Inspeccionar certificado

Revisa los datos y la vigencia de un certificado digital.

Anonymous · 06/11/2026

Inspeccionar certificado

Esta herramienta lee un certificado digital (`.p12` o `.pfx`) y muestra su contenido: quién es el titular, quién lo emitió, cuánto tiempo de vigencia le queda y los certificados que contiene.

Ir a la herramienta

Para qué sirve

- Comprobar que usas el certificado correcto antes de firmar documentos o de iniciar un proceso de certificación.
- Revisar la fecha de vencimiento y saber si necesitas renovarlo.
- Verificar el RUN, el nombre y el correo del titular.
- Obtener el certificado público, la cadena de confianza o la clave privada en formato PEM, por ejemplo para configurarlos en otro sistema.
- Revisar un certificado de prueba recién creado.

Para qué no sirve

- No valida el certificado ante el SII ni ante la autoridad certificadora: solo muestra lo que el archivo contiene.
- No modifica ni renueva el certificado.
- No sirve para firmar documentos; para eso usa Firmar XML u otras herramientas de firma.

Tu certificado no se guarda

El archivo y su contraseña se usan solo para mostrar la información en pantalla. No se almacenan de forma permanente.

Antes de empezar

Necesitas:

- El archivo del certificado, en formato `.p12` o `.pfx`.

- La contraseña con la que está protegido.

Si solo quieres probar la herramienta, puedes crear un archivo con el certificado digital de prueba.

Paso a paso

1. Abre la herramienta

Verás dos campos: el archivo del certificado y su contraseña.



2. Selecciona el archivo e ingresa la contraseña

Haz clic en **Seleccionar archivo**, elige tu `.p12` o `.pfx` y escribe la contraseña del certificado. Ambos campos son obligatorios.



3. Inspecciona

Presiona el botón **Inspeccionar certificado**. La página mostrará los datos del certificado.

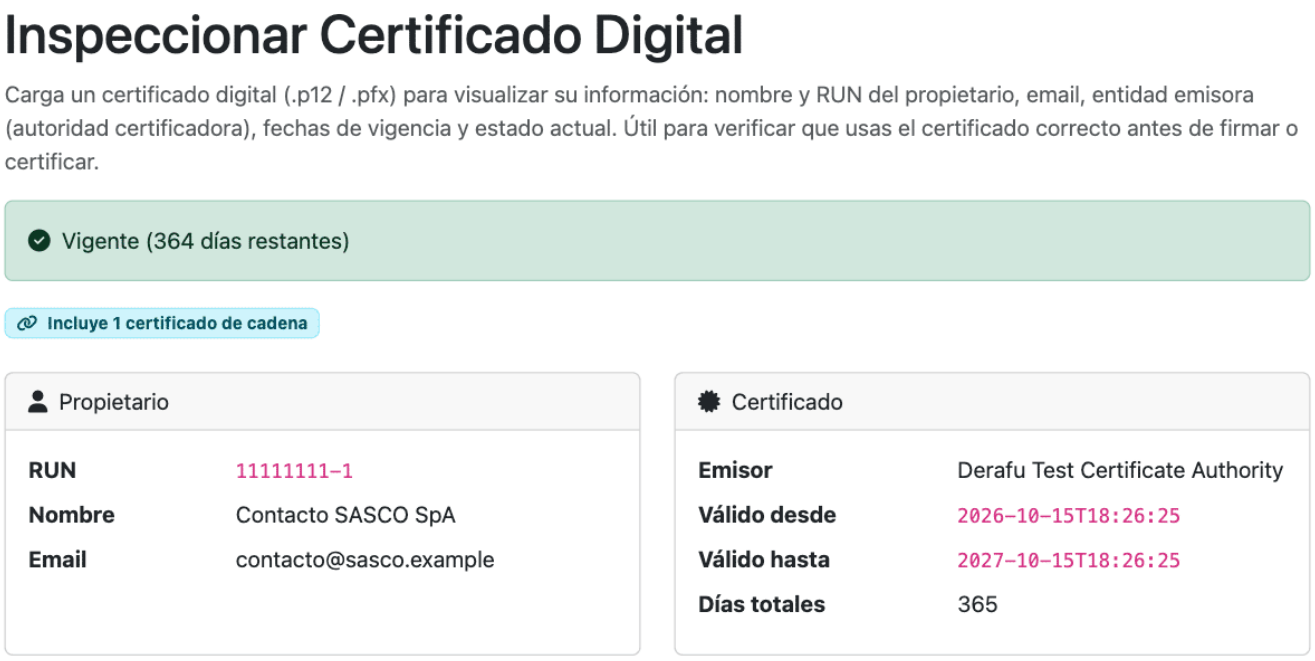
Cómo leer el resultado

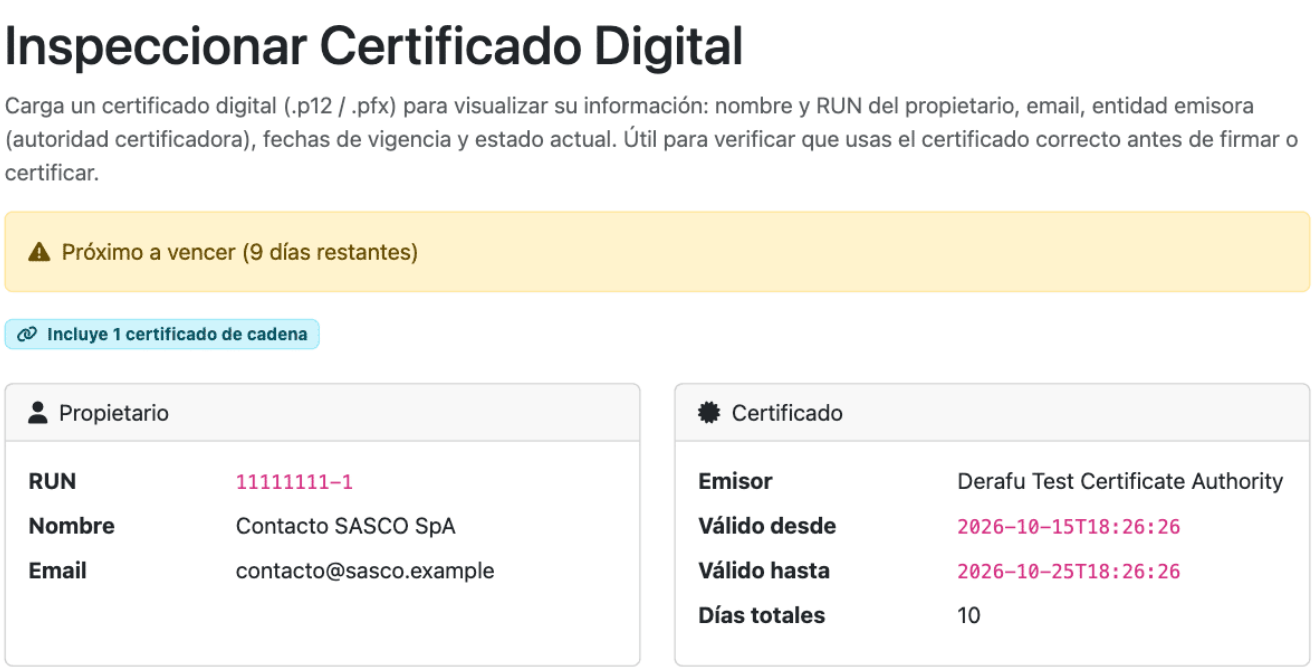
Estado de vigencia

En la parte superior aparece un recuadro con el estado actual del certificado:

Estado	Significado
Vigente (verde)	El certificado está dentro de su período de validez y le quedan más de 30 días.
Próximo a vencer (amarillo)	Está vigente, pero le quedan 30 días o menos. Conviene renovarlo.
Vencido (rojo)	Ya pasó su fecha de vencimiento y no se debe usar.

Debajo del estado se indica si el archivo incluye certificados de cadena.





Datos del certificado

- **Propietario:** RUN, nombre y correo del titular.
- **Certificado:** entidad emisora, fecha desde la cual es válido, fecha hasta la cual es válido y total de días de vigencia.

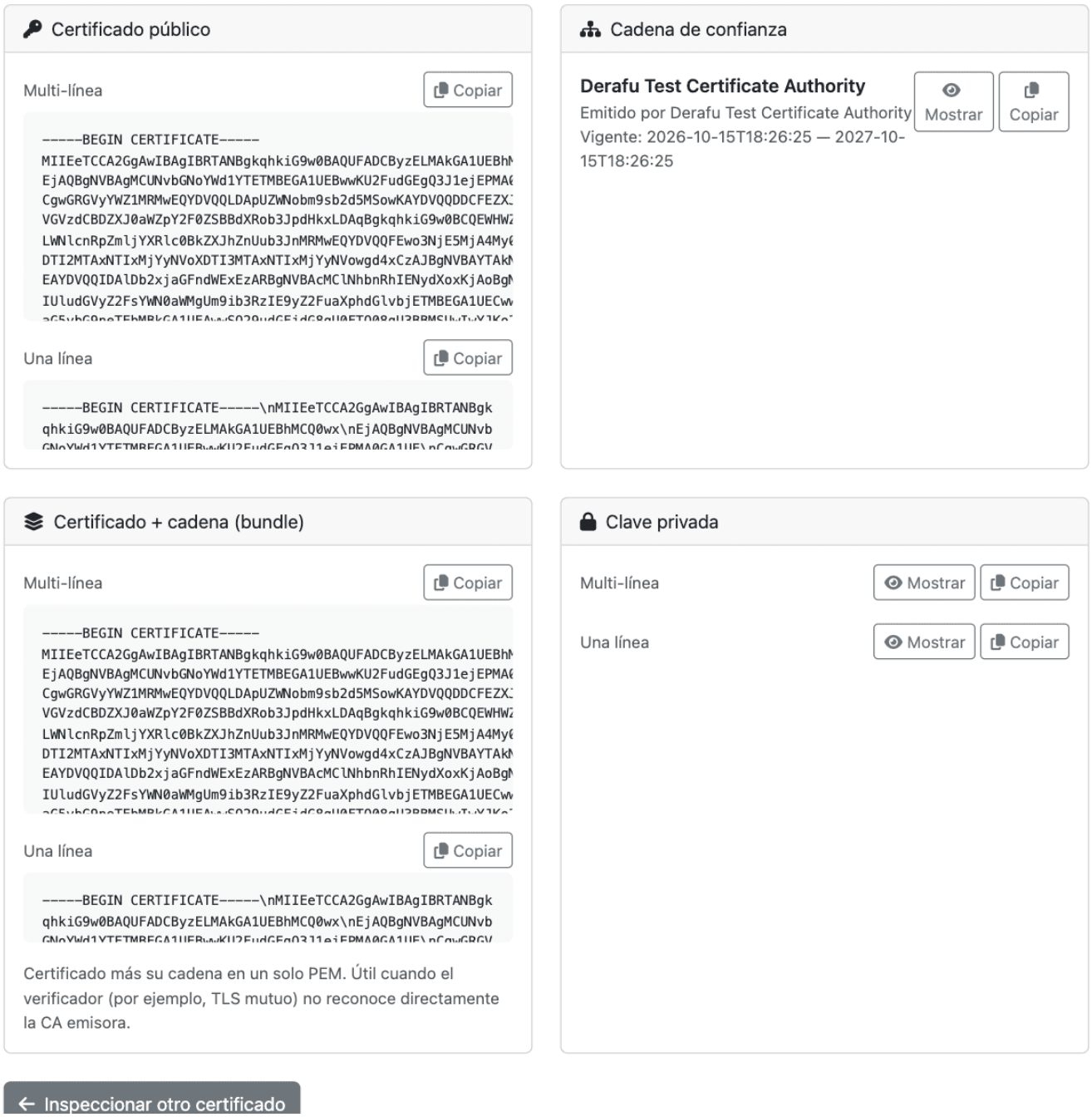
Certificados y claves en formato PEM

Más abajo la herramienta entrega, cada uno en versión multilínea y en una sola línea, con botones **Copiar** y, en los casos sensibles, **Mostrar**:

- **Certificado público.**
- **Cadena de confianza:** los certificados de las autoridades que respaldan al certificado.
- **Certificado + cadena (bundle):** ambos en un solo PEM, útil cuando otro sistema no reconoce por sí solo a la entidad emisora.
- **Clave privada:** permanece oculta hasta que presionas **Mostrar**.

Cuida la clave privada

La clave privada te permite firmar en nombre del titular. No la compartas ni la copies a lugares inseguros.



Al final de la página, el botón **Inspeccionar otro certificado** te devuelve al formulario.

Errores frecuentes

Si el archivo o la contraseña no son correctos se muestra el mensaje **«No se pudo leer el certificado. Verifica que el archivo y la contraseña sean correctos.»**



Revisa estos puntos:

- La contraseña es sensible a mayúsculas y minúsculas.
- El archivo debe ser un certificado `.p12` o `.pfx`. Otros formatos (por ejemplo un `.pem` o un archivo XML) no se pueden leer.
- Verifica que el archivo no esté dañado o incompleto.

Herramientas relacionadas

- Certificado digital de prueba
- Firmar XML
- Verificar DTE

Última actualización el 06/11/2026