VERIFICACIÓN DE LA INTEGRIDAD DE LA INFORMACIÓN

En este soporte se ha incluido un fichero que hace uso del mecanismo criptográfico MD5 (“Message-Digest Algorithm 5”, que puede traducirse como “Algoritmo 5 de resumen del mensaje”) para poder verificar la integridad de la documentación. Esto significa que cualquier persona puede comprobar si está utilizando una copia íntegra del original o si, por el contrario, algún documento de ella ha sido alterado.

¿Qué es MD5?

MD5 es un algoritmo informático ampliamente utilizado que, mediante ciertas funciones matemáticas, obtiene un "resumen" de cualquier secuencia de datos y, en particular, de un archivo o documento.

El resumen generado por el algoritmo, que se representa habitualmente con una cadena de 32 caracteres, recibe varios nombres: "resumen" y "huella" son algunos de ellos, que proceden de los términos utilizados originalmente en inglés ("digest", "fingerprint", "hash"), términos que también se pueden encontrar en la documentación que se consulte en otros idiomas.

El algoritmo MD5 tiene varias características que lo hacen particularmente interesante. En primer lugar, su aplicación a una misma entrada obtiene siempre la misma salida. Por otro lado, pequeñas diferencias en los documentos de entrada generan normalmente grandes diferencias en la salida, lo que hace que cualquier modificación en el documento original se vea reflejada en el resumen. Además, la probabilidad de que dos documentos distintos generen la misma huella es muy baja. Para terminar, y aunque su utilidad a efectos de verificación es escasa, es imposible averiguar el contenido del documento original a partir de su resumen.

MD5 es un algoritmo público y estandarizado por los organismos que acuerdan las tecnologías utilizadas en Internet, existiendo multitud de herramientas disponibles públicamente para calcular el resumen de cualquier documento.

¿Cómo se puede verificar la integridad de la documentación?

En general, para verificar utilizando MD5 que un documento no ha sido alterado hay que calcular su resumen MD5 aplicándole el algoritmo y comprobar que ese resumen coincide con un valor previamente generado (normalmente por el autor del documento) y hecho público por algún medio.

En el directorio raíz de este soporte digital encontrará un fichero de texto, de nombre Check.md5, que contiene una relación de todos los archivos incluidos en el dispositivo y, para cada uno de ellos, su huella MD5. De esta forma, se puede obtener el resumen de cualquiera de los archivos que residen en el soporte y comprobar que el resultado es el mismo que el indicado en Check.md5 para ese archivo.

La consistencia de este método se basa en que el propio archivo Check.md5 no debe haber sido manipulado, lo cual puede verificarse calculando a su vez su huella MD5 y contrastándola con el valor publicado en la sección correspondiente a "Presupuestos Generales del Estado" del Portal de la Administración Presupuestaria del Ministerio de Hacienda y Administraciones Públicas, en la dirección de Internet http://www.pap.minhap.gob.es.

Resumiendo, la verificación de un archivo cualquiera es un proceso que consta de dos pasos: en primer lugar ha de verificarse la integridad del archivo Check.md5 (una sola vez) y, a continuación, verificar la del fichero objeto de la comprobación apoyándose en el contenido de Check.md5.

El archivo Check.md5 se ha construido durante el proceso de generación del original de la documentación.

Referencias

Portal de la Administración Presupuestaria del Ministerio de Hacienda y Administraciones Públicas:

http://www.pap.minhap.gob.es

Referencia del algoritmo MD5:

http://www.ietf.org/rfc/rfc1321.txt

En muchos sitios de Internet se puede encontrar información de carácter introductorio sobre MD5. Uno de estos sitios es la wikipedia:

http://es.wikipedia.org/wiki/MD5

Ese mismo sitio proporciona información sobre dispositivos de almacenamiento:

http://es.wikipedia.org/wiki/Memoria_flash
http://es.wikipedia.org/wiki/CD-ROM

Para conseguir herramientas MD5 en Internet, puede realizarse una petición al buscador utilizado habitualmente que incluya el término "MD5" y algunos de estos otros: "utilidad", "verificar", "tool", "verify".