

Manual del Portafirmas iOS v1.5

Revisión 1.0

Índice de contenidos

[1 Descarga del portafirmas 3](#_Toc30085926)

[2 Portafirmas iOS 4](#_Toc30085927)

[2.1 Selección del servidor Portafirmas 4](#_Toc30085928)

[2.1.1 Agregar nuevo servidor 5](#_Toc30085929)

[2.1.2 Modificar un servidor existente 5](#_Toc30085930)

[2.1.3 Eliminar un servidor 6](#_Toc30085931)

[2.2 Acceso con certificado local 6](#_Toc30085932)

[2.3 Acceso con certificado remoto (Cl@ve Permanente) 7](#_Toc30085933)

[3 Bandejas de peticiones 10](#_Toc30085934)

[3.1 Listados de peticiones 10](#_Toc30085935)

[3.2 Procesado de peticiones 10](#_Toc30085936)

[3.2.1 Firma con certificado remoto 12](#_Toc30085937)

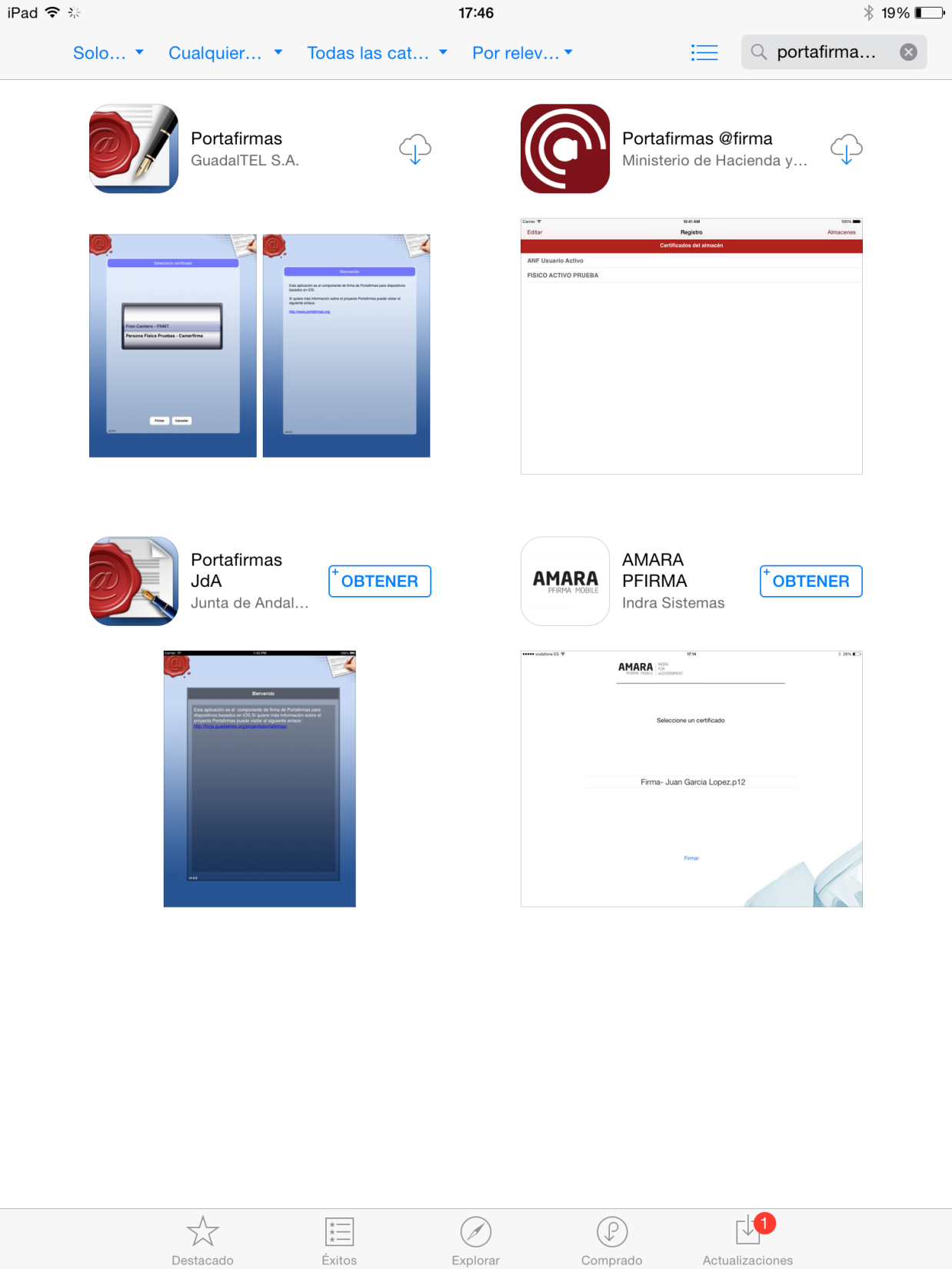
[3.3 Detalle de petición 14](#_Toc30085938)

[ANEXO 1. Importar certificado de usuario desde la aplicación “Archivos” (“Files”) 16](#_Toc30085939)

[ANEXO 2. Importar certificado de usuario desde iTunes 17](#_Toc30085940)

# Descarga del portafirmas

El primer paso para el acceso al Portafirmas desde Apple iOS es la descarga de la aplicación desde la Apple Store. Para encontrarla podemos buscar por “Portafirmas @firma”.

****

A continuación, pulsaremos sobre el icono de instalación:

****

# Portafirmas iOS

El portafirmas del Ministerio de Política Territorial y Función Pública es una plataforma web para la gestión del flujo de peticiones de firma que permite a sus usuarios revisar dichas peticiones, firmarlas, darles el visto bueno o rechazarlas. El ministerio dispone de dos despliegues de su portafirmas, pero también lo distribuye para que otros organismos puedan implantarlo.

La aplicación móvil del portafirmas permite el acceso a cualquier instancia del portafirmas del ministerio, o a cualquier instancia del mismo desplegada por otros organismos. La aplicación móvil permite a sus usuarios acceder y realizar las operaciones básicas sobre las peticiones de firma de dicho usuario.

Un usuario sólo podrá acceder a una instancia del portafirmas si previamente se le ha creado una cuenta en el mismo. Cualquier persona que pueda acceder al portafirmas a través de la web podrá acceder al mismo portafirmas desde la aplicación móvil.

El portafirmas móvil utiliza certificados electrónicos reconocidos tanto para el acceso a la cuenta del usuario para la firma de sus peticiones. Estos pueden ser:

* Certificados locales instalados en el dispositivo.
* Certificados en la nube de Cl@ve Permanente.

Por defecto, los accesos se realizarán mediante certificados instalados en el dispositivo, pero un usuario puede activar el uso de los certificados remotos mediante la opción “Usar certificados remotos” de la pantalla principal de la aplicación móvil.

El certificado, local o remoto, permite al portafirmas identificar a la persona que intenta acceder y con ello identificar su cuenta del portafirmas seleccionado. Esto quiere decir que no es necesario dar de alta este certificado en el servicio portafirmas y que, si tiene cuenta en más de un portafirmas, podrá acceder a todos ellos con el mismo certificado.

## Selección del servidor Portafirmas

El portafirmas móvil permite tener configuradas múltiples instancias de Portafirmas, por lo que antes de acceder deberá seleccionar cuál desea utilizar. La aplicación tiene configurados por defecto los dos siguientes servidores Portafirmas del ministerio:

* Portafirmas General AGE
* Portafirmas RedSARA

Un usuario puede acceder a cualquiera de estos portafirmas, dar de alta otros, editarlos o eliminarlos.

Desde la pantalla de inicio de la aplicación se puede seleccionar Portafirmas al que se va a acceder mediante la opción “SERVIDOR” (Fig. 2.4).

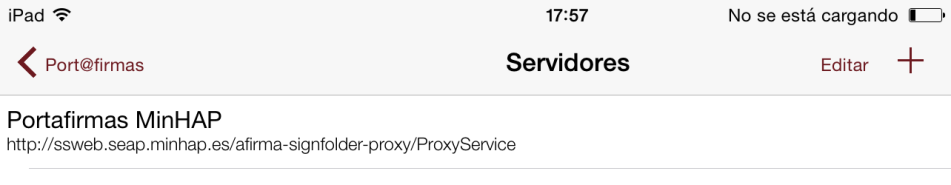
****

Fig. 2.4

En el listado que se muestra al usuario, pulsaremos sobre el Portafirmas al que deseemos acceder y pulsaremos sobre la opción “Seleccionar” del menú contextual.

### Agregar nuevo servidor

Para agregar un servidor distinto a los que vienen por defecto, pulsaremos en el símbolo ‘+’, tras lo que se nos mostrará una pantalla (Fig. 2.1) en la que podremos introducir el alias o nombre con el que queremos referirnos al nuevo Portafirmas y la URL del mismo. A continuación, pulsaremos el botón “Guardar”.

****

Fig. 2.1

### Modificar un servidor existente

Para editar un servidor que ya tenemos dado de alta en la lista de servidores, debemos pulsar en el elemento correspondiente del listado y pulsar sobre la opción “Editar” del menú contextual. En este diálogo podemos modificar el nombre y la URL del servidor. Para aplicar los cambios, pulsaremos sobre el botón “Guardar”.

### Eliminar un servidor

Para eliminar un servidor portafirmas deberemos desplazar hacia la izquierda el elemento correspondiente del listado de servidores, tras lo que aparecerá un botón “Eliminar” en el lado derecho del mismo. Al pulsar sobre este botón eliminaremos el servidor.

Si se eliminan todos los servidores del listado, automáticamente se volverán a agregar los servidores por defecto.

## Acceso con certificado local

Para acceder al portafirmas seleccionado con certificado local, deberemos haber importado al dispositivo y registrado en la aplicación el certificad. La importación del certificado en la aplicación se puede hacer directamente desde la aplicación mediante la app “Archivos” o a través de iTunes y un dispositivo de sobremesa al que se conecte el dispositivo móvil. Ambas alternativas se describen en los apartados ANEXO 1 Importar certificado de usuario desde la aplicación “Archivos” (“Files”) y ANEXO 2 Importar certificado de usuario desde iTunes.

Una vez añadido un certificado a la aplicación deberemos registrarlo.

1. Desde la pantalla de inicio accederemos al apartado “CERTIFICADO” que aparecerá con el valor “Sin especificar”.
2. En esa nueva pantalla nos aparecerá el listado de certificados, primeramente, vacía. Para agregar el certificado importado, pulsaremos el símbolo ‘+’ de la esquina superior derecha.
3. En la nueva pantalla seleccionaremos el almacén importado en la aplicación (Figura 2.2), **introducimos la contraseña del almacén** y pulsamos el botón “Registrar” (Figura 2.3).
4. En el listado de certificados, ahora seleccionaremos el certificado registrado y la aplicación nos mostrará un mensaje con el resultado del proceso (Figura 2.4).

**Advertencia:** Se han encontrado algunos tipos de certificados que, por un problema en las funciones de gestión de certificado de iOS, pueden registrarse en la aplicación, pero no es posible utilizarlos.

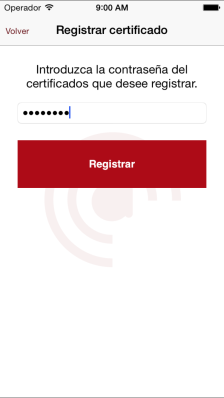
****

Fig. 2.2 Fig. 2.3 Fig. 2.4

Para el uso del certificado local, comprobaremos que la opción “Usar certificados remotos” de la pantalla principal se encuentra desactivada. A continuación, pulsaremos el botón “Acceder”. Si el establecimiento de sesión es correcto, el usuario será redirigido a la pantalla de peticiones pendientes de firmar.

**Un usuario sólo podrá acceder a un servicio de portafirmas si dispone de una cuenta en el mismo**. De no ser así, se producirá un error de conexión.

**Advertencia:** El certificado seleccionado es el que se utilizará tanto para la autenticación del usuario (mediante un proceso de validación realizado por el propio Portafirmas web), como para la firma de las peticiones. Por este motivo, se recomienda que se utilice siempre un certificado de firma (no repudio) para acceder a la aplicación.

## Acceso con certificado remoto (Cl@ve Permanente)

Primeramente, hay que tener en cuenta que no todos los servicios de portafirmas permiten el uso de certificado remoto. Consulte con su proveedor de su portafirmas si tiene dudas acerca de la disponibilidad de esta opción.

Para acceder al portafirmas seleccionado con certificado remoto, deberemos habernos dado previamente de alta en Cl@ve y activar nuestro usuario de Cl@ve Permanente. Puede obtener más información sobre los procedimientos necesarios en:

<https://clave.gob.es/clave_Home/Clave-Permanente.html>

Para configurar el Portafirmas móvil para el uso del certificado remoto, marcaremos la opción “Usar certificados remotos” de la pantalla principal de la aplicación. A continuación, pulsaremos el botón “Acceder”.



La aplicación móvil accederá a su cuenta de portafirmas con certificado remoto por medio de Cl@ve Permanente que necesita que el usuario introduzca su DNI y los datos de autenticación. La aplicación mostrará para esto la página web de Cl@ve Permanente en donde el usuario podrá introducir su DNI y la contraseña de Cl@ve. Seguidamente deberá pulsar el botón “Autenticar >”.



Al autenticarse, el usuario recibirá un SMS con un código en el número de móvil que haya dado de alta en Cl@ve. En la siguiente pantalla, el usuario deberá insertar el código recibido y pulsar el botón “Autenticar >”.

# Bandejas de peticiones

## Listados de peticiones

Al entrar en el portafirmas, se accede a la pantalla que muestra la bandeja de peticiones que el usuario tiene pendientes por firmar. También pueden verse, a través de las opciones de la parte inferior de la pantalla los listados de peticiones rechazadas y peticiones firmadas.

****

En estos listados se pueden encontrar las peticiones de firma y visto bueno que, respectivamente, están pendientes de procesar, se han rechazado y se han procesado correctamente.

## Procesado de peticiones

Desde el listado de peticiones pendientes podemos acceder a las diferentes acciones disponibles (Firma/Visto Bueno/Rechazo). Para ello debemos pulsar el botón “Seleccionar” situado arriba a la derecha (Fig. 3.1). Veremos cómo, después de hacerlo, la lista se nos muestra en modo edición de manera que podemos seleccionar las peticiones que queramos procesar (Fig. 3.2). Una vez seleccionada alguna petición los botones inferiores de “Firmar/Visto Bueno” y “Rechazar” se habilitarán para que podamos pulsarlos y procesar como queramos las peticiones seleccionadas (Fig. 3.3).

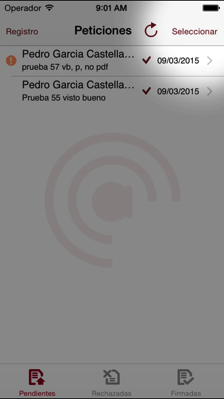
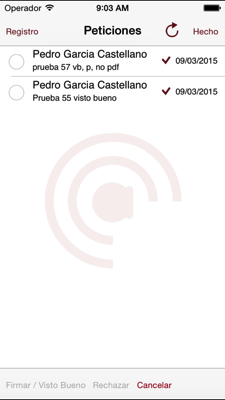
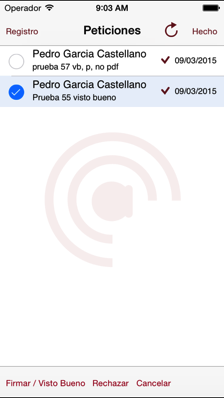
**** **** ****

Fig. 3.1 Fig. 3.2 Fig. 3.3

Cuando un usuario pulsa el botón “Firmar/Visto Bueno” de la parte inferior de la pantalla después de seleccionar una o más peticiones se le mostrará el número de cada tipo y se le pedirá confirmación antes de procesarlas.

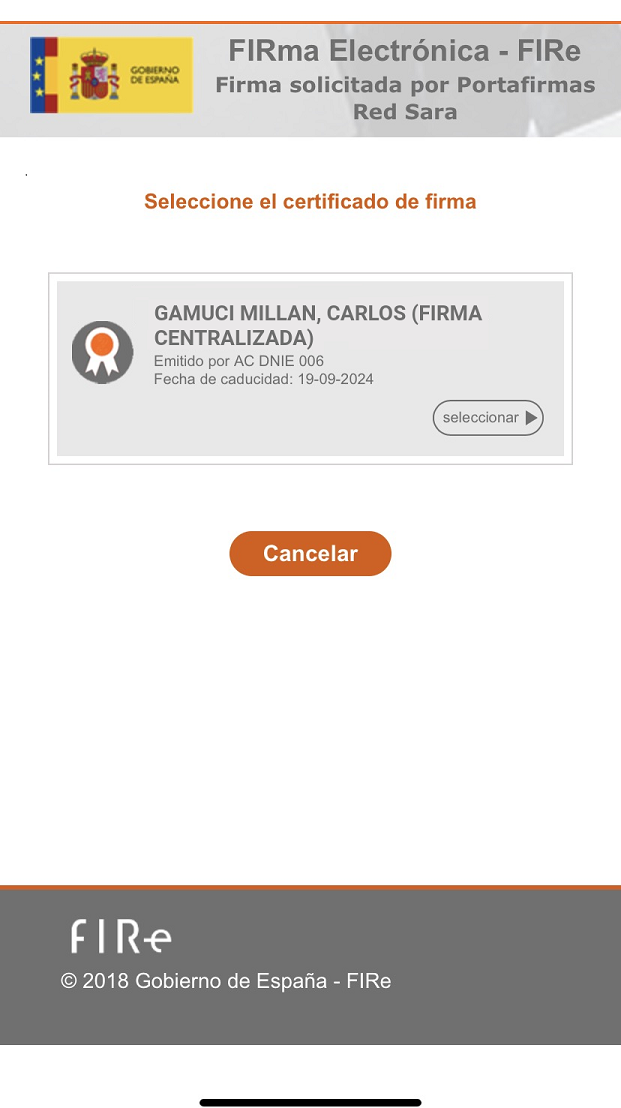
En caso de haberse utilizando un certificado local para autenticarse en el sistema, la aplicación utilizará ese mismo certificado para firmar las peticiones, sin necesidad de que el usuario tenga que volver a seleccionarlo. Si, en cambio, se accedió con un certificado remoto, se utilizará el certificado remoto de firma para firmar las peticiones. Este proceso se describe en el apartado 3.2.1 Firma con certificado remoto. Las operaciones de visto bueno no requieren el uso del certificado de firma.

Cuando el usuario pulse el botón “Rechazar”, se le pedirá confirmación de la operación y que introduzca el motivo del rechazo de las peticiones seleccionadas para que este quede registrado y llegue a la aplicación o persona que solicitó la firma. El motivo de rechazo introducido aplicará a todas las peticiones actualmente seleccionadas. Si no se especifica motivo de rechazo se aplicará un texto de rechazo genérico.

Al procesar una petición, si el proceso se realiza correctamente, la petición pasa a la bandeja de “Firmadas”. Al rechazar peticiones, estas pasan a la bandeja de “Rechazadas”.

### Firma con certificado remoto

Las operaciones de firma con certificado remoto se realizan con el certificado de Cl@ve Firma a través de la plataforma FIRe. Al iniciar el proceso de firma se abrirá una ventana para la selección del certificado remoto de firma. Seleccionaremos este certificado pulsando su botón “seleccionar”.



A continuación, se nos mostrará la pantalla de autorización del proceso de firma en la que se podrá ver el DNI del usuario y se deberá introducir la contraseña de Cl@ve y el código recibido por SMS en el número de teléfono que se dio de alta. Finalmente, se pulsará el botón “Continuar” para completar el proceso de firma.



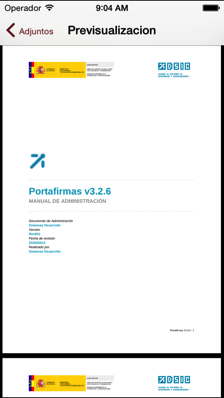
Al finalizar la firma volveremos a ser redirigidos al listado de peticiones pendientes.

## Detalle de petición

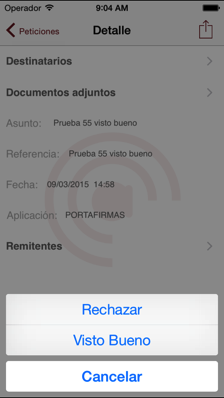
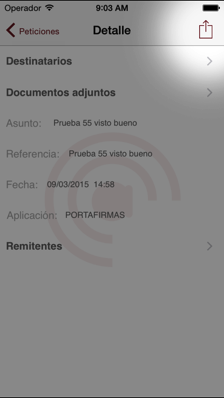
Desde los listados de peticiones podemos acceder al detalle de cualquiera de ellas para obtener información de la misma, como su mensaje o los documentos que la acompañan.

****

También es posible revisar los documentos incluidos en la petición:

****

Las acciones de “Firma/Visto Bueno” y “Rechazo” pueden ejecutarse desde la pantalla de detalle de una petición pendiente de firmar. Para hacerlo, sólo debemos pulsar sobre el botón superior derecho y después sobre la opción deseada.

****

Procesar una petición desde esta pantalla equivale a hacerlo desde el listado de peticiones seleccionando sólo una petición.

1. Importar certificado de usuario desde la aplicación “Archivos” (“Files”)

Para importar en la aplicación un certificado desde la aplicación “Archivos” deberemos acceder al listado de certificados de la aplicación a través de la opción “CERTIFICADO” de la página principal. Seguidamente pulsaremos sobre el símbolo ‘+’ situado en la esquina superior derecha de la aplicación. Desde esta pantalla seleccionaremos el enlace “**Añadir más almacenes desde Files App**” (Fig. A1.1), tras lo cual se nos abrirá la aplicación “Archivos”.

Desde la aplicación Archivos podremos seleccionar el archivo PKCS#12 que contenga nuestro certificado y que tengamos en nuestro dispositivo móvil, en iCloud o en cualquier otra ubicación disponible (Fig. A1.2 y A1.3). Al hacerlo, el archivo aparecerá disponible en el listado de “Almacenes Disponibles” de la aplicación.

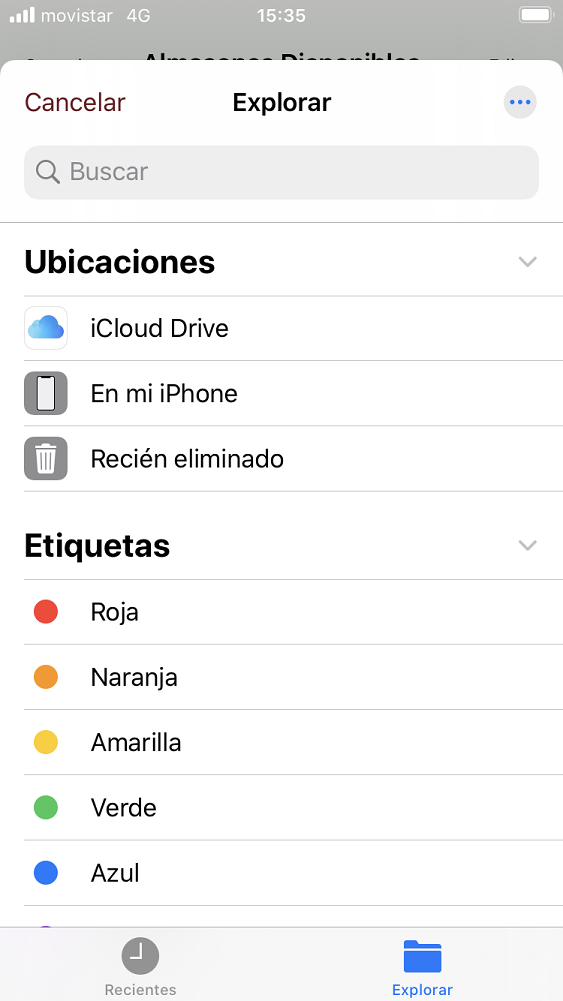
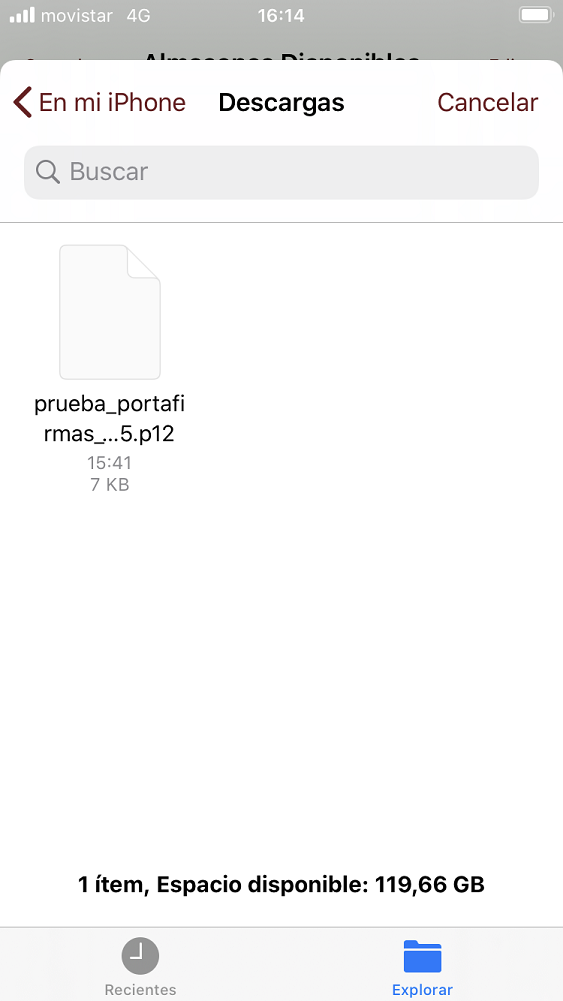
  

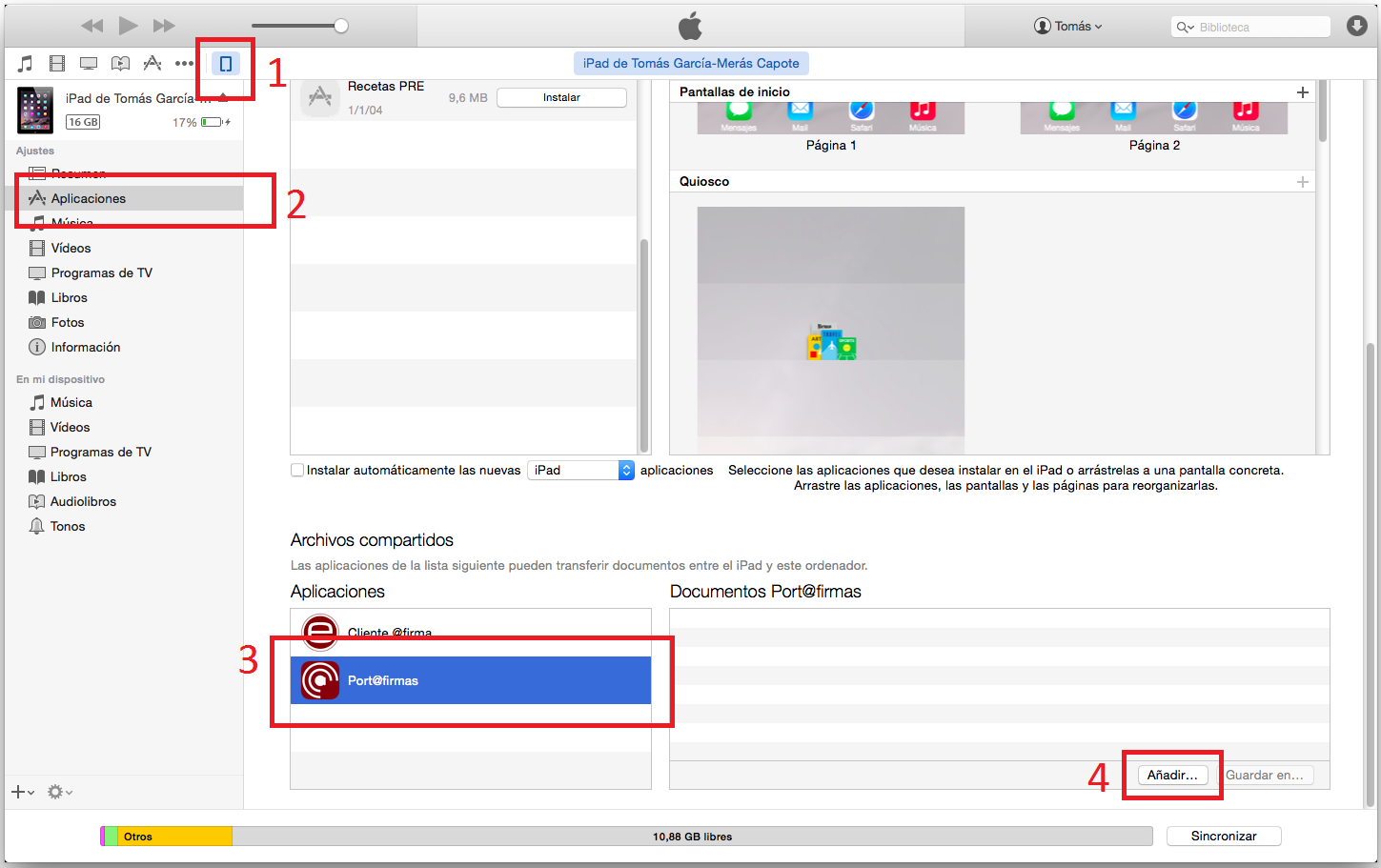
Fig. A1.1 Fig. A1.2 Fig. A1.3

Una vez importado el archivo de almacén, se deberá registrar el certificado en la aplicación como se describe en el apartado 2.2 Acceso con certificado local.

1. Importar certificado de usuario desde iTunes

Para importar a la aplicación un certificado desde iTunes, tendremos que conectar por cable nuestro dispositivo móvil con el equipo macOS o Windows en el que tengamos instalada la aplicación. Desde iTunes se debe seleccionar el dispositivo conectado (Paso 1), navegar hasta la pestaña de “**Aplicaciones**” (Paso 2) y posicionarnos en el final de la página.

Una vez ahí deberíamos ver la aplicación Port@firmas en la parte izquierda de la pantalla dentro de la columna “**Aplicaciones**”. Si la seleccionamos (Paso 3) la columna de la derecha se actualizará para dejarnos añadir archivos. Utilizamos el botón “**Añadir**” (Paso 4) para agregar los **almacenes de certificados** (ficheros .p12/.pfx) que queramos.

****

Una vez importado el archivo de almacén, se deberá registrar el certificado en la aplicación como se describe en el apartado 2.2 Acceso con certificado local.

[Creative Commons License](#Licencia_Creative_Commons)

Esta obra está bajo una licencia [Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 Unported](#Licencia_Creative_Commons).