



## INSTALACIÓN DE CERTIFICADO SOFTWARE Android

# ACA PLUS

## Pásate a ACA Plus

A PARTIR DE 2025 LA VERSIÓN ACTUAL DE ACA DEJARÁ DE ESTAR OPERATIVA

### ACA Plus te ofrece más.



**Movilidad**  
Accede sin límites,  
sin necesidad de  
tarjeta y lector.



**Agilidad**  
Un acceso rápido  
a la firma digital y  
disponible desde  
el móvil.



**Garantía Profesional**  
La única firma  
que te identifica  
como abogado y abogada.



**Protección**  
Dota de seguridad  
a tus comunicaciones  
y documentos.



**Y un PLUS de Versatilidad**  
Usa ACA Plus  
desde tantos dispositivos  
como necesites.



## ÍNDICE

Requisitos de Instalación.....	2
PASO 1: Descarga del certificado .....	2
PASO 2: Instalación del certificado .....	5
PASO 3: Instalación App “Cliente @firma móvil” desde la Play Store / AppGallery.....	6
PASO 4: Instalación App “Certificado digital FNMT” desde la Play Store / AppGallery .	8
ATENCIÓN .....	12

## Requisitos de Instalación

Antes de comenzar la instalación, es necesario descargar el archivo que contiene el certificado (extensión. p12 o .pfx). Puedes hacerlo directamente desde tu dispositivo móvil (Paso 1) o descargarlo en un ordenador y enviarlo través de correo electrónico, o cualquier otra forma de transferencia de archivos.

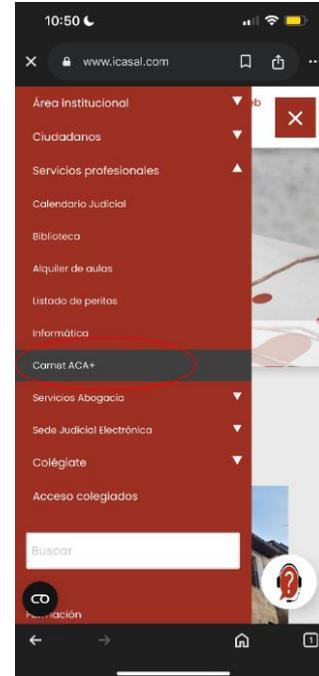
**Para disfrutar de las principales funciones que nos proporciona el certificado es necesaria la instalación de las aplicaciones de “Cliente @firma móvil”.**

Este manual está confeccionado siguiendo los pasos en un dispositivo Samsung, con Android v.11 pero es compatible generalmente con el resto de las versiones de Android.

Para acceder a las páginas webs compatibles con el certificado digital se recomienda el uso del navegador nativo (por defecto) de tu dispositivo Android.

## PASO 1: Descarga del certificado

1. Entramos en la página web del Colegio ([www.icasal.com](http://www.icasal.com)) y hacemos clic en las tres rayitas
2. Entramos en “Servicios Profesionales” y luego “Carnet ACA+”



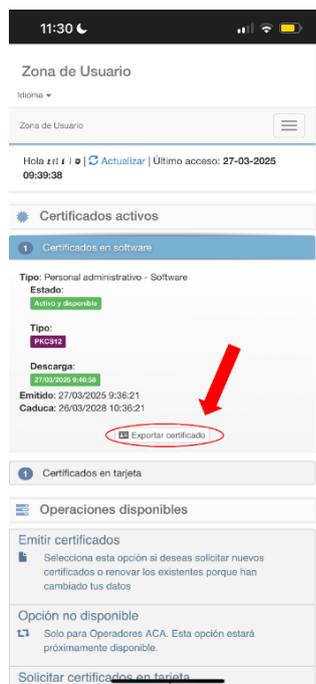
3. Deslizamos hasta llegar a hacer  
Clic en “Zona de usuario”



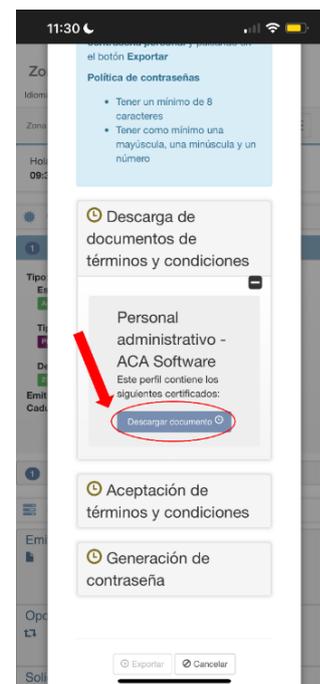
4. Clic en la opción de “Usuario y código de un solo uso”



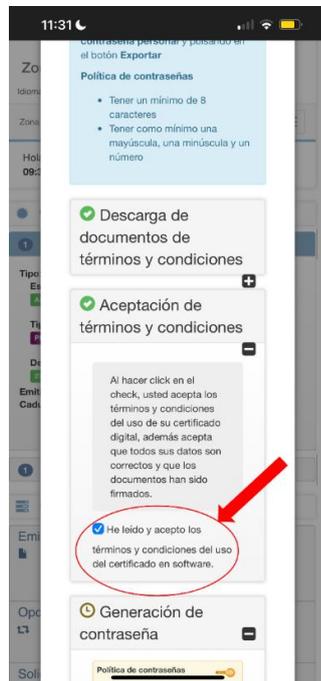
5. En el apartado de “Certificado de Software” le damos a “Exportar certificado”



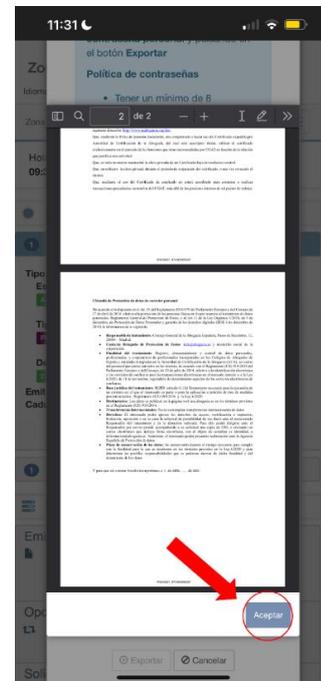
6. Clic en descargar documento



7. Aceptamos los términos y condiciones

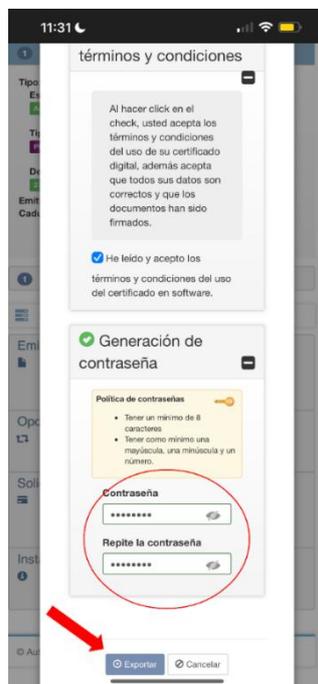


8. Damos clic en "Aceptar"



9. Introducimos la contraseña que queremos

Asignar al archivo exportado, la anotamos y hacemos clic en "Exportar"



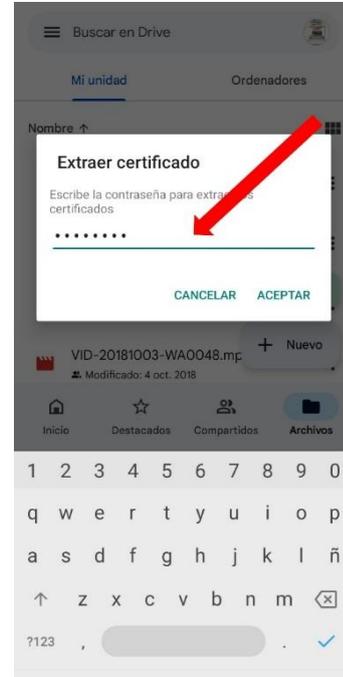
Este último paso descarga un archivo que debe almacenarse en el dispositivo. Este archivo es el CERTIFICADO.

## PASO 2: Instalación del certificado

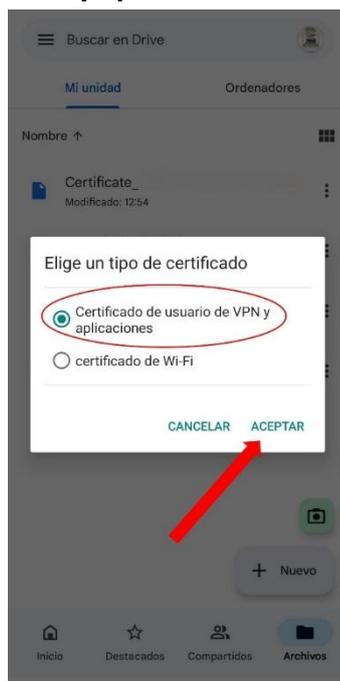
1. Hacemos de nuevo clic en el certificado una vez se encuentre en nuestras descargas



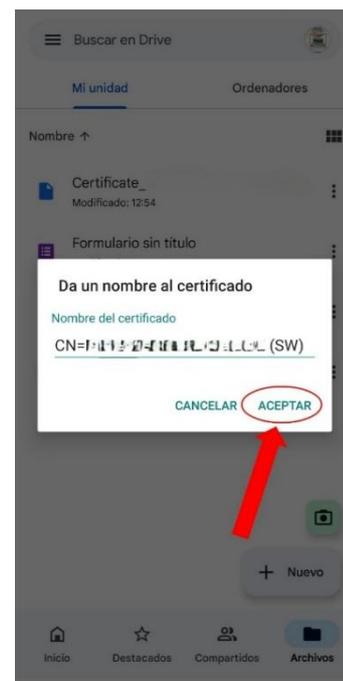
2. Introducimos la contraseña utilizada en la descarga del certificado y clic en “aceptar”.



3. Elegimos la opción de “certificado de usuario de VPN y aplicaciones”



4. Clic en “ACEPTAR”

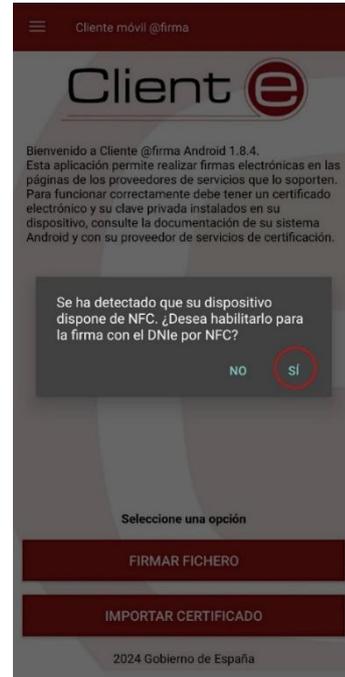


**PASO 3: Instalación App “Cliente @firma móvil” desde la Play Store / AppGallery**

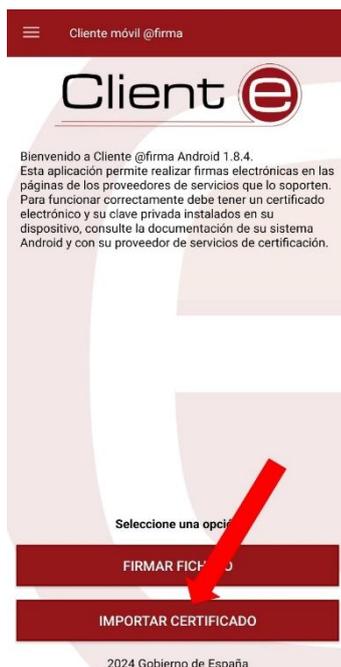
5. Procedemos a descargar la APP **Cliente @firma.**



6. Una vez descargada la APP entramos en ella y aceptamos las condiciones de NFC dándole a “**SÍ**”



7. Hacemos clic en “**IMPORTAR CERTIFICADO**”



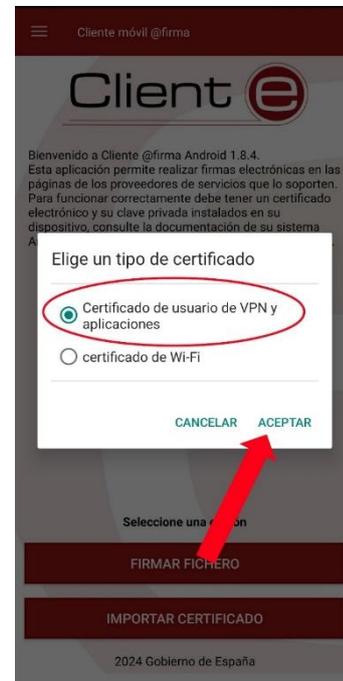
8. Seleccionamos nuestro certificado.



9. Introducimos la misma contraseña que la utilizada anteriormente:



10. Elegimos de nuevo el tipo de certificado de nuevo “Certificado de usuario de VPN y aplicaciones”



11. Hacemos clic en “ACEPTAR” y nuestro certificado estará instalado.



## PASO 4: Instalación App “Certificado digital FNMT” desde la Play Store / AppGallery

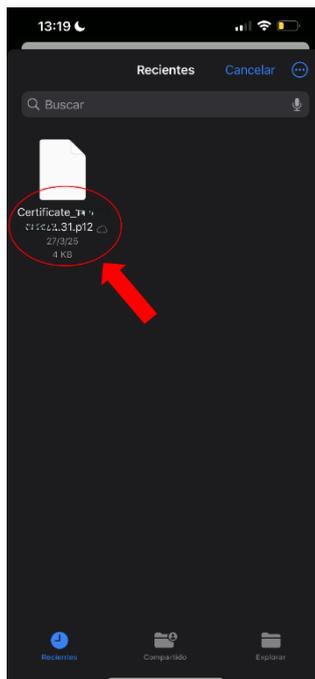
1º Entramos en la aplicación y hacemos clic en “Mis certificados Instalados”.



2º Clic en “Importar Certificado Digital”.



3º Seleccionamos nuestro certificado.



4º Introducimos la contraseña con la que guardamos el Certificado Digital



5º Nos aseguramos que es el certificado correcto y le damos a **“Importar”**.



6º Ya estaría la importación a la aplicación y podríamos ver nuestros certificados instalados.



7º En este apartado podemos visualizar nuestros certificados instalados en la aplicación.



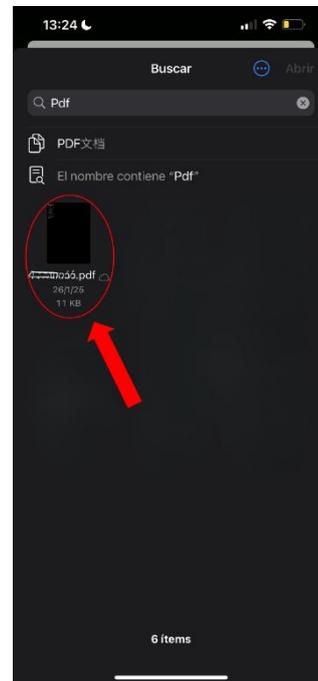
8º Ahora para **firmar un documento**, le damos clic a las tres rallitas de la esquina superior derecha y le damos a **“Firmar Archivos”**.



9º Seleccionamos el certificado con el que queremos firmar.



10º Seleccionamos el archivo PDF en cuestión para firmarlo.



11º Ya estaría nuestro fichero firmado correctamente.



## IMPORTANTE



Es extremadamente recomendable añadir una capa extra de seguridad a la hora de utilizar tu certificado desde tu dispositivo, aunque en Android de forma nativa no es posible, sería conveniente una aplicación de terceros.

Cabe destacar que los documentos firmados desde un dispositivo Android con el certificado **no tendrán una firma visible**. Aunque el documento constará como firmado, esta no se mostrará de forma física en el propio archivo.

## ATENCIÓN

Los pasos descritos en este manual están diseñados para la instalación de un certificado digital ACA+ en un dispositivo Android v.11. Es importante advertir que el Colegio de la Abogacía de Salamanca declina cualquier responsabilidad que pueda acaecer por la utilización de este u otros manuales.

Desde el Colegio recomendamos la instalación en el dispositivo de una capa extra de seguridad, aunque en Android de forma nativa no es posible, sería conveniente una aplicación de terceros. Esto aumentará la seguridad en tu dispositivo Android, aunque es importante destacar que ninguna medida de seguridad es infalible. El proceso descrito en este manual no garantiza una seguridad total, ya que siempre existen riesgos inherentes a los sistemas informáticos y a la tecnología en general.

El Colegio de la Abogacía de Salamanca no se hace responsable por cualquier pérdida, daño o acceso no autorizado que pudiera ocurrir, incluso después de seguir los procedimientos de seguridad recomendados.

### **Recomendaciones adicionales para garantizar la seguridad de su dispositivo:**

1. **Contraseña Segura:** Asegúrate de utilizar una contraseña fuerte y única para bloquear su dispositivo
2. **No Compartas tu Contraseña:** Nunca compartas tu contraseña, ni la de su dispositivo con nadie.
3. **Actualización del Sistema:** Mantén siempre actualizado el sistema operativo, ya que las actualizaciones frecuentemente corrigen vulnerabilidades de seguridad.
4. **Uso de Antivirus y Seguridad Adicional:** Considera utilizar aplicaciones de seguridad adicionales, como antivirus o aplicaciones de gestión de contraseñas.
5. **Cuidado con Phishing y Malware:** No abras correos electrónicos, mensajes o enlaces de fuentes desconocidas.
6. **Cierre de Sesiones:** Asegúrate de cerrar sesión en las aplicaciones que utilizan su certificado digital.

Recuerde que la seguridad de su dispositivo y datos depende en gran medida de las precauciones que tome. Mantener un control adecuado sobre su dispositivo y sus credenciales es crucial para evitar posibles amenazas.