

## INTRODUCCIÓN

La Organización Médica Colegial y el Colegio desean ofrecer a los colegiados las máximas garantías de seguridad en su trabajo en internet. La firma electrónica nos proporciona los mecanismos ideales para conseguir este objetivo.

Con esta guía de uso ponemos al servicio de los colegiados todo el proceso de instalación y gestión de la tarjeta criptográfica del Colegio.

Además se encuentran los procedimientos de gestión que pueden utilizar los colegiados como usuarios del certificado electrónico.

## HERRAMIENTAS NECESARIAS

El colegiado necesita:

- Un **ordenador** con un sistema operativo MS Windows 2000, XP o Vista
- Conexión a **Internet** (se recomienda ADSL), a la que está conectado el ordenador.
- Un **lector** de tarjetas criptográficas conectado al ordenador
- El **software SafeSign** proporcionado por el Colegio y que encontrará en el apartado "Software" del CD.
- La **tarjeta** criptográfica, a nombre del colegiado, proporcionada por el Colegio.
- La **carta** que el colegiado ha recibido en su domicilio, en la que se incluyen los números PIN y PUK, necesarios para utilizar la tarjeta.

## SOFTWARE SAFESIGN

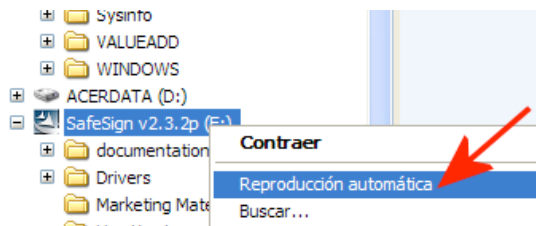
Esta aplicación permite la gestión de la tarjeta criptográfica de la OMC.

Además, consigue que el certificado electrónico incluido en la tarjeta sea reconocido por los diversos programas de Microsoft Windows.

### PASO 1:

---

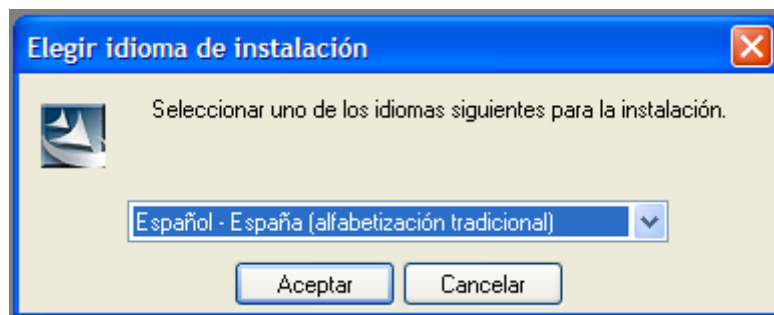
- Poner el CD (que viene con el pack de la OMC) en el ordenador donde tenemos el lector de tarjetas.
- El cd debe arrancar automáticamente, si no, iremos al explorador del windows y realizaremos la función manualmente.



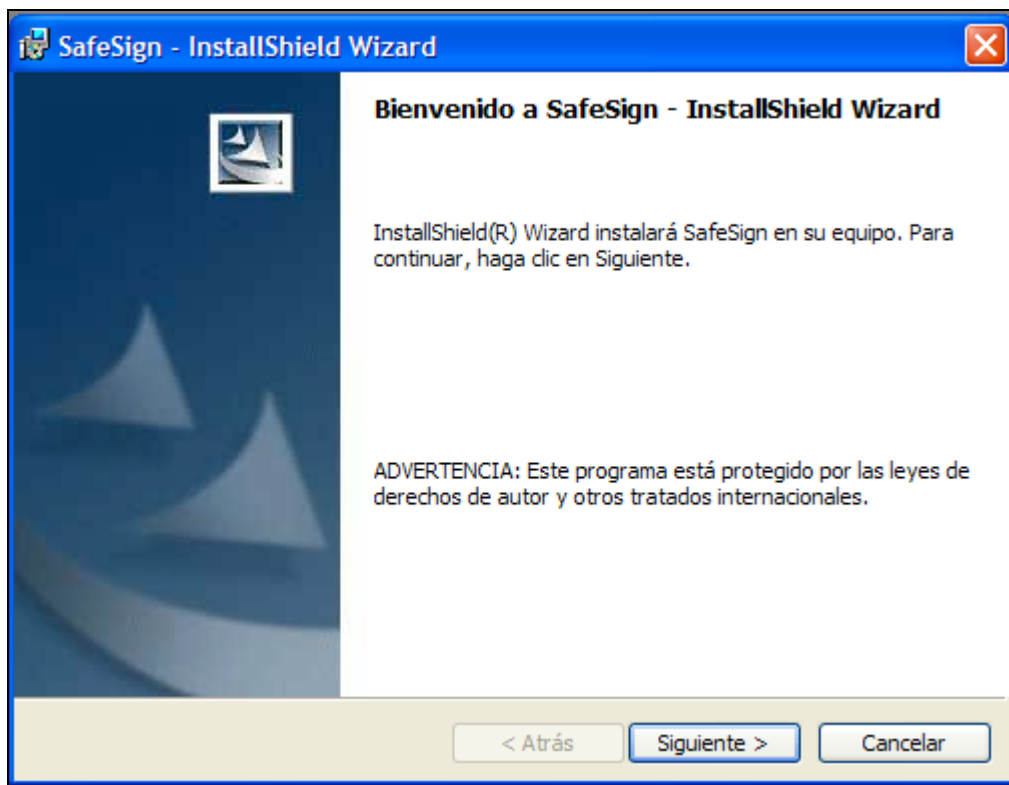
### PASO 2:

---

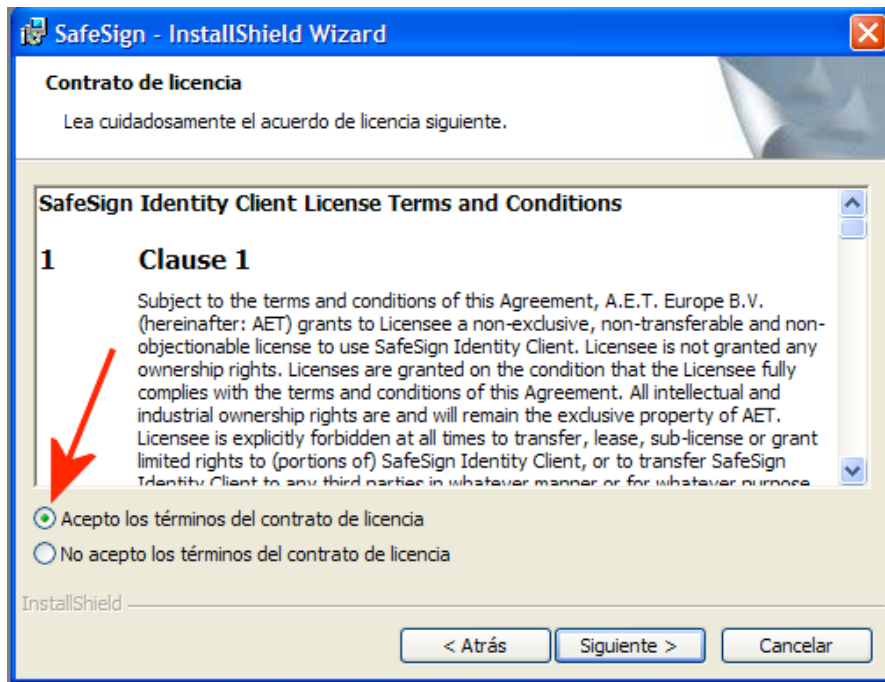
- Se instalará el programa safesign



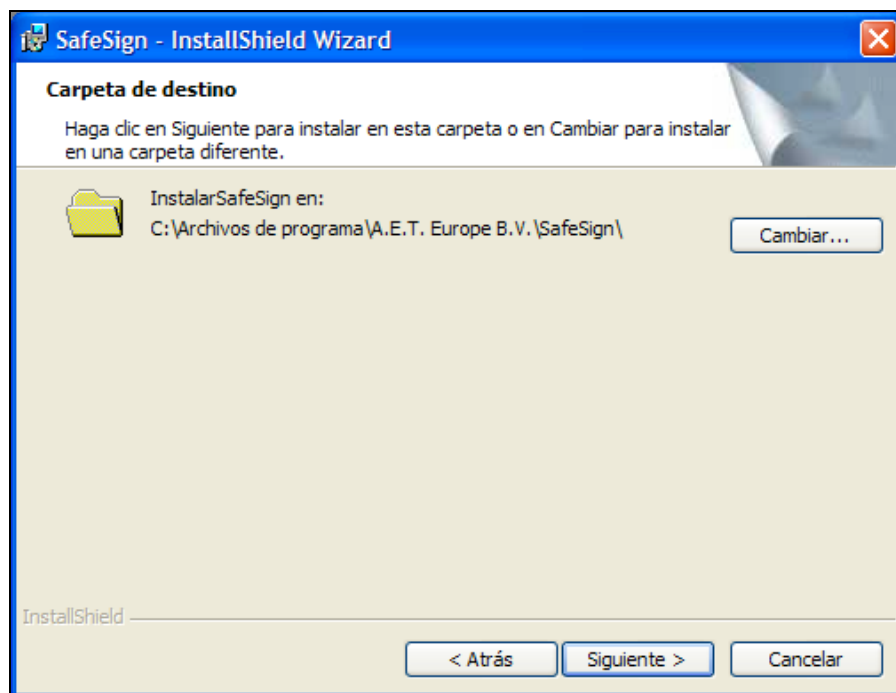
Podemos elegir el idioma deseado



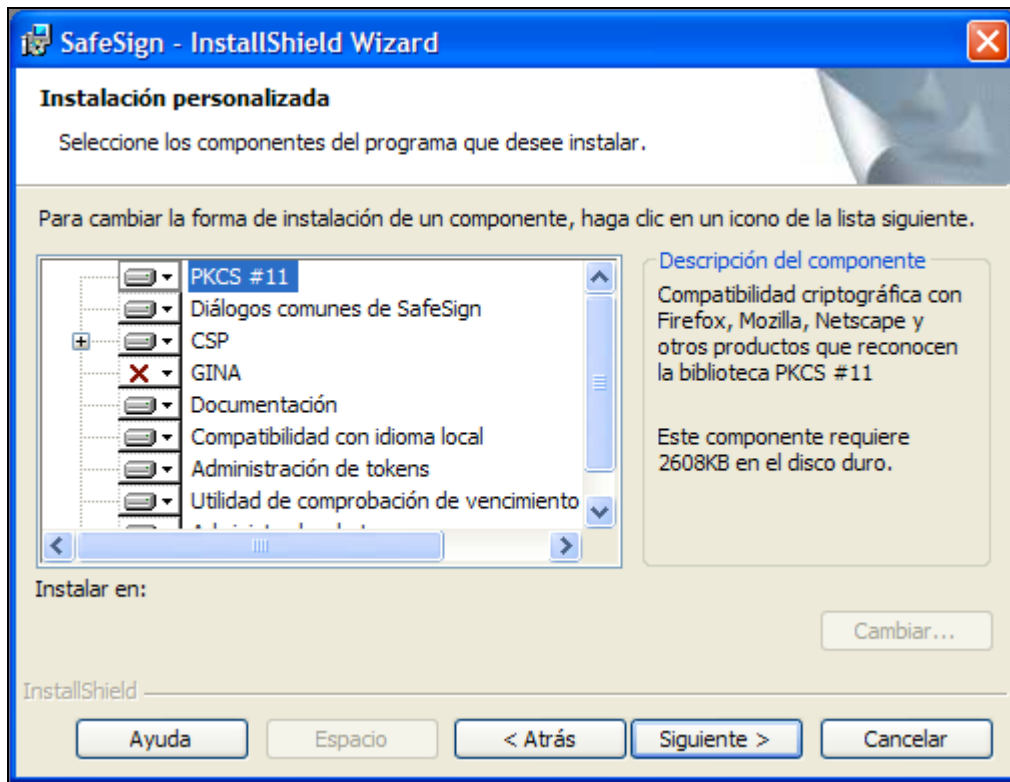
Debemos aceptar la licencia. [Tenemos que hacer un clic manualmente en "Acepto los términos del contrato de licencia"]



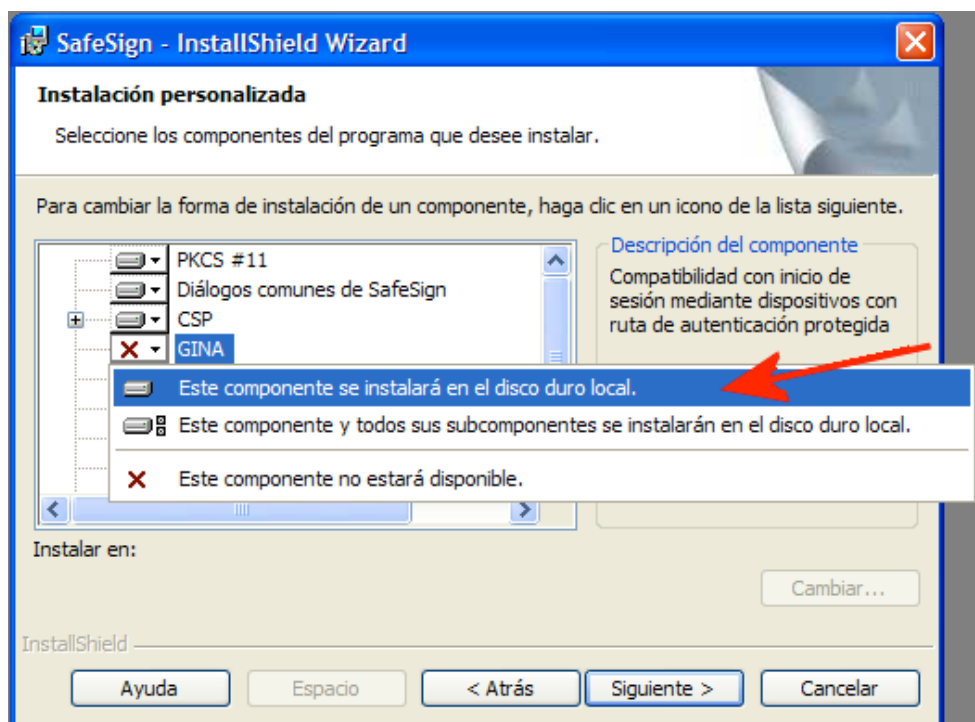
Si no hay ningún inconveniente, podemos aceptar la carpeta que nos propone el programa. [Hacer clic en "siguiete"]

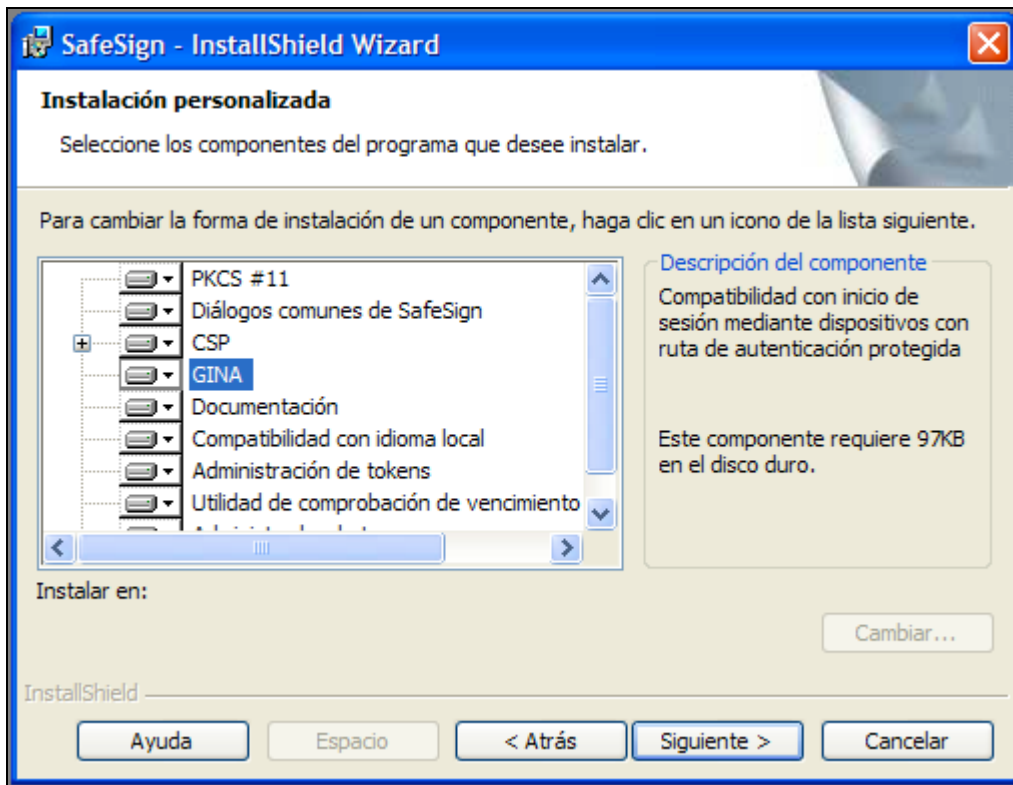


Personalizaremos la instalación

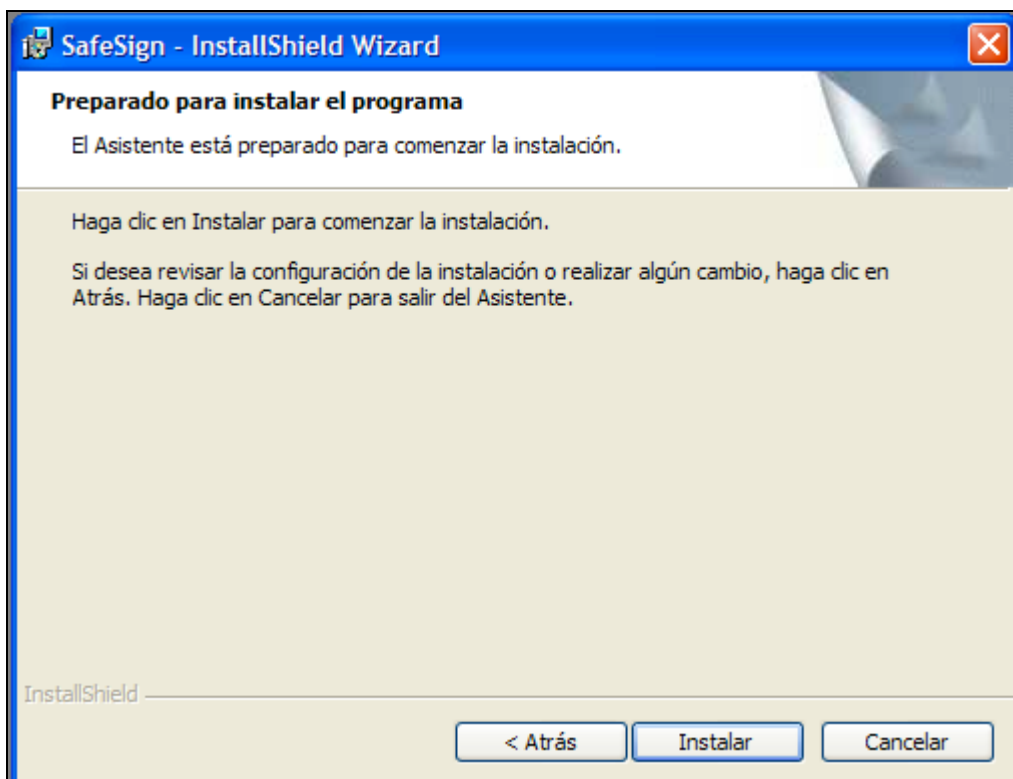


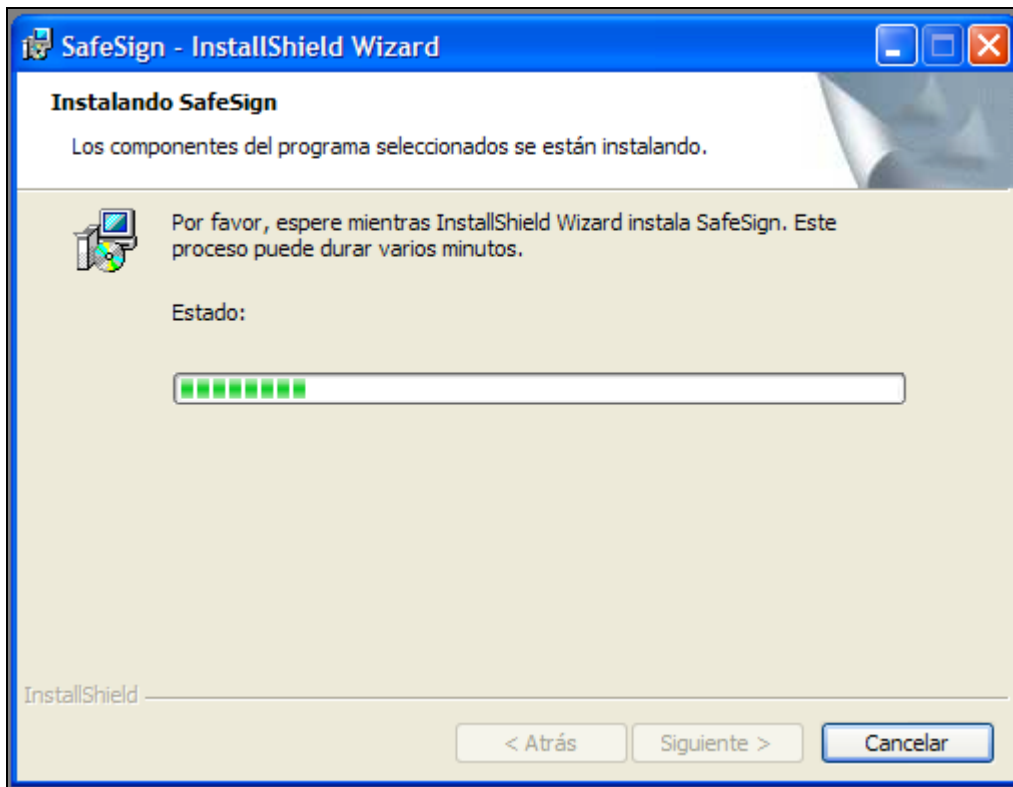
Tenemos que incluir el apartado GINA como muestra la imagen



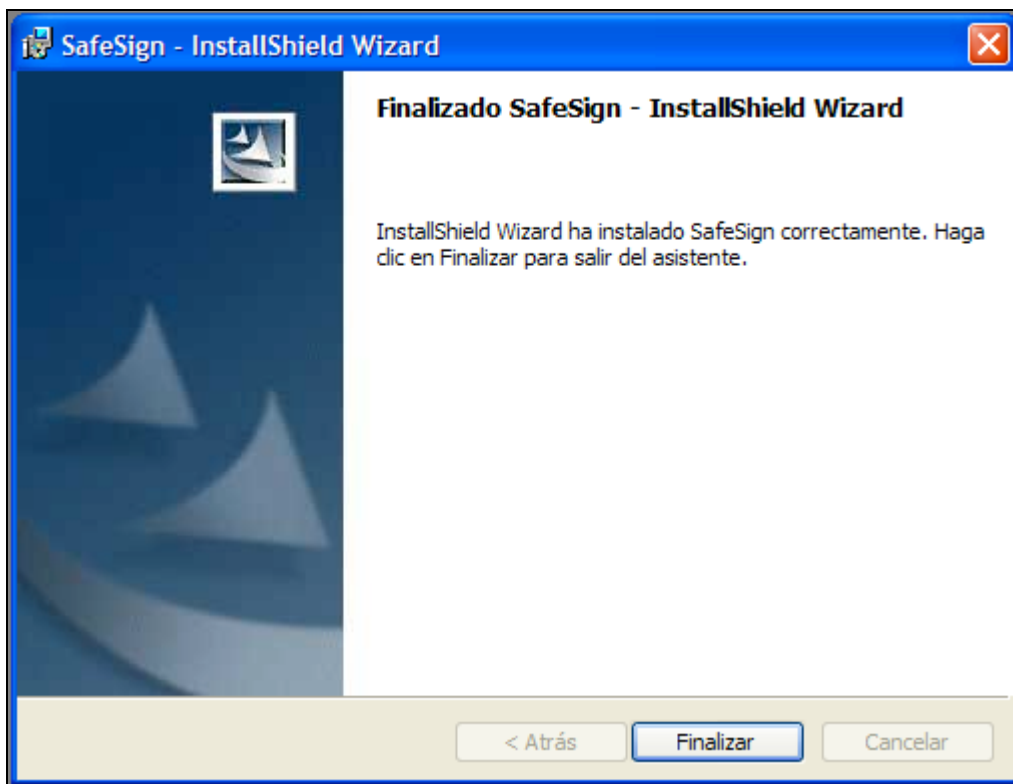


Hacemos clic en instalar





Se ha terminado la instalación general de la aplicación



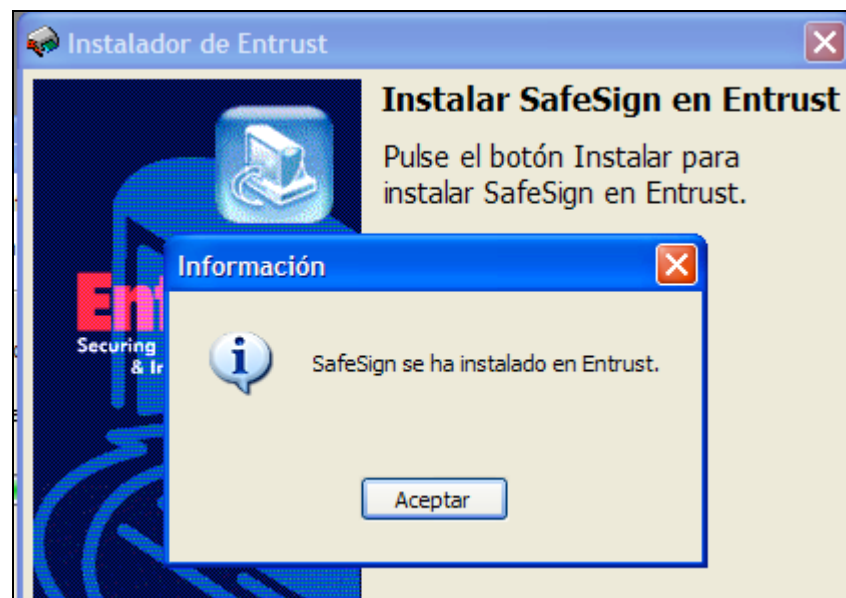
### PASO 3 (opcional) Entrust

---

Puede ser necesaria la instalación de la opción "entrust".



Hacemos un clic en "instalar".





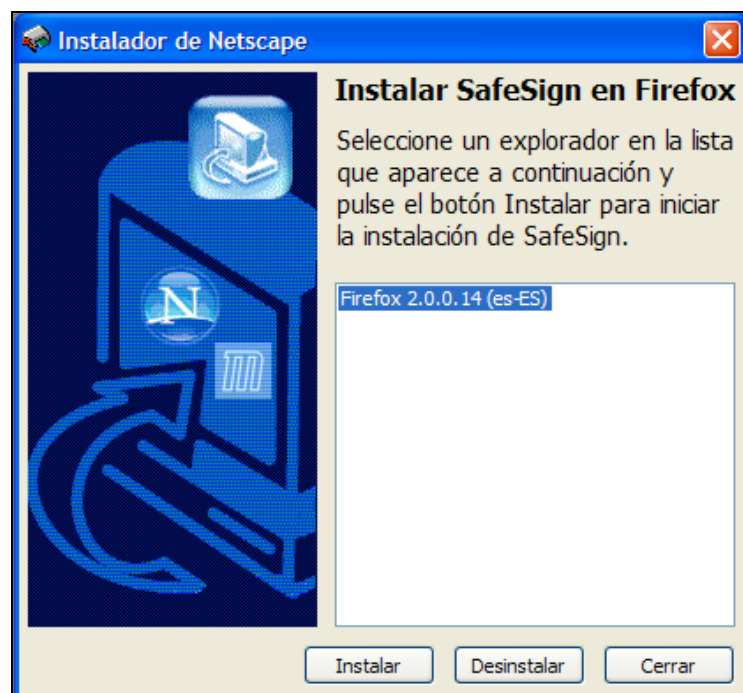
## PASO 4 (opcional) Firefox

---

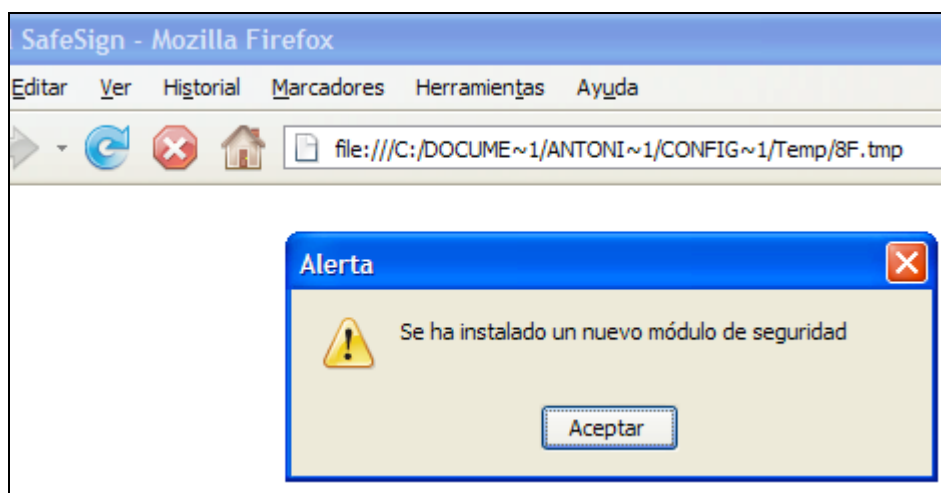
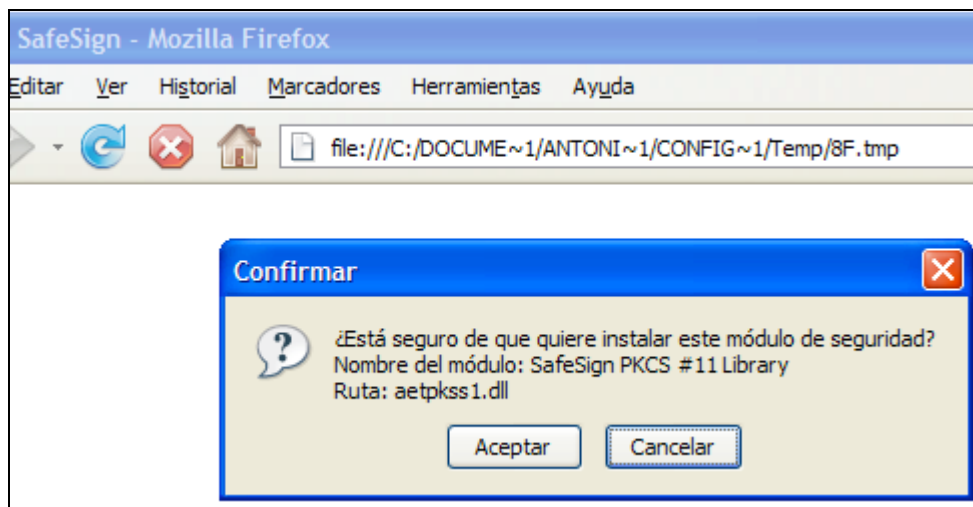
Puede ser necesaria la instalación de la opción para los programas de Mozilla (Firefox - Thunderbird)



Seleccionamos el programa y hacemos clic en "instalar".



La instalación abrirá nuestro navegador Firefox. Debemos aceptar cuando se nos pregunte.



Para terminar haremos un clic en "cerrar"



## PASO 5. VER MI CERTIFICADO

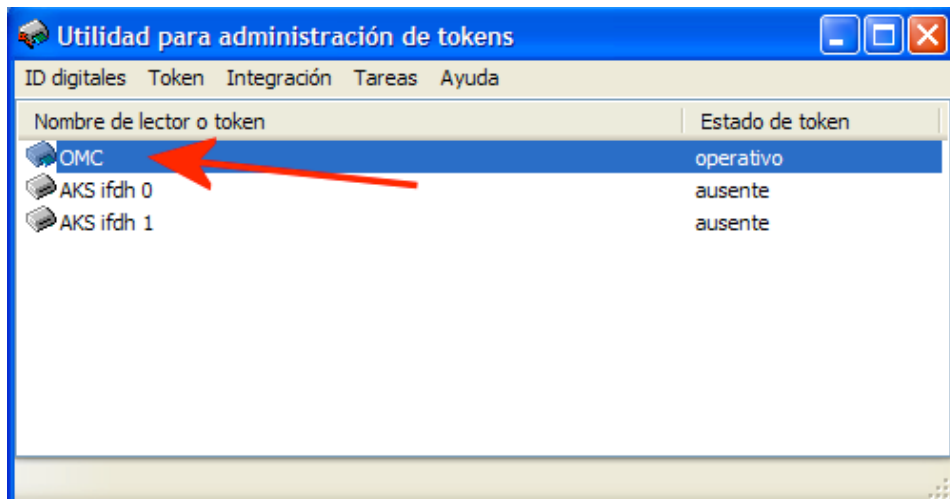
---

Para visualizar nuestro certificado vamos al "inicio" del windows y buscamos la carpeta "SafeSign Standard". Escogemos la opción "Administración de tokens".

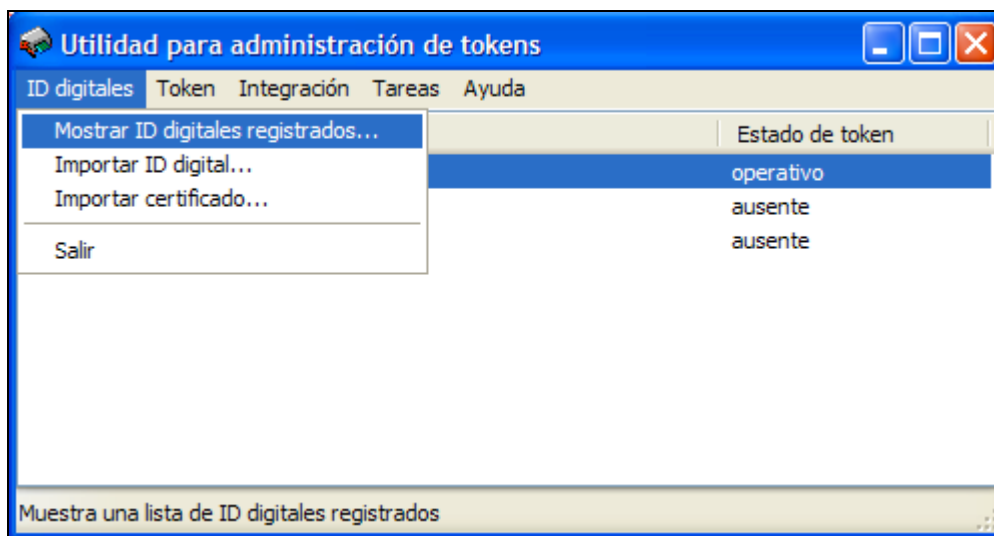
Ahora debe introducir la tarjeta en el lector



Observamos como ya nos aparece la tarjeta OMC en la aplicación.



Elegiremos la opción "Mostrar ID digitales registrados"



Observaremos qué certificados tenemos en nuestro ordenador.

## ID digitales



### ID digitales personales:

Emitido para	Emitido por	Fecha de vencimiento	Etiqueta	Etiqueta de token
Isacio Sigüero Zurdo	OMC	2011-05-05 02:00:00	Isacio Sigüero Z...	OMC
Isacio Sigüero Zurdo	OMC	2011-05-05 02:00:00	Isacio Sigüero Z...	OMC
Isacio Sigüero Zurdo	OMC	2011-05-05 02:00:00	Isacio Sigüero Z...	OMC
Isacio Sigüero Zurdo	OMC	2011-05-05 02:00:00	Isacio Sigüero Z...	OMC

### Detalles de ID digital

#### Contenido de certificado:

Campo	Valor

#### Ruta de certificado:

Emitido para	Emitido por	Fecha de vencimiento	Almacén de cer...

Transferir ID a token

Importar cadena de confianza

Eliminar ID digital

Ver certificado

Actualizar

Comprobar vencimiento

Cerrar

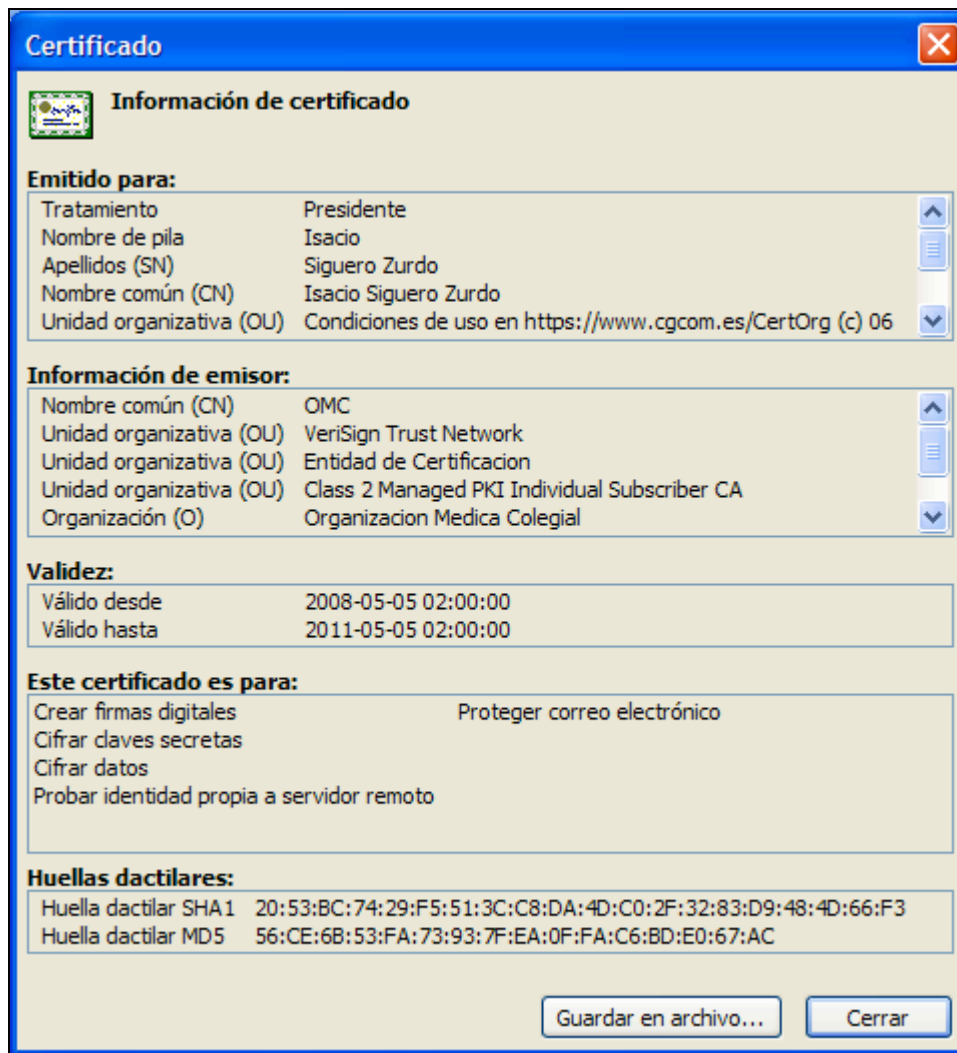
Si hacemos un clic en la opción "Comprobar vencimiento" la aplicación os indicará qué certificados están a punto de caducar.

The screenshot shows a software window titled "ID digitales". It contains a table of "ID digitales personales:" with columns for "Emitido para", "Emitido por", "Fecha de vencimiento", "Etiqueta", and "Etiqueta de token". One row is clearly visible for "Isacio Sigüero Zurdo" issued by "OMC" with a expiration date of "2011-05-05 02:00:00".

Below the table is a section "Detalles de ID digital" with a "Contenido de certificado:" field. A dialog box titled "Información" is overlaid on the interface, displaying an information icon and the text: "No caducará ningún ID digital en los próximos 30 días". An "Aceptar" button is located at the bottom of the dialog box.

Emitido para	Emitido por	Fecha de vencimiento	Etiqueta	Etiqueta de token
Isacio Sigüero Zurdo	OMC	2011-05-05 02:00:00	Isacio Sigüero Z...	OMC

Si hacemos un clic en la opción "ver certificado" la aplicación nos enseñará el contenido del certificado que hayamos señalado.



The screenshot shows a window titled "Certificado" with a close button in the top right corner. The window contains the following information:

**Información de certificado**

**Emitido para:**

Tratamiento	Presidente
Nombre de pila	Isacio
Apellidos (SN)	Siguero Zurdo
Nombre común (CN)	Isacio Sigüero Zurdo
Unidad organizativa (OU)	Condiciones de uso en <a href="https://www.cgcom.es/CertOrg">https://www.cgcom.es/CertOrg</a> (c) 06

**Información de emisor:**

Nombre común (CN)	OMC
Unidad organizativa (OU)	VeriSign Trust Network
Unidad organizativa (OU)	Entidad de Certificación
Unidad organizativa (OU)	Class 2 Managed PKI Individual Subscriber CA
Organización (O)	Organizacion Medica Colegial

**Validez:**

Válido desde	2008-05-05 02:00:00
Válido hasta	2011-05-05 02:00:00

**Este certificado es para:**

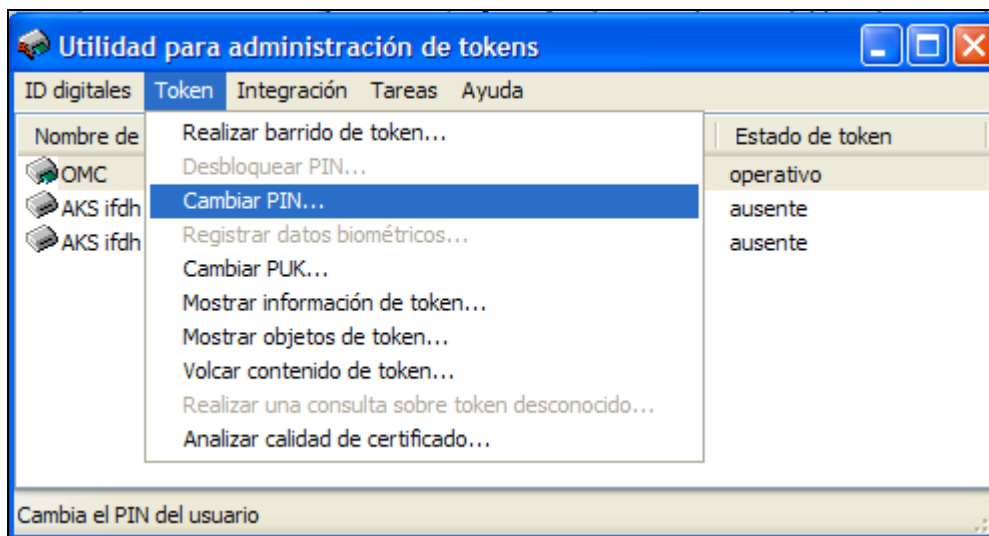
Crear firmas digitales	Proteger correo electrónico
Cifrar claves secretas	
Cifrar datos	
Probar identidad propia a servidor remoto	

**Huellas dactilares:**

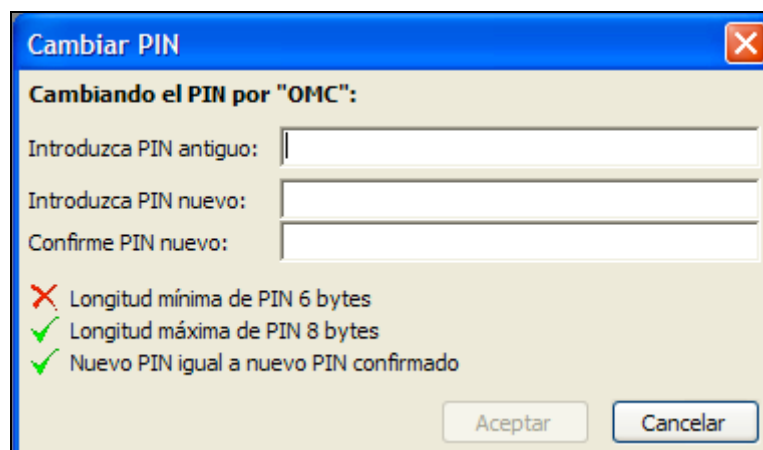
Huella dactilar SHA1	20:53:BC:74:29:F5:51:3C:C8:DA:4D:C0:2F:32:83:D9:48:4D:66:F3
Huella dactilar MD5	56:CE:6B:53:FA:73:93:7F:EA:0F:FA:C6:BD:E0:67:AC

At the bottom of the window, there are two buttons: "Guardar en archivo..." and "Cerrar".

La aplicación nos permite el cambio del número PIN



Sólo debemos incluir nuestro actual PIN y el que nosotros deseamos.



## REVOCACIÓN DEL CERTIFICADO

El procedimiento de revocación está definido en la Política de Certificación y en la Declaración de Prácticas de Certificación.



Un colegiado puede revocar su certificado cuando se produzca:

- a) Finalización de la relación jurídica de prestación de servicios entre la Entidad de Certificación de la OMC y el suscriptor.
- b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado.
- c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
- d) Infracción del colegiado de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
- e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
- f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y poseedor de claves.
- g) Solicitud del suscriptor de revocación del certificado.

## **LISTAS DE REVOCACIÓN**

Para depositar nuestra confianza en un certificado debemos consultar las listas de certificados que la Entidad de Certificación de la OMC ha revocado. Estas listas se pueden encontrar en las siguientes direcciones:

<http://crl1.cgcom.es/crl/ec-cgcom.crl>

<http://crl2.cgcom.es/crl/ec-cgcom.crl>

## **PÉRDIDA DE LA TARJETA CRIPTOGRÁFICA**

En caso de pérdida o sustracción, se debe comunicar urgentemente al Colegio.

## **CONSULTAS**

Para todas aquellas consultas que se deseen realizar sobre este servicio deben dirigirse al teléfono 902 365 121.