El archivo 'resolucion_123.pdf' genera el siguiente hash con SHA-256

## 3. Uso del Hash en SGDEA y BPM

En sistemas como DIGIFILE SGDEA y DIGIFILE BPM, el hash se usa para:

- Verificar integridad: Almacenar el hash del documento cuando se genera o firma, y recalcularlo cuando se consulta para detectar cambios.
- Control de versiones: Detectar si dos versiones son idénticas o han sido alteradas.
- Trazabilidad documental: El hash forma parte del registro de auditoría y puede asociarse a la bitácora del proceso BPM.
- Exportación segura: Al generar un AIP o cerrar un expediente, el hash se incluye en el metadato de preservación para validación futura.
- Interoperabilidad: En esquemas como e-Codex, MoReq o XAdES, el hash permite validar documentos transferidos entre entidades.

## 4. Buenas Prácticas y Recomendaciones Técnicas

Para garantizar una implementación segura y auditable del hash:

- Usar SHA-256 o superior como estándar institucional.
- Guardar el hash en campos protegidos de la base de datos.
- Incluir el hash en los metadatos PREMIS o Dublin Core.
- Asociar cada hash al usuario y proceso que lo generó.
- Validar automáticamente el hash al abrir o exportar el documento.
- Generar logs de comparación entre hashes actuales y originales.

El hash debe ser considerado un elemento esencial de la arquitectura de confianza digital institucional.

## Conclusión

El uso de funciones hash en la gestión documental es un componente técnico indispensable para garantizar la integridad, trazabilidad y autenticidad de los documentos electrónicos. Su aplicación coherente dentro de plataformas como DIGIFILE permite cumplir con estándares archivísticos, jurídicos y tecnológicos, fortaleciendo la gobernanza digital y la confiabilidad institucional.