Plugin de hashes 1.0

Manual de plugin de AutoFirma

Índice de contenidos

1 Introducción 3
2 Requisitos mínimos 4
3 Instalación del plugin 5
4 Integración 9
4.1 Operaciones soportadas a través de diálogos gráficos 9
4.1.1 Calcular huella digital 9
4.1.2 Comprobar huella digital 10
4.1.3 Calcular huella digital en directorio 10
4.1.4 Comprobar huella digital en directorio 11
4.2 Operaciones soportadas a través de línea de comandos 12
4.2.1 Generación de hashes 13
4.2.2 Comprobación de hashes 13
5 Especificaciones 15
5.1 Algoritmos de hash 15
5.2 Codificación 15
5.3 Propiedades de configuración 15
6 Formatos de fichero 17
6.1 Fichero de hash de directorios en XML 17
6.2 Fichero de hash de directorios en TXT 19
6.3 Fichero de informe de comprobación de directorios 20

1 Introducción

AutoFirma es una herramienta de escritorio con interfaz gráfica que permite la ejecución de operaciones de firma de ficheros locales en entornos de escritorio (Windows, Linux y macOS). También puede utilizarse a través de consola o ser invocada por otras aplicaciones mediante protocolo para la ejecución de operaciones de firma. Esta herramienta admite la instalación de plugins que modifican su comportamiento o le proporcionan nuevas funcionalidades.

El presente documento describe las capacidades del plugin de AutoFirma para la generación y comprobación de hashes (huellas digitales) de ficheros y directorios.

AutoFirma y su plugin de hashes son productos de Software Libre que se pueden usar, a su elección, bajo licencia *GNU General Public License* versión 2 (GPLv2) o superior o bajo licencia *European Software License* 1.1 (EUPL 1.1) o superior.

Puede consultar la información relativa al proyecto Cliente @firma, dentro del cual se encuentra AutoFirma, y descargar el código fuente y los binarios de la aplicación en la siguiente dirección Web:

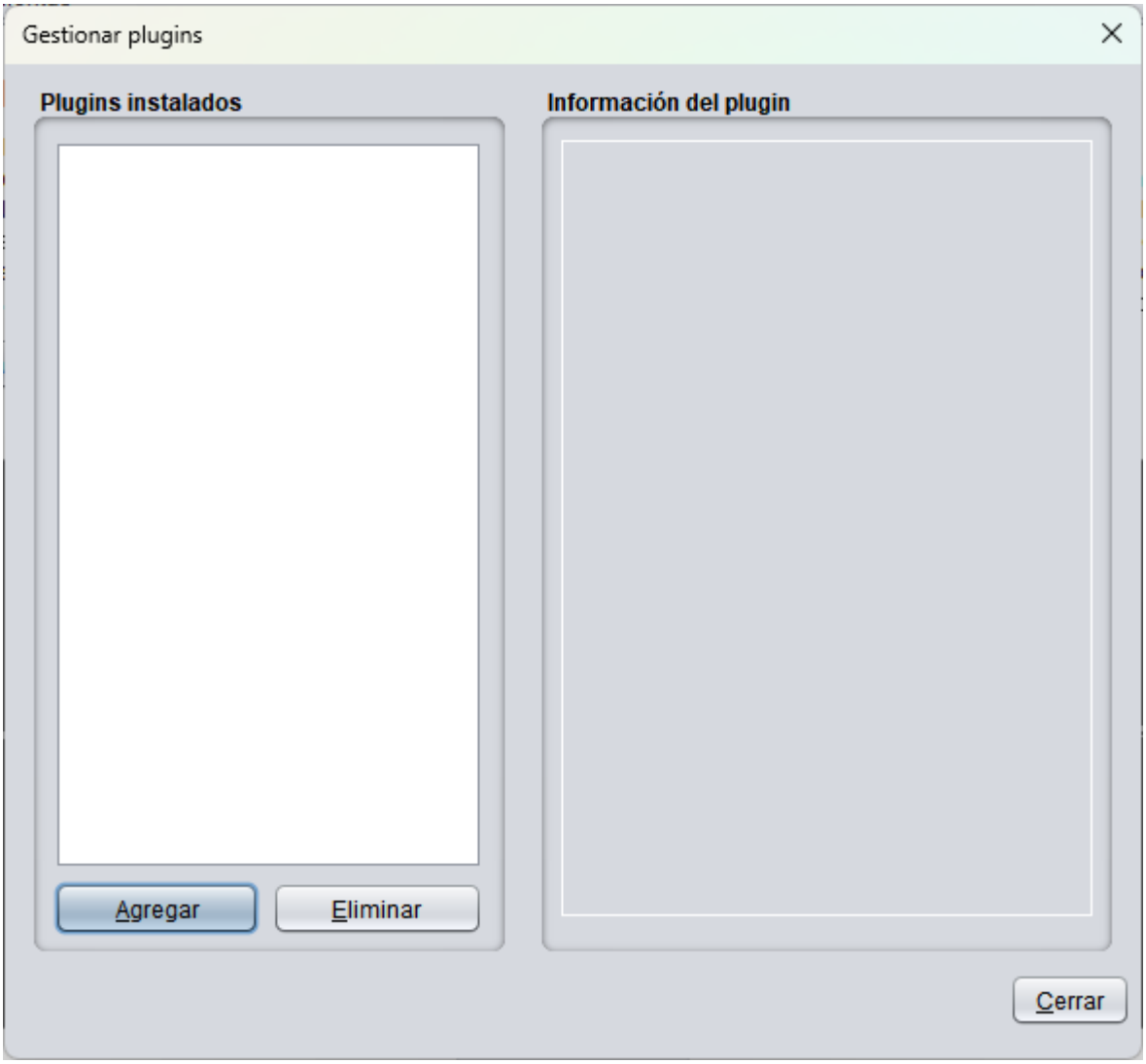
https://administracionelectronica.gob.es/ctt/clienteafirma#.X1o8YcH7RPY

2 Requisitos mínimos

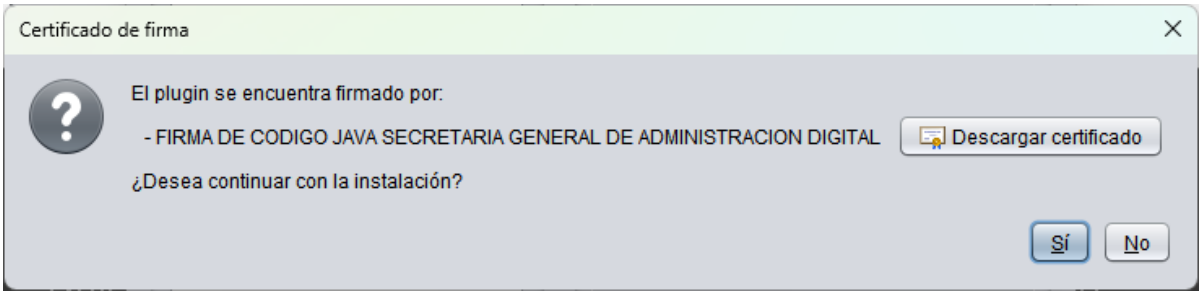
Para el uso del plugin de hashes 1.0 es necesario tener instalado AutoFirma 1.8.0 o superior.

3 Instalación del plugin

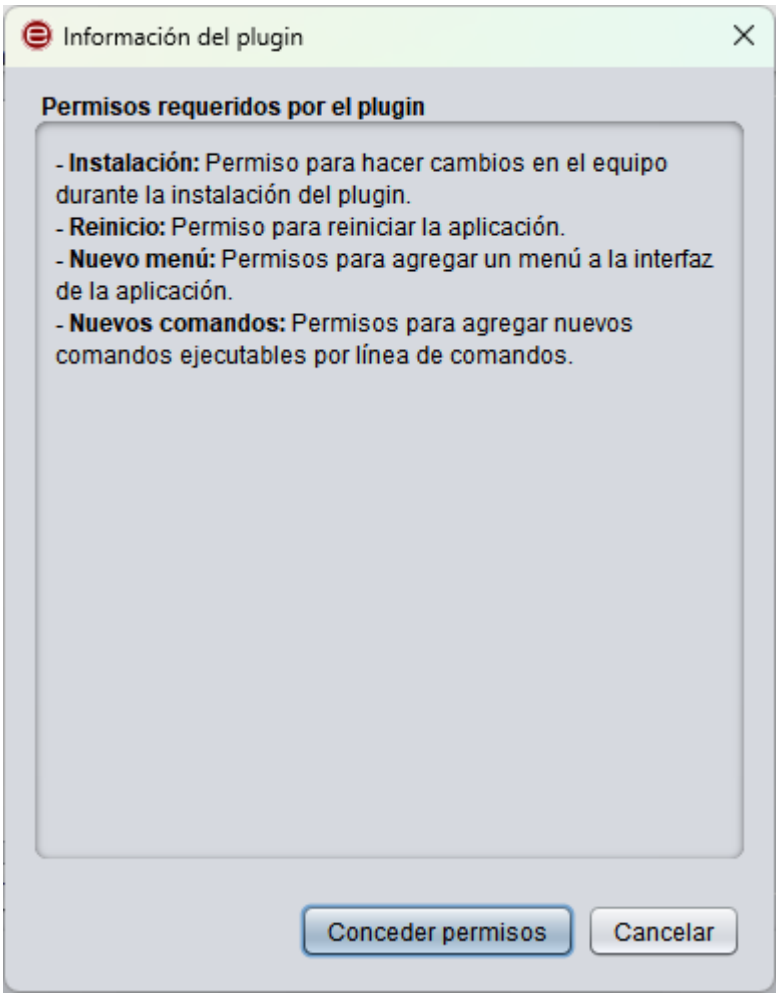
La instalación del plugin de hashes se realiza desde el diálogo de Gestión de plugins de AutoFirma, accesible desde la opción “Gestionar plugins” del menú de la aplicación.



Desde este diálogo el usuario puede pulsar el botón Agregar y seleccionar el fichero “.jar” del plugin de hashes. Tras esto, se mostrará al usuario declarada del firmante del plugin y se podrá descargar y ver el certificado de firma para poder comprobarlo.



Si deseamos continuar con la instalación, pulsamos en el botón "Sí", tras lo que se nos mostrará un diálogo con el listado de permisos necesarios. Podemos cancelar el proceso de instalación pulsando el botón "No".



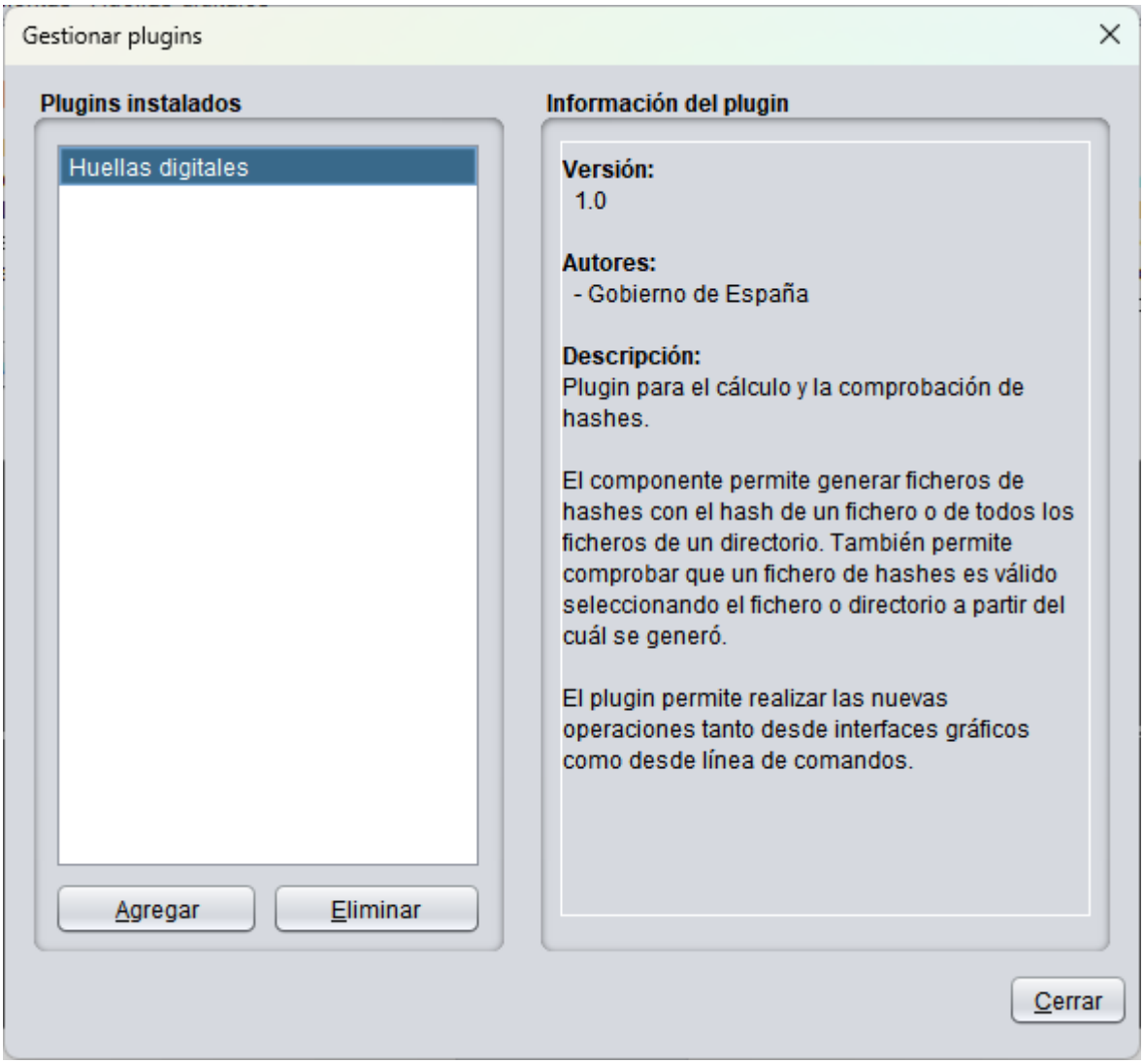
Los permisos requeridos son:

- Instalación: En sistemas Windows, es necesario para integrar las opciones de cálculo y comprobación de hashes en el menú contextual del usuario para ficheros y directorios.

- Reinicio: Se necesita para reiniciar la aplicación después de la instalación.
- Nuevo menú: Necesario para agregar el nuevo menú “Huellas digitales” a la interfaz de AutoFirma.
- Nuevos comandos: Permitirá agregar las nuevas funciones de cálculo y comprobación de hashes a las opciones disponibles de AutoFirma a través de línea de comandos.

Si se está conforme con estos permisos, se debe pulsar en el botón “Conceder permisos” para proceder con la instalación. En caso contrario, se puede pulsar el botón “Cancelar” para abortar la instalación.

Una vez instalado el plugin, se preguntará si se desea reiniciar la aplicación (no el sistema). Tras el reinicio el usuario tendrá disponibles las funciones del plugin y podrá consultar su información desde el mismo diálogo de gestión de plugins.



En sistemas Windows, la instalación del plugin hará aparecer nuevas opciones en el menú contextual del usuario para ficheros y directorios, con los que podrá acceder rápidamente a las funciones de generación y comprobación de hashes.

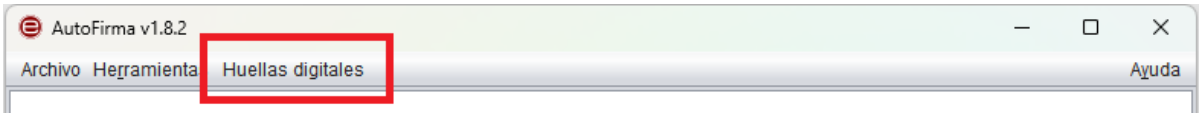
4 Integración

El plugin se integra en AutoFirma a 3 niveles:

- Proporciona diálogos gráficos para el cálculo y la comprobación de hashes de ficheros y directorios.
- Proporciona comandos para ejecutar por consola las operaciones de cálculo y comprobación de hashes.
- En Windows, agrega al menú contextual de los ficheros la opción de calcular el hash del fichero o directorio, y al de los ficheros de hash la función de comprobar hash.

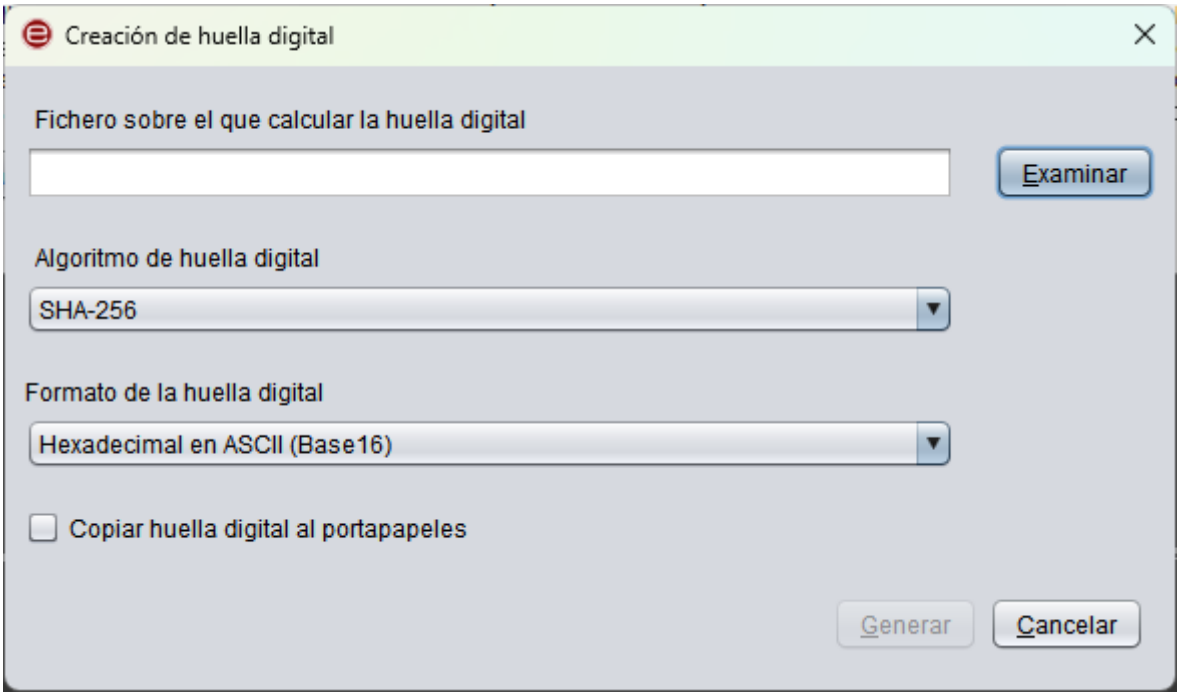
4.1 Operaciones soportadas a través de diálogos gráficos

El usuario puede acceder a las funciones del plugin desde el menú “Huellas digitales” que le aparece en la barra de menús de AutoFirma.



4.1.1 Calcular huella digital

Permite generar el hash de un fichero.



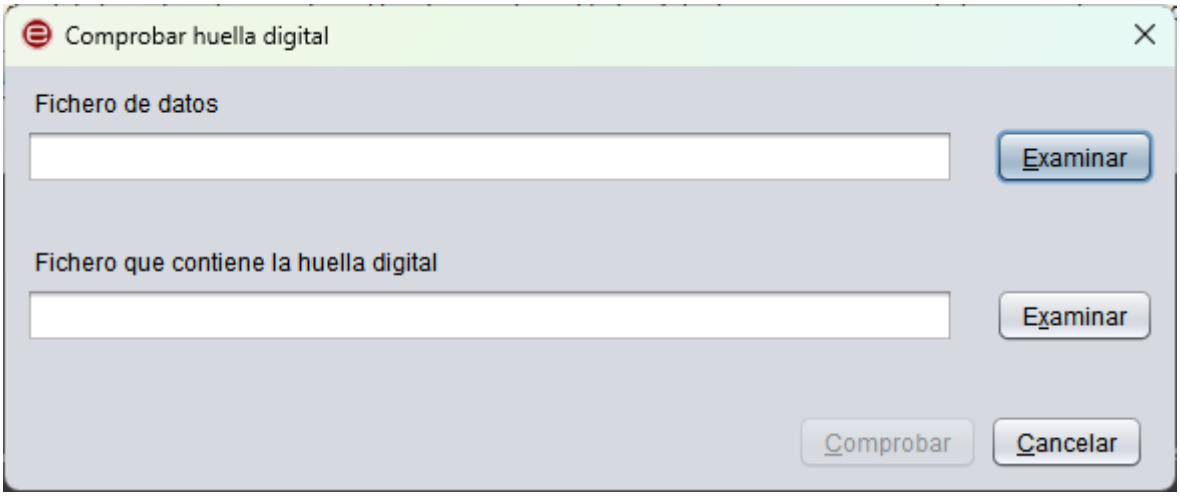
Desde esta ventana el usuario seleccionará el fichero del que desea calcular el hash, indicará el algoritmo de hash y el formato (codificación) que desea emplear para guardarlo. Además, puede seleccionar la opción “Copiar huella al portapapeles” para que, además de poder guardarlo en

fichero, se hash de los datos se guarde en el portapapeles del sistema y así poder pegarlo en cualquier documento como texto. En caso de seleccionar que el hash se copie al portapapeles y el formato binario, la versión copiada en el portapapeles estará codificada en hexadecimal, ya que los datos binarios no son adecuados para luego pegarse como texto.

La extensión por defecto del fichero de hash variará según la codificación elegida: los hashes en hexadecimal se almacenan en ficheros con extensión ".hexhash", para los Base 64 se utiliza ".hashb64" y para los hashes en binario ".hash".

4.1.2 Comprobar huella digital

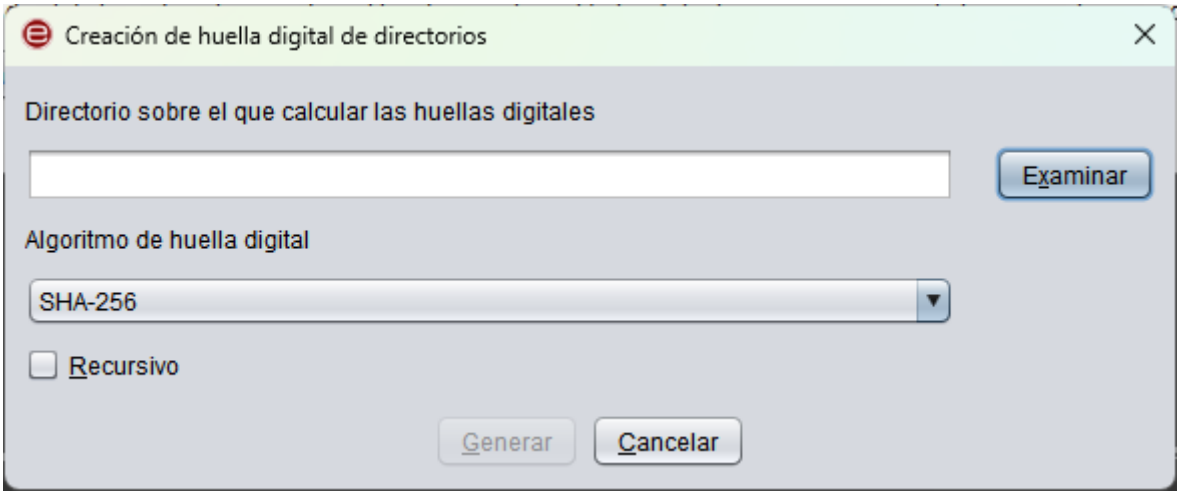
Permite comprobar si un hash se corresponde con el de un fichero.



Desde esta ventana seleccionaremos el fichero de datos del que queremos comprobar el hash y el fichero de hash. Al pulsar el botón "Comprobar", la aplicación nos indica si el hash seleccionado se corresponde con el del fichero o no.

4.1.3 Calcular huella digital en directorio

Permite seleccionar un directorio para generar los hashes de los ficheros que contiene.



El diálogo nos permite seleccionar el directorio con los ficheros y el algoritmo de huella que se desea emplear. Adicionalmente, nos permite seleccionar la opción "Recursivo" para indicar que, además de los ficheros que se encuentren directamente en el directorio, se desea generar la huella de los ficheros de todos los subdirectorios del directorio seleccionado.

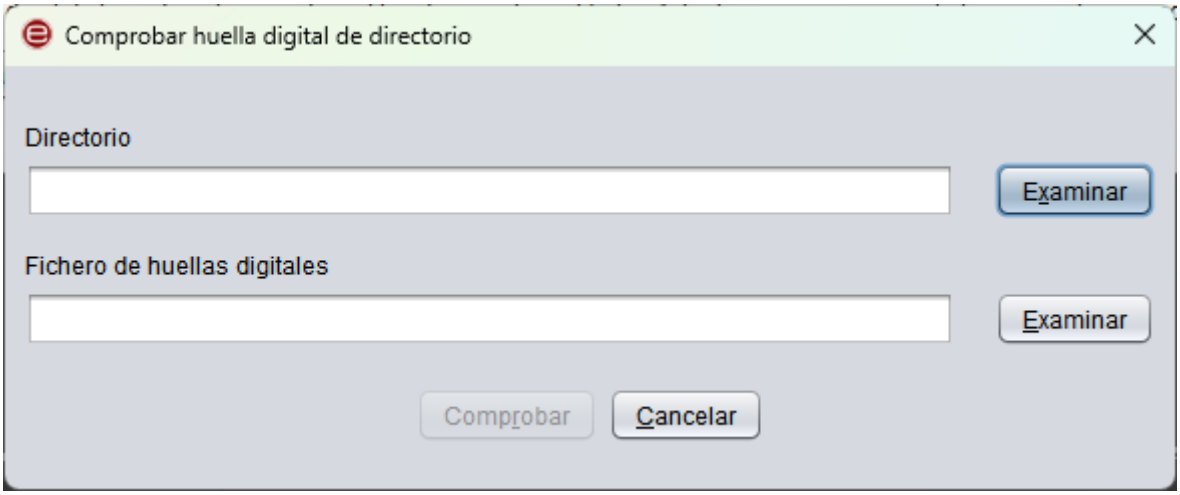
El resultado de la operación se almacenará en un fichero. El formato de este fichero vendrá determinado por el tipo seleccionado en el diálogo de guardado, pudiendo ser:

- Huellas digitales en formato XML (.hashfiles): Este formato almacena los hashes en una estructura XML en la que los guarda codificados tanto en hexadecimal como en base 64. Esta es la opción por defecto y recomendada. Para conocer la estructura del fichero, consulte el apartado 6.1 Fichero de hash de directorios en XML.
- Huellas digitales en formato TXT (.txthashfiles): Este formato almacena los datos en un formato propio de texto. Este formato se mantiene por compatibilidad, pero su implementación es parcial y no se recomienda su uso a través de esta interfaz. Para conocer la estructura del fichero, consulte el apartado 6.2 Fichero de hash de directorios en TXT.

Desde el diálogo de guardado se podrá seleccionar si el fichero almacenará los datos en un formato selección podremos indicar Los hashes se podrán generar con cualquiera de los algoritmos soportados y se almacenarán en una estructura XML que contendrá los hashes en formatos Base 64 y hexadecimal.

4.1.4 Comprobar huella digital en directorio

Permite comprobar las huellas digitales de los ficheros un directorio.



El diálogo nos permite seleccionar el directorio de los datos originales y el fichero con los hashes que se quieren comprobar. Que la comprobación incluya a los ficheros de los subdirectorios dependerá de si al generar los hashes se seleccionó esta opción o no.

Como resultado se indica si la comprobación finalizó correctamente o si se detectó algún problema. Adicionalmente, nos permite almacenar un fichero de informe XML en el que se indica el resultado de la comprobación de cada fichero de hash. El informe puede incluir hasta 4 listados de ficheros:

- Ficheros de los que se comprobó que el hash es correcto.
- Ficheros de los que se comprobó que el hash es incorrecto.
- Ficheros de los que no se encontró el hash.
- Ficheros que no se encontraron a pesar de haber un hash asociado.

Aquellos listados en los que no haya ficheros se omitirán.

Para conocer la estructura del fichero, consulte el apartado 0 La generación de los hashes de un directorio puede almacenarse en un fichero de texto con una estructura definida por el propio AutoFirma. El uso de este tipo de ficheros se utiliza para simplificar el procesado automático de la respuesta desde línea de comandos.

La estructura de este tipo de ficheros es la siguiente:

- Las primeras líneas incluyen una serie de cabeceras, antecedidas por punto y coma (';') y separadas por salto de línea. Las cabeceras aceptadas son:
  - `charset`: Juego de caracteres en el que esta codificado el fichero.
  - `hashAlgorithm`: Algoritmo de hash empleado para calcular el hash de todos los ficheros.
  - `recursive`: Si se procesaron los ficheros de los subdirectorios ("`true`") o no ("`false`").

- Las líneas que siguen incluyen el listado de ficheros procesados (uno por línea). Cada línea está compuesta por:
  - La ruta relativa de un fichero.
  - Un punto y coma (';') como separador.
  - El hash del fichero en hexadecimal.

Un ejemplo de este tipo de fichero es:

```
;charset=UTF-8
;hashAlgorithm=SHA-512
;recursive=true
prenodo2\catalina.out;CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36
CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E
prenodo1\catalina.out;D0967DA528F2CD78386FAC3EA3101CF9F126983DA51B42F77AECA9485B0
4D78163455EE38D32B859E7803F3EB602581F365523C56E442C84A42B568A40C29916
prenodo1\localhost.2023-08-
01.log;D260B1B3BCD5AB3D647175D9B2346BB57321CC63C56E608AF2EDC4037428C5648C620CD64D
C78791A2AD1D3EF74CC5773AA71C355FE6297C461B2517C46655C4
prenodo1\catalina.2023-08-
01.log;8D5129325EB4C1E3DBCE4D3B31561D3EC22246C543EE192241979CE651A4017D193B335860
2BEC095D78CAA0F851359B912575D63EF26359BA8900FBFF2572E2
```

Este fichero corresponde con el resultado de calcular los hashes SHA-512 de forma recursiva de los ficheros de un directorio. Nótese que el hash que se calcula de cada fichero se codifica en hexadecimal sin la 'h' al final, contrariamente a lo que se hace cuando se calcula el hash hexadecimal de un único fichero o cuando el resultado del hash de directorio se compone en XML.

Fichero de informe de comprobación de directorios.

4.2 Operaciones soportadas a través de línea de comandos

La instalación del plugin agrega las siguientes operaciones para ser utilizadas con AutoFirma a través de línea de comandos:

- `createdigest`: Permite generar los hashes de un fichero o directorio.
- `checkdigest`: Permite comprobar los hashes de un fichero o directorio.

Al igual que el resto de los comandos de AutoFirma, para indicar ficheros de entrada o salida por comando se deberá utilizar la ruta absoluta del fichero.

4.2.1 Generación de hashes

Permite indicar un fichero o directorio para generar sus hashes. Se pueden consultar las opciones disponibles para esta operación con el parámetro "`-help`".

```
Sintaxis:
```

```
      AutoFirma createdigest FICHERO [opciones...]  - Calcula la huella digital
de un fichero
      AutoFirma createdigest DIRECTORIO [opciones...]  - Calcula la huella
digital de los ficheros de un directorio

    Parametros:
      FICHERO          (Ruta del fichero del que calcular la huella digital)
      DIRECTORIO       (Ruta del directorio del que calcular las huellas
digitales)

    Opciones de fichero:
      -gui                    (Realiza la operacion con entorno grafico)
      -o FICHERO              (Ruta del fichero de salida con la huella digital)
      -halgorithm ALGORITMO   (Algoritmo de huella digital. Por defecto: SHA-256)
      -hformat FORMATO        (Formato de salida del fichero)
         hex                  (Formato hexadecimal. Por defecto)
         b64                  (Formato Base 64)
         bin                  (Formato binario. Requiere fichero de salida.)

    Opciones de directorio:
      -gui                    (Realiza la operacion con entorno grafico)
      -o FICHERO              (Ruta del fichero de salida)
      -halgorithm ALGORITMO   (Algoritmo de huella digital. Por defecto: SHA-256)
      -hformat FORMATO        (Formato de salida del fichero)
         xml                  (Formato de la salida XML. Por defecto)
         txt                  (Formato de la salida texto plano)
      -r                      (Procesar los ficheros de los subdirectorios)
```

Las opciones de configuración permitidas son las descritas en la ayuda del comando.

El hash del fichero (o la estructura de hashes en caso de ser un directorio) se devuelve como salida del comando o, si se indicó la opción "-o", se guardará en un fichero.

El parámetro "-gui" abre la interfaz gráfica de AutoFirma con la configuración indicada. Este parámetro tiene utilidad cuando se utiliza la operación como parte de un proceso del usuario que ya requiera de su intervención.

4.2.2 Comprobación de hashes

Permite comprobar que hashes generados anteriormente se corresponden con los de un fichero o directorio. Se pueden consultar las opciones disponibles para esta operación con el parámetro "-help".

```
Sintaxis:
      AutoFirma checkdigest [FICHERO] [opciones...]  - Comprueba la huella
digital de un fichero
      AutoFirma checkdigest [DIRECTORIO] [opciones...]  - Comprueba las huellas
digitales de los ficheros de un directorio
```

```
    Parametros:
      FICHERO      (Ruta del fichero del que comprobar la huella digital)
      DIRECTORIO   (Ruta del directorio del que comprobar las huellas digitales)

    Opciones de fichero:
      -gui            (Realiza la operacion con entorno grafico. Obligatorio si
no se indica fichero/directorio)
      -i FICHERO      (Ruta del fichero de entrada con la huella digital)

    Opciones de directorio:
      -gui            (Realiza la operacion con entorno grafico. Obligatorio si
no se indica fichero/directorio)
      -i FICHERO      (Ruta del fichero de entrada con las huellas digitales)
      -o FICHERO      (Ruta del fichero de salida con el informe de validacion)
```

Las opciones de configuración permitidas son las descritas en la ayuda del comando.

El resultado del comando es un texto con el resultado de la operación. En el caso de una validación correcta de los hashes de fichero o directorio se devolverá la cadena "`Comprobacion de huella digital finalizada sin errores`".

El parámetro "`-gui`" muestra únicamente un dialogo con el resultado de la validación. En caso de haber pedido guardar el informe de la validación de un directorio también se almacenará. Este parámetro tiene utilidad cuando se utiliza la operación como parte de un proceso del usuario que ya requiera de su intervención.

5 Especificaciones

5.1 Algoritmos de hash

Todas las operaciones de generación de hash permiten generar los hashes con los algoritmos:

- SHA-256 (Por defecto)
- SHA-384
- SHA-512
- SHA-1 (Desaconsejado por razones de seguridad)

5.2 Codificación

El plugin permite codificar los hashes de fichero de los siguientes modos:

- **Base 64**: El hash se guarda en forma de texto compuesto por el juego de caracteres convencional de Base 64 (caracteres Unicode del '0' al '9', de la 'a' a la 'z', de la 'A' a la 'Z' y los caracteres '/' y '+'). No se aplican saltos de línea y se realiza el relleno final con el carácter '='.
- **Hexadecimal** (Base 16): El hash se guarda en forma de texto compuesto por el juego de caracteres estándar (caracteres Unicode del '0' al '9' y de la 'A' a la 'F'). No se agregan espacios ni ningún otro tipo de separador interno y se terminada la cadena con el carácter 'h' para su correcta identificación.
    - **Advertencia**: En el formato de fichero TXT de cálculo de los hashes de un directorio, se emplea la codificación hexadecimal para el hash, pero este no contiene la 'h' al final.
- **Binario**: El hash se guarda directamente en binario, sin codificar.

La generación de hashes de directorios no permite elegir la codificación y utiliza siempre la Base 64 y la hexadecimal.

La función de comprobación de hashes admite únicamente hashes codificados según estas especificaciones.

5.3 Propiedades de configuración

El plugin de hashes guarda la configuración establecida por el usuario para poder usarla como configuración por defecto en sucesivas operaciones. Estas preferencias se almacenan en el sistema. En el caso de Windows, se almacenan concretamente en las preferencias de usuario del registro. La clave en la que se guardan las preferencias es:

```
HKEY_CURRENT_USER\Software\JavaSoft\Prefs\es\gob\afirma\plugin\hash
```

Esas preferencias no son más que los valores que por defecto se mostrarán al usuario y este es libre de modificarlas en cualquier momento a través de los diálogos del plugin.

Las claves de cadena en las que se guardan las distintas preferencias son:

Clave	Tipo	Descripción
createHashAlgorithm	`String`	Algoritmo de huella digital por defecto para la creación de huellas digitales. Esta preferencia debe tener uno de estos valores: • `SHA1` • `SHA-512` (Por defecto) • `SHA-384` • `SHA-256`
createHashCopyToClipBoard	`true/false`	Copiar huella al portapapeles. El valor `true` (por defecto) indica que, por defecto, se debe copiar al portapapeles del sistema el valor de huella generado. El valor `false` indica que no se copie.
createHashFormat	`String`	Formato en el que almacenar la huella digital de un fichero. Esta preferencia debe tener uno de estos valores: • `hex`: Codificada en hexadecimal. Valor por defecto. • `b64`: Codificada en Base 64. • `bin`: Binario sin

		codificar.
createHashDirectoryAlgorithm	`String`	Algoritmo de huella digital por defecto para la creación de huellas digitales de directorios. Esta preferencia debe tener uno de estos valores: • `SHA1` • `SHA-512` (Por defecto) • `SHA-384` • `SHA-256`
createHashDirectoryRecursive	`true/false`	Procesar subdirectorios en la operación de cálculo de huella digital de directorios. El valor `true` (por defecto) hace que se procesen, mientras que el valor `false` configura que no se procesen.

6 Formatos de fichero

6.1 Fichero de hash de directorios en XML

La generación de los hashes de un directorio puede almacenarse en un fichero XML. Este fichero se estructura según el siguiente XSD:

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<!-- Listado de ficheros -->
<xs:element name="entries">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="entry" type="entryType" maxOccurs="unbounded"/>
      </xs:sequence>

      <!-- Algoritmo de hash -->
```

```
      <xs:attribute name="hashAlgorithm" type="xs:string" use="required"/>
      <!-- Si la operacion incluia subdirectorios -->
      <xs:attribute name="recursive" type="xs:boolean" default="false"/>
    </xs:complexType>
</xs:element>

<!-- Entrada con los hashes de un fichero -->
<xs:element name="entryType">
  <xs:complexType>
    <!-- Hash base 64 del fichero -->
    <xs:attribute name="hash" type="xs:string" use="required"/>
    <!-- Hash hexadecimal del fichero -->
    <xs:attribute name="hexhash" type="xs:string" use="required"/>
    <!-- Ruta relativa con respecto al directorio de origen -->
    <xs:attribute name="name" type="xs:string" use="required"/>
  </xs:complexType>
</xs:element>
</xs:schema>
```

Un ejemplo de XML de hashes de directorio sería:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<entries hashAlgorithm="SHA-512" recursive="true">
    <entry hash="z4PhNX7vuL3xVChQ1m2AB9Yg5AULVxXcg_SpIdNs6c5H0NE8XYXysP-
DGNKHfuwvY7kxvUdBeoGlODJ6-SfaPg=="
hexhash="CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C
5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3Eh"
name="prenodo2\catalina.out"/>
    <entry hash="0JZ9pSjyzXg4b6w-oxAc-
fEmmD2lG0L3euypSFsE14FjRV7jjTK4WeeAPz62AlgfNlUjxW5ELISkK1aKQMKZFg=="
hexhash="D0967DA528F2CD78386FAC3EA3101CF9F126983DA51B42F77AECA9485B04D78163455EE3
8D32B859E7803F3EB602581F365523C56E442C84A42B568A40C29916h"
name="prenodo1\catalina.out"/>
    <entry
hash="0mCxs7zVqz1kcXXZsjRrtXMhzGPFbmCK8u3EA3QoxWSMYgzWTceHkaKtHT73TMV3OqccNV_mKXx
GGyUXxGZVxA=="
hexhash="D260B1B3BCD5AB3D647175D9B2346BB57321CC63C56E608AF2EDC4037428C5648C620CD6
4DC78791A2AD1D3EF74CC5773AA71C355FE6297C461B2517C46655C4h"
name="prenodo1\localhost.2023-08-01.log"/>
    <entry
hash="jVEpMl60wePbzk07MVYdPsIiRsVD7hkiQZec5lGkAX0ZOzNYYCvsCV14yqD4UTWbkSV11j7yY1m
6iQD7_yVy4g=="
hexhash="8D5129325EB4C1E3DBCE4D3B31561D3EC22246C543EE192241979CE651A4017D193B3358
602BEC095D78CAA0F851359B912575D63EF26359BA8900FBFF2572E2h"
name="prenodo1\catalina.2023-08-01.log"/>
</entries>
```

El XML anterior se correspondería con el fichero de hashes de un directorio. Se ha calculado el hash SHA-512 de los ficheros del directorio y sus subdirectorios. En el directorio se encontraron 4 ficheros en dos subdirectorios distintos y de cada uno se incluye su ruta relativa, su hash Base 64 y su hash en hexadecimal.

6.2 Fichero de hash de directorios en TXT

La generación de los hashes de un directorio puede almacenarse en un fichero de texto con una estructura definida por el propio AutoFirma. El uso de este tipo de ficheros se utiliza para simplificar el procesado automático de la respuesta desde línea de comandos.

La estructura de este tipo de ficheros es la siguiente:

- Las primeras líneas incluyen una serie de cabeceras, antecedidas por punto y coma (';') y separadas por salto de línea. Las cabeceras aceptadas son:
  - `charset`: Juego de caracteres en el que esta codificado el fichero.
  - `hashAlgorithm`: Algoritmo de hash empleado para calcular el hash de todos los ficheros.
  - `recursive`: Si se procesaron los ficheros de los subdirectorios ("`true`") o no ("`false`").
- Las líneas que siguen incluyen el listado de ficheros procesados (uno por línea). Cada línea está compuesta por:
  - La ruta relativa de un fichero.
  - Un punto y coma (';') como separador.
  - El hash del fichero en hexadecimal.

Un ejemplo de este tipo de fichero es:

```
;charset=UTF-8
;hashAlgorithm=SHA-512
;recursive=true
prenodo2\catalina.out;CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36
CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3E
prenodo1\catalina.out;D0967DA528F2CD78386FAC3EA3101CF9F126983DA51B42F77AECA9485B0
4D78163455EE38D32B859E7803F3EB602581F365523C56E442C84A42B568A40C29916
prenodo1\localhost.2023-08-
01.log;D260B1B3BCD5AB3D647175D9B2346BB57321CC63C56E608AF2EDC4037428C5648C620CD64D
C78791A2AD1D3EF74CC5773AA71C355FE6297C461B2517C46655C4
prenodo1\catalina.2023-08-
01.log;8D5129325EB4C1E3DBCE4D3B31561D3EC22246C543EE192241979CE651A4017D193B335860
2BEC095D78CAA0F851359B912575D63EF26359BA8900FBFF2572E2
```

Este fichero corresponde con el resultado de calcular los hashes SHA-512 de forma recursiva de los ficheros de un directorio. Nótese que el hash que se calcula de cada fichero se codifica en

hexadecimal sin la 'h' al final, contrariamente a lo que se hace cuando se calcula el hash hexadecimal de un único fichero o cuando el resultado del hash de directorio se compone en XML.

6.3 Fichero de informe de comprobación de directorios

La validación de los hashes de un directorio produce un informe XML con el resultado de la validación de los hashes de cada uno de los documentos. Este informe cumple con la estructura definida por el siguiente XSD:

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<!-- Listado de resultados de la comprobacion -->
<xs:element name="entries">
    <xs:complexType>
      <xs:sequence>
        <!-- Listados de ficheros con hash correcto -->
        <xs:element name="matching_hash" type="matchType"/>
        <!-- Listados de ficheros con hash erróneo -->
        <xs:element name="not_matching_hash" type="matchType"/>
        <!-- Listados de ficheros que no se encontraron. -->
        <xs:element name="hash_without_file" type="matchType"/>
        <!-- Listados de ficheros encontrados para los que no hay hash -->
        <xs:element name="file_without_hash" type="matchType"/>
      </xs:sequence>

      <!-- Algoritmo de hash -->
      <xs:attribute name="hashAlgorithm" type="xs:string" use="required"/>
      <!-- Si la operacion incluia subdirectorios -->
      <xs:attribute name="recursive" type="xs:boolean" default=”false”/>
    </xs:complexType>
</xs:element>

<!-- Listado de comprobaciones individuales -->
<xs:element name="matchType">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="entry" type="entryType" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
</xs:element>

<!-- Entrada con los hashes de un fichero -->
<xs:element name="entryType">
  <xs:complexType>
    <!-- Hash base 64 del fichero -->
    <xs:attribute name="hash" type="xs:string" use="required"/>
    <!-- Hash hexadecimal del fichero -->
    <xs:attribute name="hexhash" type="xs:string" use="required"/>
    <!-- Ruta relativa con respecto al directorio de origen -->
    <xs:attribute name="name" type="xs:string" use="required"/>
```

```
  </xs:complexType>
</xs:element>
</xs:schema>
```

Un ejemplo de informe de validación de los hashes de directorio sería:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<entries hashAlgorithm="SHA-256" recursive="false">
    <matching_hash>
        <entry name="afirma-ui-simpleafirma-plugin-hash-1.8.jar"/>
        <entry name="AF_manual_plugin_hashes_1_0.pdf"/>
    </matching_hash>
    <hash_without_file>
        <entry name="afirma-ui-simpleafirma-plugin-hash-1.8.jar.hexhash"/>
    </hash_without_file>
</entries>
```

El XML anterior se correspondería con el de un informe de validación de los hashes de un directorio en el que se usó el algoritmo SHA-256 y sólo se procesaron los ficheros del directorio padre (no se calculó el hash de forma recursiva).

El resultado de la validación arroja que se ha validado correctamente que dos de los ficheros del directorio no han cambiado (tienen el mismo hash). Sin embargo, hay un fichero que se ha eliminado del directorio (se ha encontrado su hash, luego existía cuando se calculó el hash del directorio, pero ahora no se encuentra el fichero).

Nótese que de los cuatro tipos de resultado que pueden darse (hash correcto, hash incorrecto, fichero sin hash y hash sin fichero) sólo aparecen los listados en los que se produce alguna ocurrencia durante la validación.