



## Conexión WiFi con certificado de la FNMT en Windows

Red Corporativa de la Xunta de Galicia

CONTROL DE VERSIONES Y DISTRIBUCIÓN			
<b>NOMBRE DEL DOCUMENTO:</b>	Conexión Wifi con certificado de la FNMT en Windows	<b>VERSIÓN:</b>	01.00
<b>COD. DEL DOCUMENTO:</b>			
<b>ELABORADO POR:</b>	Centro de Xestión de Rede	<b>Fecha:</b>	27/02/2024
<b>VALIDADO POR:</b>		<b>Fecha:</b>	
<b>APROBADO POR:</b>		<b>Fecha:</b>	

REGISTRO DE CAMBIOS		
Versión	Causa de la nueva versión	Fecha de aprobación

LISTA DE DISTRIBUCIÓN (opcional)		
Nombre	Número de copia	Área/Centro/Localización

#### CLÁUSULA DE CONFIDENCIALIDAD

Este documento es propiedad de la AMTEGA (Agencia para la Modernización Tecnológica de Galicia). Deberá utilizar dicho material exclusivamente para los servicios que fueron acordados con la AMTEGA y que requieren necesariamente de su utilización. Dicho compromiso incluye la prohibición de la reproducción parcial o total del material mencionado, por cualquier medio o método.

## Índice

1. INTRODUCCIÓN.....	4
2. INSTALACIÓN DEL CERTIFICADO.....	5
2.1. WINDOWS.....	5
3. CONEXIÓN A LA RED.....	12
3.1. WINDOWS.....	12
4. CONDICIONES DE USO:.....	17
Medidas de seguridade de obrigado cumprimento	
Monitorización	
Protección de Datos	

## 1. INTRODUCCIÓN

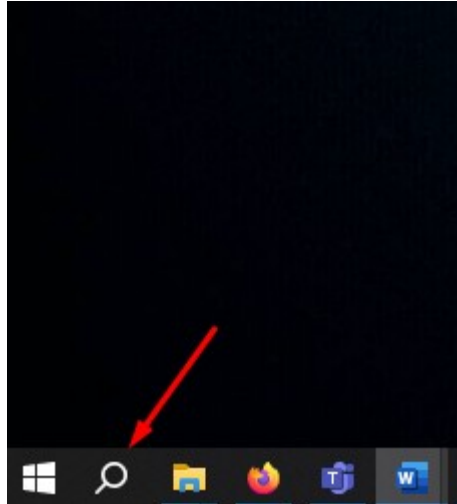
El objetivo del presente documento es describir los pasos para realizar la conexión a la red WiFi, utilizando un certificado digital emitido por la Fábrica Nacional de Moneda y Timbre (FNMT).

## 2. INSTALACIÓN DEL CERTIFICADO

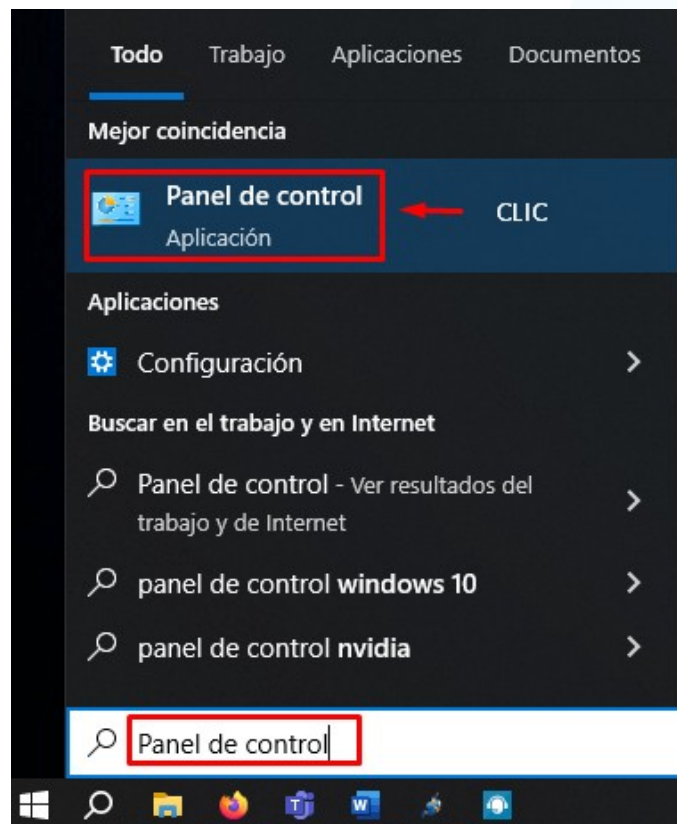
### 2.1. WINDOWS

En los sistemas con Windows 10 / 11 procedemos de la siguiente manera:

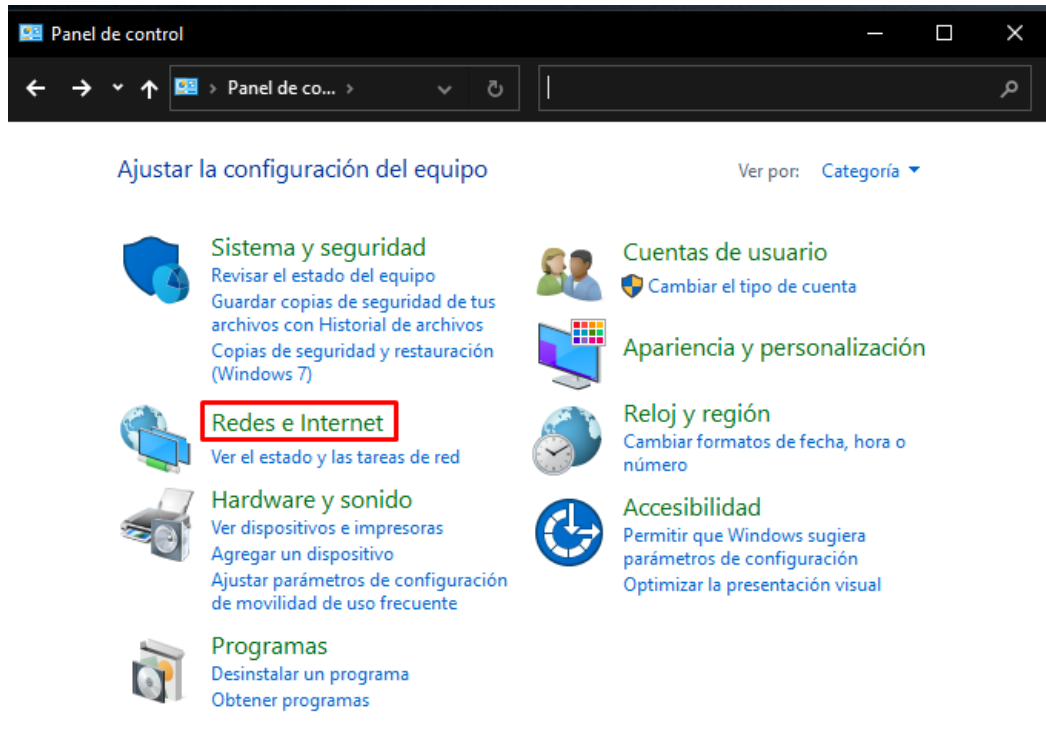
Desde el Escritorio, nos dirigimos a la zona inferior izquierda y hacemos clic sobre el botón de Buscar.



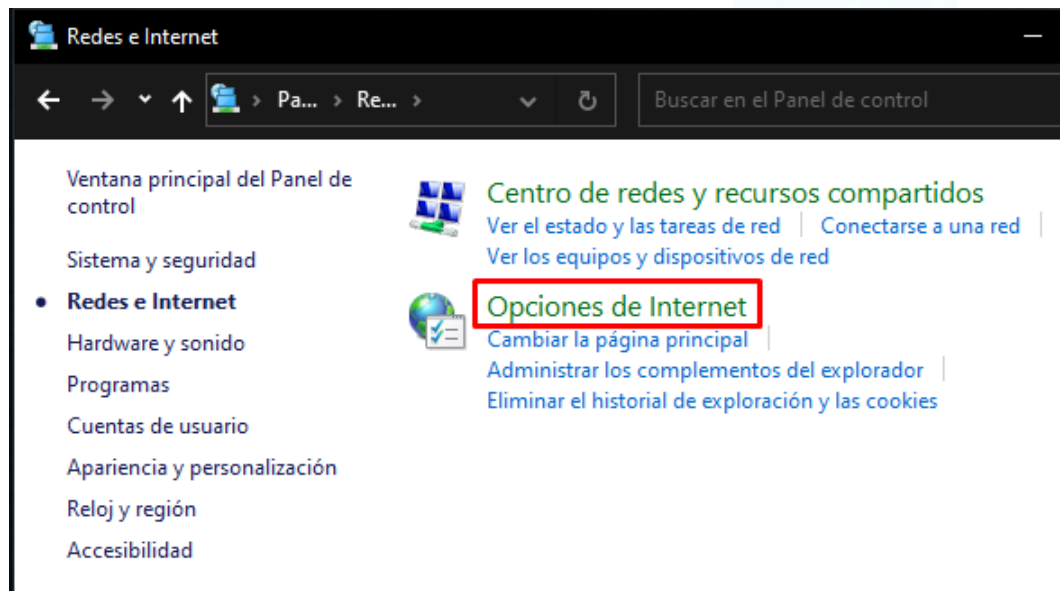
A continuación, tecleamos Panel de control y hacemos clic en el primer resultado.



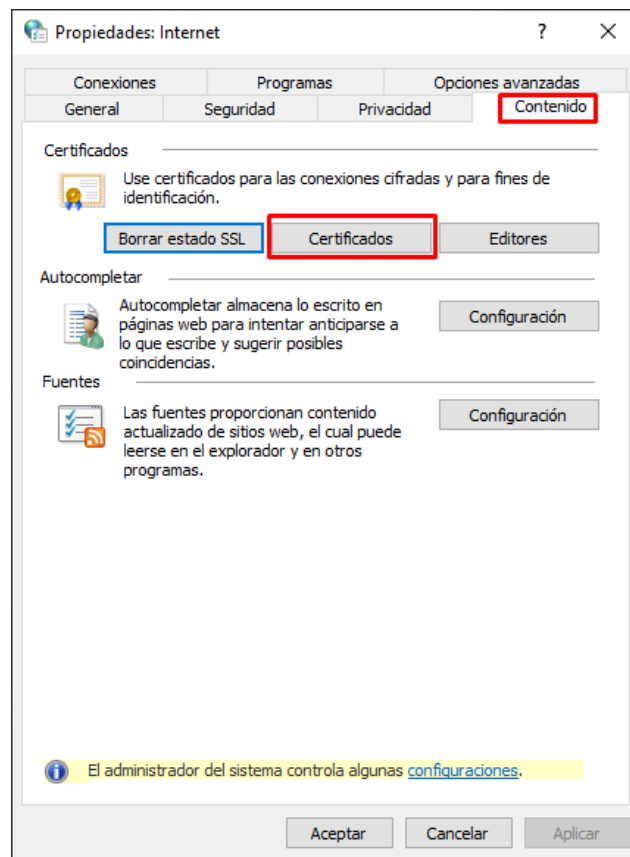
Dentro del Panel de Control, nos dirigimos a *Redes e Internet*:



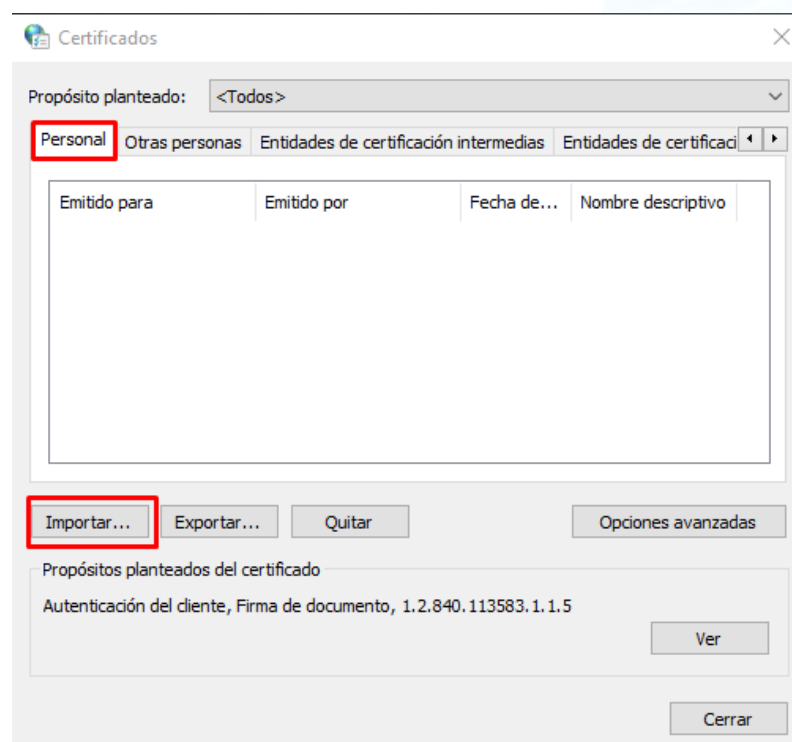
En la siguiente pantalla elegimos el enlace *Opciones de Internet*:



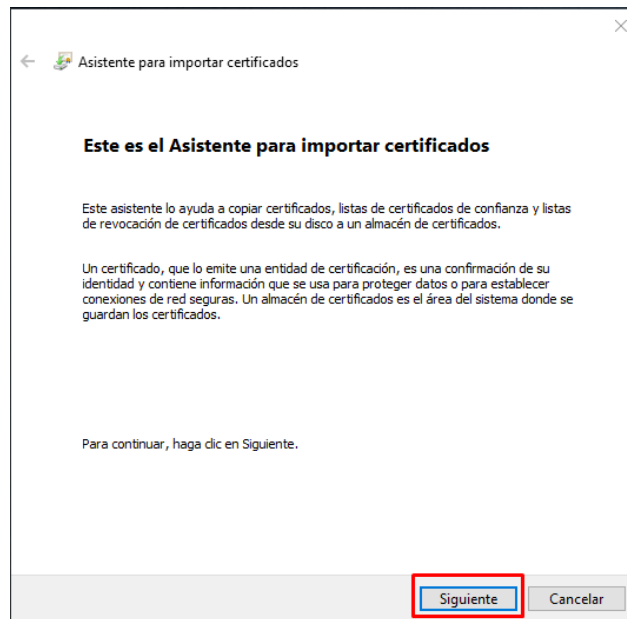
En la siguiente pantalla, nos dirigimos a la pestaña de *Contenido* y hacemos clic en *Certificados*:



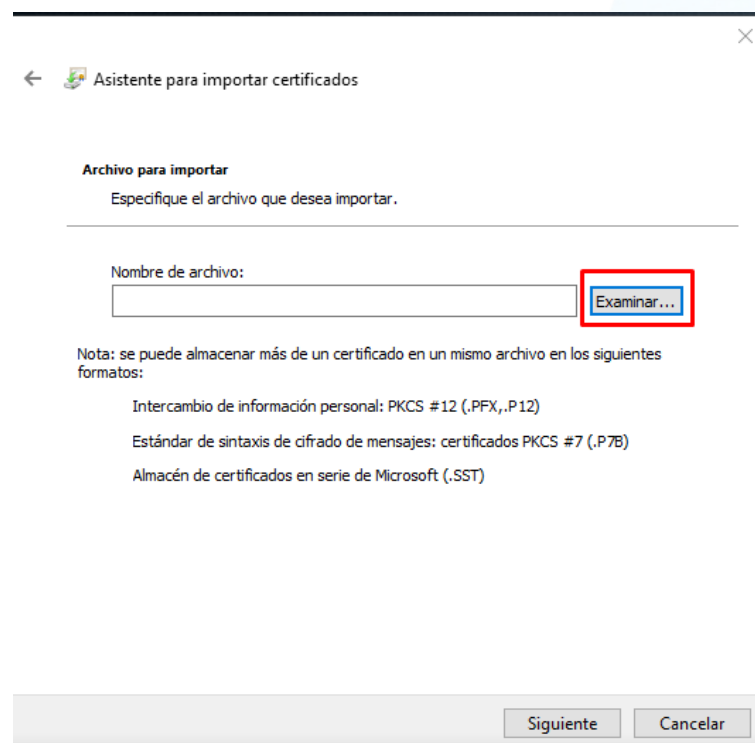
A continuación en la pestaña *Personal* hacemos clic en el botón *Importar*:



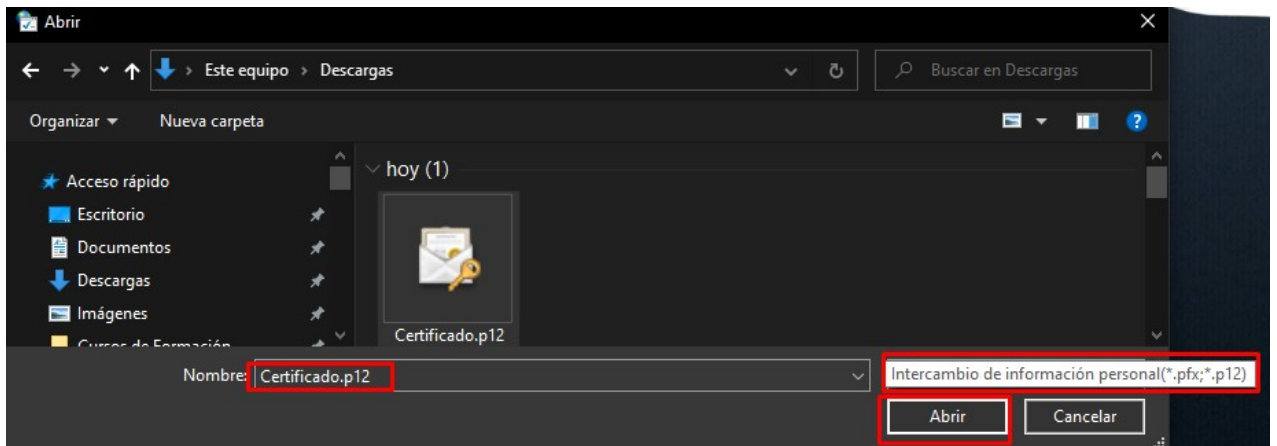
Nos aparece un asistente y avanzamos en *Siguiente*:



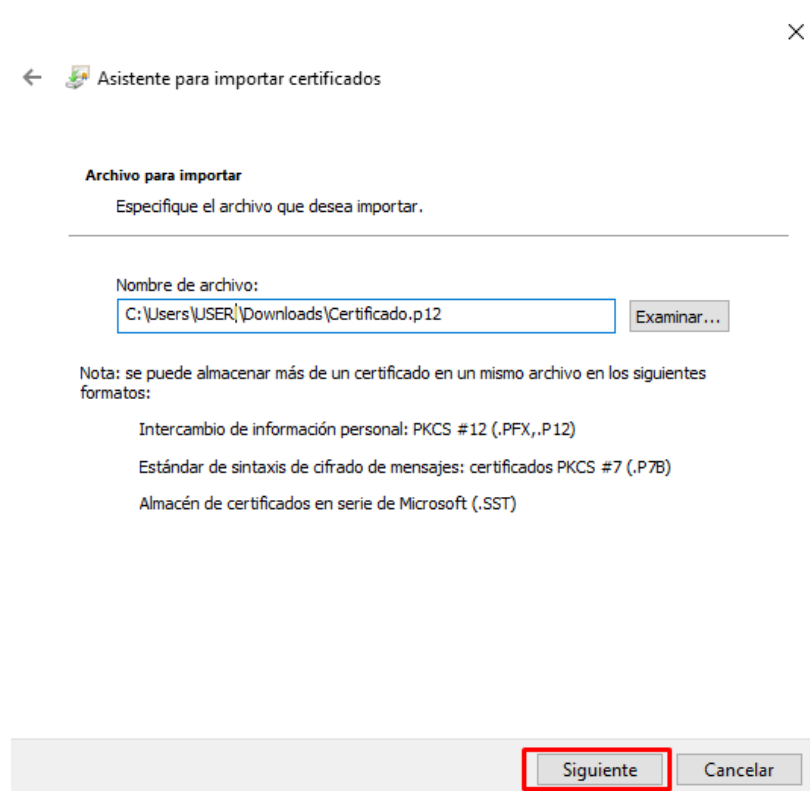
A continuación, clic sobre el botón *Examinar* y buscamos el certificado en la ruta de nuestro disco duro. Una vez localizado, seleccionamos *Abrir*:



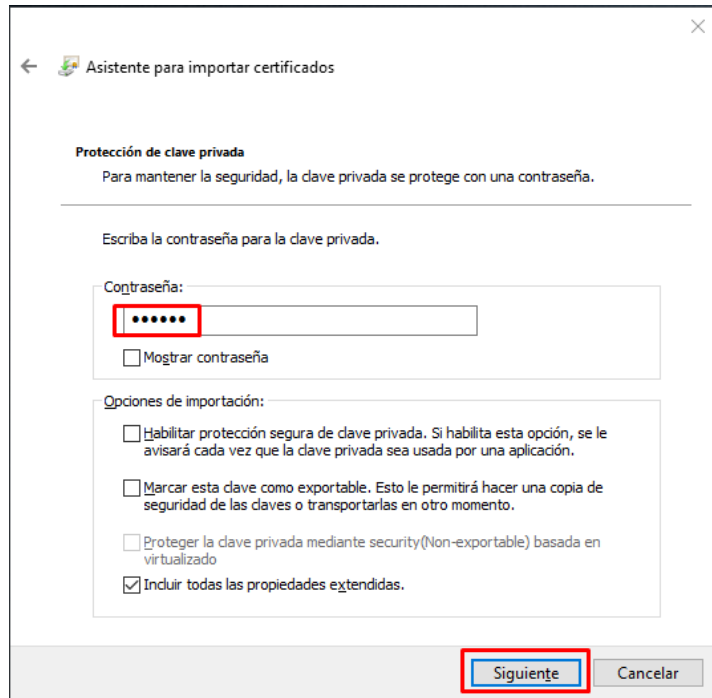




Avanzamos en *Siguiente*:



En el caso de estar protegido el certificado mediante contraseña, escribimos la contraseña y avanzamos en *Siguiente*:



← Asistente para importar certificados

**Protección de clave privada**  
Para mantener la seguridad, la clave privada se protege con una contraseña.

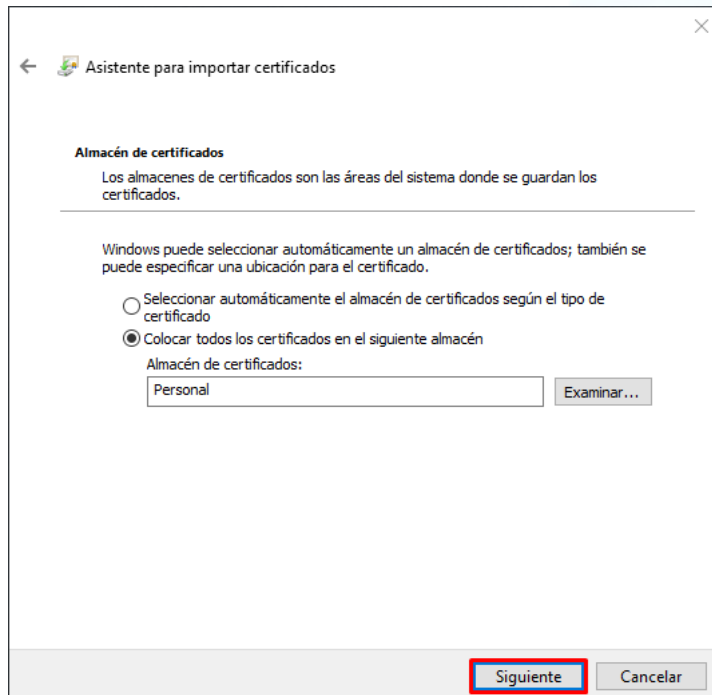
Escriba la contraseña para la clave privada.

Contraseña:  
.....  
 Mostrar contraseña

Opciones de importación:

- Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.
- Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.
- Proteger la clave privada mediante security(Non-exportable) basada en virtualizado
- Incluir todas las propiedades extendidas.

En la siguiente pantalla dejamos las opciones por defecto y seguimos avanzando en *Siguiente*:



← Asistente para importar certificados

**Almacén de certificados**  
Los almacenes de certificados son las áreas del sistema donde se guardan los certificados.

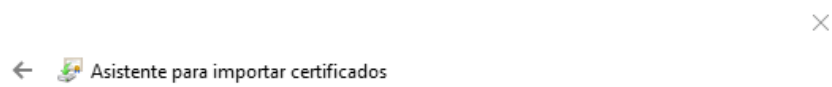
Windows puede seleccionar automáticamente un almacén de certificados; también se puede especificar una ubicación para el certificado.

Seleccionar automáticamente el almacén de certificados según el tipo de certificado

Colocar todos los certificados en el siguiente almacén

Almacén de certificados:  
Personal

Finalizamos la importación del certificado.

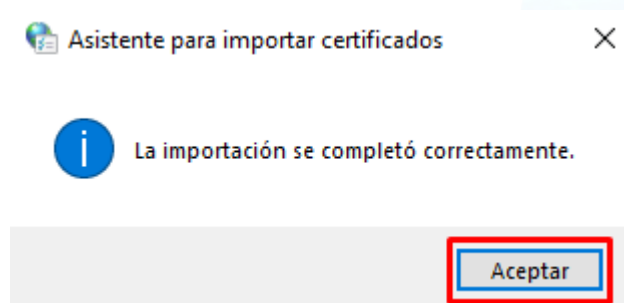
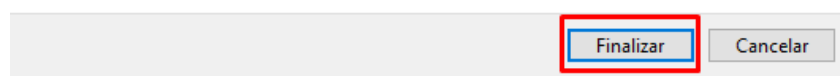


### Finalización del Asistente para importar certificados

Se importará el certificado después de hacer clic en Finalizar.

Especifíco la siguiente configuración:

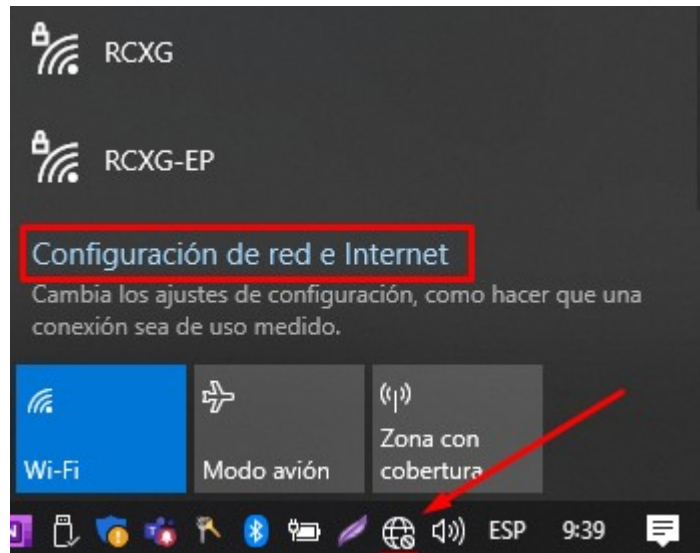
Almacén de certificados seleccionado por el usuario	Personal
Contenido	PFX
Nombre de archivo	C:\Users\... \Downloads\Certif



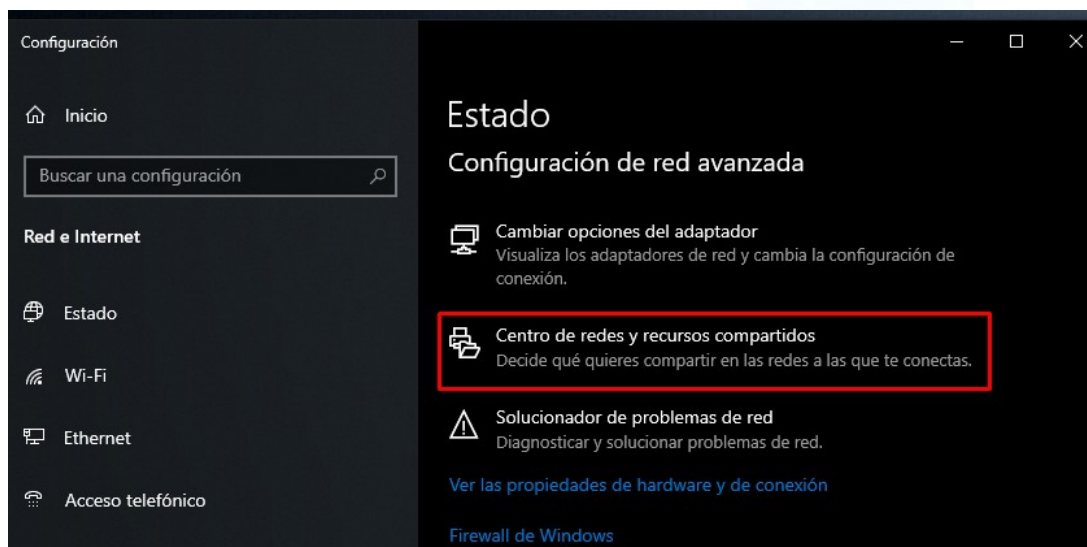
## 3. CONEXIÓN Á REDE

### 3.1. Windows

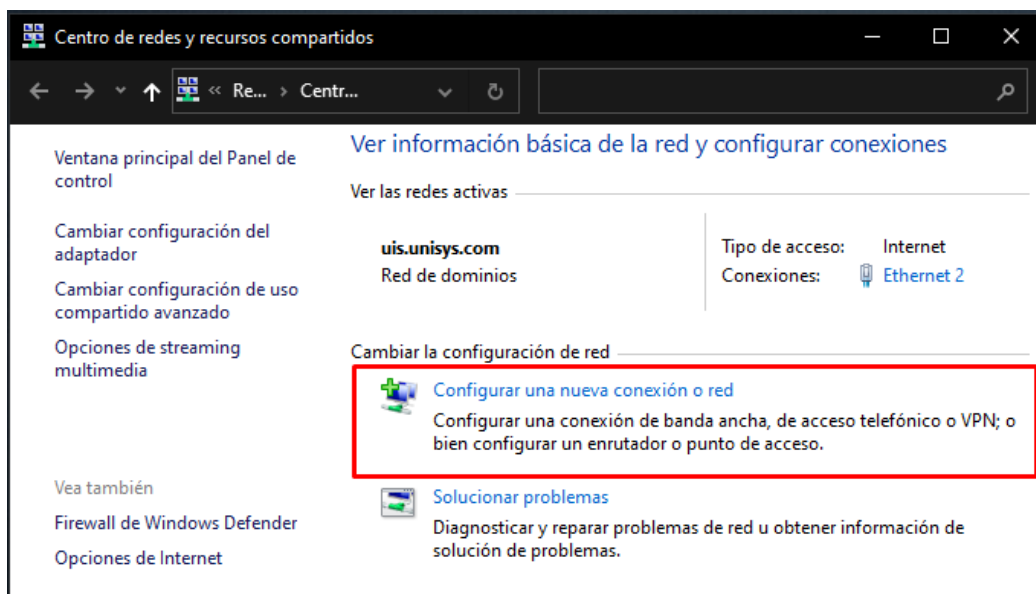
En los sistemas con Windows 10/11 procedemos de la siguiente manera:  
Desde el Escritorio, nos dirigimos a la zona inferior derecha y hacemos clic sobre el icono de las redes inalámbricas y luego clic en *Configuración de red e Internet*.



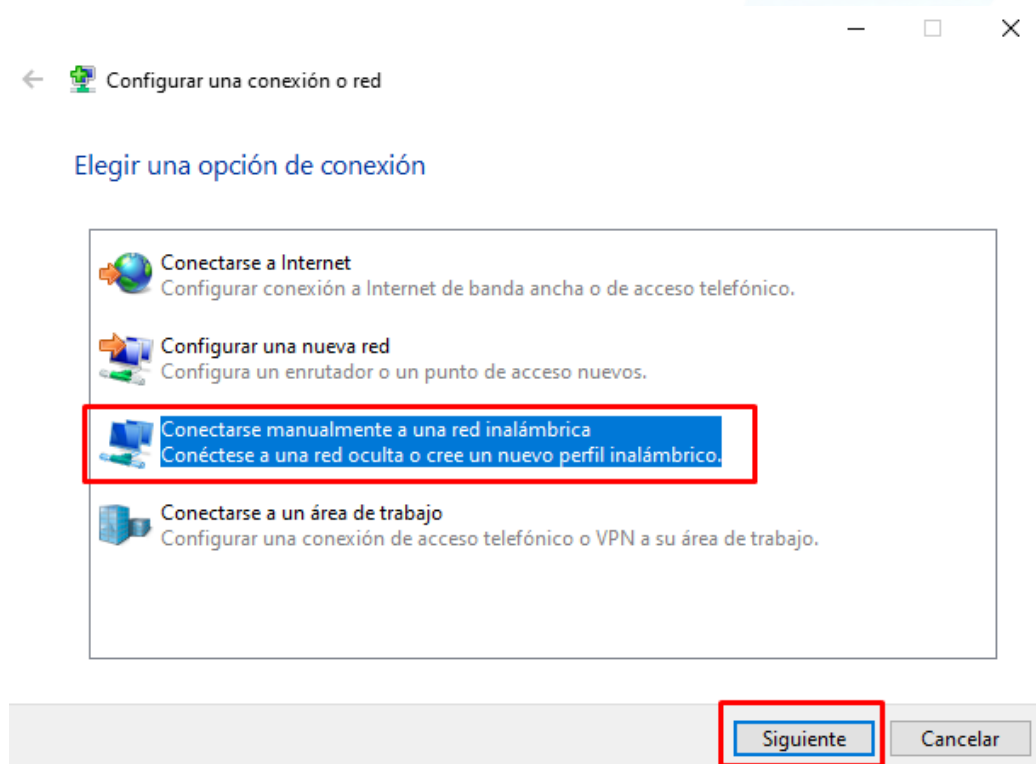
En el menú elegimos *Centro de redes y recursos compartidos*, como vemos en la imagen:



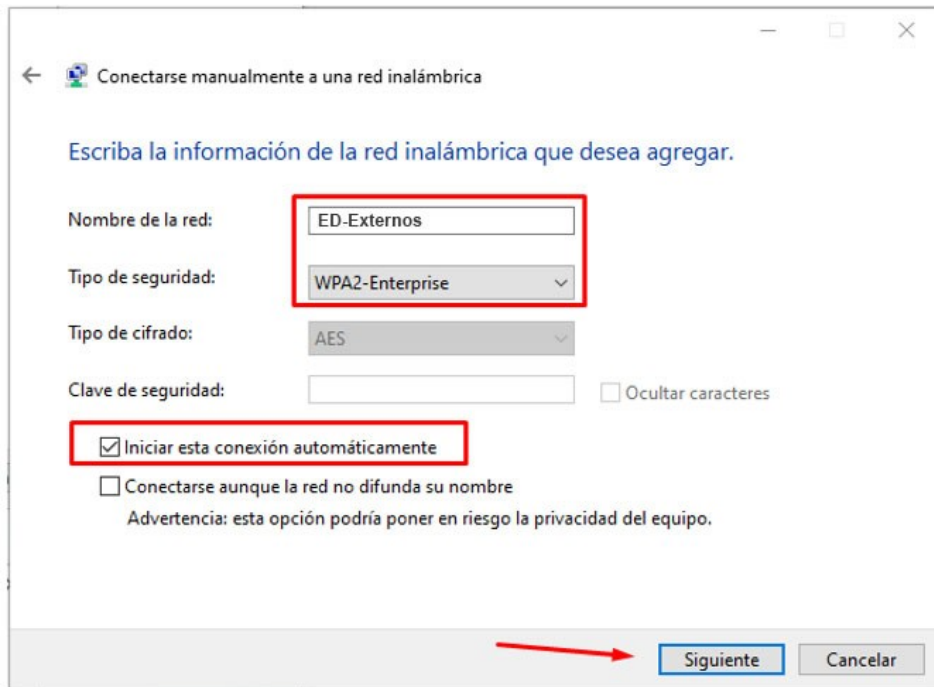
A continuación, se nos abre una pantalla y entraremos en la opción *Configurar una nueva conexión de red*:



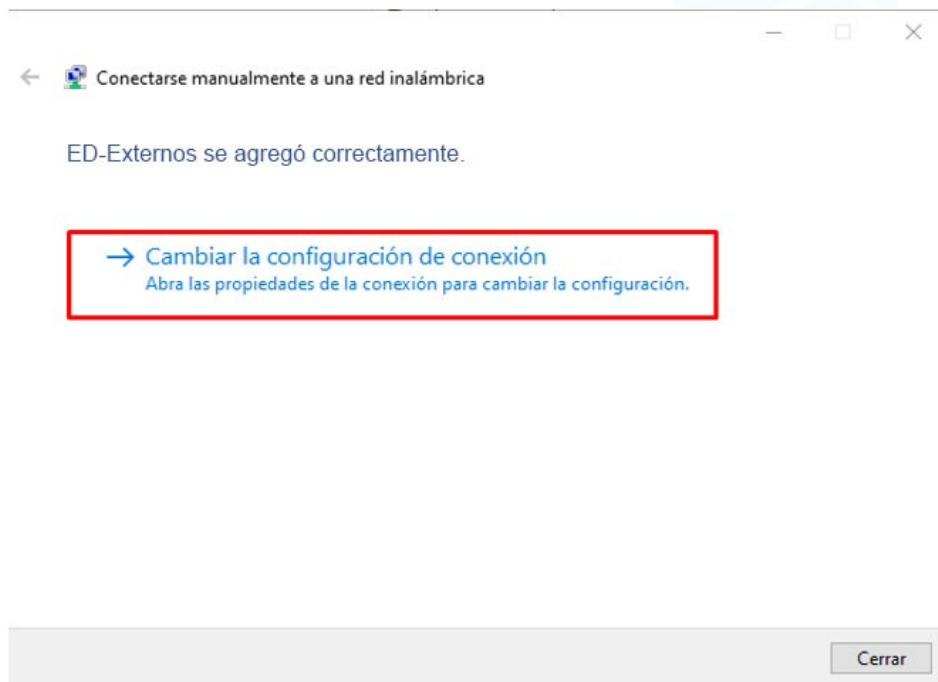
Después, escogeremos la opción *Conectarse manualmente a una red inalámbrica*:



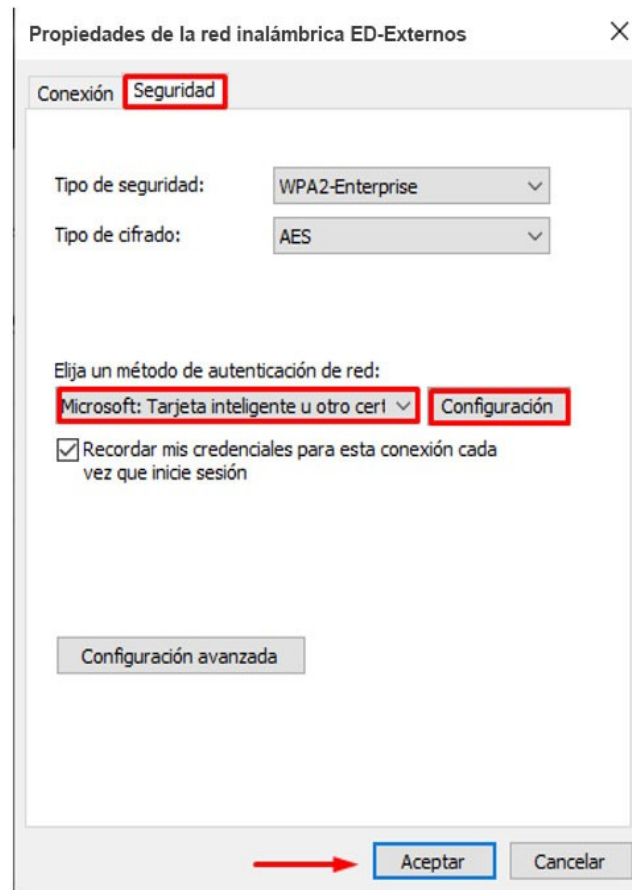
Completamos los datos en los campos tal y como vemos en la imagen y avanzamos en *Siguiente*:



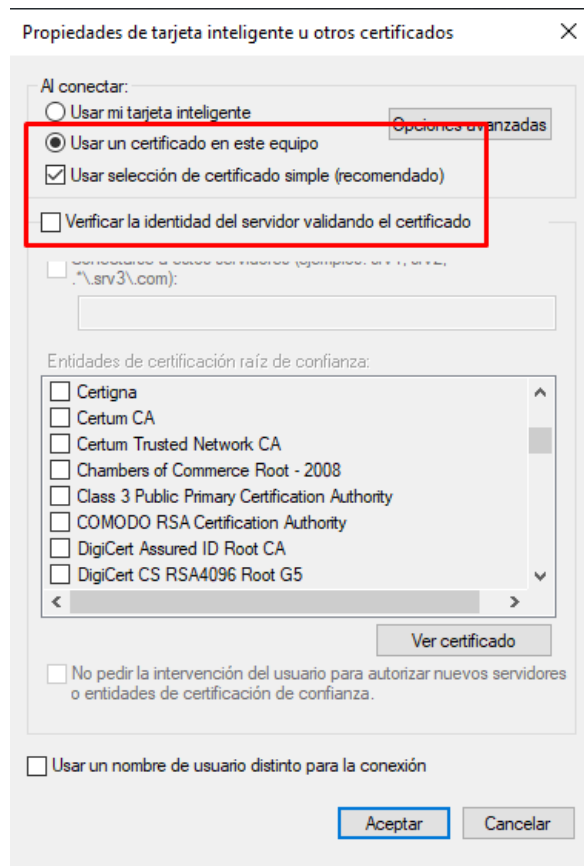
En este punto ya estaría creada la conexión. Ahora, la vamos a modificar para adaptarla a nuestro entorno. Comenzamos dando clic en *Cambiar la configuración de la conexión*:



Después, en la pestaña de *Seguridad*, modificamos el método de autenticación de la red, igual que en la imagen, y a continuación hacemos clic en el botón de *Configuración*:

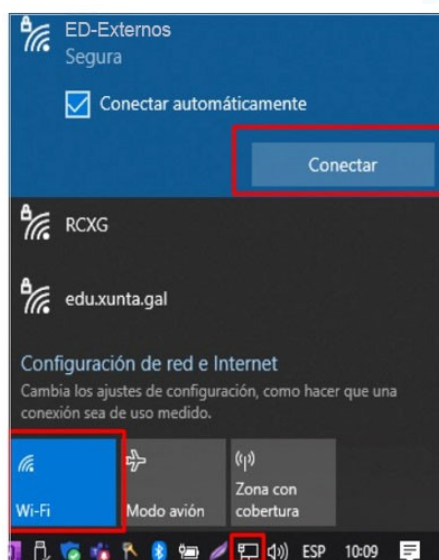


Seguidamente dejamos la configuración tal y como visualizamos en la siguiente imagen:



Continuamos el proceso, haciendo clic en *Aceptar* en todas las pantallas abiertas.

Para establecer la conexión, vamos a la parte inferior derecha de la pantalla y hacemos clic en el icono de *Redes inalámbricas*. Seleccionamos la red *ED-Externos* y pulsamos en *Conectar*. Si no encontramos a simple vista la red, empleamos la barra lateral para desplazarnos.



Elegimos nuestro certificado FNMT, seleccionándolo y clic en *ACEPTAR*



#### 4. CONDICIONES DE USO:

Con el acceso a la red Wifi el usuario acepta de modo explícito las obligaciones aquí indicadas.

##### ***Medidas de seguridad de obligado cumplimiento***

Los usuarios que accedan a la red Wifi de la Xunta de Galicia tienen que cumplir con las siguientes medidas de seguridad:

1. El equipo utilizado para conectar a la red Wifi deberá emplear un sistema operativo distribuido de forma oficial por el fabricante del mismo
2. El equipo debe tener un antivirus instalado. Este antivirus tiene que funcionar correctamente, actualizando diariamente sus firmas.
3. El equipo tiene que tener instaladas todas las actualizaciones de seguridad proporcionadas por el fabricante.

Amtega se reserva el derecho a no proporcionar o inhabilitar posteriormente el acceso Wifi si no se cumplen las medidas de seguridad indicadas.

##### ***Monitorización***

El acceso y el tráfico de las redes Wifi serán monitorizados de modo automático por las plataformas de seguridad de la Xunta con las siguientes finalidades:

1. Detección de actuaciones anómalas.
2. Detección de intrusiones.
3. Análisis forense de incidentes de seguridad o incumplimiento de las normas y políticas de seguridad.
4. Medición y estadísticas para la optimización y mejora del servicio.

##### ***Protección de Datos***

Conforme a lo establecido en la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos, le informamos de que sus datos personales serán tratados y quedarán incorporados en el fichero “*Seguridade e control de acceso*”, registrado en la Agencia Española de Protección de Datos, responsabilidad de la Agencia para la Modernización Tecnológica (Amtega), con la finalidad de gestionar las solicitudes de acceso a la red Wifi de la Xunta de Galicia y velar por la seguridad de la misma.

Para ejercer los derechos de acceso, rectificaciones, cancelaciones e oposición mediante escrito dirigido a la Agencia de Modernización Tecnológica de Galicia (Amtega), Centro de Innovación Cultural y Modernización Tecnológica de Galicia, Ciudad de la Cultura, Monte Gaiás s/n, 15781 Santiago de Compostela (A Coruña), incluyendo copia de su DNI o, de ser el caso, acreditando representación suficiente.