



SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

MiniApplet @firma

---

# Manual de instalación y gestión de AutoFirma 1.7.0

---

## Índice de contenidos

1	Introducción .....	4
1.1	Adecuación al Esquema Nacional de Seguridad .....	5
2	Requisitos mínimos .....	5
2.1	Entorno Cliente .....	5
2.1.1	AutoFirma.....	5
3	Funcionamiento de AutoFirma .....	7
3.1	Uso del DNle y otras tarjetas inteligentes.....	7
3.2	Comunicación con servicios externos .....	8
4	Enlaces de descarga .....	9
5	Instalación .....	9
5.1	Microsoft Windows.....	10
5.1.1	Desinstalación .....	15
5.1.2	Despliegue masivo de la aplicación.....	18
5.1.3	Permisos adicionales .....	19
5.2	Linux .....	20
5.2.1	Instalación por línea de comandos del instalador DEB.....	20
5.2.2	Instalación por línea de comandos del instalador RPM.....	21
5.2.3	Instalación de muestra mediante el asistente de paquetes de Ubuntu/Guadalinex .....	22
5.2.4	Desinstalación del paquete DEB.....	23
5.2.5	Desinstalación del paquete RPM .....	23
5.3	Apple OS X.....	23
5.3.1	Desinstalación .....	26
6	Gestión de AutoFirma .....	27
6.1	Comprobaciones de nuevas versiones al inicio de la aplicación.....	27
6.2	Configuración a través de fichero .....	28
6.2.1	Bloqueo de la configuración.....	29
6.2.2	Firma del fichero de configuración .....	33
6.2.3	Ejemplo de fichero de configuración .....	34
6.3	Configuración a través del registro en Microsoft Windows.....	34

6.4	Opciones configurables .....	35
6.4.1	Opciones Generales .....	35
6.4.2	Firmas PAdES (PDF) .....	38
6.4.3	Firmas CAdES.....	39
6.4.4	Firmas XAdES.....	40
6.4.5	Firmas Factura Electrónica .....	41
6.4.6	Opciones no configurables desde la ventana de preferencias .....	43
6.5	Obtención de estadísticas con Google Analytics.....	45
7	Compatibilidad del MiniApplet @firma con aplicaciones móviles y AutoFirma.....	46
8	Problemas conocidos .....	47
8.1	Al instalar AutoFirma falla la instalación de los certificados de confianza SSL.....	47
8.2	Al instalar AutoFirma en Windows se muestra el error: “Error abriendo archivo para escritura” .....	47
8.3	Al abrir Google Chrome después del proceso de instalación de AutoFirma se muestra un mensaje notificando que la configuración de la aplicación está corrupta .....	47
8.4	AutoFirma en OS X no muestra el título de los diálogos de cargar y guardado de ficheros... ..	48
8.5	Error al importar las opciones de configuración desde un fichero .....	48
8.6	AutoFirma indica que un documento PDF es demasiado grande cuando se intenta firmar con firma visible .....	48
8.7	AutoFirma se cierra inmediatamente tras ser invocado desde el navegador web .....	49
8.8	No se detectan tarjetas inteligentes en macOS.....	49
8.9	AutoFirma no puede comunicarse con el navegador en macOS .....	49

## 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 OS X). También puede utilizarse a través de consola o ser invocada por otras aplicaciones mediante protocolo para la ejecución de operaciones de firma. Esta última funcionalidad puede usarse principalmente mediante el JavaScript de despliegue del MiniApplet @firma, que permitiría que se utilizase AutoFirma en lugar del propio MiniApplet para generar las firmas de un trámite web.

Además de la versión nativa de AutoFirma, existe una versión Java WebStart que puede desplegarse para poder realizar operaciones de firma con AutoFirma desde trámites sin necesidad de que este esté instalado previamente. El despliegue de esta versión de AutoFirma también se realiza mediante el JavaScript de despliegue del MiniApplet @firma.

**El presente documento se centra principalmente en el uso de AutoFirma para firmas web por medio del JavaScript de despliegue del MiniApplet @firma.**

El cliente AutoFirma hace uso de los certificados digitales X.509v3 y de las claves privadas asociadas a estos que estén instalados en el repositorio o almacén de claves y certificados (*KeyStore*) del sistema operativo o del navegador Web (Internet Explorer, Mozilla Firefox, etc.) en caso de realizarse la operación desde un trámite web con el JavaScript de despliegue del MiniApplet @firma. También permite el uso de dispositivos externos (tarjetas inteligentes, dispositivos USB) configurados en estos almacenes de claves (como por ejemplo, el DNI Electrónico o DNle).

El cliente AutoFirma hace uso de las claves privadas asociadas a los certificados del usuario y no permite que estos salgan en ningún momento del almacén (tarjeta, dispositivo USB o navegador) ubicado en su PC.

AutoFirma no almacena ningún tipo de información personal del usuario, ni hace uso de cookies ni ningún otro mecanismo para la gestión de datos de sesión. AutoFirma sí almacena trazas de su última ejecución a efectos de ofrecer soporte al usuario si se encontrase algún error. Estas trazas de ejecución no contienen ningún tipo de información personal y la aplicación no facilita de ninguna forma el acceso a estos datos almacenados.

AutoFirma es una aplicación de Software Libre publicado que se puede usar, a su elección, bajo licencia *GNU General Public License* versión 2 (GPLv2) o superior o bajo licencia *European Software License* 1.1 (EURL 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:

<http://administracionelectronica.gob.es/es/ctt/clienteafirma>

## 1.1 Adecuación al Esquema Nacional de Seguridad

Los productos de la Suite de @firma pueden contener entre los algoritmos disponibles, algunos no recomendados por la Guía 807 del Esquema Nacional de Seguridad (ENS; editada por el Centro Criptológico Nacional, CCN) vigente en el momento de publicación de este documento. Por lo que queda bajo la responsabilidad de las aplicaciones que hacen uso de estos productos el configurar adecuadamente las llamadas a los mismos para generar el resultado esperado, válido y adecuado para ese momento y el nivel de seguridad deseado, utilizando para ello algoritmos de la familia SHA-2 tal y como especifica dicha norma para la generación de firmas electrónicas.

Puede consultar la norma vigente desde el siguiente enlace:

<https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>

## 2 Requisitos mínimos

### 2.1 Entorno Cliente

#### 2.1.1 AutoFirma

El uso de AutoFirma como herramienta de firma integrada dentro del proceso de firma de trámites web tiene los siguientes requerimientos en cuanto a entorno operativo:

- Sistema Operativo
  - Microsoft Windows 7 o superior.
    - Soportado directamente en 7, 8, 8.1 y 10.
    - En 32 o 64 bits.
  - Linux
    - Guadalinux, Ubuntu, OpenSUSE, Fedora.
  - Apple OS X Yosemite o superior.
    - Soportado directamente en Yosemite, El Capitán o Sierra.
- Navegadores Web (para la invocación por protocolo)
  - Microsoft Windows
    - Google Chrome 46 o superior.
    - Mozilla Firefox 41.0.1 o superior.
    - Microsoft Internet Explorer 8 o superior.
    - Microsoft Edge v20 o superior.
  - Linux
    - Mozilla Firefox 41.0.1 o superior.
  - Apple OS X
    - Apple Safari 9.0 o superior.
    - Google Chrome 46 o superior.

- Mozilla Firefox 41.0.1 o superior.

El uso de Microsoft Edge, versiones de Internet Explorer anteriores a la 11 (o la versión 11 en modo de compatibilidad con una versión anterior) y Safari 10 requiere que el despliegue del MiniApplet permita la comunicación a través de servidor intermedio. Consulte el manual del integrador del MiniApplet para más detalles.

En entornos macOS y Windows no es necesario que el usuario tenga instalado un entorno de ejecución de Java, ya que viene incluido en la propia aplicación. En Linux se necesita un entorno de ejecución de Java de Oracle 8 u OpenJDK 8 (marcado como dependencia en el instalador integrado de AutoFirma).

Es obligatorio que AutoFirma sea instalado antes de iniciar el trámite web en el que se usará para ejecutar las operaciones de firma.

### 3 Funcionamiento de AutoFirma

Cuando el entorno del ciudadano firmante no cuenta con un entorno de ejecución de Java instalado y un navegador Web compatible con la ejecución de Applets, el despliegue del MiniApplet deriva las tareas de firma a la aplicación AutoFirma, sin necesidad de que el integrador deba gestionar por su parte esta delegación de tareas. Para aquel integrador que desee conocer los detalles del uso de AutoFirma en trámites web, puede consultar el documento “*MCF\_manual-integrador\_ES*”.

En cualquier caso, para que AutoFirma pueda asumir cualquier operación de firma, es necesario que esté instalada en el equipo local antes de iniciar el trámite de firma. Es responsabilidad del integrador alertar de este hecho cuando sea susceptible que los usuarios no tengan instalada la aplicación.

Ya se ejecute AutoFirma como aplicación de escritorio o sea lanzada por el navegador web, AutoFirma registra la operativa de su última ejecución en un fichero de trazas en el subdirectorio oculto “.afirma” del directorio del usuario. Por ejemplo, “*C:\Users\miusuario\.afirma*”. El fichero generado tiene el nombre “*AUTOFIRMA.afirma.log.xml*”. Los ficheros de trazas del Cliente @firma en ningún caso almacenan información de carácter personal.

#### 3.1 Uso del DNIE y otras tarjetas inteligentes

El Cliente @firma utiliza la biblioteca JMulticard para permitir firmar con DNIE 2.0, DNIE 3.0 y tarjetas inteligentes de la FNMT sin necesidad de que los usuarios tengan instalados los controladores de la tarjeta. Esta biblioteca se utilizará al seleccionar la opción “Continuar con DNIE” al abrir AutoFirma o al invocar a la aplicación desde una página web e insertar el PIN de la tarjeta.

AutoFirma solicita el PIN del DNIE antes de listar los certificados del almacén y de que el usuario indique qué certificado desea utilizarla para firmar. Este comportamiento emula el de los controladores PKCS#11 de las tarjetas en donde el PIN es necesario para listar los certificados contenidos por la tarjeta y sigue la lógica de que si un usuario ha insertado el DNIE en el lector es porque lo desea utilizar. Cuando el usuario inserta el PIN, se listan sus certificados y se abre el canal seguro con la tarjeta y, en el momento de firmar, se utiliza este canal seguro para realizar la operación. A continuación, se cierra el canal seguro.

Todas las operaciones de firma realizadas posteriormente solicitarán el PIN de la tarjeta, pero sólo en el momento de realizar la firma, momento en el cual se volverá a abrir el canal seguro con la tarjeta. Este comportamiento es distinto al del controlador CSP oficial para Windows en donde sólo se pide el PIN la primera vez y se reutiliza para múltiples operaciones de firma.

Si se recargase el almacén por medio de la opción correspondiente del diálogo de selección de certificados, el controlador se reiniciaría y volvería a pedir el PIN de la tarjeta para listar los certificados.

En el caso de ejecutar AutoFirma como aplicación de escritorio en Windows y seleccionar “Usar cualquier certificado” o haberlo invocado desde Internet Explorer o Chrome y cancelar el diálogo de PIN del DNle de JMulticard, se cargará el almacén del sistema normalmente. Si se tiene instalado el controlador oficial del DNle en el equipo esto puede implicar que los certificados del DNle se listen también en el diálogo de selección de certificados ya que será el controlador oficial el que los cargue. En estos casos, también se usará el controlador oficial para realizar la firma.

Si desea utilizar siempre los controladores oficiales de DNle y tarjeta CERES instalados en su equipo y de esta forma evitar insertar el PIN de su tarjeta múltiples veces, puede desactivar la opción “Habilitar JMulticard para el uso de las tarjetas de la FNMT y DNle” desde la pestaña “General” del menú de preferencias de AutoFirma.

### 3.2 Comunicación con servicios externos

Cuando AutoFirma se comunica con servicios externos, por ejemplo, para comprobar si existe una nueva versión o para la comunicación con el navegador web a través del servidor intermedio (consulte el apartado “Compatibilidad con dispositivos móviles y AutoFirma” del manual “MCF\_manual-integrador\_ES” para más información), se utiliza la configuración de proxy de red establecida en AutoFirma y el almacén de confianza de la JRE con la cual se ejecute la aplicación.

Para saber más sobre la configuración del proxy de red en AutoFirma consulte la ayuda integrada de AutoFirma (para la configuración a través de interfaz gráfica) o las opciones de configuración referentes al proxy en el apartado “[6.4.1 Opciones Generales](#)” (para la configuración de la aplicación por parte de un administrador).

En el caso de los certificados de confianza, AutoFirma utilizará el almacén de confianza de la JRE instalada junto a la propia aplicación (en las instalaciones de Windows o macOS) o el almacén de confianza de la JRE instalada en el sistema que se utilice para ejecutarla (en el caso de Linux y AutoFirma WebStart).

Cuando AutoFirma intente acceder a un recurso de red o servicio externo sobre una comunicación SSL, rechazará la conexión en caso de que la conexión se cifrase utilizando un certificado SSL emitido por un prestador distinto a los incluidos en el almacén de confianza o cuando fuese expedido para un dominio distinto al que se intenta acceder. Esta medida de seguridad es necesaria para evitar ataques de seguridad que redireccionen las peticiones del cliente a servidores inseguros.

Para evitar problemas de conexión, asegúrese de cifrar su comunicación SSL con certificados reconocidos por defecto por Java. En caso contrario, el usuario o el administrador de los equipos deberán incluir los certificados de la entidad emisora del certificado SSL en el almacén de confianza de la JRE utilizada.

Para facilitar el despliegue a las entidades que utilizan certificados SSL emitidos por autoridades españolas, en el almacén de confianza de las JRE con las que se distribuyen las versiones de Windows y macOS se incluyen por defecto los certificados raíces de los siguientes prestadores:



- Agencia de Tecnología y Certificación Electrónica (ACCV)
- Fábrica Nacional de Moneda y Timbre (FNMT)

Así pues, AutoFirma permitirá por defecto la conexión con los servicios desplegados sobre conexiones SSL construidas con certificados de estos prestadores.

Esta lista de prestadores podrá variar en futuras versiones de AutoFirma según las solicitudes realizadas por los propios prestadores o entidades públicas que utilicen sus certificados. Requisito indispensable para incorporar un nuevo prestador a esta lista es que se trate de un prestador reconocido por el Ministerio de Energía, Turismo y Agenda Digital.

## 4 Enlaces de descarga

Para instar al usuario que se instale AutoFirma, rediríjalo a la siguiente página web:

<http://firmaelectronica.gob.es/Home/Descargas.html>

## 5 Instalación

La instalación de AutoFirma en el sistema del usuario se asemeja a la instalación de cualquier otra aplicación. Sin embargo, el proceso de instalación incluye un paso de vital importancia para la compatibilidad del aplicativo con los despliegues del MiniApplet para su uso en trámites web.

La comunicación entre la página web y AutoFirma se realiza cuando es posible a través de un socket SSL a través del cual la información viaja siempre cifrada mediante la clave privada de un certificado generado durante el proceso de instalación. Para que sea posible la comunicación entre el navegador web y AutoFirma será necesario que durante la instalación se genere el par de claves con el que se realizará la comunicación, que este se almacene en disco y que el certificado generado sea dado de alta en los almacenes de confianza de los navegadores del sistema. Debido a las medidas de seguridad establecidas por cada navegador web, es posible que esto implique la aparición de un diálogo gráfico de seguridad en el que se debe conceder permisos para realizar esta operación.

El proceso de instalación y configuración de AutoFirma registra el resultado de la operativa de generación del par de claves y su instalación en los almacenes de confianza del sistema. Este fichero se almacena por defecto en el directorio *“.afirma”* dentro del directorio de usuario del usuario que instaló la aplicación. El nombre del fichero de trazas es *“AUTOFIRMA\_CONFIGURATOR.afirma.log.xml”*.

En el caso de Linux y OS X, la instalación se realiza con el usuario administrador y el log se guarda en el directorio temporal del sistema o, si no se puede ahí, en *“/var/tmp”* para facilitar su acceso.

## 5.1 Microsoft Windows

La instalación de AutoFirma en Windows requiere que un usuario con permisos de administrador ejecute la aplicación de instalación. Esta aplicación de instalación se distribuye con el nombre “AutoFirma\_X.Y.Z\_W.exe”, donde X, Y y Z son los números de versión y W, la arquitectura de sistema para la que está preparada. Por ejemplo, “AutoFirma\_1.6.0\_32.exe” se correspondería con AutoFirma versión 1.6.0 para sistema de 32bits.

AutoFirma es compatible con Windows 7 o superior en 32 y 64 bits (x86 o x64). Una vez instalada, puede usarse desde prácticamente cualquier navegador Web. Los navegadores oficialmente soportados son:

- Microsoft Internet Explorer 8 y superiores
- Google Chrome 46 o superior
- Mozilla Firefox 41.0.2 o superior
- Microsoft Edge v20 o superior

AutoFirma puede funcionar correctamente con otros navegadores (Apple Safari, Opera, etc.), pero no se ofrece soporte sobre ellos.

El uso de Microsoft Edge o versiones de Internet Explorer anteriores a la 11 (o la versión 11 en modo de compatibilidad con una versión anterior) requiere que el despliegue del MiniApplet permita la comunicación a través de servidor intermedio. Consulte el manual del integrador del MiniApplet para más detalles.

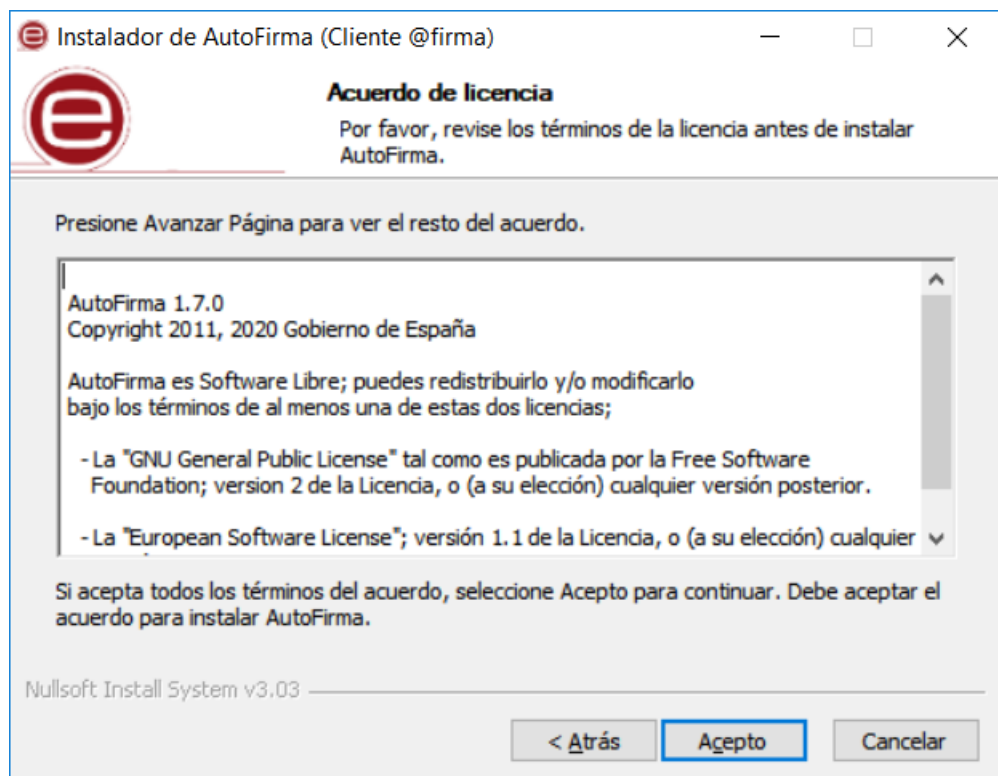
AutoFirma se distribuye en versiones de 32 y 64 bits para Windows. Esta diferenciación afecta únicamente a la cantidad de recursos del sistema que la aplicación es capaz de utilizar. Si se desea utilizar AutoFirma para la generación de firmas de ficheros grandes se deberá usar la versión de 64 bits de AutoFirma.

La instalación es un sencillo asistente con los siguientes pasos:

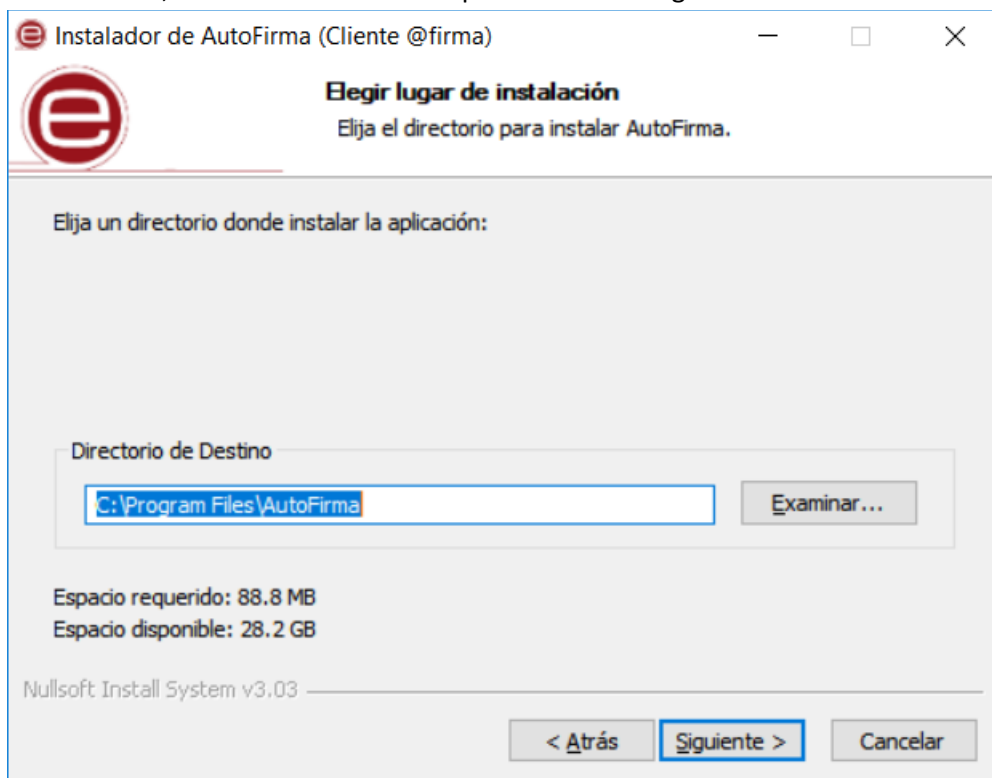
Inicio del instalador:



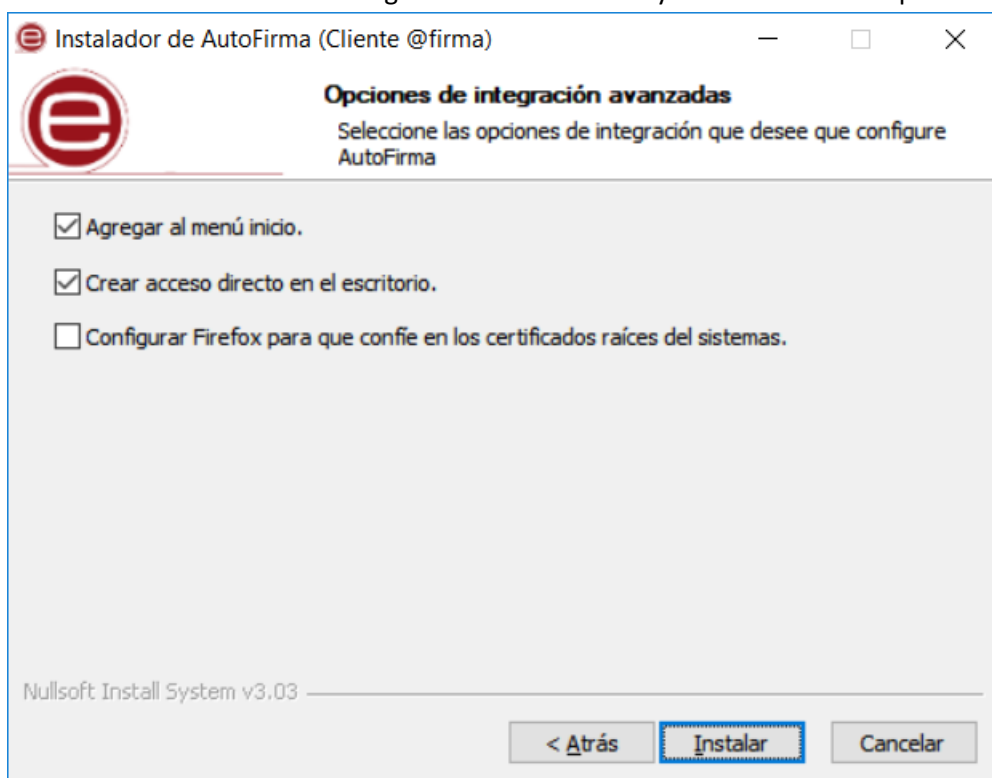
Acuerdo de licencia



Al aceptar el acuerdo, se suceden las distintas pantallas de configuración:



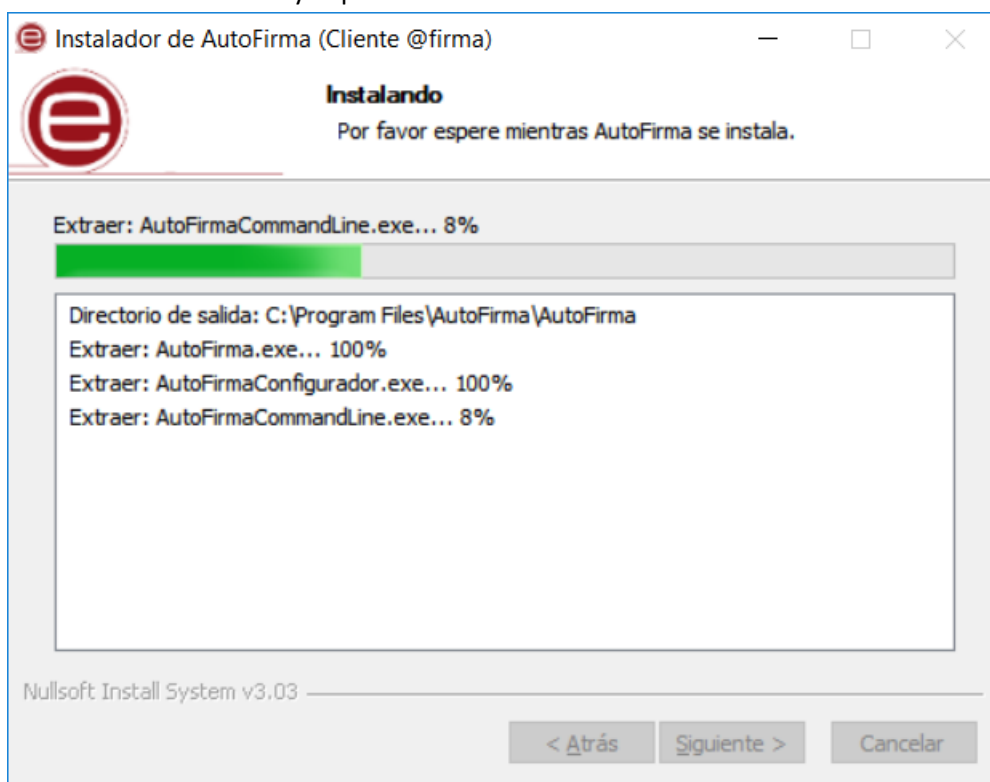
El directorio de instalación en donde se guardarán los ficheros y certificados de la aplicación.



Las opciones de integración avanzadas ofrecidas son:

- Agregar al menú inicio: Al activarlo, se creará un submenú en el menú inicio de Windows con accesos directos a AutoFirma y a su desinstalador.
- Crear acceso directo en el escritorio: Al activarlo, se creará un acceso directo en el escritorio de Windows.
- Configurar Firefox para que confíe en los certificados raíz del sistema: Al activarlo, se modificará la configuración de Firefox para que confíe en los certificados SSL expedidos por los prestadores de confianza del sistema, sin necesidad de que estos prestadores estén dados de alta en el almacén confianza del navegador.

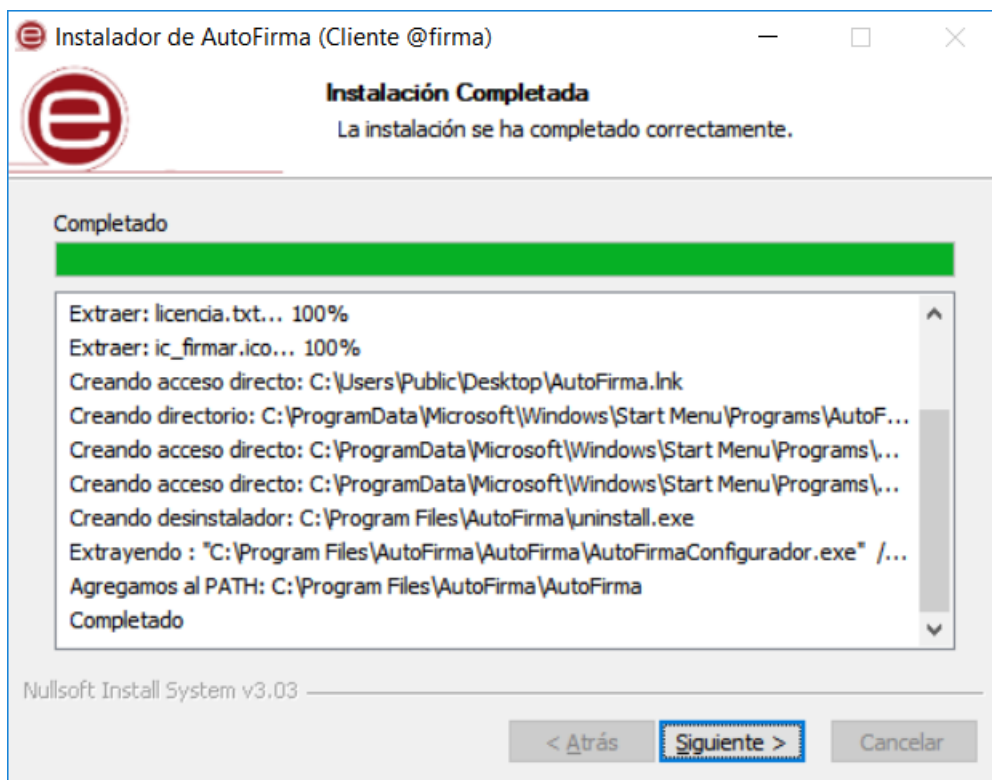
El proceso de instalación extrae y copia los ficheros necesarios.



**ADVERTENCIA:** El proceso de instalación afecta a los perfiles de Mozilla Firefox y a la configuración de Google Chrome. Estos navegadores se cerrarán automáticamente durante el proceso de instalación desatendido mediante el instalador MSI. Si se utiliza el instalador EXE, será necesario que el usuario cierre manualmente estos navegadores.

Téngase en cuenta que el navegador Google Chrome puede quedar abierto incluso después de cerrar su ventana. En esos casos, aparecerá un icono en el área de notificaciones del escritorio del usuario y deberá cerrarse a través de la opción proporcionada en el menú contextual de este icono.

Al completarse el instalador, se mostrará el mensaje de “Completado”.



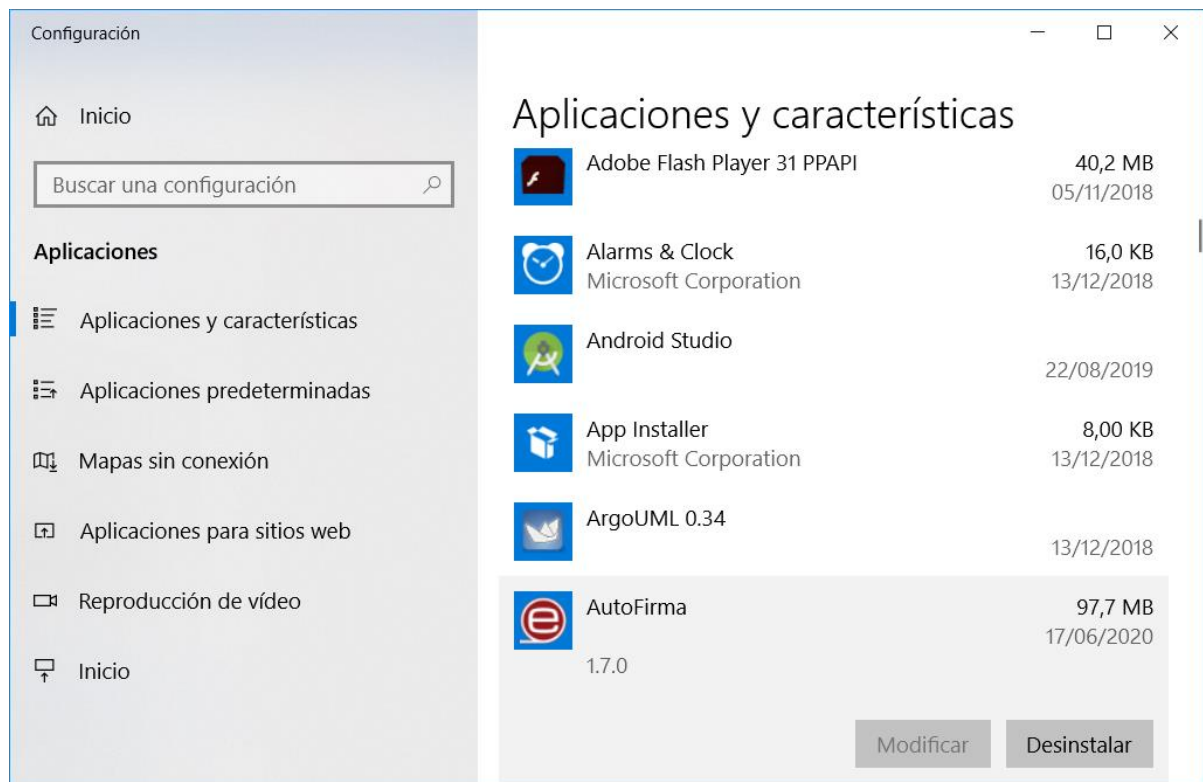
Al pulsar el botón "Siguiete", se mostrará el resultado de la instalación.



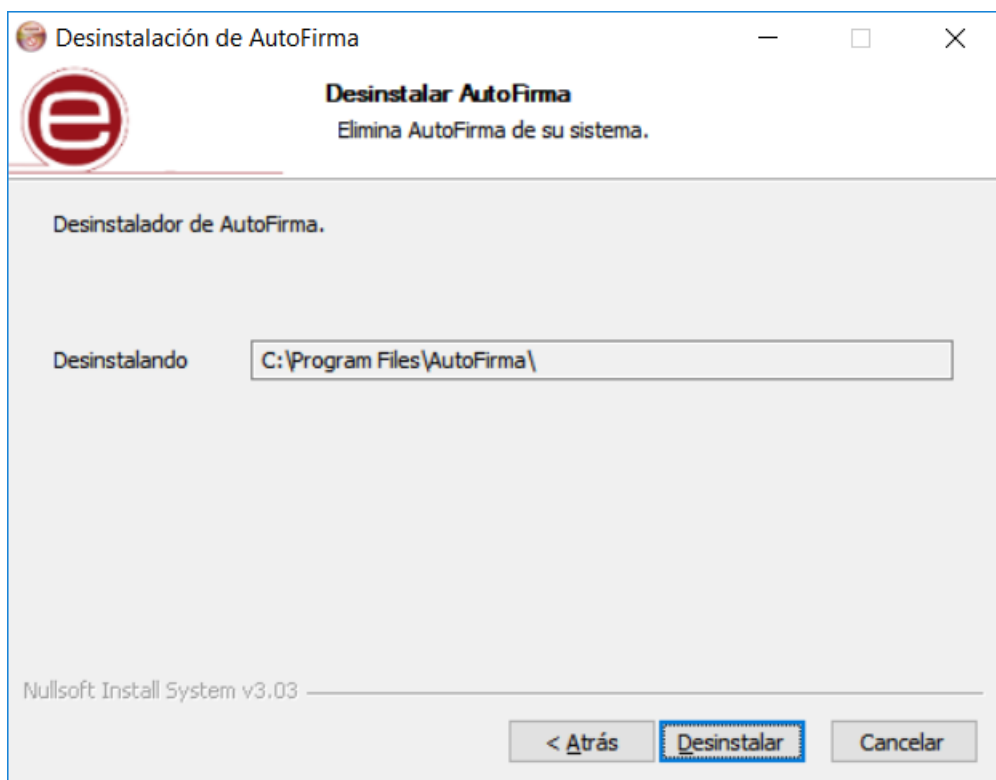
Una vez completada la instalación, las aplicaciones Web que integren el proceso de firma con el Cliente @firma podrán usar su versión instalada de AutoFirma para firmar.

### 5.1.1 Desinstalación

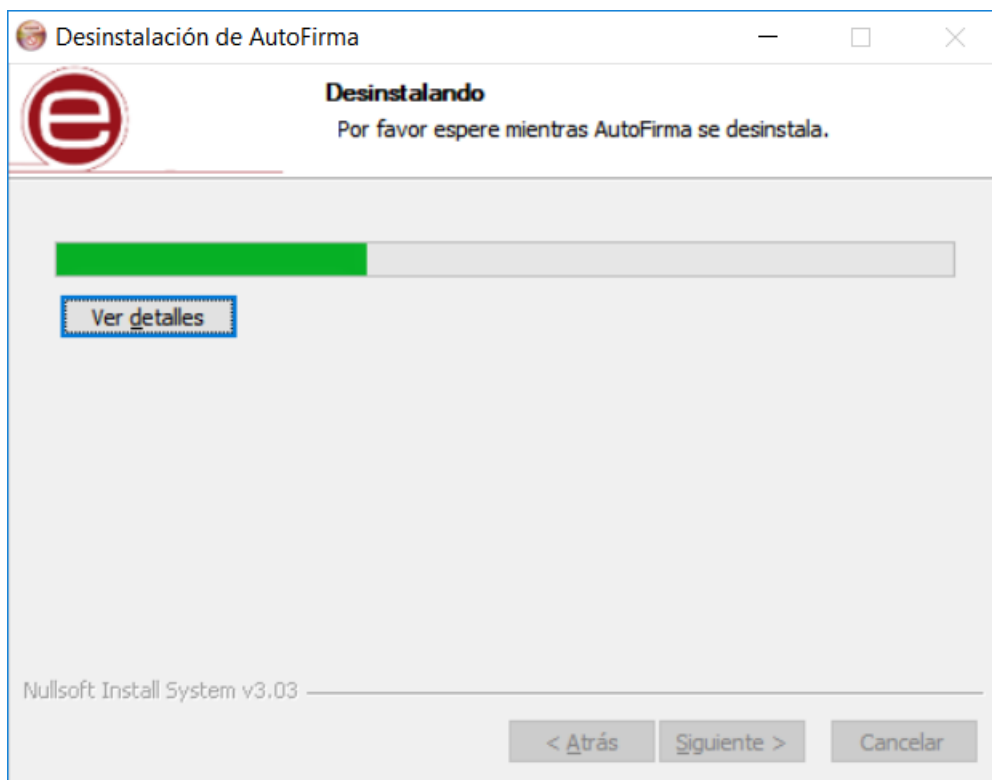
La desinstalación del programa puede hacerse, como es habitual en Windows, desde el apartado “Programas y características” del “Panel de control” del sistema operativo (siempre por parte de un usuario con permisos de administrador):



Una vez lanzado, el desinstalador presenta un sencillo asistente:







**ADVERTENCIA:** El proceso de desinstalación afecta a los perfiles de Mozilla Firefox y a la configuración de Google Chrome. Estos navegadores se cerrarán automáticamente durante el proceso de desinstalación desatendido mediante el instalador MSI. Si se utiliza el instalador EXE, será necesario que el usuario cierre manualmente estos navegadores.

Téngase en cuenta que el navegador Google Chrome puede quedar abierto incluso después de cerrar su ventana. En esos casos, aparecerá un icono en el área de notificaciones del escritorio del usuario y deberá cerrarse a través de la opción proporcionada en el menú contextual de este icono.



Cuando el proceso termina, la aplicación habrá sido desinstalada de Windows.

### 5.1.2 Despliegue masivo de la aplicación

AutoFirma también se distribuye en forma de instalador MSI (32 y 64bits) orientado a su despliegue masivo por parte de un administrador que gestione las aplicaciones de un conjunto de usuarios.

En caso de existir versiones previas de AutoFirma instaladas en los equipos de los usuarios, se recomienda proceder a la desinstalación de las mismas antes de instalar la nueva versión. Si se instalase AutoFirma como parte de un despliegue masivo y el usuario hubiese instalado AutoFirma (mediante su instalador EXE) en el mismo equipo, es posible que ambas versiones convivan en el equipo, aunque sólo la última atendería las peticiones realizadas mediante protocolo. Sin embargo, al desinstalar una de estas versiones, es posible que la otra dejase de funcionar.

El instalador MSI realiza la instalación silenciosa en el equipo de los usuarios. El administrador debe asegurarse, en cualquier caso, de que el proceso de instalación no se realiza mientras los usuarios trabajan en sus equipos, ya que los navegadores Chrome y Firefox se cerrarán durante la instalación/desinstalación.

Para realizar la instalación silenciosa mediante consola, se puede emplear el comando:

```
msiexec /i "_RUTA_\AutoFirma_installer.msi" /quiet
```

Para su desinstalación, se emplearía este otro:

```
msiexec /x "_RUTA_\AutoFirma_installer.msi" /quiet
```

Consulte el manual de su software de instalación masiva de aplicaciones para saber cómo realizar el despliegue sobre múltiples máquinas.

### 5.1.2.1 *Parámetro de configuración*

El instalador MSI de AutoFirma soporta los siguientes parámetros para adecuar la instalación a los requisitos del organismo:

- CREATE\_ICON
  - Permite indicar si se desea que se cree el icono de AutoFirma en el escritorio del usuario. Si se indica el valor "false" el icono no se creará. En cualquier otro caso, sí se creará.
  - Ejemplo:
    - Para una que no se cree el icono en el escritorio de los usuarios:

```
msiexec /i AutoFirma_installer.msi /quiet CREATE_ICON="false"
```

- FIREFOX\_SECURITY\_ROOTS
  - Permite indicar si se desea configurar Firefox para que confíe en los certificados raíz del almacén entidades de confianza de Windows. Si se indica el valor "true", se configurará esta opción de Firefox. En cualquier otro caso, no se modificará la configuración.
  - Ejemplo:
    - Para una que no se cree el icono en el escritorio de los usuarios:

```
msiexec /i AutoFirma_installer.msi /quiet FIREFOX_SECURITY_ROOTS="true"
```

### 5.1.3 *Permisos adicionales*

Es probable que después de la instalación de AutoFirma, al ejecutarlo como aplicación de escritorio o como parte de un proceso de firma Web, la máquina virtual de Java instalada junto con AutoFirma solicite permisos para el acceso a Internet pasando por el Firewall de Windows. Este permiso es necesario para que AutoFirma pueda realizar la búsqueda de actualizaciones y completar la comunicación con el navegador web en los procesos de firma web en los que sustituye al MiniApplet.

En el caso de un despliegue masivo de AutoFirma, sería necesario que el administrador del sistema concediese estos permisos para el ejecutable "javaw.exe" del JRE residente en el directorio de instalación de AutoFirma.

## 5.2 Linux

La instalación de AutoFirma en Linux debe ser realizada por un usuario con permisos de administrador. Se distribuyen varias versiones del instalador de AutoFirma para Linux:

- **AutoFirma\_X.Y.Z.deb**: Instalador DEB para distribuciones derivadas de Debian/Ubuntu.
- **autofirma-X.Y.Z-1.noarch.rpm**: Instalador RPM para distribuciones derivadas de RedHat/Fedora.
- **autofirma-X.Y.Z-1.noarch\_SUSE.rpm**: Instalador RPM para distribuciones derivadas de SUSE.
  - **NOTA:** Se han encontrado problemas de compatibilidad con el Firefox por defecto instalado con el sistema operativo con el entorno KDE. En este caso, Firefox no atiende las llamadas realizadas por la página para que abra la aplicación. Se recomienda la instalación del Firefox oficial de la web de Mozilla.

En los nombres anteriores, las letras X, Y y Z (opcional) son los números de versión. Por ejemplo “AutoFirma\_1.6.deb” correspondería a AutoFirma versión 1.6 para distribuciones Ubuntu/Debian.

Todos los instaladores incluyen la misma versión de AutoFirma, pero cada uno de ellos está preparado para la instalación en un conjunto distinto de distribuciones de Linux. La diferencia entre los dos instaladores RPM son las dependencias declaradas, dado que las NSS Tools se encuentran con distinto nombre en los repositorios por defecto de algunas distribuciones.

Para poder ejecutar AutoFirma son necesarias las siguientes dependencias, así que estas se comprueban durante el proceso de instalación:

- JRE (Java Runtime Environment) de Oracle u OpenJDK (versión 8 o superior).
- Biblioteca NSS Tools.

El funcionamiento de AutoFirma está verificado en distribuciones Ubuntu, Fedora y OpenSuse. Una vez instalada, puede usarse como aplicación de escritorio e invocarse desde los navegadores web Mozilla Firefox y Google Chrome.

Hay dos opciones de instalación: por línea de comandos y desde la interfaz de escritorio.

La instalación por ambos medios dejará la aplicación instalada por defecto en el directorio:

```
/usr/lib/AutoFirma
```

### 5.2.1 Instalación por línea de comandos del instalador DEB

Para instalación por línea de comandos, en una consola ejecutaremos:

```
sudo dpkg -i RUTA_INSTALABLE_AUTOFIRMA
```

Donde `RUTA_INSTALABLE_AUTOFIRMA` es la ruta al instalador en función de la distribución escogida.

Si no tenemos instaladas las dependencias anteriormente listadas, se nos mostrarán mensajes de advertencia al respecto. En caso de ser así, podremos instalar estas bibliotecas con el comando:

```
sudo apt-get -f install
```

Después de esto, se debe volver a ejecutar el comando de instalación de AutoFirma para asegurar su correcta instalación:

```
sudo dpkg -i RUTA_INSTALABLE_AUTOFIRMA
```

### 5.2.1.1 Instalación de Oracle Java con el fichero tar.gz de Oracle

Si se tuviese Oracle Java instalado en el sistema mediante el fichero tar.gz de la web de Oracle, la JRE no habrá quedado registrada en el gestor de paquetes. En ese caso, cuando se intente instalar AutoFirma, el gestor de paquetes considerará que no se cumplen los requisitos necesarios y se negará a instalarlo. Para forzar al uso de la JRE de Oracle se debe:

1. Instalar la biblioteca "libnss3-tools". Esta biblioteca es requisito indispensable de la aplicación:

```
sudo apt-get install libnss3-tools
```

2. Configurar la variable `JAVA_HOME` con la JRE instalada y su directorio "bin" como parte del `PATH` del sistema. Esto se puede hacer, por ejemplo, editando el fichero `/etc/environment` y agregando a la variable `PATH` la ruta del directorio bin de Java y la nueva variable:

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/usr/java/jre1.8.0_121/bin"
JAVA_HOME="/usr/java/jre1.8.0_121"
```

Podemos hacer que el sistema recargue la configuración de este fichero (y así no sea necesario reiniciarlo) con el comando:

```
source /etc/environment
```

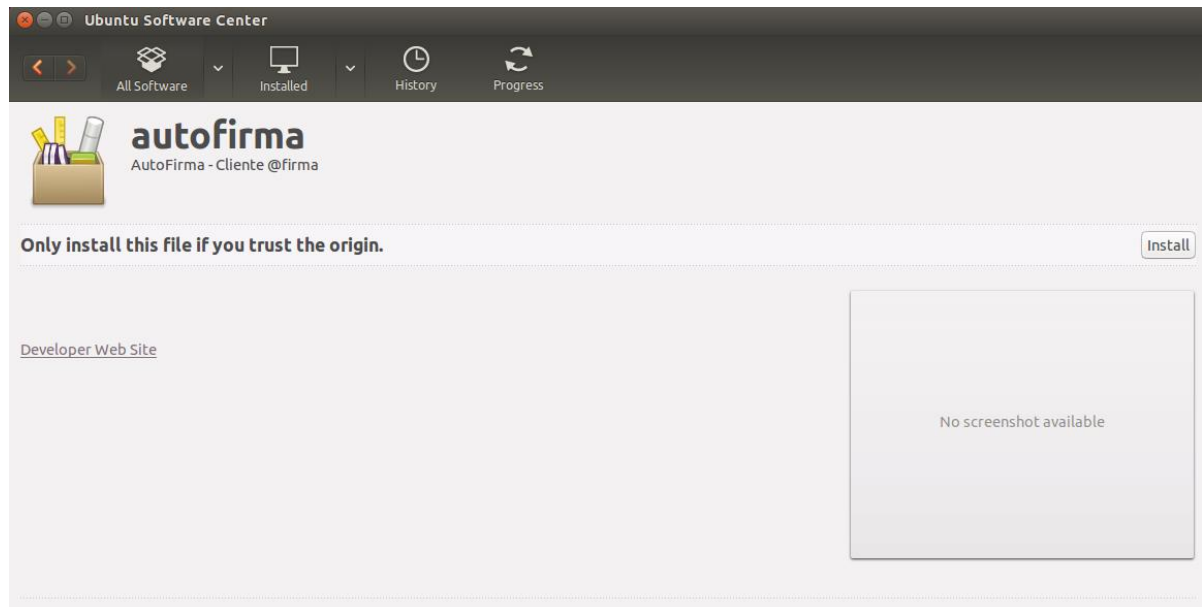
### 5.2.2 Instalación por línea de comandos del instalador RPM

Para instalación por línea de comandos, en una consola ejecutaremos:

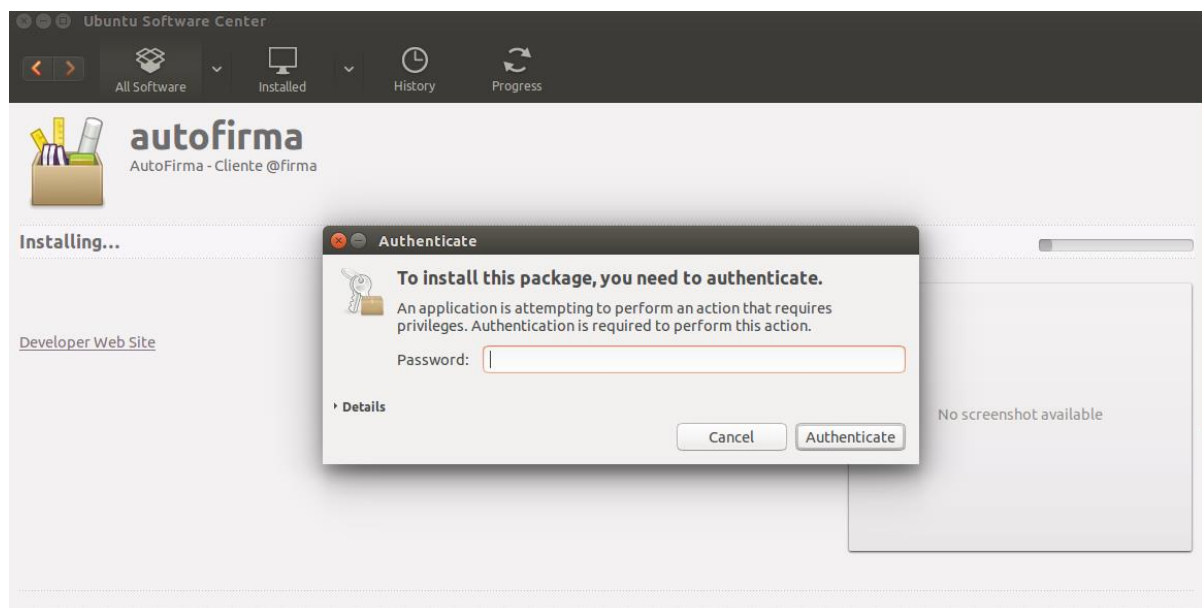
```
sudo rpm -i autofirma-X.Y.Z.noarch.rpm
```

### 5.2.3 Instalación de muestra mediante el asistente de paquetes de Ubuntu/Guadalinex

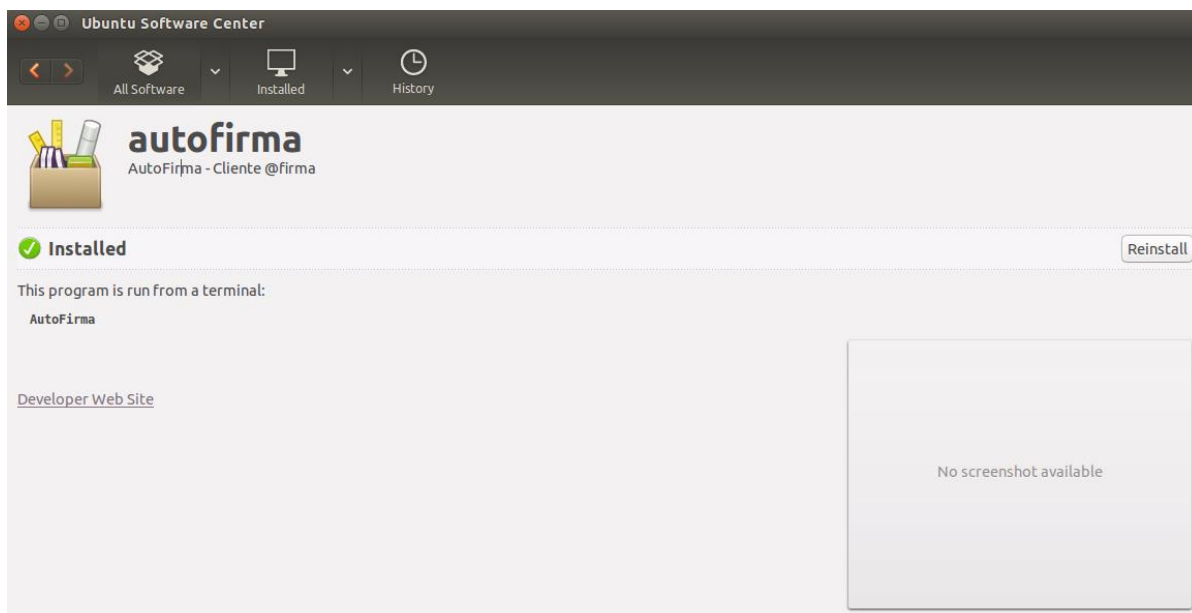
Para la instalación mediante el asistente de paquetes, se debe hacer doble clic en el fichero de la distribución (.deb). Se abrirá una ventana similar a la siguiente.



Se debe pulsar el botón instalar, que se encuentra arriba a la derecha. Si no se tienen permisos de administrador, el sistema solicitará la clave de “súper usuario” para poder realizar la instalación.



Si no ha ocurrido ningún problema, se mostrará un mensaje de confirmación.



#### 5.2.4 Desinstalación del paquete DEB

Para realizar la desinstalación del sistema se puede utilizar el siguiente comando.

```
sudo apt-get remove --purge autofirma
```

Cuando el proceso termina, la aplicación ha sido correctamente desinstalada del sistema.

#### 5.2.5 Desinstalación del paquete RPM

Para realizar la desinstalación del sistema se puede utilizar el siguiente comando.

```
sudo rpm -e autofirma
```

Cuando el proceso termina, la aplicación ha sido correctamente desinstalada del sistema.

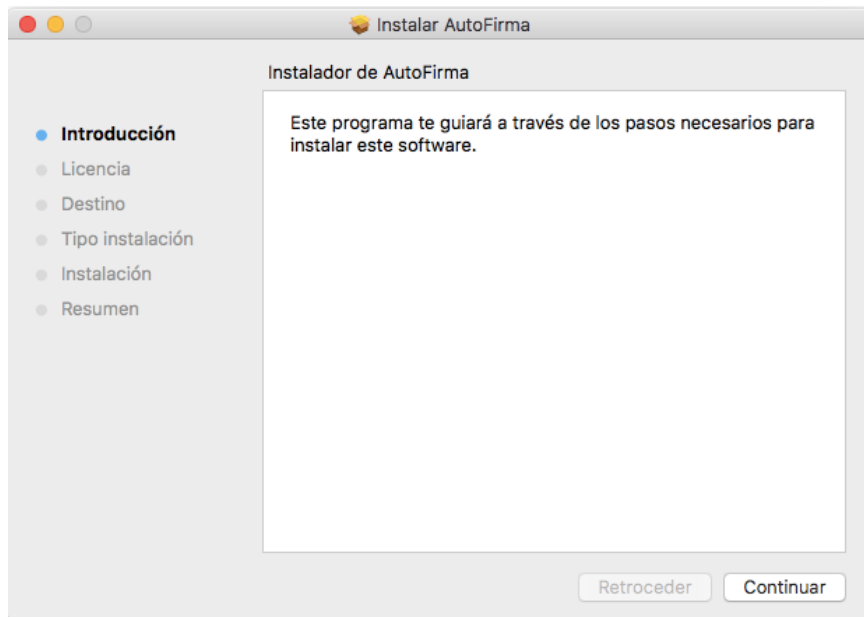
### 5.3 Apple OS X

La instalación de AutoFirma en OS X debe realizarla un usuario con permisos de administrador. El archivo de instalación se distribuye con el nombre "AutoFirma\_X.Y.Z.pkg", donde X, Y y Z (opcional) son los números de la versión. Por ejemplo, "AutoFirma\_1.6.pkg" correspondería a AutoFirma versión 1.6.

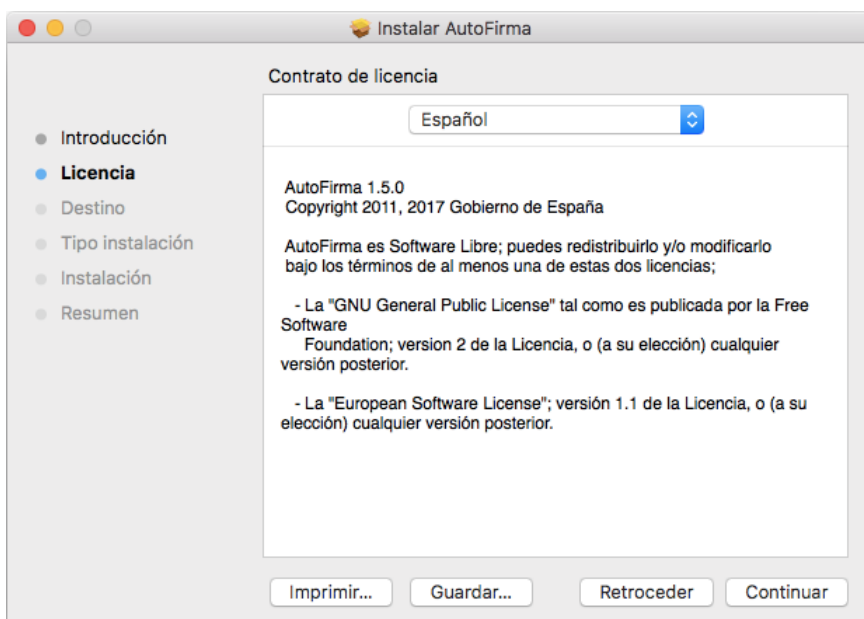
AutoFirma es compatible con las versiones de OS X Yosemite, El Capitán y Sierra. Los navegadores compatibles son Apple Safari, Google Chrome y Mozilla Firefox.

Para la instalación de la aplicación, se debe hacer doble clic sobre el fichero. El sistema abrirá el asistente que se encargará de realizar los pasos a seguir para la correcta instalación de la aplicación.

Para iniciar el proceso de instalación, hay que pulsar el botón "Continuar".



Una vez leída la licencia del producto se puede pulsar "Continuar". En ese momento, se indicará que se debe aceptar la licencia. Al pulsar el botón "Aceptar" se acepta la licencia y continúa con la instalación.

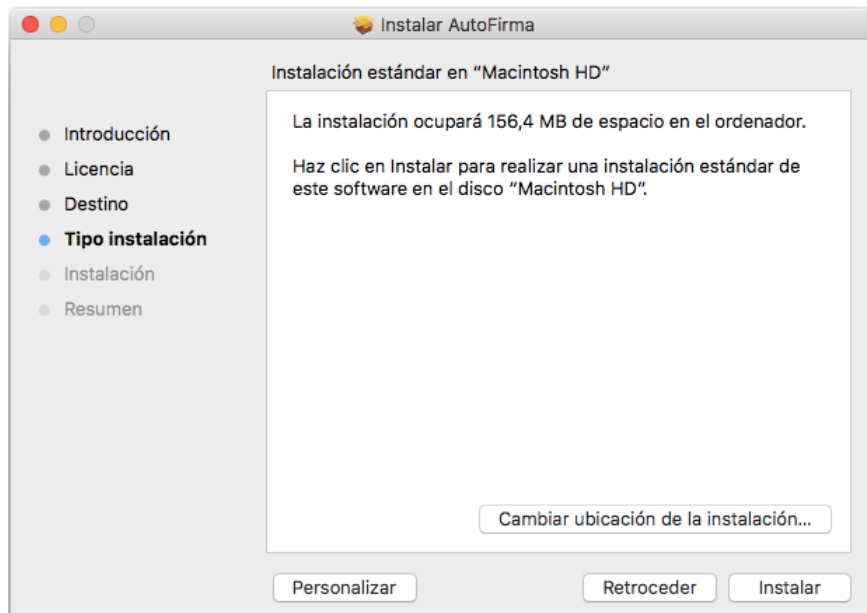




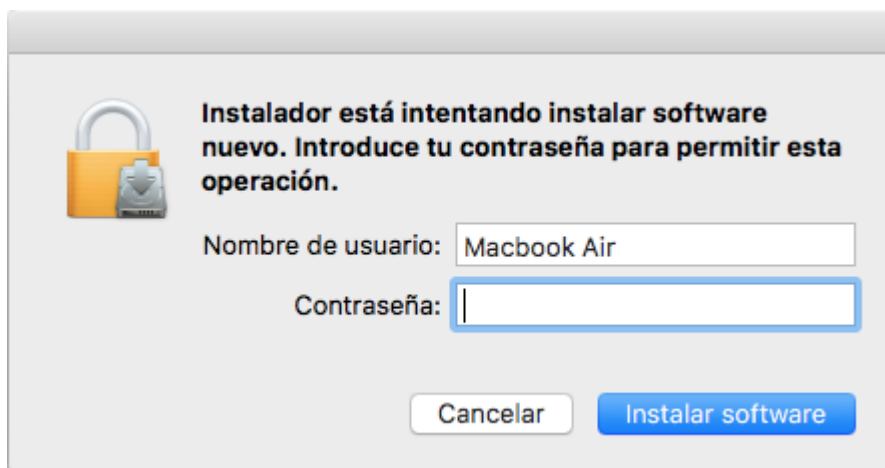
Se puede seleccionar la unidad de disco en la que se debe instalar la aplicación. Se debe seleccionar el disco principal y pulsar “Continuar”.



Finalmente, se informa de cuanto espacio en disco ocupará la aplicación. Una vez se pulsa el botón “Instalar” se comienza la instalación del producto.



Para completar la instalación será necesario indicar el nombre de usuario y contraseña de un usuario con permisos de administrador, ya que será necesario instalar certificados de confianza en el almacén del sistema y Firefox.



En caso de detectarse que el navegador Mozilla Firefox está en ejecución, se pedirá al usuario que lo cierre para continuar con el proceso de instalación.

Finalmente, se informará del resultado de la instalación.



### 5.3.1 Desinstalación

Para desinstalar la aplicación basta con eliminar la carpeta que se generó en el directorio /Applications.

También es recomendable eliminar los certificados identificados como "AutoFirma ROOT" y "127.0.0.1" del llavero de Mac. Puede realizarse esto accediendo a la aplicación "Acceso a Llaveros", seleccionándose el llavero "Sistema" y eliminando del listado los certificados mencionados.

## 6 Gestión de AutoFirma

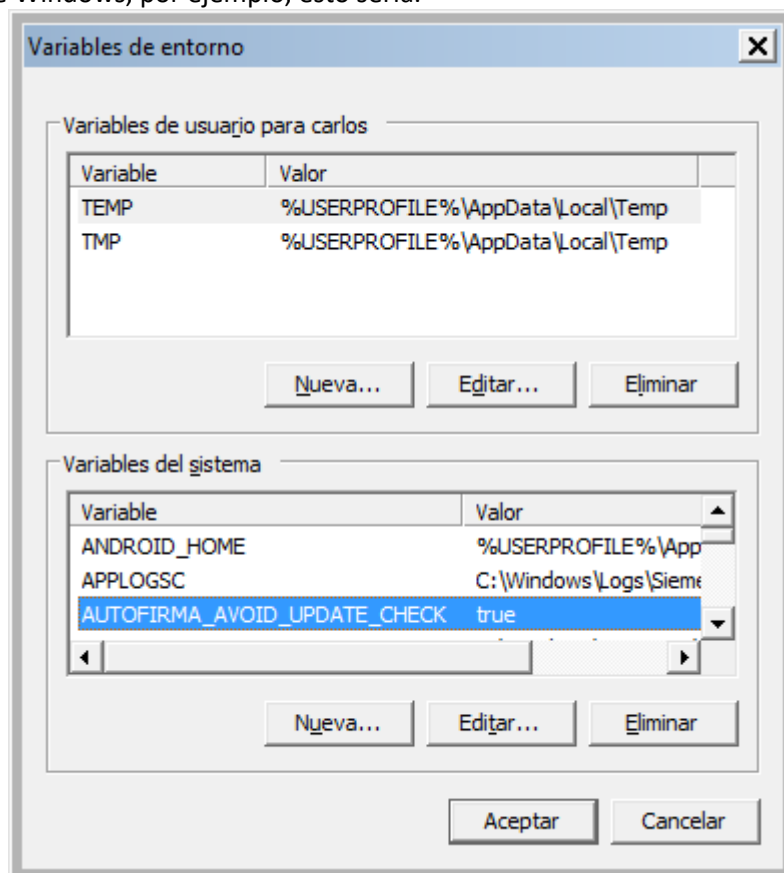
### 6.1 Comprobaciones de nuevas versiones al inicio de la aplicación

AutoFirma siempre comprueba al arrancar si hay una versión más actual disponible para descarga desde la página Web del proyecto para evitar que se realicen trámites de firma con una versión obsoleta o antigua que pudiese tener instalada el ciudadano.

Es posible deshabilitar esta comprobación de diversas maneras:

- Un usuario puede desactivar la actualización por medio de la opción “Buscar actualizaciones al inicio” en la pestaña General del menú de preferencias de la aplicación.
- Un usuario o administrador puede desactivar la actualización por medio del fichero de configuración con la opción [checkForUpdates](#). Consulte el apartado “Configuración a través de fichero” para más información.
- Un usuario o administrador puede desactivar la actualización estableciendo, a nivel de sistema operativo, la siguiente variable de entorno [AUTOFIRMA\\_AVOID\\_UPDATE\\_CHECK](#) con el valor `true`. Es posible que sea necesario reiniciar el equipo para que la JVM detecte correctamente el nuevo valor de esta variable.

En el caso de Windows, por ejemplo, esto sería:



La inhabilitación de las comprobaciones de actualización sólo sería recomendable en entornos controlados (corporativos, internos a una administración, etc.) o cuando se sepa de problemas de incompatibilidad de las nuevas versiones con alguna aplicación. Por regla general, siempre es conveniente descargar e instalar las últimas versiones disponibles.

La URL a la que se conecta AutoFirma por defecto para comprobar la existencia de actualizaciones es:

<http://estaticos.redsara.es/comunes/autofirma/autofirma.version>

El código de versión de AutoFirma 1.6 es: **7**

En caso de detectarse una nueva versión, AutoFirma permitirá al usuario abrir la página de descarga de la aplicación. La página que se abrirá por defecto es:

<http://firmaelectronica.gob.es/Home/Descargas.html>

Tanto la URL del código de la versión más reciente de AutoFirma como la URL de descarga se pueden configurar mediante el fichero de configuración. Esto es útil para evitar en entornos controlados que AutoFirma informe a los usuarios de las actualizaciones oficiales de la aplicación y no sea hasta que los administradores comprueben su correcto funcionamiento cuando se les notifique y se les redirija a una web de descargas del propio organismo. Esto se realiza mediante las opciones [updater.url.version](#) y [updater.url.site](#). Consulte el apartado “Configuración a través de fichero” para más información.

El administrador de red debe asegurar que los equipos de los usuarios tienen acceso a estas URL si se desea que sean los propios usuarios los encargados de identificar las nuevas versiones e instalarlas en sus equipos.

## 6.2 Configuración a través de fichero

AutoFirma permite que se configure a través de un fichero importado desde la pestaña General del panel de Preferencias de la aplicación. Esta opción está orientada principalmente a su uso por parte de administradores que hagan despliegues de la aplicación y que requieren que sus usuarios utilicen siempre unas propiedades concretas de firma.

El fichero de configuración debe tener como extensión “.afconfig”.

Es importante notar que las propiedades establecidas a través del menú de preferencias sólo afectan a la ejecución de la aplicación en modo escritorio. En las operaciones de firma solicitadas desde un navegador web siempre se utilizará la configuración de firma proporcionada en la operación. Excepción a esto es la configuración de proxy, que afectará a la ejecución de la aplicación en ambas modalidades.

Este fichero no tiene porqué contener todas las propiedades que admite la aplicación, puede contener sólo aquellas que deseamos configurar. Si se importa un fichero que no define el valor de alguna propiedad, esta propiedad tendrá asignada el valor por defecto de la aplicación o, si se modificó previamente, el valor que ya tuviese asignado.

Las opciones que se podrán configurar serán todas aquellas que pueden establecerse a través del panel de preferencias de la aplicación, además de alguna opción adicional.

El listado completo de opciones configurables aparece en el apartado [“6.4 Opciones configurables”](#).

El fichero de configuración en cuestión, será un fichero PList, compuesto por un diccionario con el listado de claves y valores de las propiedades. Las claves siempre se designarán mediante una cadena de texto y el valor puede ser una cadena (String) o un valor de tipo verdadero/falso (true/false).

Este fichero PList puede firmarse con una firma en formato XAdES Enveloped. Si se delega en los usuarios la importación del fichero de configuración, puede pedir que comprueben el firmante del fichero con una herramienta externa como VALIDe para que confirmen que se firmó con el certificado adecuado.

### 6.2.1 Bloqueo de la configuración

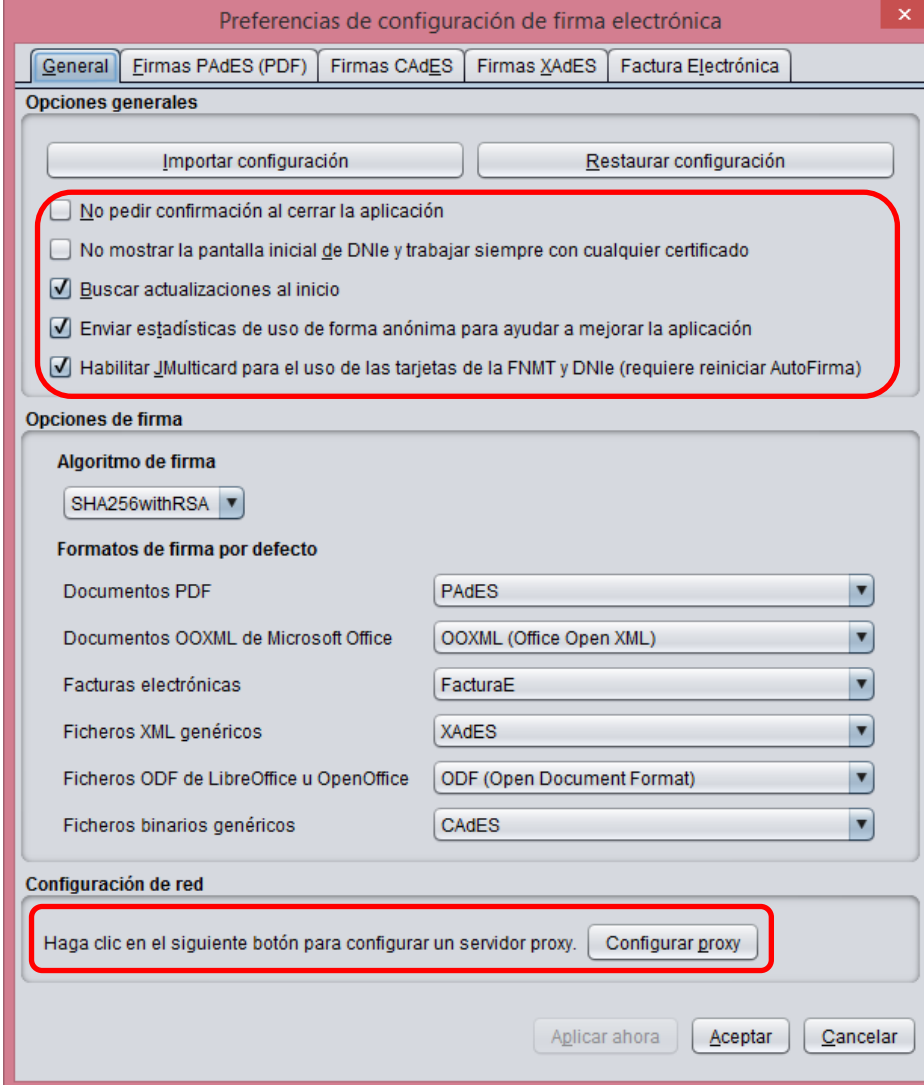
Un uso interesante de la configuración de la aplicación entre los usuarios de un organismo o entidad es que permite bloquear las opciones que el usuario va a poder modificar. Hay opciones que son especialmente interesantes de fijar para que se apliquen a todas las firmas, como las políticas de firma, y otras que no se pueden bloquear debido a que afectan en gran medida al contexto de cada firma, como el lugar de realización de la firma o si se quiere hacer visible la firma de los PDF.

La configuración de la aplicación puede bloquearse por medio de la opción “preferencesUnprotected”, como se describe en el apartado [“6.4.6 Opciones no configurables desde la ventana de preferencias”](#).

Se indican aquí las propiedades del panel de preferencias que el usuario va a poder seguir configurando aunque se bloquee la configuración general de la aplicación:

#### Pestaña General

- No pedir confirmación al cerrar la aplicación
- No mostrar la pantalla inicial de DNIe y trabajar siempre con cualquier certificado
- Buscar actualizaciones al inicio
- Enviar estadísticas de uso de forma anónima para ayudar a mejorar el uso de la aplicación
- Configuración del proxy



Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAdES Firmas XAdES Factura E|lectrónica

Opciones generales

Importar configuración Restaurar configuración

No pedir confirmación al cerrar la aplicación

No mostrar la pantalla inicial de DN|e y trabajar siempre con cualquier certificado

Buscar actualizaciones al inicio

Enviar estadísticas de uso de forma anónima para ayudar a mejorar la aplicación

Habilitar M|ulticard para el uso de las tarjetas de la FNMT y DN|e (requiere reiniciar AutoFirma)

Opciones de firma

Algoritmo de firma

SHA256withRSA

Formatos de firma por defecto

Documentos PDF	PAdES
Documentos OOX ML de Microsoft Office	OOX ML (Office Open XML)
Facturas electrónicas	FacturaE
Ficheros XML genéricos	XAdES
Ficheros ODF de LibreOffice u OpenOffice	ODF (Open Document Format)
Ficheros binarios genéricos	CAdES

Configuración de red

Haga clic en el siguiente botón para configurar un servidor proxy. Configurar proxy

Aplicar ahora Aceptar Cancelar

### Pestaña Firmas PAdES

- Metadatos para firmas PAdES
- Firma visible

Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAAdES Firmas XAdES Factura Electrónica

Configuración de la política de firma

Ninguna política

Metadatos de las firmas PAdES

Razón por la que se firma el documento

Ciudad en la que se realiza la firma

Contacto del firmante (usualmente una dirección de correo electrónico)

Opciones de firma

Formato avanzado de firma

PAdES-BES

Firma visible

Permitir firmas visibles en el PDF

Restaurar configuración

Aplicar ahora Aceptar Cancelar

### Pestaña Firmas XAdES

- Metadatos de las firmas XAdES

Preferencias de configuración de firma electrónica

General Firmas PAdES (PDF) Firmas CAdES Firmas XAdES Factura Electrónica

Configuración de la política de firma

Ninguna política

Metadatos de las firmas XAdES

Ciudad en la que se realiza la firma

Provincia en la que se realiza la firma

Código postal del lugar en el que se realiza la firma

País en el que se realiza la firma

Cargo atribuido al firmante

Opciones de firma

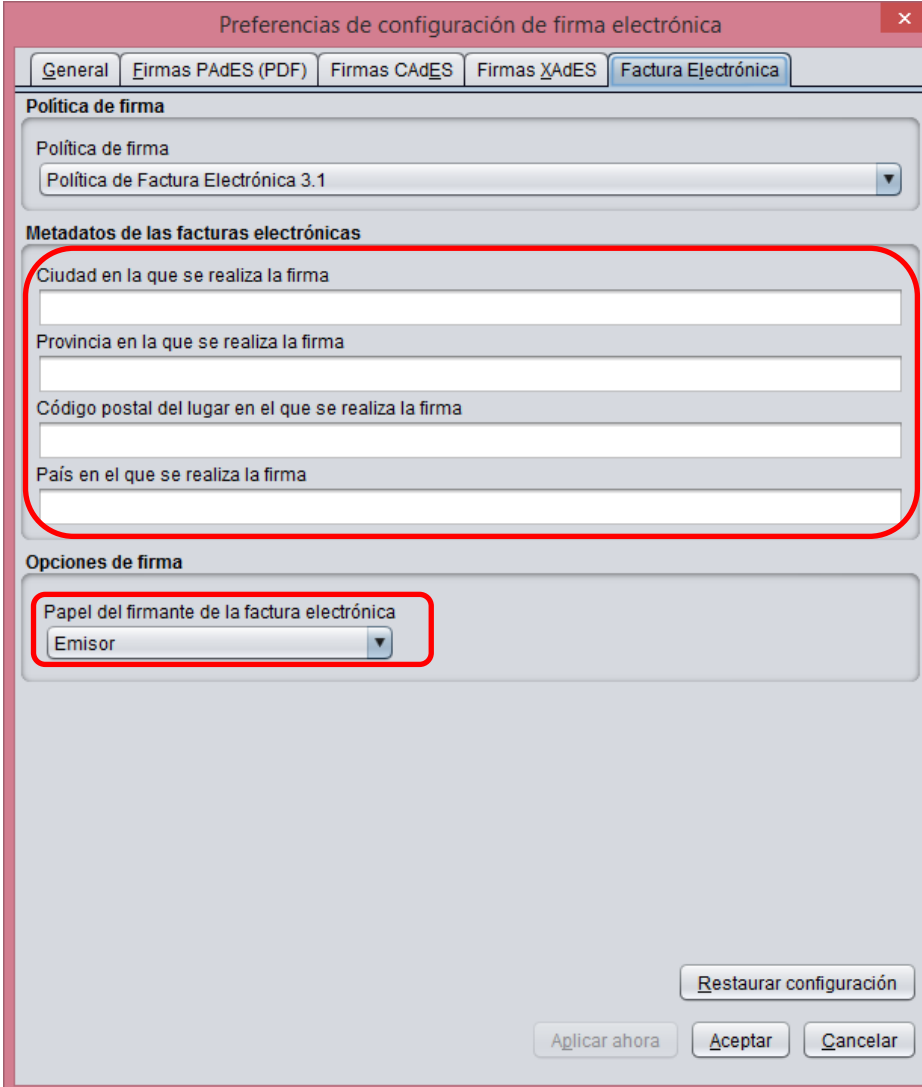
Formato de las firmas XAdES

XAdES Detached

### Pestaña Factura electrónica

- Metadatos de las facturas electrónicas
- Papel del firmante de la factura electrónica





### 6.2.2 Firma del fichero de configuración

El fichero de configuración deberá estar firmado con una firma XAdES Enveloped y un certificado emitido por la autoridad intermedia definida por el Ministerio de Defensa en el momento de empaquetar la aplicación AutoFirma para su distribución.

El administrador encargado de configurar y distribuir este fichero puede firmarlo con la propia herramienta AutoFirma. Los pasos para preparar la aplicación para la firma de este fichero son:

1. Disponer del certificado de firma en el almacén prioritario configurado en la aplicación o en el almacén por defecto, si no se dispone del certificado en tarjeta criptográfica.
2. Desde la pestaña de configuración "General" de las preferencias de la aplicación, configurar que los "Ficheros XML genéricos" se firmen con firma "XAdES".

3. En la pestaña “Firma XAdES” de las preferencias de la aplicación, configurar que el formato de firma XAdES sea “XAdES Enveloped”.

A continuación, podrá firmarse el fichero de configuración normalmente, seleccionando como certificado de firma el configurado en el primer paso.

### 6.2.3 Ejemplo de fichero de configuración

A continuación se muestra el contenido de un fichero simple de configuración:

```
<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
  <dict>
    <key>caDesImplicitMode</key>
    <string>attached</string>
    <key>createHashAsBase64</key>
    <true/ >
  </dict>
</plist>
```

En este fichero se establece que las firmas CADES contengan por defecto los datos firmados (`caDesImplicitMode`) y que las huellas digitales realizadas se generen en base 64 (`createHashAsBase64`). El resto de la configuración del usuario permanecerá tal como estaba en el momento de importar el fichero de configuración.

En este ejemplo, el fichero de configuración no está firmado.

## 6.3 Configuración a través del registro en Microsoft Windows

Es común que en los entornos controlados de usuarios se disponga de herramientas para el despliegue masivo de aplicaciones y que estas también permitan la configuración del sistema alterando directamente el registro de Microsoft Windows. Cuando este es el caso, el administrador del sistema podrá configurar el comportamiento de AutoFirma modificando diversas claves de registro.

AutoFirma almacena en el registro de Windows todas las opciones de configuración establecidas mediante el panel de preferencias o un fichero de configuración importado. Concretamente, la configuración de AutoFirma se almacena en la clave de registro:

`HKEY_CURRENT_USER\Software\JavaSoft\Prefs\es\gob\afirma\standalone\ui\preferences`

Un administrador puede establecer a través del registro todas las opciones declaradas en el apartado “[6.4 Opciones configurables](#)” para determinar así el comportamiento de AutoFirma.

## 6.4 Opciones configurables

Las opciones de configuración que se pueden establecer mediante fichero o a través del registro de Windows se presentan a continuación, separadas según la pestaña del panel de preferencias en la que se encuentran y reunidas en un apartado “Opciones globales” aquellas que no puede configurar directamente el usuario.

### 6.4.1 Opciones Generales

Clave	Tipo	Descripción
<code>omitAskOnClose</code>	<code>true/false</code>	Evita la confirmación al cerrar la aplicación o no. Un valor de <code>true</code> en esta preferencia permitirá cerrar la aplicación sin ningún diálogo de advertencia. Un valor de <code>false</code> (por defecto) hará que se muestre un diálogo para que el usuario confirme que realmente desea cerrar la aplicación.
<code>hideDnieStartScreen</code>	<code>true/false</code>	No mostrar la pantalla inicial de uso de DNle. Un valor de <code>true</code> en esta preferencia hace que nunca se muestre la pantalla inicial que sugiere al usuario el uso directo del DNle como almacén de claves. Un valor de <code>false</code> (por defecto) hará que se muestre esta pantalla al inicio siempre que se detecte un lector de tarjetas en el sistema.
<code>checkForUpdates</code>	<code>true/false</code>	Buscar actualizaciones al iniciar la aplicación. Un valor de <code>true</code> (por defecto) en esta preferencia hace que, al iniciar la aplicación, se compruebe automáticamente si hay publicadas versiones más actuales. Un valor de <code>false</code> hará que no se haga esta comprobación.

<code>useAnalytics</code>	<code>true/false</code>	Envía estadísticas de uso. El valor <code>true</code> (por defecto) hace que, al arrancar, la aplicación envíe de forma anónima estadísticas de uso a <i>Google Analytics</i> . El valor <code>false</code> hará que no se envíe ningún dato.
<code>enabledJmulticard</code>	<code>true/false</code>	Habilita el uso de JMulticard para la firma con DNle y tarjetas CERES. El valor <code>true</code> (por defecto) hace que tanto al seleccionar “Usar cualquier certificado” en la pantalla principal como cuando se invoca a AutoFirma desde un navegador, se utilice JMulticard si el usuario selecciona un certificado en tarjeta CERES o DNle. El valor <code>false</code> hará que se utilicen los controladores oficiales de estas tarjetas para listar los certificados y firmar con ellos.
<code>signatureAlgorithm</code>	<code>String</code>	Algoritmo de firma. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> <li>• SHA1withRSA</li> <li>• SHA256withRSA (Por defecto)</li> <li>• SHA384withRSA</li> <li>• SHA512withRSA</li> </ul>
<code>defaultSignatureFormatPdf</code>	<code>String</code>	Formato en el que se firmarán los documentos PDF. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> <li>• PAdES (Por defecto)</li> <li>• CAdES</li> <li>• XAdES</li> </ul>
<code>defaultSignatureFormatOoxml</code>	<code>String</code>	Formato en el que se firmarán los documentos OOXML. Esta preferencia

		<p>debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• OOXML (Office Open XML) (Por defecto)</li> <li>• CAdES</li> <li>• XAdES</li> </ul>
<code>defaultSignatureFormatFacturae</code>	String	<p>Formato en el que se firmarán las facturas electrónicas. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• FacturaE (Por defecto)</li> <li>• CAdES</li> <li>• XAdES</li> </ul>
<code>defaultSignatureFormatXml</code>	String	<p>Formato en el que se firmarán los documentos XML. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• XAdES (Por defecto)</li> <li>• CAdES</li> </ul>
<code>defaultSignatureFormatOdf</code>	String	<p>Formato en el que se firmarán los documentos ODF (LibreOffice, OpenOffice.org...). Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• ODF (Open Document Format) (Por defecto)</li> <li>• CAdES</li> <li>• XAdES</li> </ul>
<code>defaultSignatureFormatBin</code>	String	<p>Formato en el que se firmarán los ficheros binarios. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• CAdES (Por defecto)</li> <li>• XAdES</li> </ul>

<code>proxySelected</code>	<code>true/false</code>	Habilita o deshabilita la configuración particular de proxy. El valor <code>true</code> configura que se aplique la configuración particular indicada a continuación, mientras que el valor <code>false</code> (por defecto) no la habilitaría.
<code>proxyHost</code>	<code>String</code>	URL del servicio del servidor proxy.
<code>proxyPort</code>	<code>String</code>	Número de puerto para la comunicación con el servidor proxy.
<code>proxyUsername</code>	<code>String</code>	Nombre de usuario con el que acceder al servidor proxy.
<code>proxyPassword</code>	<code>String</code>	Contraseña del usuario para la conexión con el servidor proxy.

#### 6.4.2 Firmas PAdES (PDF)

Clave	Tipo	Descripción
<code>padesPolicyIdentifier</code>	<code>String</code>	Identificador de la política de firma para PAdES.
<code>padesPolicyIdentifierHash</code>	<code>String</code>	Huella digital, en Base64, del identificador de la política de firma para PAdES.
<code>padesPolicyIdentifierHashAlgorithm</code>	<code>String</code>	Algoritmo de la huella digital del identificador de la política de firma para PAdES. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> <li>• SHA1 (Por defecto)</li> <li>• SHA-512</li> <li>• SHA-384</li> </ul>

		<ul style="list-style-type: none"> <li>SHA-256</li> </ul>
<code>padesPolicyQualifier</code>	String	Calificador de la política de firma para PAdES.
<code>padesSignReason</code>	String	Motivo de la firma en firmas PAdES.
<code>padesSignProductionCity</code>	String	Ciudad de firma para firmas PAdES.
<code>padesSignerContact</code>	String	Contacto del firmante en firmas PAdES.
<code>padesBasicFormat</code>	String	<p>Formato de firma PAdES. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>PAdES-BES</li> <li>PAdES Básico (Por defecto)</li> </ul>
<code>padesVisibleSignature</code>	true/false	Si está establecido a true, establece por defecto que se pida al usuario que determine mediante diálogos gráficos los parámetros de una firma visible PDF y se inserte como tal en el documento. Si está a false (valor por defecto), se realizarán firmas invisibles PDF.

### 6.4.3 Firmas CADES

Clave	Tipo	Descripción
<code>caadesPolicyIdentifier</code>	String	Identificador de la política de firma para CADES.
<code>caadesPolicyIdentifierHash</code>	String	Huella digital, en Base64, del

		identificador de la política de firma para CAdES.
<code>caDesPolicyIdentifierHashAlgorithm</code>	String	Algoritmo de la huella digital del identificador de la política de firma para CAdES. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> <li>• SHA1 (Por defecto)</li> <li>• SHA-512</li> <li>• SHA-384</li> <li>• SHA-256</li> </ul>
<code>caDesPolicyQualifier</code>	String	Calificador de la política de firma para CAdES.
<code>caDesImplicitMode</code>	String	Indica si la firma CAdES debe realizarse en modo implícito ( <i>attached</i> ) (por defecto) o no ( <i>detached</i> ).

#### 6.4.4 Firmas XAdES

Clave	Tipo	Descripción
<code>xadesPolicyIdentifier</code>	String	Identificador de la política de firma para XAdES.
<code>xadesPolicyIdentifierHash</code>	String	Huella digital, en Base64, del identificador de la política de firma para XAdES.
<code>xadesPolicyIdentifierHashAlgorithm</code>	String	Algoritmo de la huella digital del identificador de la política de firma para XAdES. Esta preferencia debe tener uno de estos valores: <ul style="list-style-type: none"> <li>• SHA1 (Por defecto)</li> </ul>



		<ul style="list-style-type: none"> <li>• SHA-512</li> <li>• SHA-384</li> <li>• SHA-256</li> </ul>
<b>xadesPolicyQualifier</b>	String	Calificador de la política de firma para XAdES.
<b>xadesSignatureProductionCity</b>	String	Ciudad en la que se realiza la firma.
<b>xadesSignatureProductionProvince</b>	String	Provincia en la que se realiza la firma.
<b>xadesSignatureProductionPostalCode</b>	String	Código postal en la que se realiza la firma.
<b>xadesSignatureProductionCountry</b>	String	País en la que se realiza la firma.
<b>xadesSignerClaimedRole</b>	String	Cargo supuesto para el firmante.
<b>xadesSignFormat</b>	String	<p>Formato de las firmas XAdES. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• XAdES Detached</li> <li>• XAdES Enveloping (Por defecto)</li> <li>• XAdES Enveloped</li> </ul>

#### 6.4.5 Firmas Factura Electrónica

Clave	Tipo	Descripción
<b>facturaEPolicy</b>	String	<p>Versión de la política de firma de factura electrónica. Los valores posibles son:</p> <ul style="list-style-type: none"> <li>• 3.0: Política de firma 3.0.</li> <li>• 3.1: Política de firma 3.1 (por defecto).</li> </ul>

		<p>Esta propiedad configura el resto de propiedades de la política de firma de factura cuando se establece desde la interfaz gráfica. Al establecerlo mediante fichero de configuración es necesario establecer también las siguientes 3 propiedades: <code>facturaePolicyIdentifier</code>, <code>facturaePolicyIdentifierHash</code> y <code>facturaePolicyIdentifierHashAlgorithm</code></p>
<b>facturaePolicyIdentifier</b>	String	<p>Establece el identificador de la política de firma de factura electrónica.</p> <p>Para configurar la política de firma 3.0 se debe establecer el valor:  <code>http://www.facturae.es/politica de firma formato facturae/politica de firma formato facturae v3_0.pdf</code></p> <p>Para configurar la política de firma 3.0 se debe establecer el valor:  <code>http://www.facturae.es/politica_de_firma_formato_facturae/politica_de_firma_formato_facturae_v3_1.pdf</code></p>
<b>facturaePolicyIdentifierHash</b>	String	<p>Establece la huella digital de la política de firma de factura electrónica.</p> <p>Para configurar la política de firma 3.0 se debe establecer el valor:  <code>xmfh8D/Ec/hHeE1IB4zPd61zHIY=</code></p> <p>Para configurar la política de firma 3.0 se debe establecer el valor:  <code>Ohixl6upD6av8N7pEvDABhEL6hM=</code></p>
<b>facturaePolicyIdentifierHashAlgorithm</b>	String	<p>Algoritmo de la huella digital del identificador de la política de firma de factura electrónica.</p> <p>Para configurar las políticas de firma 3.0 y 3.1 se</p>

		debe establecer el valor: SHA1
<code>facturaeSignatureProductionCity</code>	String	Ciudad en la que se realiza la firma.
<code>facturaeSignatureProductionProvince</code>	String	Provincia en la que se realiza la firma.
<code>facturaeSignatureProductionPostalCode</code>	String	Código postal en el que se realiza la firma.
<code>facturaeSignatureProductionCountry</code>	String	País en el que se realiza la firma.
<code>facturaeSignerRole</code>	String	Rol ejercido por el firmante en el proceso de firma. Debe tener uno de estos valores: <ul style="list-style-type: none"> <li>• Emisor (Por defecto)</li> <li>• Receptor</li> <li>• Tercero</li> </ul>

#### 6.4.6 Opciones no configurables desde la ventana de preferencias

Clave	Tipo	Descripción
<code>preferencesBlocked</code>	true/false	Proteger cambios en preferencias. Un valor de <code>true</code> en esta preferencia indica que deben limitarse las opciones de configuración mediante interfaz gráfico, apareciendo de forma deshabilitada (solo para consulta). Un valor de <code>false</code> habilitará que cualquier opción de configuración pueda ser alterada por parte del usuario mediante el interfaz gráfico.

<p><code>createHashAsBase64</code></p>	<p>true/false</p>	<p>Si está establecido a <code>true</code> (valor por defecto), se generan las huellas digitales de fichero en base64. Si es <code>false</code>, se generarán en binario.</p>
<p><code>createHashDirectoryAlgorithm</code></p>	<p>String</p>	<p>Algoritmo de huella digital por defecto para la creación de huellas digitales. Esta preferencia debe tener uno de estos valores:</p> <ul style="list-style-type: none"> <li>• SHA1</li> <li>• SHA-512 (Por defecto)</li> <li>• SHA-384</li> <li>• SHA-256</li> </ul>
<p><code>updater.url.version</code></p>	<p>String</p>	<p>URL remota del fichero que define el código de versión de la versión más reciente de AutoFirma.</p> <p>Consulte el apartado “Comprobaciones de nuevas versiones al inicio de la aplicación” para más detalles.</p>
<p><code>updater.url.site</code></p>	<p>String</p>	<p>URL de la página web desde la que descargar las nuevas versiones de AutoFirma.</p> <p>Consulte el apartado “Comprobaciones de nuevas versiones al inicio de la aplicación” para más detalles.</p>

## 6.5 Obtención de estadísticas con Google Analytics

AutoFirma utiliza Google Analytics para recoger información acerca de su uso. Esta información se limita al hecho de haber ejecutado AutoFirma y la IP del equipo. En ningún momento se recoge información personal del usuario u otra información del equipo más que la IP asignada.

A la información recabada sólo puede acceder el grupo de trabajo del Cliente @firma y este se compromete a que su uso se limita a conocer el número aproximado de usuarios de la herramienta.

La obtención de estos datos se realiza en segundo plano al ejecutarse AutoFirma y el resultado de su obtención y envío no afecta al uso de la propia herramienta. Así pues, AutoFirma podría no llegar a enviar los datos obtenidos, por ejemplo, por encontrarse detrás de un proxy de red, sin que esto afecte a su funcionalidad.

El usuario puede deshabilitar el envío de información a Google Analytics desde el panel de preferencias de la herramienta. También se puede configurar que deje de enviarse esta información por medio de la variable de entorno `es.gob.afirma.doNotSendAnalytics`. En caso de establecer esta variable a `“true”` se deshabilitará el envío de información. En caso contrario, se seguirá enviando.

En caso de configurarse la mencionada variable, no se enviará ninguna información a Google Analytics, independientemente de que el usuario haya configurado o no el envío de los datos a través del menú de preferencias de AutoFirma.

## 7 Compatibilidad del MiniApplet @firma con aplicaciones móviles y AutoFirma

El MiniApplet @firma 1.6 es compatible con:

- AutoFirma v1.4.2 y superiores.
- Cliente @firma móvil Android v1.4
- Cliente @firma móvil iOS v1.4

**Advertencia:** El uso de versiones de AutoFirma anteriores a la 1.6 en despliegues del MiniApplet 1.6 podría conllevar errores cuando se utilicen las nuevas funcionalidades de esta versión.

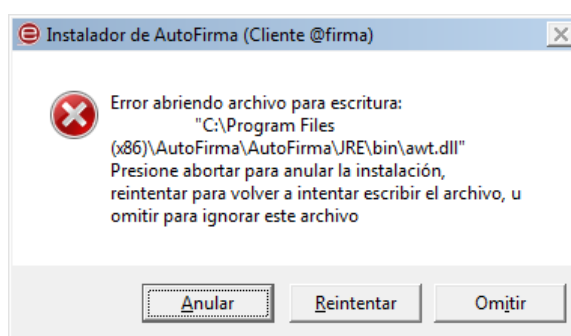
## 8 Problemas conocidos

### 8.1 Al instalar AutoFirma falla la instalación de los certificados de confianza SSL

AutoFirma requiere permisos de administrador para ser instalado y para insertar el certificado de confianza SSL para el funcionamiento de la firma en los trámites online. Si no puede instalar AutoFirma o el certificado de confianza, solicite al administrador de su sistema que realice la instalación de la aplicación.

### 8.2 Al instalar AutoFirma en Windows se muestra el error: “Error abriendo archivo para escritura”

Es posible que durante la instalación se le muestre un error como el que sigue:



Si ya tenía instalado AutoFirma, compruebe que este no se está ejecutando, en cuyo caso el instalador no podrá sobrescribir los ficheros de instalación. Cierre AutoFirma y pulse el botón reintentar.

Si AutoFirma no se está ejecutando, es posible que el archivo en cuestión se encuentre bloqueado por una ejecución o intento de instalación previo. Reinicie su equipo y pruebe a instalar nuevamente la aplicación.

### 8.3 Al abrir Google Chrome después del proceso de instalación de AutoFirma se muestra un mensaje notificando que la configuración de la aplicación está corrupta

El navegador Google Chrome incluye en su configuración un listado de protocolos que considera seguros para la llamada a aplicaciones externas. Durante el proceso de instalación de AutoFirma se registra el protocolo “afirma” en este listado seguro de Chrome para que las invocaciones desde el navegador se realicen correctamente. Para hacer este registro el propio proceso de instalación necesita que se cierre la aplicación para agregar el protocolo al listado correspondiente. Cuando se utiliza el instalador EXE de la aplicación, el proceso de instalación solicitará al usuario que cierre la

aplicación (en caso de aparecer el icono de Chrome en la barra de tareas del sistema operativo debe cerrarse también). En el caso del instalador MSI, el navegador se cierra automáticamente.

En algunas situaciones en las que el instalador podría no poder completar el proceso de registro, el fichero de configuración de Chrome podría quedar en un estado inconsistente. En estos casos, al iniciarse de nuevo el navegador, detectará el problema y anunciará al usuario esta corrupción de datos mediante una ventana de advertencia que nos permitirá restaurar las propiedades por defecto.

Seguidamente, el navegador restaurará las propiedades configuración y volverá a funcionar normalmente. En este caso, el usuario recibirá mensajes de advertencia al usar AutoFirma desde Chrome para realizar firmas, aunque esto no impedirá que funcione normalmente.

Durante el proceso de desinstalación de AutoFirma se realiza el proceso inverso al de instalación y se elimina el protocolo “afirma” del listado de protocolos seguros registrados en Chrome. Este proceso podría derivar en algunas circunstancias a la misma corrupción de la configuración del navegador.

#### **8.4 AutoFirma en OS X no muestra el título de los diálogos de cargar y guardado de ficheros**

Las nuevas versiones de OS X omiten el título de los diálogos de carga y guardado de ficheros. En caso en que el integrador delegue en AutoFirma la selección y el guardado de las firmas generadas, debería tener la precaución de informar al usuario de esto para que en todo momento sepa qué operación está realizando (carga de un fichero de datos para firma, carga de un fichero de firma para cofirma/contrafirma, guardado de una firma generada...).

#### **8.5 Error al importar las opciones de configuración desde un fichero**

Si generase un fichero de configuración para la importación de las opciones de configuración en AutoFirma y al importarlo se mostrase el mensaje de error “El fichero de preferencias es inválido, no se realizará ningún cambio en la configuración”, es probable que el fichero utilizado no sea un XML válido o que tenga algún problema de codificación. Verifique que su fichero de configuración está bien formado y que la codificación utilizada es correcta.

#### **8.6 AutoFirma indica que un documento PDF es demasiado grande cuando se intenta firmar con firma visible**

Cuando AutoFirma crea la previsualización de un documento PDF, lo carga en memoria y crea miniaturas de cada una de sus páginas. Esta tarea requiere una gran cantidad de memoria y es posible que no pueda completarse porque la aplicación no pueda reservar suficiente. Este problema suele darse con documentos PDF de gran tamaño o con un gran número de páginas. La probabilidad aumenta considerablemente en equipos con instalaciones de 32bits de AutoFirma, ya que no permiten reservar toda la memoria necesaria. También puede ocurrir en equipos con 2Gb de memoria o menos.



Se recomienda que los usuarios de sistemas operativos de 64bits utilicen AutoFirma de 64bits para reducir la probabilidad de sufrir este error.

## 8.7 AutoFirma se cierra inmediatamente tras ser invocado desde el navegador web

Cuando se abre AutoFirma por petición de un navegador web inmediatamente se abre una conexión entre ambas aplicaciones. Si AutoFirma detecta cualquier problema que evita que se pueda establecer esa comunicación, se cierra. Esto dará lugar a que, pasado un tiempo, la página web que intentó realizar la operación de firma informe de que no se pudo conectar con AutoFirma.

Si se encuentra en esta situación, utilice la función de “Restaurar instalación” de AutoFirma. Esta función permitirá reestablecer la configuración y los recursos necesarios para que se pueda establecer la comunicación entre el navegador y AutoFirma.

La función de “Restauración instalación” se encuentra disponible en el menú de herramientas de AutoFirma.

## 8.8 No se detectan tarjetas inteligentes en macOS

Muchas tarjetas inteligentes no disponen de los controladores necesarios para su uso a través del llavero de Apple (almacén utilizado por AutoFirma cuando se usa a través de Safari, Chrome o como aplicación de escritorio). En el caso concreto del DNIE, AutoFirma es capaz de utilizarlo por medio del controlador Java que incorpora, pero con el resto de tarjetas no es posible.

Para utilizar tarjetas criptográficas en macOS, instale sus controladores PKCS#11 como dispositivos de seguridad en Mozilla Firefox y utilice AutoFirma a través de este navegador.

## 8.9 AutoFirma no puede comunicarse con el navegador en macOS

En algunos casos la instalación de AutoFirma en macOS finaliza sin errores, pero no se instala el perfil de seguridad que permiten que AutoFirma se comunique de forma segura con el navegador web. En estos casos, al realizar una operación de firma, se arrancará correctamente AutoFirma, pero este no será capaz de transmitir el resultado de la firma al navegador web. Esto puede generar un error del navegador con el texto “No se ha podido conectar con AutoFirma.”.

Para solventar este problema será necesario configurar manualmente la confianza en los certificados de AutoFirma.

Para ello:

1. Acceda a la aplicación “Acceso a llavero”.
2. Acceda al llavero “SISTEMA” y a la opción “Certificados”.
3. En el listado de certificados mostrados deben aparecer los certificados “127.0.0.1” y “AutoFirma ROOT”. Si el icono que aparece junto a estos muestra el signo ‘+’, se confía en

los certificados y la comunicación con AutoFirma debería funcionar correctamente. Si no, continúe con el proceso.

4. Haga clic sobre el certificado "127.0.0.1" y pulse en la opción "Confiar".
5. En el diálogo que debe haber aparecido, despliegue el listado "Al utilizar este certificado" y seleccione la opción "Confiar siempre".
6. Repita los pasos 4 y 5 para el certificado "AutoFirma ROOT".
7. Compruebe que en ambos certificados aparece ahora el símbolo '+' junto a su icono.
8. Cierre la ventana de los llaveros.
9. Introduzca la contraseña de su usuario en el diálogo para confirmar el cambio en la configuración de seguridad.



Esta obra está bajo una licencia [Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 Unported](https://creativecommons.org/licenses/by-nc-sa/3.0/).