# Gestión de Certificado Digital

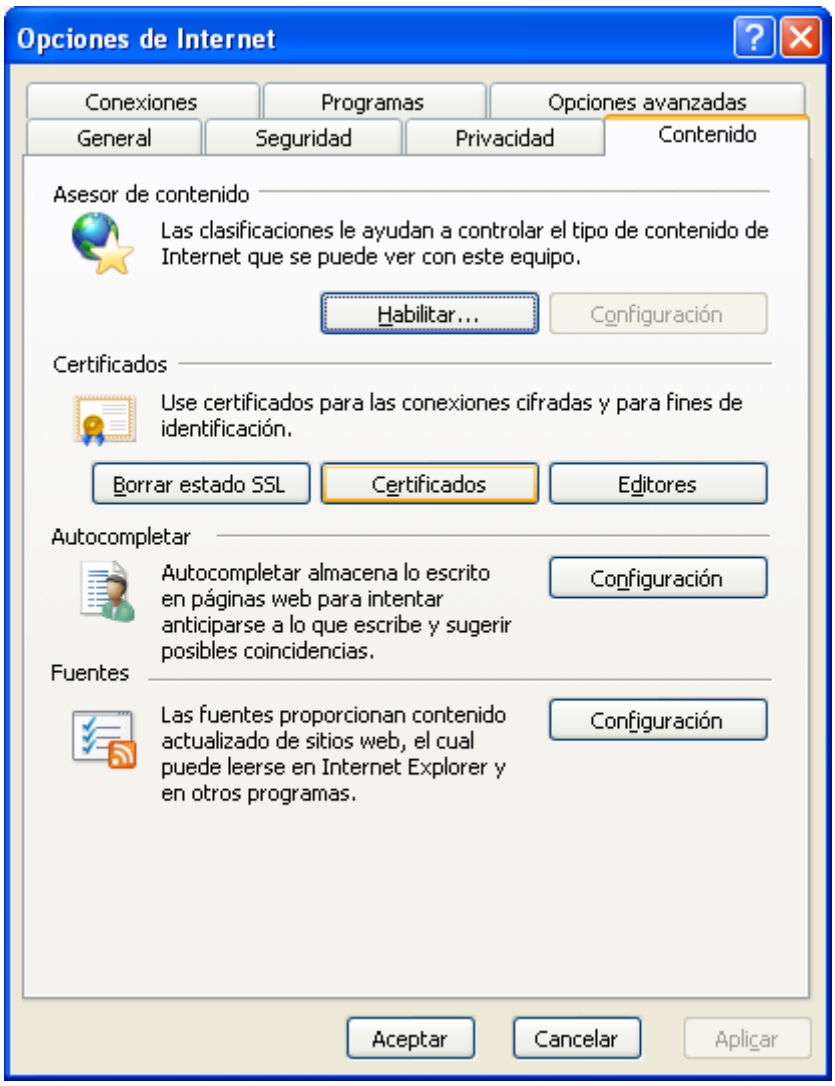
## Contenido

# Introducción

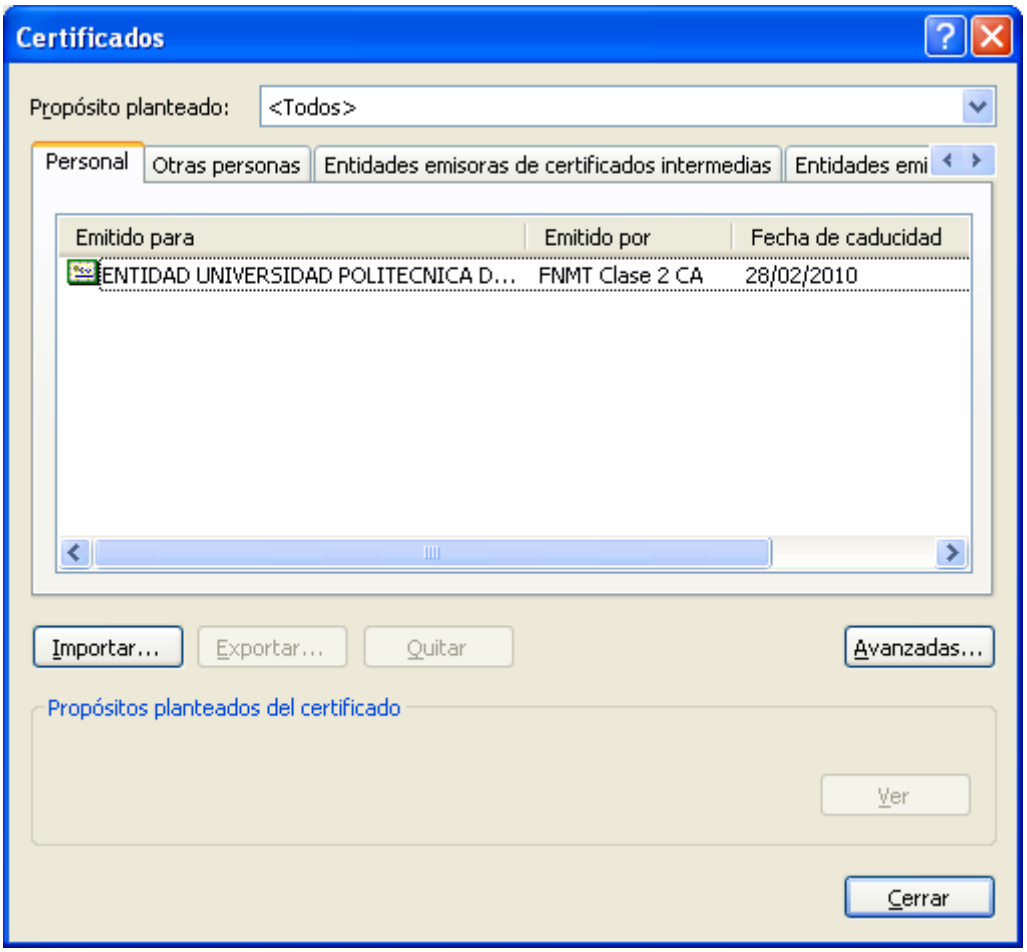
Los certificados digitales o certificados de usuarios son ficheros instalados en el Explorador que identifican de forma única y con efectos legales al usuario que lo utiliza, por tanto es necesario guardar las máximas medidas de seguridad en la instalación y almacenamiento de copias de seguridad. Este manual muestra cómo **Importar**, **Exportar**, **Quitar** y **Renovar** certificados.

* Para configurar el certificado digital en el cliente de correo electrónico ver documento **Correo Electrónico Seguro**

Para gestionar los certificados de usuario hay que dirigirse a las Opciones de Internet desde el Menú Herramientas del Explorador, y pinchar sobre el botón “Certificados”:



Aparecerán los certificados instalados en el equipo y mostrará a quién se ha emitido, autoridad certificadora y fecha de caducidad:




Podemos hacer desde esta ventana lo siguiente:

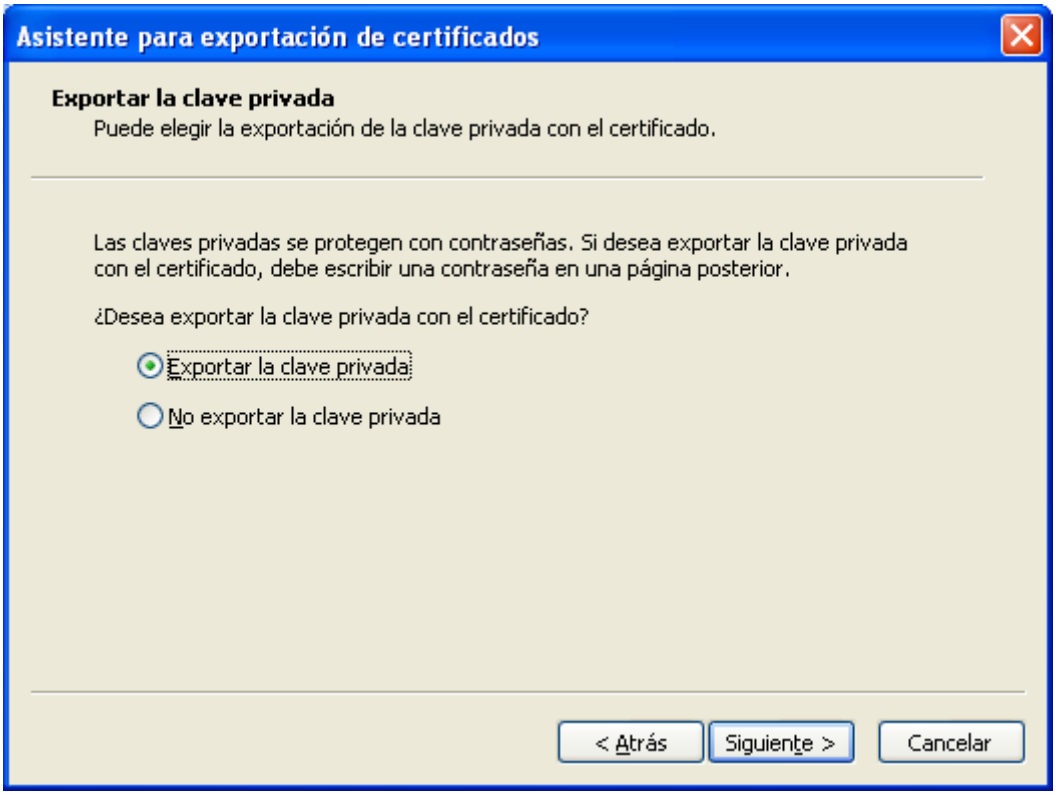
**Exportar certificado** (hacer copia de seguridad): debemos seleccionar el certificado en cuestión pinchando sobre él con el ratón y después pulsar sobre Exportar.

**Importar certificado** (Agregar certificado de otra persona o un certificado renovado): para ello debemos pulsar sobre el botón Importar para indicar al sistema dónde debe buscarlo.

**Quitar certificado** (si ha caducado): seleccionamos el certificado que deseemos eliminar porque ha caducado o porque ya no debe estar operativo en esta máquina y pulsamos en el botón Quitar.

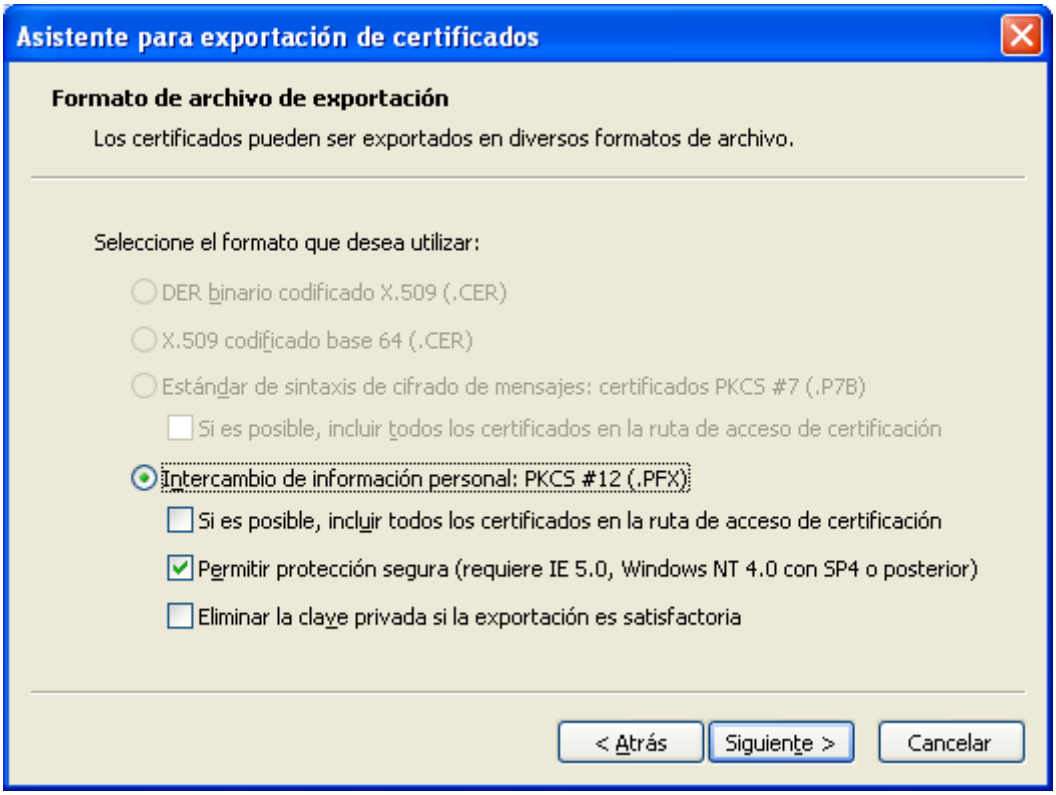
## Exportar certificado

Al seleccionar la opción Exportar, se ejecuta el Asistente para exportación de certificados, en la primera pantalla debemos indicarle si exportamos la clave privada. Si lo que queremos es que el certificado funcione en otro equipo debemos seleccionar "Exportar la clave privada".



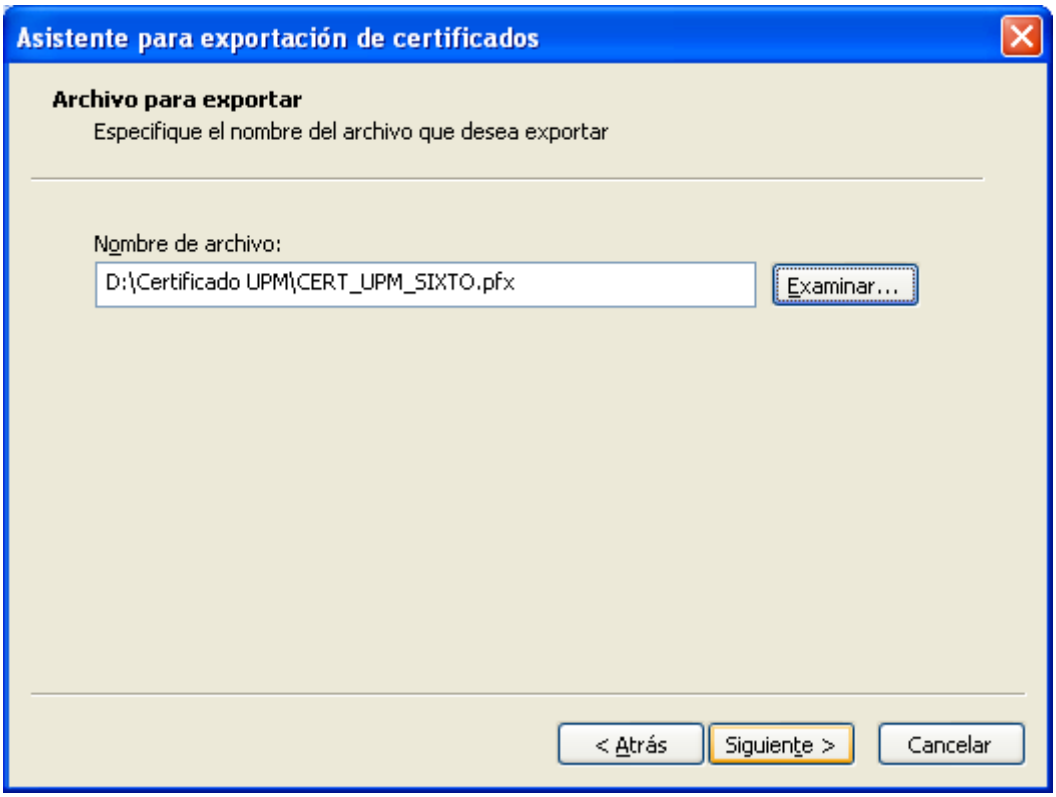

* La opción "Exportar la clave privada" implica que el fichero generado contiene lo necesario para que el certificado se instale y funcione en cualquier equipo, por tanto hay que tener cautela en estos dos aspectos:

- Debemos tener **control sobre el fichero** generado, para lo cual se recomienda guardar un solo fichero con clave privada en un lugar seguro.
- **La contraseña de exportación** es necesaria para instalar de nuevo el certificado, por lo que se recomienda tomar las medidas de seguridad necesarias para recordar la contraseña y controlar el uso no autorizado.



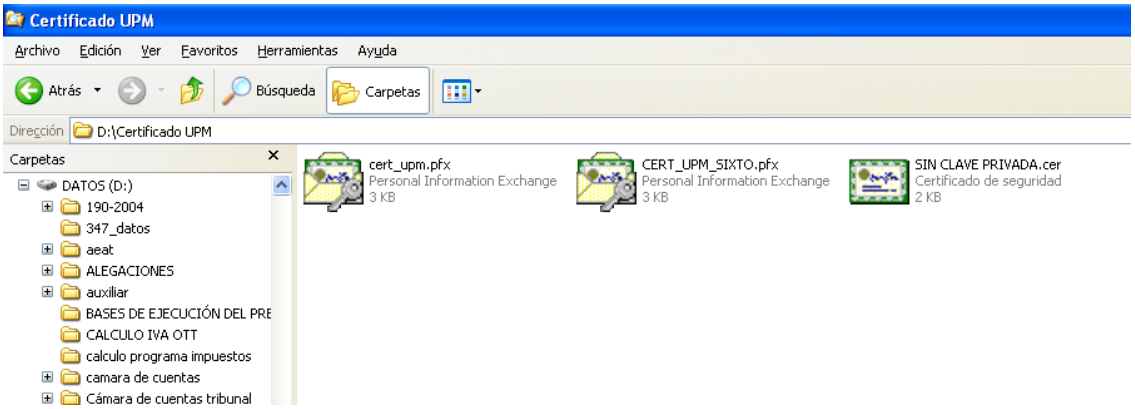

Dejaremos las opciones por defecto del Formato de archivo de exportación (.PFX con protección segura), y seguidamente deberemos introducir una contraseña. Esta contraseña protege la instalación no autorizada del certificado.


El Asistente confirmará la ubicación donde guardará el certificado, con extensión .PFX



Los archivos .pfx contienen la clave privada que permite utilizar el certificado en otro equipo y piden la contraseña que se utilizó para la exportación, para evitar la instalación no autorizada.

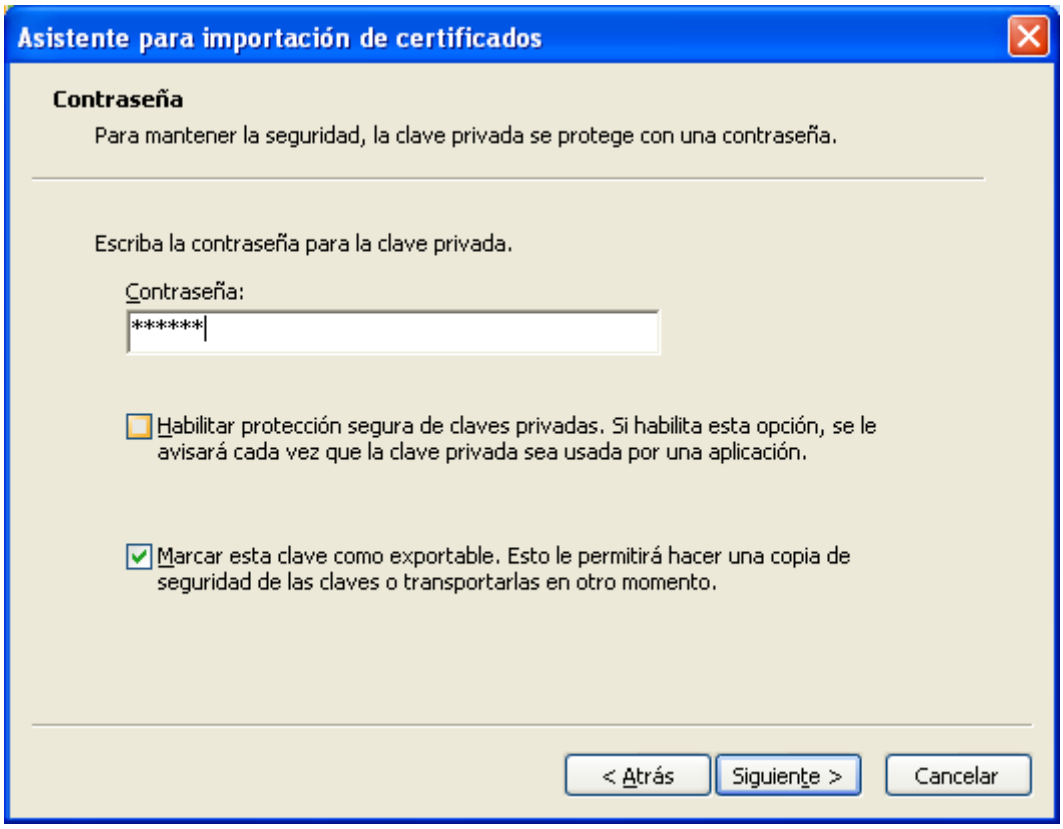
Los archivos .cer no contienen la clave privada y sólo valen como copia de seguridad en el equipo que previamente se le ha instalado el certificado.




## Importar certificado

Si seleccionamos la opción Importar se ejecutará el Asistente para importación de certificados, donde deberemos indicar la ubicación del archivo .PFX

Si el certificado que queremos importar tiene la clave privada nos pedirá la contraseña que se utilizó en la exportación, para impedir la instalación no autorizada del certificado.




Si queremos tener la posibilidad de generar el archivo de instalación del certificado desde el equipo donde se está instalando seleccionaremos “Marcar esta clave como exportable”. Si tenemos un archivo .PFX con clave privada y contraseña de exportación no es necesario marcar esta opción, aunque debemos tener presente que desde el equipo no se podrá generar el archivo de instalación del certificado.

La opción “Habilitar protección segura…” hace que el sistema muestre un mensaje adicional cada vez que usamos el certificado.

# Renovar el Certificado

La renovación de los certificados digitales se puede llevar a cabo desde dos meses antes de la fecha de caducidad. Por tanto es necesario comprobar primero que estamos en dicho periodo. El trámite se realiza de forma On-line mediante el certificado próximo a caducar y a través de la web http://www.cert.fnmt.es

* La Renovación del certificado de usuario requiere de la instalación de un componente así como de la configuración avanzada de las opciones del explorador, por lo que es necesario que el proceso relatado a continuación sea llevado a cabo por personal técnico informático.

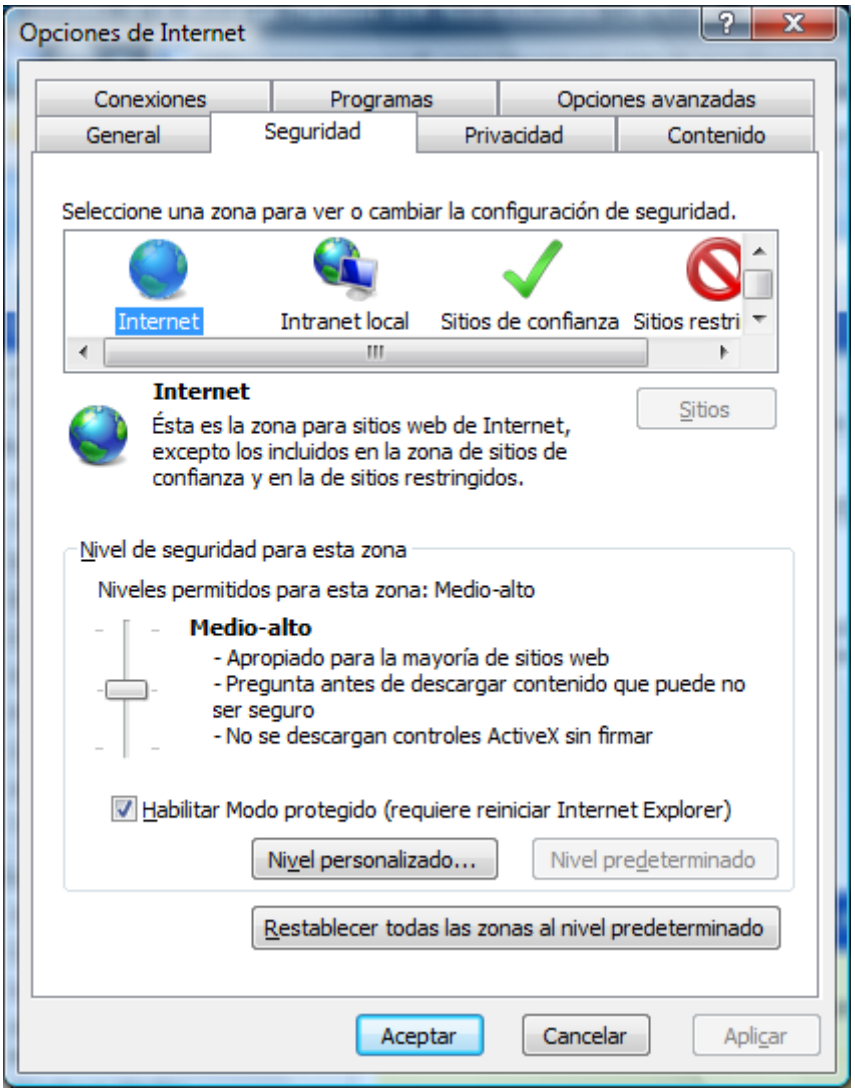
Durante la renovación se solicita la instalación de componentes ActiveX CAPICOM. CAPICOM es un componente de Microsoft que se utiliza para firmar datos y código digitalmente, comprobar firmas digitales, proteger la privacidad de datos, hacer hash de datos y cifrar y descifrar datos, entre otras aplicaciones.

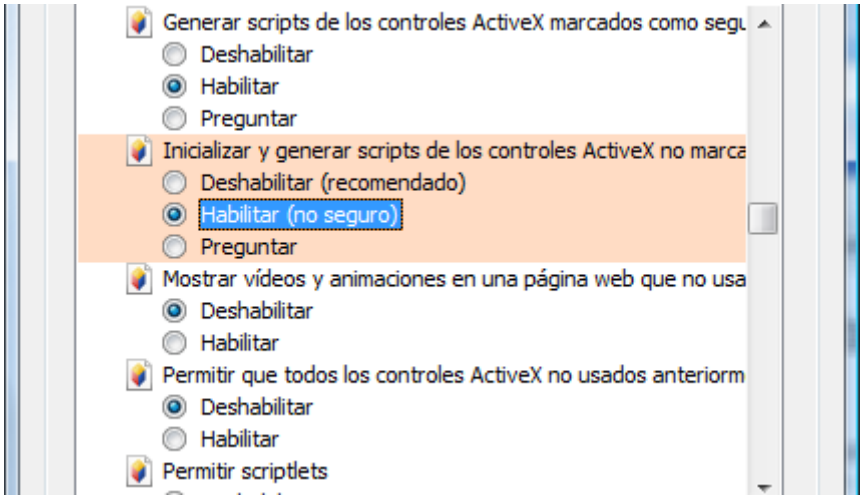
Es necesario por tanto **instalar previamente** los archivos redistribuibles de CAPICOM 2.1.0.1 Este enlace los descarga desde la Página Oficial de Microsoft (requiere permisos administrativos):

http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=860ee43a-a843-462f-abb5-ff88ea5896f6


Una vez instalado el Componente CAPICOM podemos proceder a la renovación desde el perfil del usuario, para ello es necesario **habilitar la Opción Avanzada** del IE: "Inicializar y generar scripts de los controles de ActiveX no marcados como seguros para scripts". Esta opción hay que cambiarla en la Zona de Internet de la pestaña Seguridad, no vale con meter la pagina www.cert.fnmt.es en Sitios de Confianza. Estos cambios generan problemas de seguridad y es recomendable hacerlo por los técnicos informáticos. Una vez realizada la solicitud de renovación se debe devolver la configuración de seguridad al estado original.

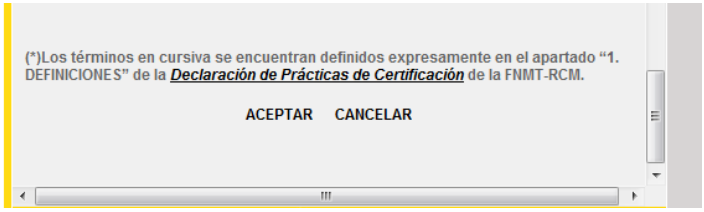
Para ello pulsamos en el botón “Nivel personalizado” de la Zona Internet y seleccionamos



Una vez instalado los componentes CAPICOM y configurado el Explorer podemos acceder a renovar el certificado desde http://www.cert.fnmt.es.


Para renovar el certificado pincharemos sobre "1.-Solicitar la renovación" y habrá que aceptar la "Declaración de prácticas de certificación"




Al pulsar Aceptar deberemos seleccionar el certificado y seguir los pasos. Podemos modificar los datos del usuario si no son correctos. Durante el proceso habrá que realizar las acciones de "Firmar" y "Enviar" que es lo que requiere la instalación de los componentes CAPICOM y la configuración avanzada del explorador.

Se generará un número con el que se podrá descargar el certificado pasados unos minutos del mismo modo que si fuese uno nuevo.