



# Manual de Usuario

**UKC Desktop para MacOS**

# Contenido

1. Introducción .....	3
2. Certificado digital remoto con UKC Desktop.....	3
2.1. Instalar el programa UKC Desktop .....	3
2.2. Configuración del programa UKC Desktop.....	5
2.2.1. Contenido y configuración en MacOS .....	5
2.2.2. Inicio de sesión en SignCloud .....	6
2.3. Cómo utilizar el programa UKC Desktop .....	7
2.4. Firma electrónica de un documento en MacOS .....	8
2.5. Ejemplo de firma electrónica de un documento en MacOS .....	9, 11
2.6. Desbloqueo de PIN .....	12

# 1. Introducción

El presente manual recoge una guía de usuario para el uso de los certificados digitales remotos almacenados en SignCloud (nube de Digifirma) en Mac OS.

En el capítulo 2 se explica cómo utilizar el certificado digital remoto.

## 2. Certificado digital remoto con UKC Desktop en macOS

El presente documento tiene el objetivo de guiar al usuario a través del software UKC Desktop para el uso de certificados digitales custodiados en el sistema SignCloud de Digifirma.

En él se detalla el proceso de instalación del UKC Desktop, así como su uso. A través de la aplicación middleware UKC Desktop, el usuario podrá de manera muy sencilla firmar electrónicamente y autenticarse en páginas web. Para ello se requieren las credenciales utilizadas en el proceso de generación del certificado (Usuario, Contraseña y código PIN)

### 2.1. Instalar el programa UKC Desktop

A continuación, se detalla el procedimiento para llevar a cabo la instalación del software UKC Desktop.

1. Descargar el programa UKC Desktop.
2. Ejecutar el archivo y seguir el proceso de instalación.
3. Instalar software
4. Cerrar el instalador una vez completada la instalación.

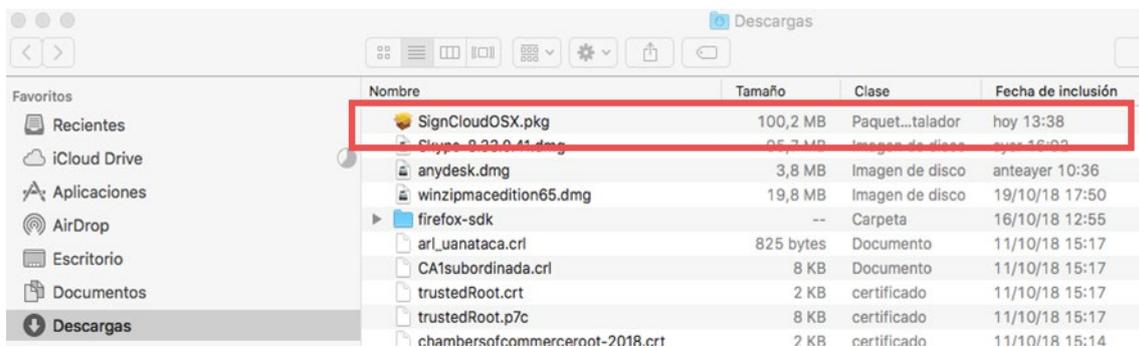


Figura 1. Descarga en MacOS de SignCloud

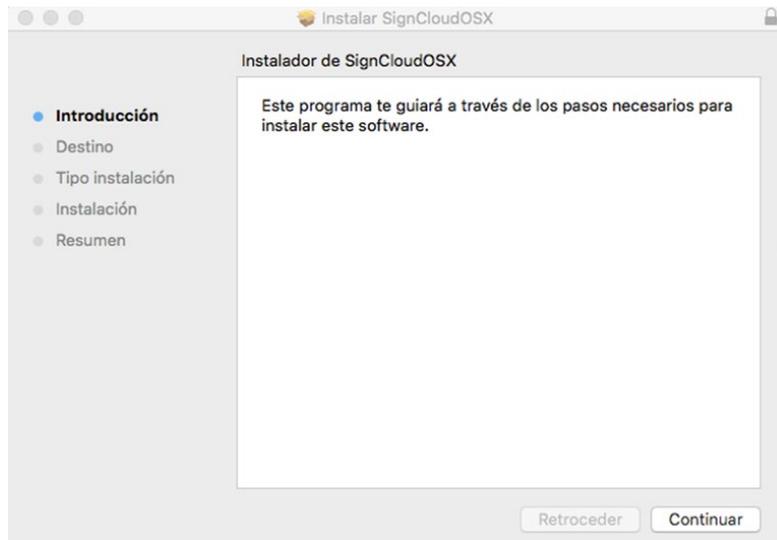


Figura 2. Asistente instalación de UKC Desktop MacOS de SignCloud.

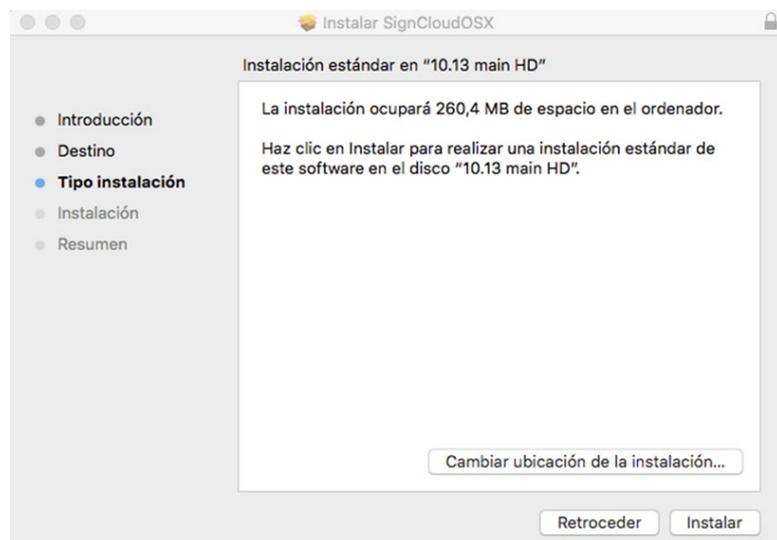


Figura 3. Asistente ubicación instalación de UKC Desktop MacOS de SignCloud

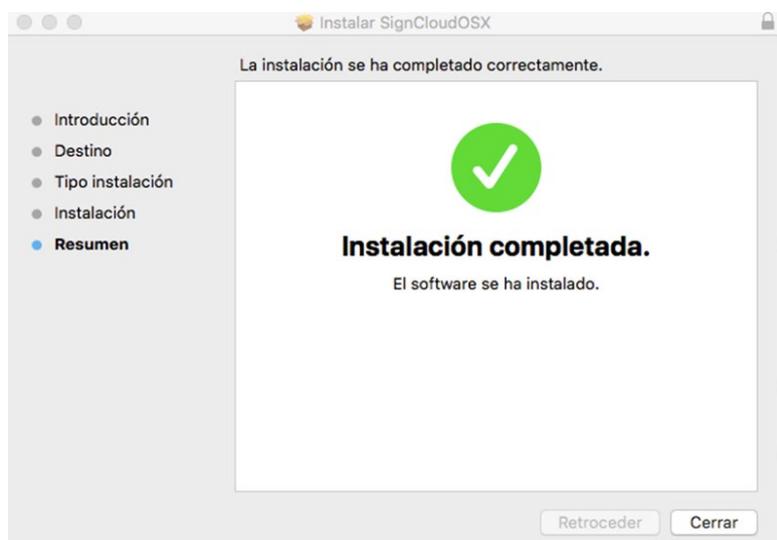


Figura 4. Instalación completada de UKC Desktop macOS de SignCloud

## 2.2. Configuración del programa UKC Desktop en MacOS

Para poder utilizar las funcionalidades de UKC Desktop con certificados remotos es necesario disponer de un certificado digital emitido en el sistema SignCloud de Digifirma. Esta identidad o certificado remoto tiene asociadas las siguientes credenciales, que permiten utilizar los servicios de firma electrónica:

- Usuario (entregado en mano en el documento “Carta de Credenciales”, cuando el usuario se identificó en la autoridad de registro.
- Contraseña (contenida en el email que le fue enviado al usuario, cuando éste se identificó en la autoridad de registro)
- Código PIN (elegido e introducido por el usuario cuando se generó el certificado digital)

El programa UKC Desktop se ejecuta automáticamente cuando se arranca el MacOS. Para acceder a la aplicación, debemos presionar el icono que aparece en la barra de tareas.



Figura 5. UKC Desktop en la barra de herramientas superior

### 2.2.1. Contenido y configuración en MacOS

Una vez abierto UKC Desktop, nos muestra la ventana principal:



Figura 6. Ventana principal de UKC Desktop

Esta vista principal está compuesta por un menú superior con diferentes opciones. Cada una de estas opciones permite llevar a cabo tareas diversas. A continuación, se definen en detalle cada una de ellas:

#### Archivo:

- **Salir.** Esta opción cierra la aplicación UKC Desktop.

## Configuración:

- **Red:** En caso de ser necesario, permite configurar un servidor Proxy.
- **Tarjeta/Token:** Desde esta opción podremos gestionar las credenciales PIN (cambiar y desbloquear) y PUK (cambiar) de las tarjetas y tokens criptográficos del fabricante Bit4id que eventualmente estén conectados a la Mac.
- **SignCloud:** Esta opción permite gestionar los certificados digitales custodiados en el sistema SignCloud de Digifirma.
  - Iniciar sesión en el sistema SignCloud a través de la opción “Conectar”. La aplicación solicitará las credenciales necesarias.
  - Para cerrar sesión en el sistema SignCloud debemos utilizar la opción “Desconectar”.
  - Durante el inicio de sesión, el sistema permite memorizar (“Memorizar esta acción”) las credenciales “Usuario” y “Contraseña” para evitar introducirlas cada vez que ejecutemos la aplicación.
  - Marcando la opción “Descartar Credenciales” borraremos la información memorizada.
  - Se puede cambiar la contraseña asociada a nuestro certificado digital remoto a través de la opción “Cambiar contraseña”. Cualquier tipo de cambio en las credenciales (PIN, PUK y contraseña) del certificado digital remoto requiere contar con las credenciales en vigor.
- **Acerca...:** Muestra información acerca de la versión de UKC Desktop instalada.

### 2.2.2. Inicio de sesión en SignCloud

El inicio de sesión permite acceder al certificado digital custodiado en el sistema SignCloud de Digifirma, cargándola en la MAC y constituye la fase de identificación del usuario. No obstante, para poder utilizar dicho certificado digital en los servicios de firma y/o autenticación, necesitaremos el código PIN (sea estático o dinámico), completando así el proceso de autenticación para el desbloqueo de la firma.

Para poder iniciar sesión en el sistema SignCloud, seleccionamos dentro de “Configuración” la opción “SignCloud” y seguidamente “Conectar...”:

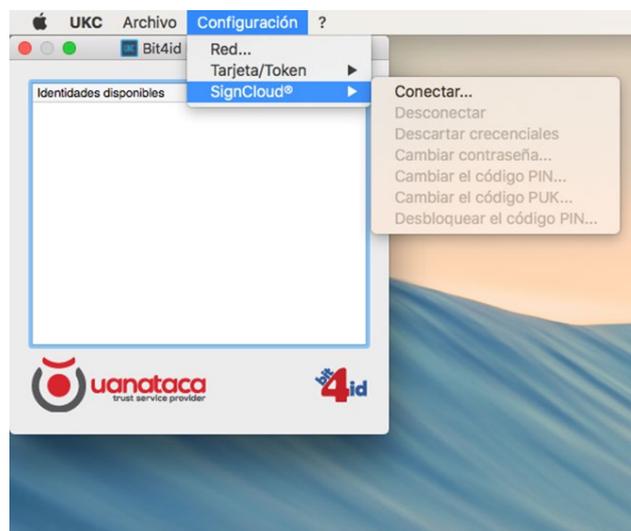


Figura 8. Conectarse al sistema SignCloud

La aplicación muestra una ventana donde debemos introducir las credenciales identificativas “Usuario” y “Contraseña” asociados a nuestro certificado digital remoto.

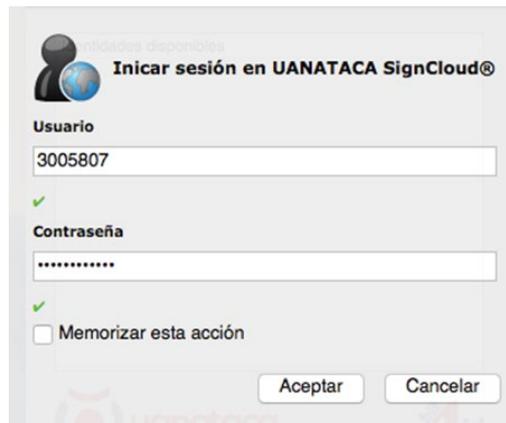


Figura 9. Iniciar sesión en SignCloud

A partir de este momento, el certificado digital remoto se encuentra cargado en el sistema y listo para ser utilizado.



Figura 10. Vista de certificados digitales disponibles

### 2.3. Cómo utilizar el programa UKC Desktop

UKC Desktop actúa como un proveedor de identidades digitales remotas en el sistema. Esto quiere decir que no es un motor de firma electrónica en sí mismo, ya que no genera firmas PAdES, XAdES o CAdES por sí solo.

En otras palabras, las aplicaciones instaladas en el sistema que sean motores de firma (Ej. PDF Adobe Acrobat Reader, Microsoft Word, 4identity, AutoFirma, etc.) harán uso de los certificados digitales ofrecidos por UKC Desktop para llevar a cabo las firmas electrónicas.

## 2.4. Firma electrónica de un documento en MacOS

Para firmar un documento utilizando PDF Adobe Acrobat Reader con un certificado digital en MacOS por primera vez, se tiene que configurar primero. Los pasos a seguir son:

1. Ir a "Preferencias"



Figura 11. Configuración Adobe Acrobat Reader con certificado digital en MacOS

2. Seleccionar "Firmas"
3. Ir a "Crear y administrar identidades para firmar"

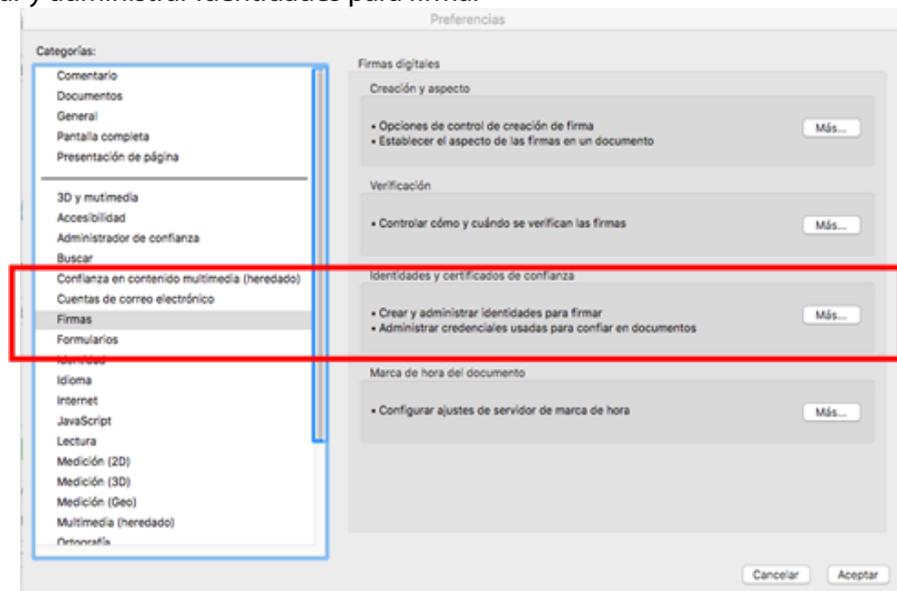


Figura 12. Configuración Adobe Acrobat Reader con certificado digital en macOS

4. Seleccionar "Módulos y distintivos PKCS#11"
5. Adjuntar módulo



Figura 13. Configuración Adobe Acrobat Reader con certificado digital en macOS

6. Insertar la siguiente ruta en la "Ruta de biblioteca":

/Applications/UniversalKeychain/UniversalKeychain.app/Contents/Resources/pkcs11/libbit4p11.so

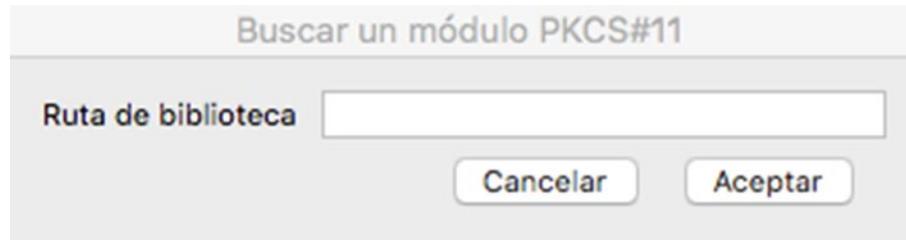


Figura14. Configuración Ruta de biblioteca Adobe Acrobat Reader con certificado digital en macOS

La configuración estará realizada y ya podrá firmar documentos con el programa Adobe PDF Reader.

## 2.5. Ejemplo de firma electrónica de un documento en MacOS

Una vez configurado nuestro certificado digital en PDF Adobe Acrobat Reader, a continuación, se muestra un ejemplo de cómo firmar un documento. Abrir el documento PDF que se desea firmar desde la aplicación Adobe Acrobat Reader.

1. Acceder al menú "Herramientas" y seleccione "Certificados".
2. En la barra "Certificados" abrir la opción "Firmar Digitalmente".

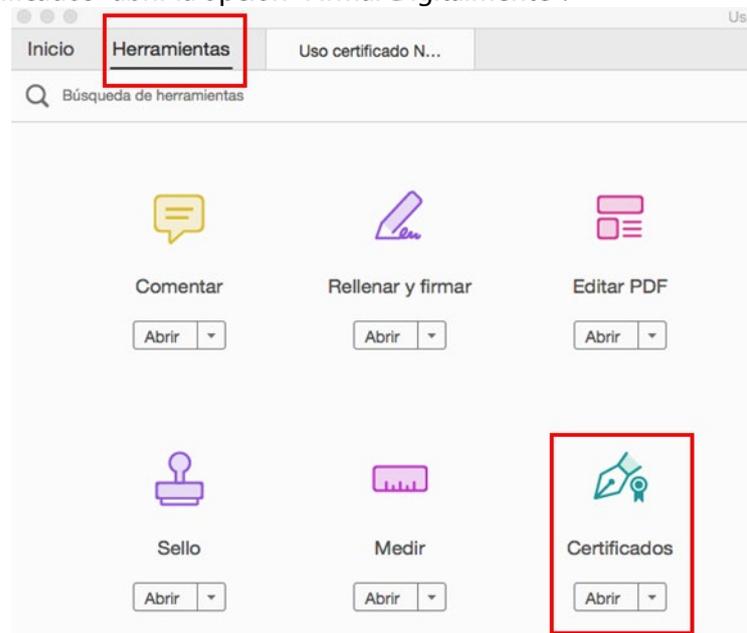


Figura 15. Herramientas en el sistema (PDF Adobe Acrobat Reader)

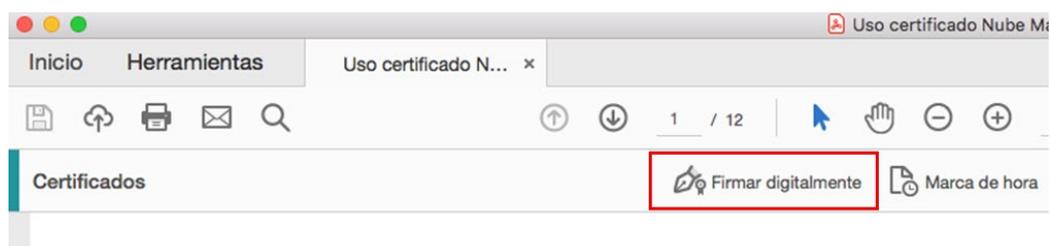


Figura 16. Firmar digitalmente en el sistema (PDF Adobe Acrobat Reader)

3. A continuación, aparece el menú de firma y los certificados digitales disponibles. Seleccione y pulse continuar.

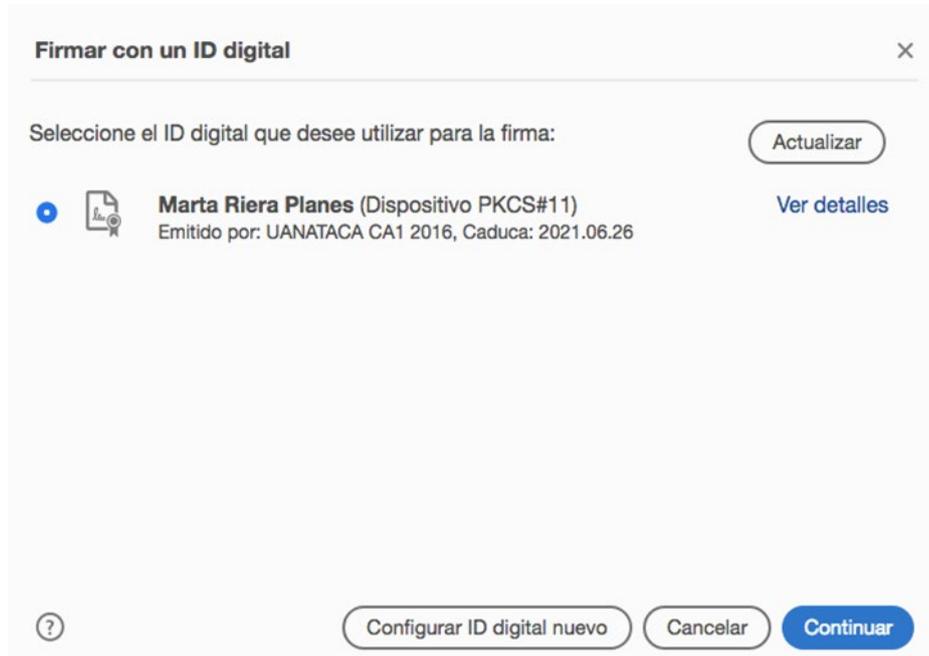


Figura 17. Seleccionar el certificado digital en el sistema (PDF Adobe Acrobat Reader)

4. Seguidamente se muestra el menú de firma. Presionamos Firmar.

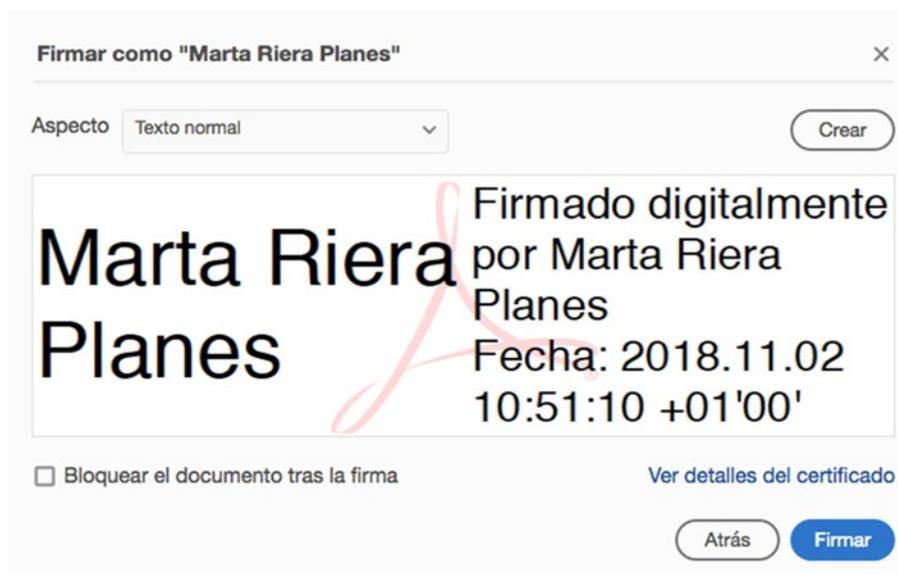


Figura 18. Menú de firma

5. Guardamos el documento a firmar.

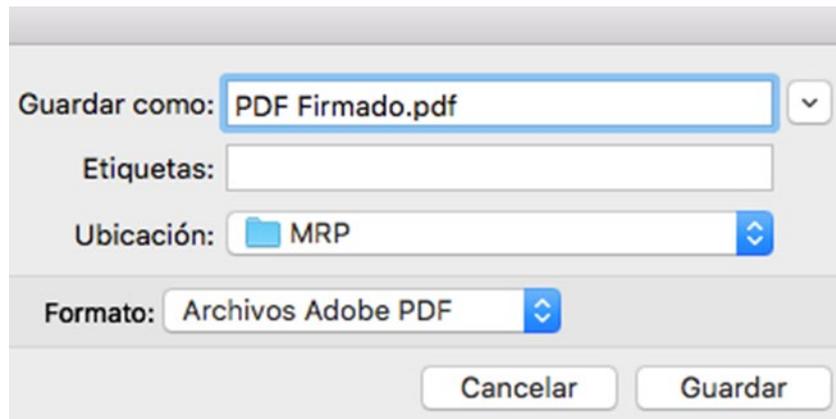


Figura 19. Guardar documento a firmar

6. UKC Desktop solicitará el código PIN para autorizar la firma electrónica del documento.

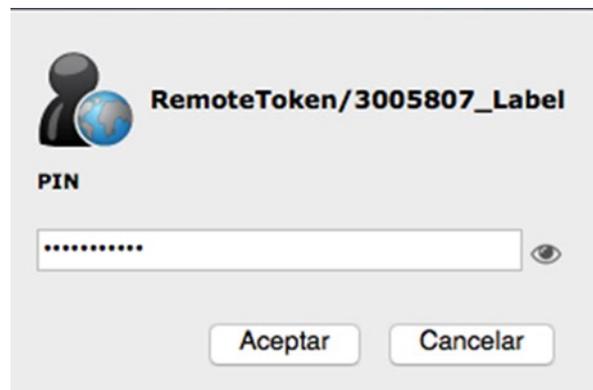


Figura 20. Inserción de PIN de firma por parte del usuario en UANATACA UKC Desktop

7. Al introducir el código PIN de forma satisfactoria, la firma electrónica del documento se llevará a cabo.



Figura 21. Firma electrónica válida

## 2.6. Desbloqueo de PIN

En caso su PIN quede bloqueado por intentos fallidos, debe acceder al siguiente enlace para restablecer el mismo: <https://www.uanataca.com/lcimpl/reset?customer=digifirma>



Figura 22. Pantalla Desbloqueo PIN

En esta pantalla debe colocar sus credenciales: nombre de usuario y contraseña, luego recibirá en el correo electrónico registrado un código OTP/confirmación que deberá introducirlo y posteriormente introducir su nuevo PIN dos veces.

**NOTA: Este código PIN debe contener al menos por 2 números, 2 letras y 8 caracteres.**

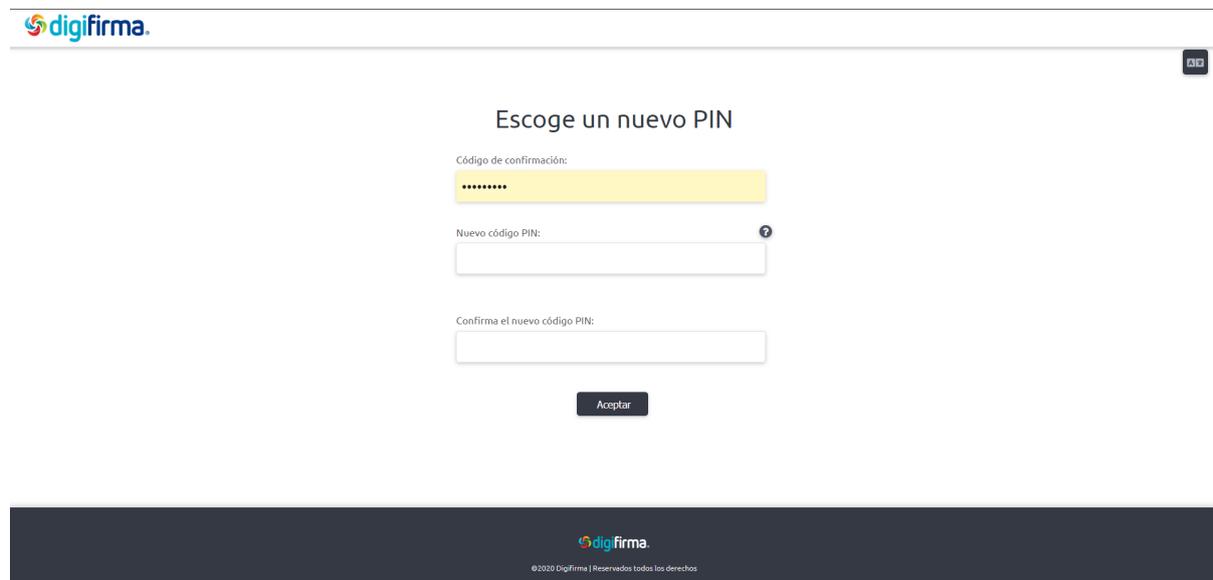


Figura 23. Pantalla para escoger nuevo PIN