VALENCIA21

CERTIFICADO DIGITAL

Schritt-für-Schritt

Vorweg zu beachten:

Beim Erstellen des spanischen „certificado digital“ (der ACCV) sind insbesondere folgende Punkte zu beachten:

1. **Frist von zwei Wochen**
   Ab dem Zeitpunkt, an dem Sie Ihren PRU-Code (den 10-stelligen Code) erhalten haben, haben Sie **zwei Wochen Zeit**, um das Zertifikat zu generieren. Verpassen Sie diesen Zeitraum, wird der Code ungültig und Sie müssen einen neuen beantragen.
2. **Genaues Eingeben des Codes**
   Der Code besteht aus Groß- und Kleinbuchstaben sowie Ziffern und umfasst 10 Zeichen. Achten Sie darauf, ihn exakt einzugeben. Sie haben **maximal drei Versuche**, um den Code korrekt einzugeben. Bei einem dritten Fehlschlag verfällt der Code ebenfalls, und Sie müssen einen neuen beantragen.
3. **Gleicher Browser und Rechner**
   Es ist sehr wichtig, die Zertifikatserstellung auf demselben Rechner (und mit demselben Browser) durchzuführen, auf dem Sie ursprünglich den Antrag gestellt bzw. den Code angefordert hast. Das hängt damit zusammen, dass beim Antrag in der Regel ein Schlüsselpaar im Browser oder Betriebssystem erzeugt wird, auf das bei der Zertifikatsgenerierung zurückgegriffen wird.
4. **Anleitung auf der Website befolgen**
   In dem Dokument ist ein Link angegeben (z. B. `https://genera.accv.es/...`), über den Sie den Zertifizierungsprozess starten. Halte dich genau an die dort beschriebenen Schritte.
5. **Zertifikat sicher aufbewahren**
   Sobald das Zertifikat erfolgreich generiert ist, sollten Sie es sicher speichern oder exportieren (falls möglich), da es Ihre digitale Identität im Netz repräsentiert. Ein Verlust kann bedeuten, dass Sie erneut durch den Beantragungsprozess müssen.
6. **Neubeantragung bei Problemen**
   Läuft die Frist ab, geben Sie den Code dreimal falsch ein oder haben Sie sonstige technische Probleme, müssen Sie den Prozess über einen neuen Antrag (also einen neuen PRU-Code) von vorne beginnen.

Haftungsausschluss:

Diese Anleitung wurde mit größter Sorgfalt erstellt, jedoch können sich behördliche Verfahren und Anforderungen jederzeit ändern.

Es wird **keine Gewähr für die Aktualität, Vollständigkeit oder Richtigkeit** der Informationen übernommen. Bitte prüfen Sie offizielle Quellen, bevor Sie die beschriebenen Schritte durchführen. Die Nutzung erfolgt auf eigene Verantwortung.

Falls Sie veraltete oder fehlerhafte Informationen entdecken, freue ich mich über einen Hinweis zur Aktualisierung.

VALENCIA21

ES

Agencia de Tecnología y Certificación Electrónica by istec.

¿AYUDA? CONTACTA

Generación del certificado digital en fichero

NIF/NIE:

Código:

Recuerda que dispones de 3 intentos para enviar el código correcto.

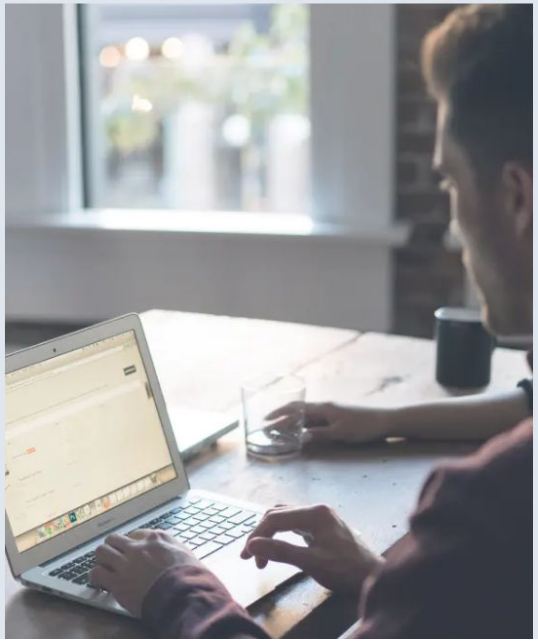
LIMPIAR FORMULARIO

AUTENTICAR CÓDIGO

1. Geben Sie hier Ihre NIE ein

2. Geben Sie hier den Code (Código de Generación de Certificados de Ciudadano) ein, den Sie ausgehändigt bekommen haben. Sie haben max. 3 Versuche

3. Anklicken



Agencia de Tecnología y Certificación Electrónica by istec.

VALENCIA21

¿AYUDA? CONTACTA

Generación del certificado digital en fichero

Información de la petición

Tus certificados se van a generar con la información que se muestra a continuación.

NIF/NIE [redacted]

Nombre [redacted]

Primer apellido [redacted]

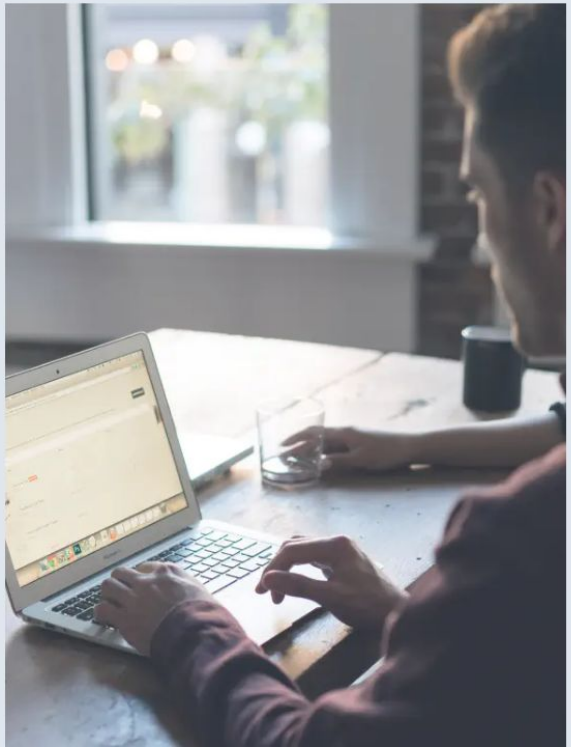
Segundo apellido

E-mail [redacted]

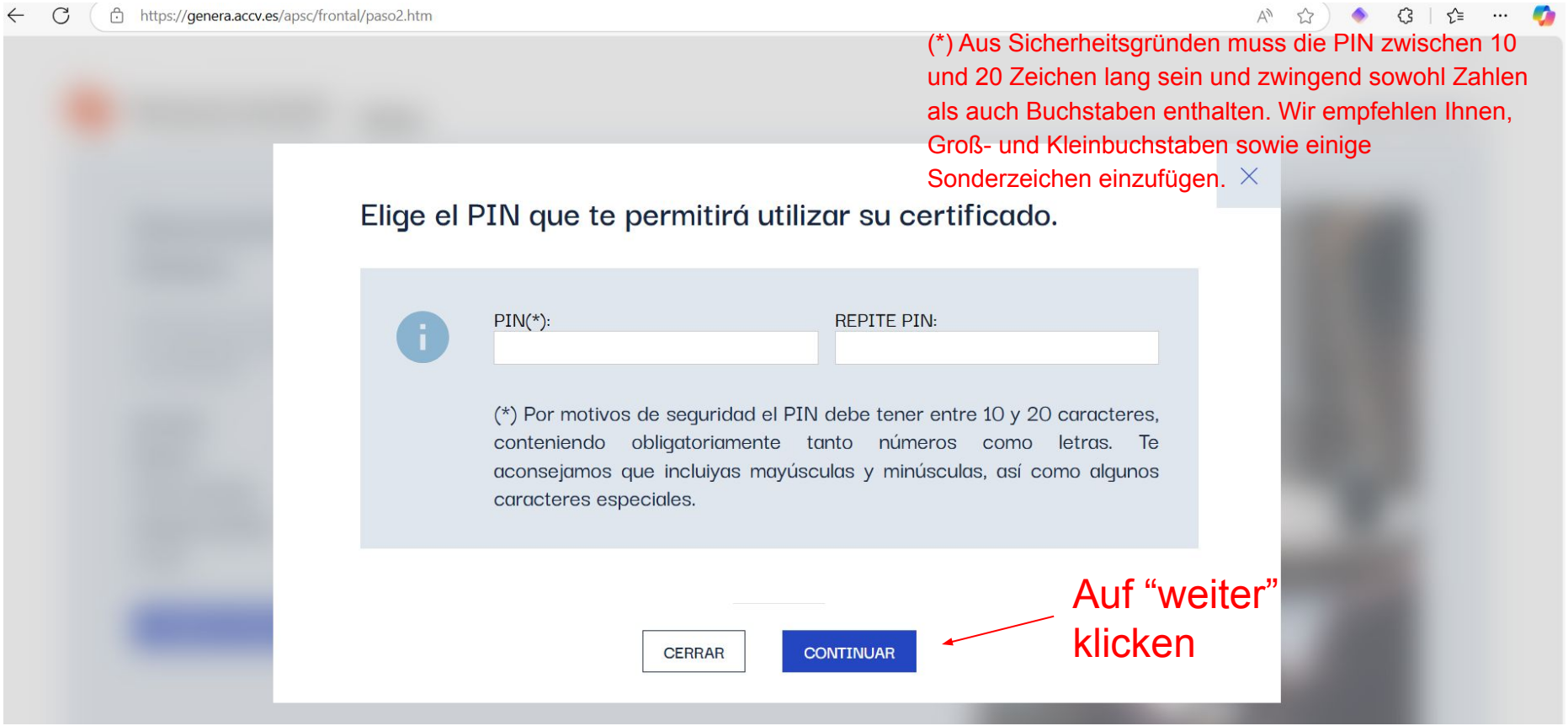
GENERAR CERTIFICADOS

1. Hier erscheinen die Daten (NIE, Namen, Nachnamen, E-Mail), die man schon für die NIE angegeben hat

2. Anklicken



1. Wählen Sie die PIN, mit der Sie Ihr Zertifikat verwenden können.



VALENCIA21

https://genera.accv.es/apsc/frontal/paso2.htm

Descargas

[redacted]

Abrir archivo

Ver más

Agencia de Tecnología y Certificación Electrónica by istec.

Generación del certificado digital en fichero

Download der Certificado Digital- Datei

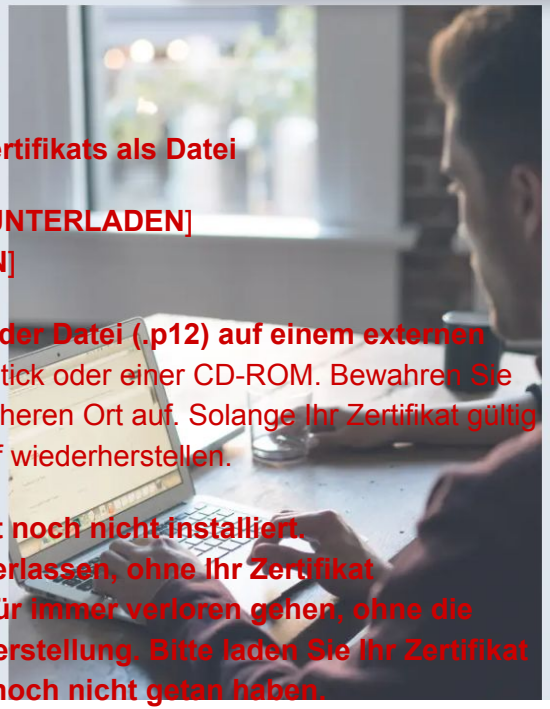
Tu certificado: DESCARGAR

PIN: VER PIN

Guarda una copia de respaldo del fichero .p12 en un dispositivo externo como una memoria USB o un CD-ROM. Dispositivo que deberás conservar en un lugar seguro. De ese modo, mientras tu certificado permanezca en vigor, podrás recuperarlo cuando lo necesites.

Aun no has instalado el certificado. Para hacerlo sigue las instrucciones que puedes encontrar en este enlace: https://www.accv.es/manuales-y-guias/.

Si sales de esta página sin descargar tu certificado éste se perderá para siempre sin posibilidad de recuperarlo. Por favor, descarga tu certificado ahora si todavía no lo has hecho.

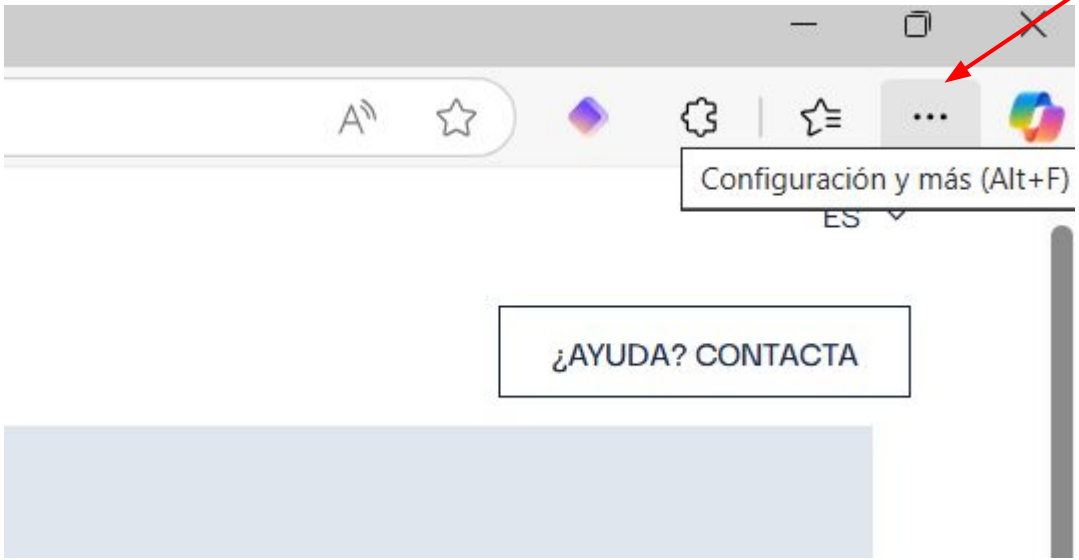


Erstellung des digitalen Zertifikats als Datei

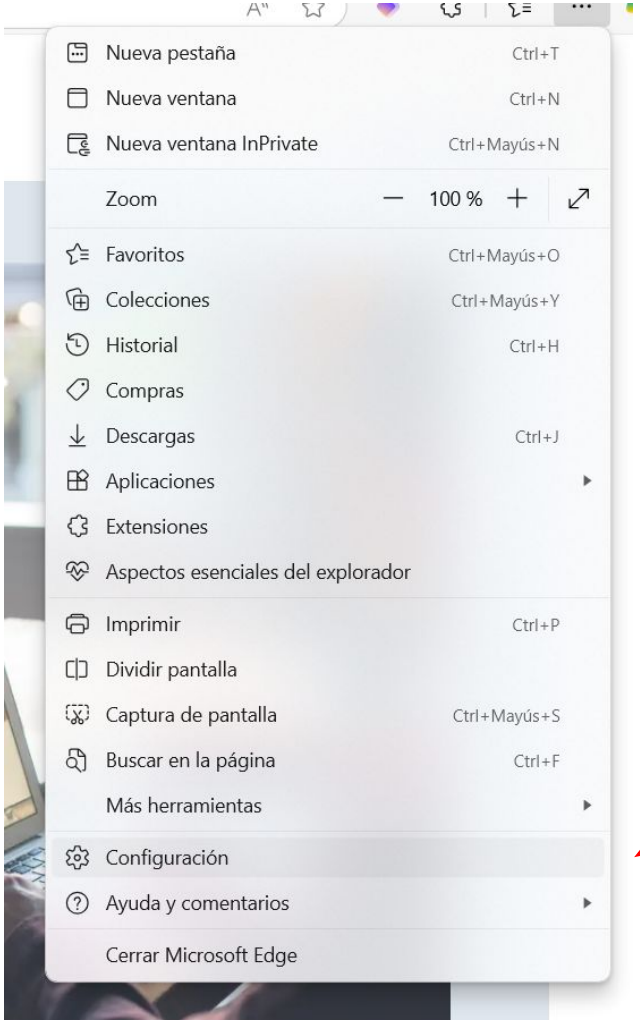
- **Ihr Zertifikat: [HERUNTERLADEN]**
- **PIN: [PIN ANZEIGEN]**

💾 **Sichern Sie eine Kopie der Datei (.p12) auf einem externen Medium**, z. B. einem USB-Stick oder einer CD-ROM. Bewahren Sie dieses Medium an einem sicheren Ort auf. Solange Ihr Zertifikat gültig ist, können Sie es bei Bedarf wiederherstellen.

⚠️ **Sie haben das Zertifikat noch nicht installiert.**
⚠️ **Wenn Sie diese Seite verlassen, ohne Ihr Zertifikat herunterzuladen, wird es für immer verloren gehen, ohne die Möglichkeit einer Wiederherstellung. Bitte laden Sie Ihr Zertifikat jetzt herunter, falls Sie es noch nicht getan haben.**



Zum Installieren des Certificado Digital oben rechts die drei Punkte beim Microsoft Edge Browser anklicken.



VALENCIA21

Klick auf “Configuración”, bzw. “Einstellungen”.

VALENCIA21

Configuración

certificados

- Perfiles
- Privacidad, búsqueda y servicios
- Apariencia
- Copilot y barra lateral
- Página de inicio, inicio y pestaña nueva
- Cortar, copiar y pegar
- Cookies y permisos del sitio
- Navegador predeterminado
- Idiomas
- Descargas
- Accesibilidad
- Sistema y rendimiento
- Protección infantil
- Impresoras
- Teléfono y otros dispositivos
- Restablecer configuración

1. Geben Sie in das Suchfeld “certificados” bzw. “Zertifikate” ein

Seguridad

Administrar la configuración de seguridad de Microsoft Edge

Administrar certificados

Administrar configuración y certificados HTTPS/SSL

2. Klick auf “Administrar certificados” bzw. “Zertifikate verwalten”

SmartScreen de Microsoft Defender

Ayúdame a protegerme contra descargas y sitios malintencionados con SmartScreen de Microsoft Defender

Bloquear aplicaciones potencialmente no deseadas

Bloquea las descargas de aplicaciones que no tienen muy buena reputación y que pueden causar comportamientos inesperados

Protección contra errores ortográficos en sitios web

¿Está satisfecho con la protección contra errores ortográficos en sitios web?

Advertirme si he escrito mal la dirección de un sitio y puedo ser dirigido a un sitio potencialmente malicioso.

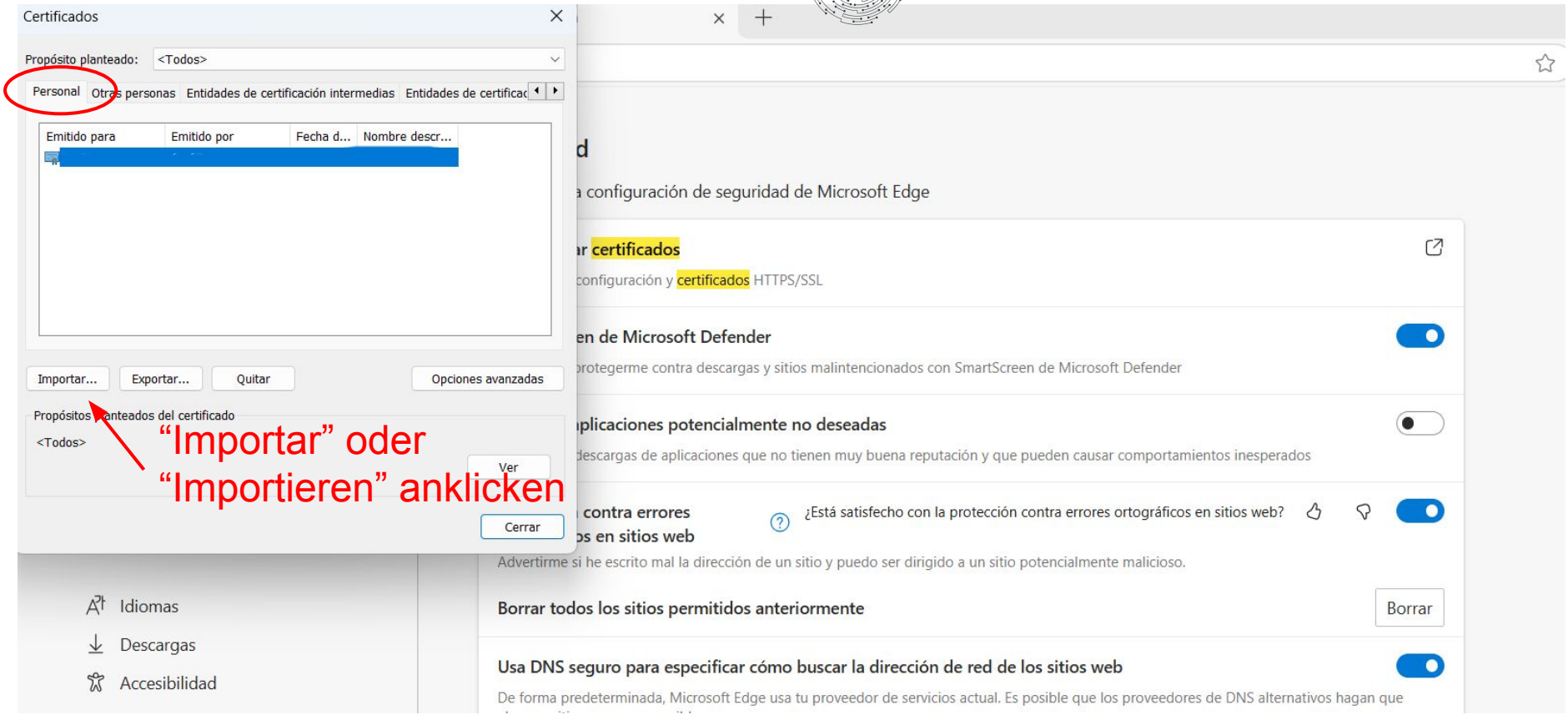
Borrar todos los sitios permitidos anteriormente

Borrar

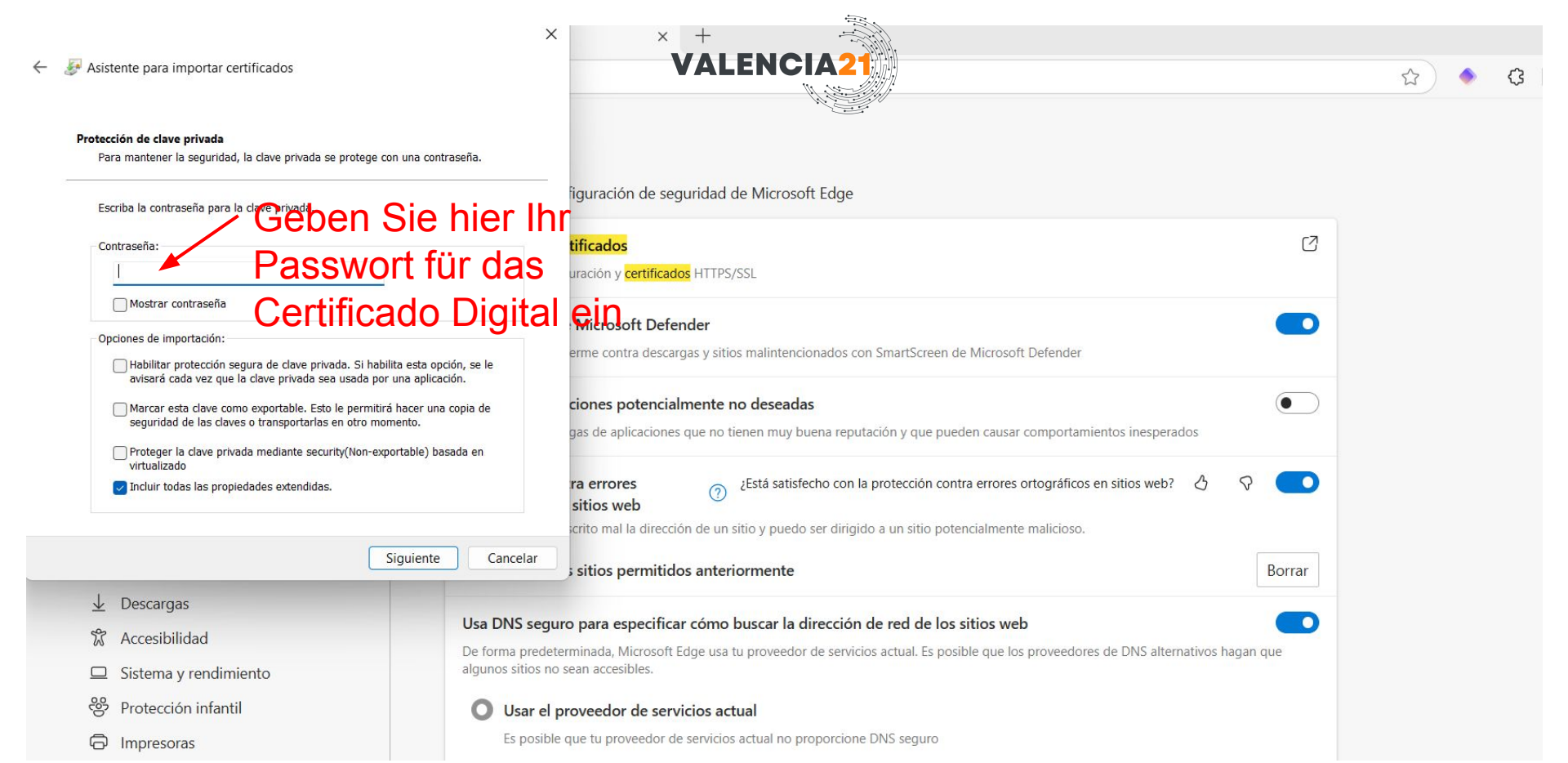
Usa DNS seguro para especificar cómo buscar la dirección de red de los sitios web

De forma predeterminada, Microsoft Edge usa tu proveedor de servicios actual. Es posible que los proveedores de DNS alternativos hagan que algunos sitios no sean accesibles.

- **Usar el proveedor de servicios actual**
  Es posible que tu proveedor de servicios actual no proporcione DNS seguro
- **Elegir un proveedor de servicios**
  Selecciona un proveedor de la lista o escribe un proveedor personalizado

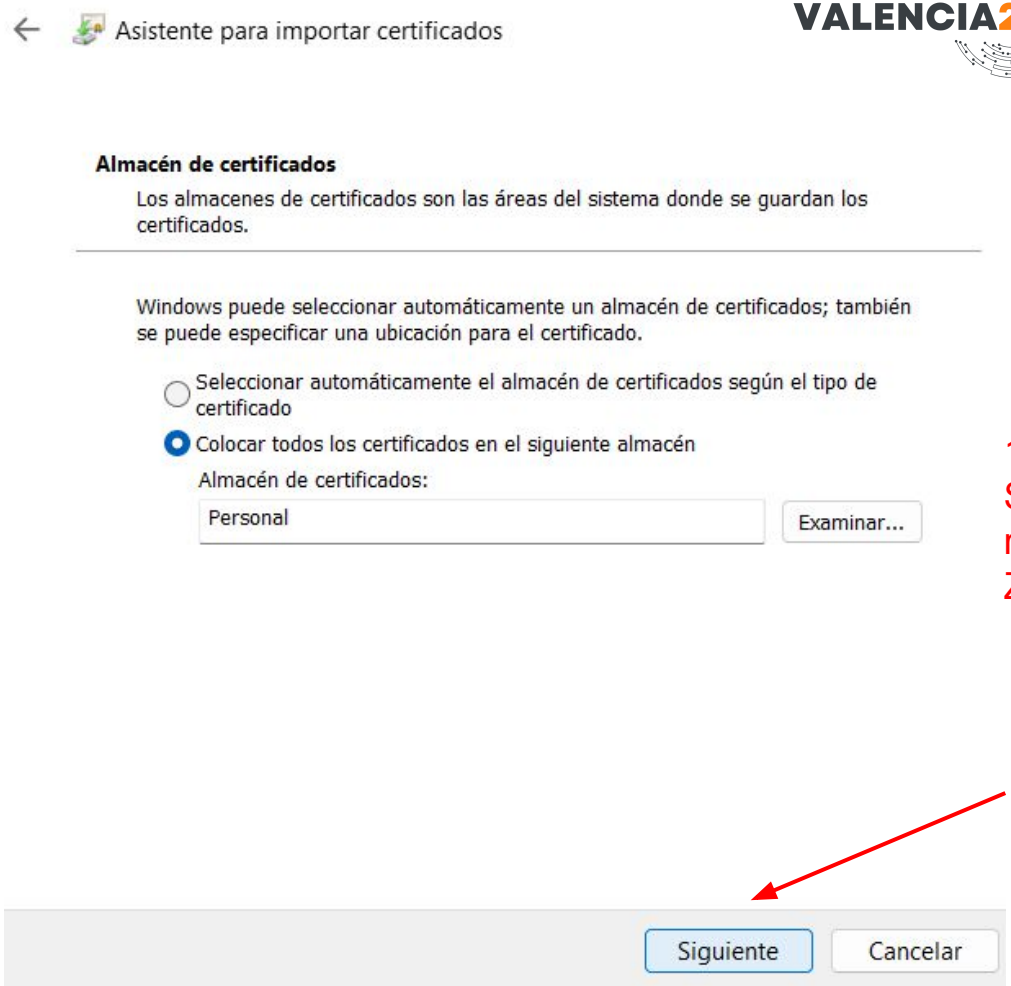

Certificados
Propósito planteado: <Todos>
Personal
Otras personas
Entidades de certificación intermedias
Entidades de certificac
Emitido para
Emitido por
Fecha d...
Nombre descr...
Importar...
Exportar...
Quitar
Opciones avanzadas
Propósitos planteados del certificado
<Todos>
Ver
Cerrar
“Importar” oder
“Importieren” anklicken
Idiomas
Descargas
Accesibilidad
d
a configuración de seguridad de Microsoft Edge
r certificados
configuración y certificados HTTPS/SSL
en de Microsoft Defender
rotegerme contra descargas y sitios malintencionados con SmartScreen de Microsoft Defender
plicaciones potencialmente no deseadas
descargas de aplicaciones que no tienen muy buena reputación y que pueden causar comportamientos inesperados
contra errores
os en sitios web
¿Está satisfecho con la protección contra errores ortográficos en sitios web?
Advertirme si he escrito mal la dirección de un sitio y puedo ser dirigido a un sitio potencialmente malicioso.
Borrar todos los sitios permitidos anteriormente
Borrar
Usa DNS seguro para especificar cómo buscar la dirección de red de los sitios web
De forma predeterminada, Microsoft Edge usa tu proveedor de servicios actual. Es posible que los proveedores de DNS alternativos hagan que


Asistente para importar certificados
Archivo para importar
Especifique el archivo que desea importar.
Nombre de archivo:
Examinar...
Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:
Intercambio de información personal: PKCS #12 (.PFX,.P12)
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
Almacén de certificados en serie de Microsoft (.SST)
Siguiente
Cancelar
Wählen Sie durch Klick auf "Examinar oder "Durchsuchen" die heruntergeladene Datei aus
VALENCIA21
figuración de seguridad de Microsoft Edge
tificados
uración y certificados HTTPS/SSL
Microsoft Defender
os malintencionados con SmartScreen de Microsoft Defender
potencialmente no deseadas
gas de aplicaciones que no tienen muy buena reputación y que pueden causar comportamientos inesperados
ra errores
sitios web
¿Está satisfecho con la protección contra errores ortográficos en sitios web?
crito mal la dirección de un sitio y puedo ser dirigido a un sitio potencialmente malicioso.
s sitios permitidos anteriormente
Borrar
Usa DNS seguro para especificar cómo buscar la dirección de red de los sitios web
De forma predeterminada, Microsoft Edge usa tu proveedor de servicios actual. Es posible que los proveedores de DNS alternativos hagan que algunos sitios no sean accesibles.
Descargas
Accesibilidad
Sistema y rendimiento


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.
Siguiente
Cancelar
Geben Sie hier Ihr Passwort für das Certificado Digital ein
VALENCIA21
figuración de seguridad de Microsoft Edge
tificados
uración y certificados HTTPS/SSL
Microsoft Defender
erme contra descargas y sitios malintencionados con SmartScreen de Microsoft Defender
ciones potencialmente no deseadas
gas de aplicaciones que no tienen muy buena reputación y que pueden causar comportamientos inesperados
ra errores
sitios web
¿Está satisfecho con la protección contra errores ortográficos en sitios web?
crito mal la dirección de un sitio y puedo ser dirigido a un sitio potencialmente malicioso.
sitios permitidos anteriormente
Borrar
Usa DNS seguro para especificar cómo buscar la dirección de red de los sitios web
De forma predeterminada, Microsoft Edge usa tu proveedor de servicios actual. Es posible que los proveedores de DNS alternativos hagan que algunos sitios no sean accesibles.
Usar el proveedor de servicios actual
Es posible que tu proveedor de servicios actual no proporcione DNS seguro
Descargas
Accesibilidad
Sistema y rendimiento
Protección infantil
Impresoras

1. Diese beiden Optionen sollten “markiert” sein.

2. “Siguiente”, bzw. “Weiter” klicken



1. In diesem Fall ist der voreingestellte Speicherort **„Personal“** (Persönlich) der richtige Speicherort für persönliche Zertifikate.

2. Dann “Siguiente”, bzw. “weiter”

Asistente para importar certificados

VALENCIA21

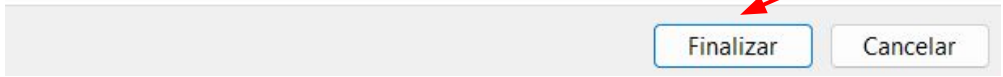
Finalización del Asistente para importar certificados

Se importará el certificado después de hacer clic en Finalizar.

Especificó la siguiente configuración:

Almacén de certificados seleccionado por el usuario	Personal
Contenido	PFX
Nombre de archivo	[redacted]

Klick auf “Finalizar”, “beenden”



Überprüfen, ob das Zertifikat korrekt installiert ist:

In Windows:

1. Öffnen Sie die **Zertifikatsverwaltung**:
   - Drücken Sie `Windows-Taste + R`, geben Sie `certmgr.msc` ein, und drücken Sie Enter.
2. Gehen Sie zum Bereich **Persönlich > Zertifikate**.
   - Hier sollte Ihr neues Zertifikat sichtbar sein. Es wird mit Ihrem Namen oder der Organisation angezeigt.
3. Prüfen Sie das Ablaufdatum:
   - Klicken Sie doppelt auf das Zertifikat und stellen Sie sicher, dass das **Gültigkeitsdatum** korrekt ist.

In Ihrem Browser (Edge/Chrome):

1. Öffnen Sie die **Einstellungen** → **Datenschutz, Suche und Dienste** → **Zertifikate verwalten**.
2. Unter **Persönlich** sollte das Zertifikat ebenfalls sichtbar sein.