Autoridad de Certificación

THOMAS SIGNE
Soluciones Tecnológicas Globales

Proceso de Compra Online de Certificado de Firma Electrónica Avanzada

Información del documento

Nombre	Proceso de Compra Online de Certificado de Firma Electrónica Avanzada
Realizado por	THOMAS SIGNE
País	CHILE
Versión	1.3
Tipo de documento	Confidencial
Código	THS-CL-AC-CV-09

Historial de versiones

Versión	Fecha	Descripción
1.0	20/05/2021	Elaboración de documento inicial.
1.1	16/09/2021	Cambio de imagen de THS. Se cambia la codificación del documento de THS-CL-AC-PR-12 a THS-CL-AC-CV-09 de acuerdo con el GSIGNE-GRAL-PR-01 Control de la información Documentada Ed 2.6. El código antiguo estaba duplicado.
1.2	04/10/2021	Cambios indicados por la EA
1.3	28/10/2021	Cambios indicados por la EA

ÍNDICE

1. OBJETIVO

Detallar las operaciones involucradas en el proceso de emisión y Enrolamiento en línea para obtener un certificado de Firma Electrónica Avanzada, en adelante FEA, almacenado y protegido en el Hardware Security Module (HSM) centralizado de Thomas Signe.

2. PROCESO DE COMPRA ONLINE DE CERTIFICADO DE FIRMA ELECTRONICA AVANZADA

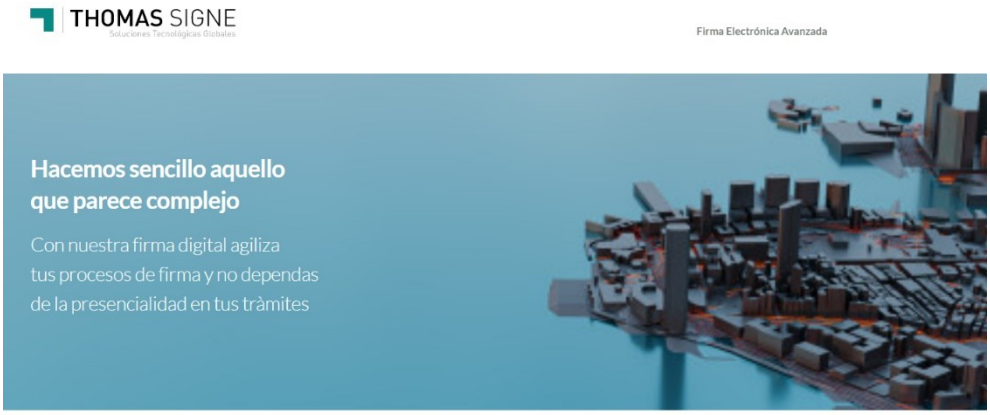
Existen dos métodos para realizar el proceso de compra de un certificado de Firma Electrónica Avanzada.

1) A través de la página web de Thomas Signe y un proceso de compra online con Marketplace (MKP)
2) A través de un agente comercial de Thomas Signe desde el Sistema de Autoridad de Registro (SAR)

2.1. PROCESO DE COMPRA A TRAVÉS DE LA PÁGINA WEB Y MARKETPLACE DE THOMAS SIGNE (MKP)

Se explica a continuación el flujo de adquisición de FEA por parte del Solicitante:

1) **Ingresar al sitio Thomas Signe:** El solicitante de FEA Ingresa al Sitio Marketplace Thomas Signe.



2) **Requisitos de Enrolamiento en Línea:** Se muestran los requisitos que debe tener el solicitante para realizar el enrolamiento en línea. Se muestra el siguiente mensaje:

Estimado usuario antes de pagar el certificado con validación 100% online tome en cuenta lo siguiente

- **Primer Requisito**: Usted deberá realizar el pago a través de la pasarela de pago KHIPU.
- **Segundo requisito.** Usted deberá disponer de su clave única. Si no tiene clave única deberá solicitarla en el Registro Civil.
- **Tercer requisito**: Usted Deberá responder de manera efectiva 4 de las 5 preguntas del desafío en caso de responder con errores el proceso no será exitoso.

En caso de que el proceso no será exitoso usted podrá disponer de las siguientes opciones:

A. Acudir de manera presencial a realizar el proceso de validación de identidad en las oficinas de Thomas Signe Chile ubicadas en Avenida presidente Kennedy lateral 5600 oficina 806.
Esta validación será realizada de manera presencial por los operadores de registro de la Autoridad de Certificación

B. Solicitar Validación a domicilio u oficina (Solo para Región Metropolitana) a través de los siguientes canales de comunicación
Correo Electrónico: comercial@thomas-signe.cl
Teléfonos: +56 2325977821, +56 23398998

La validación de identidad a domicilio tiene los siguientes costos según la comuna donde se encuentre el suscriptor del certificado

Las Condes, La Reina, Vitacura, Ñuñoa, Santiago, Providencia	CLP $ 7,990
Lo Barnechea	CLP $ 10,990
La Florida Macul	CLP $ 18,990
a. Colina	CLP $ 26,990

Esta validación será realizada de manera presencial por los operadores de registro de la Autoridad de Certificación

C. Solicitar el reverso del pago a través de los medios de contacto
comercial@thomas-signe.cl
Teléfonos: +56 2325977821, +56 23398998

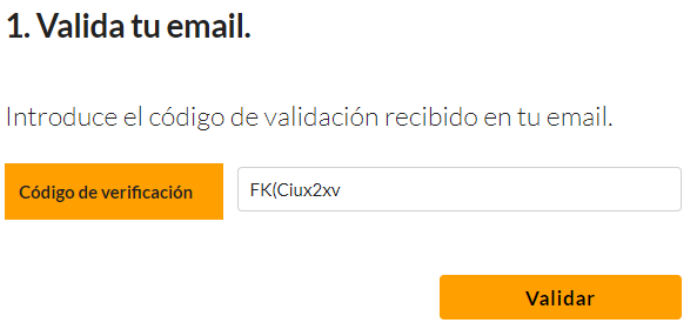
La devolución podría tomar un lapso máximo de 24 horas.

3) **Seleccionar vigencia de Certificado adquirir:** El solicitante debe seleccionar la Vigencia que va a adquirir.

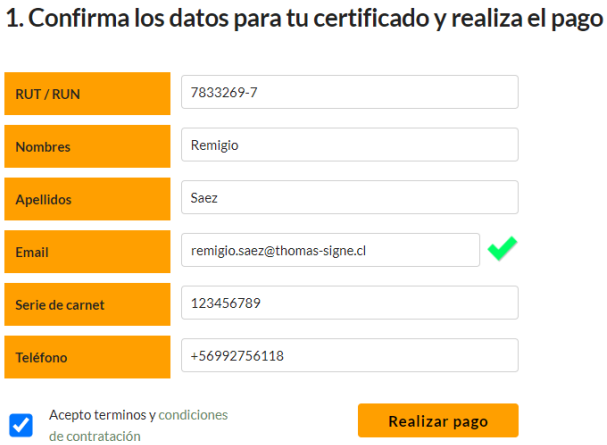
4) **Ingresar RUN, apellido, Email, Serie, Teléfono:** el solicitante debe ingresar los datos requeridos para registro del proceso y poder iniciar el proceso de validación fehaciente de identidad con Clave única más mecanismo complementario.

5) **Aceptar términos y condiciones:** el solicitante debe aceptar términos y condiciones, según Anexo I incluido en este documento.

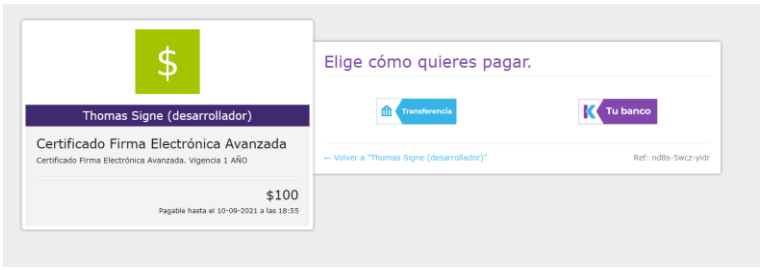
6) **Validación de OTP mail:** Se realiza validación de email ingresado del Suscriptor, mediante código OTP enviado al email indicado en el proceso de registro. Es imprescindible esta validación para iniciar el proceso de validación fehaciente de identidad más factor complementario, según Decreto 24.



7) **Registrar pago:** el solicitante accede a la pasarela de pago



8) **Seleccionar Medio de Pago:** El suscriptor puede realizar el Pago mediante Tarjeta Debito, Crédito o Transferencia



9) **Validación de Pago:** El sistema Valida el Pago realizando mediante la Plataforma.

Procesando transacción

El pago está en proceso de revisión. Una vez verificado continuará el proceso de solicitud de su certificado.

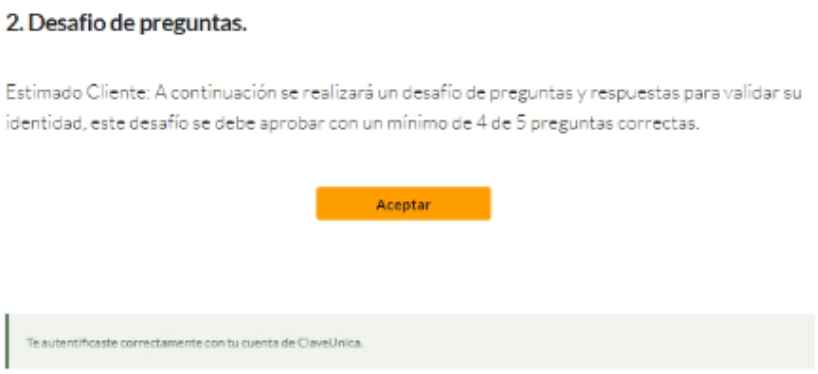
Por favor espere...

10) **Iniciando el proceso de validación de identidad**. Los siguientes pasos se corresponden con el proceso de verificación de identidad para emitir un Certificado de Firma Electrónica Avanzada (FEA) según el Decreto 24.

11) **Validación de Clave Única:** Se debe ingresar el primer factor de Autenticación que es Clave Única. Si no tiene, el proceso de enrolamiento en línea finaliza sin poder emitir el certificado FEA y se actuará como se describe en el párrafo *2.1.1 Validación de identidad no completada o no exitosa*.

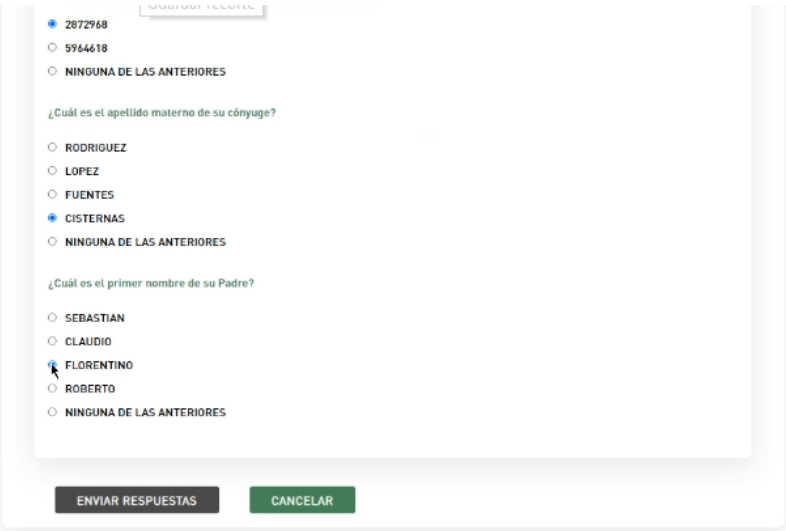
12) **Ingreso de Clave Única**

13) **Clave Única retorna RUN, Nombres y Apellidos:** Si la clave Única ingresada por el solicitante es correcta, el sistema Clave Única retorna el RUN, Nombres y Apellidos. Al superar la validación de Clave Única, la plataforma habilita el Desafío de Preguntas que es **el mecanismo complementario de verificación fehaciente de identidad**, según el Decreto 24.



14) **Valida Serie OK, CI Vigente / No Vigente:** Buro valida el estado de vigencia de la Cedula de identidad

15) **Desafío Preguntas y Respuestas:** si la cedula está vigente, se procede al desafío de preguntas y respuestas efectuadas por BURO, (actualmente EQUIFAX). Este es el mecanismo complementario de verificación fehaciente de identidad según el Decreto 24.

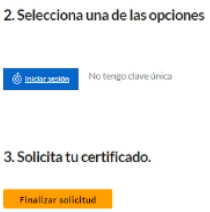


---

16) **Validar Score Desafío Preguntas:** Se valida el score de respuestas del solicitante. Si estas son 4 de 5 correctas, el proceso prosigue; en caso contrario, el proceso finaliza sin emisión del certificado y se marca para verificación presencial de identidad. Un

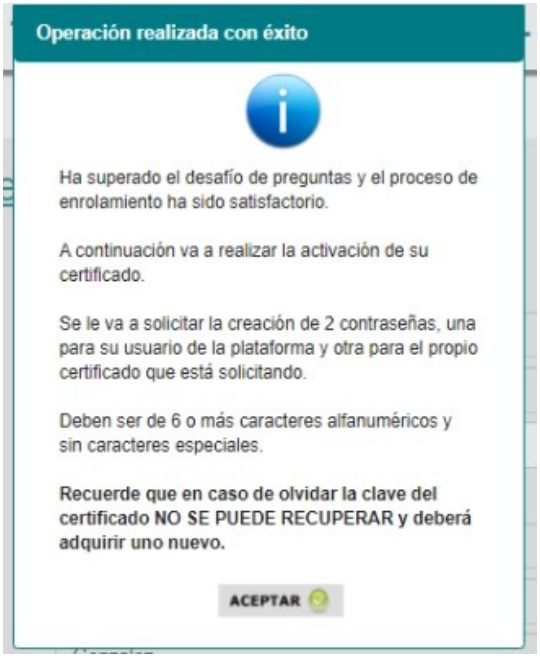
agente comercial u operador de registro de la Autoridad de Certificación se pondrá en contacto con el solicitante para programar una visita presencial y poder realizar una validación fehaciente de identidad in-situ, según el proceso descrito en el punto *2.1.1. Verificación de identidad no completada o no exitosa*.

17) **Finalizar Solicitud:** el sitio web THSC por medio de una conexión segura envía los datos de la solicitud al sistema de Autoridad de Registro (SAR) de Thomas Signe.



18) **Generación del certificado:** el certificado se genera en un sistema criptográfico FIPS 140 nivel 3, llamado HSM Centralizado. (Hardware Security Module) y el acceso al certificado es de control exclusivo a su titular, según Artículo 5 del Decreto 24 y cumpliendo con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).

19) **Activación del Certificado:** el solicitante del certificado, Realiza La activación de su Certificado.



20) **Generar Contraseñas de Fortress y Certificado FEA:** el solicitante del certificado debe crear sus Claves de Usuario y Clave de su Certificado.

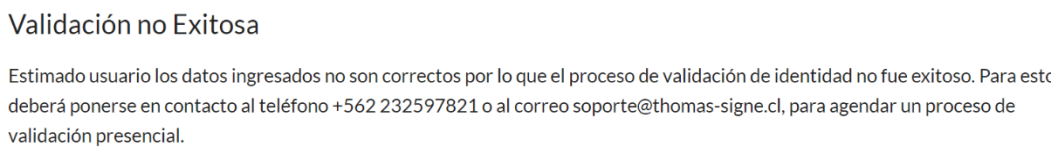
21) **Envío de email al solicitante** con la documentación del proceso e instrucciones de uso. Se incluirá el documento de términos y condiciones aceptado en los pasos anteriores según Anexo I, incluido en este documento y el enlace a las instrucciones de uso del certificado custodiado en el HSM centralizado, en la sección de Soporte – Manuales de la página web de Thomas Signe.

Soporte (thomas-signe.cl)

Para poder usar el certificado FEA en HSM Centralizado ver el apartado 3.

2.1.1. VALIDACIÓN DE IDENTIDAD NO COMPLETADA O NO EXITOSA

En cualesquiera de las validaciones realizadas durante la emisión del certificado y no se haya completado exitosamente, se le mostrará un mensaje como el que sigue, para realizar una validación de identidad presencial y continuar con el proceso de emisión del certificado. Realizada la verificación fehaciente de identidad in-situ, recibirá un enlace en su correo electrónico para continuar con el proceso en el paso 20.



El proceso de verificación de identidad presencial se realiza de la siguiente forma, indicada en las prácticas y políticas de certificación.

Una vez concretada la cita, Thomas Signe será visitado o visitará en el domicilio u oficina o por el Solicitante para realizar la validación de identidad, llevando a cabo las siguientes actividades:

- Validar presencialmente la identidad del Solicitante según el articulo 12 letra e) de la ley No 19.799
- Validación física del carné, Tomar firma, huella dactilar y confirmar el correo del Solicitante en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.
- Tomar una fotografía del Solicitante
- Mediante la conexión de internet exclusiva del Operador de registro este deberá ingresar mediante enlace seguro https las evidencias físicas digitalizadas al sistema SAR, para efectos de custodia digital y prueba de los actos de validación realizados. **Nunca haciendo uso de redes públicas o enlaces privados no seguros. El acceso al Sistema de Gestión de la Autoridad de Registro se realiza con dos factores, usuario y clave (con política de contraseñas) más el certificado de firma electrónica avanzada.**

2.1.2. VALIDACIONES REALIZADAS EN BACKEND DURANTE EL PROCESO

Para la emisión del certificado online, el Sistema de Autoridad de Registro (SAR), realiza las siguientes validaciones antes de la generación del certificado. Estas validaciones son un proceso automatizado de backend del sistema.

1) RUN informado en el proceso de registro sea válido, validando formato.
2) Validar que está informado el nombre y primer apellido
3) Validar que está informado el número serie y fecha de nacimiento de la cédula de identidad
4) Validar que está informado el email
5) Comprobación que el OTP enviado al email del solicitante es correcto.
6) Comprobación de la evidencia de la pasarela de pago ok
7) Comprobación que el RUN informado en el proceso de registro sea igual al de Clave única.
8) Evidencia de proceso correcto en clave única.
9) Verificación de los datos de nombre y apellidos de clave única con los informados en el formulario.
10) Mecanismo complementario de verificación fehaciente de identidad:
    a. Evidencia de Buró de la vigencia de la cédula de identidad
    b. Evidencia del score del Buró (4 preguntas de 5 correctas al menos)
11) Evidencia de aceptación de condiciones y lectura de las mismas.

En caso de cumplir las condiciones anteriores se procede a la emisión del certificado online y se procede a la activación del certificado con usuario de HSM Centralizado y Contraseña del certificado.

El certificado se genera en un sistema criptográfico FIPS 140 nivel 3, llamado HSM Centralizado. (Hardware Security Module) y el acceso al certificado es de control exclusivo a su titular, según Artículo 5 del Decreto 24 y cumpliendo con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).

2.1.3.ANEXO I: TÉRMINOS Y CONDICIONES DEL SERVICIO

TERMINOS Y CONDICIONES DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA

EN SU CALIDAD DE SUSCRIPTOR DE CERTIFICADO DE FIRMA ELECTRONICA USTED DEBERA DAR LECTURA DETALLADA AL SIGUIENTE ACUERDO EN FIN DE SOLICITAR, RENOVAR O REVOCAR SU SOLICITUD DE CERTIFICADO DE FIRMA ELECTRONICA. LA ACEPTACION DEL SIGUIENTE ACUERDO ESTA SUJETO A LOS SIGUIENTES TÉRMINOS Y CONDICIONES

El USUARIO DECLARA:

a) que los datos personales antes señalados son completamente verídicos y están actualizados a la fecha de este instrumento;

b) que solicita el servicio de certificación de firma electrónica por y para sí;

c) haber sido informado sobre los contenidos de este contrato los que conoce y acepta completa y plenamente.

OBLIGACIONES DEL CERTIFICADOR.

Son principales obligaciones del Certificador las siguientes:

a) Mantener un Registro de Acceso Público de Certificados;
b) Tratar los datos proporcionados por el titular del certificado única y exclusivamente para efectos de la certificación contratada teniendo prohibido utilizarlos para otros fines diferentes;
c) Conservar los datos proporcionados por el titular del certificado por a lo menos seis años desde la emisión inicial de los certificados;
d) Publicar en su sitio de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten y las normas legales y reglamentarias vigentes y aplicables en la materia;
e) Comprobar fehacientemente la identidad del solicitante;
f) En caso de cancelación de la inscripción en el registro de prestadores acreditados, o cese voluntario de actividad, comunicar inmediatamente esta circunstancia a cada uno de los USUARIOS y transferir los datos de sus certificados a otro prestador de servicios de certificación o dejarlos sin efecto en caso de oposición a la transferencia comunicada oportunamente por el USUARIO;
g) Mantener contratado un seguro por responsabilidad civil conforme a lo establecido en el artículo 14° de la ley 19.799;
h) Guardar reserva de los datos del USUARIO no divulgándolos con terceros excepto en los casos permitido por la ley y a propósito de la funcionalidad del servicio contratado;
i) Informar al USUARIO de los cambios en las condiciones de este contrato, teniendo el USUARIO 15 días corridos para rechazar dichas modificaciones y en caso de expirar dicho plazo sin hacerlo se entenderán por aceptadas;
j) Respetar en todos sus actos y procesos las disposiciones de la ley 19.628, sobre Protección de la Vida Privada y 19.496 sobre derechos del consumidor y 19.799 sobre documentos y firma electrónica y su Reglamento.
k) Para los casos de usos que corresponda, tomar todas las medidas de seguridad y control de acceso según lo dispuesto en el Decreto Supremo N°24 de 2019, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada con custodia de Certificados en HSM. Asegurando el control de acceso exclusivo por parte del suscriptor al uso del certificado digital en custodia exclusiva del CERTIFICADOR.

OBLIGACIONES DEL USUARIO.

Son obligaciones del USUARIO las siguientes:

a) mantener actualizados sus datos personales proporcionados al CERTIFICADOR;
b) proporcionar una dirección de cuenta de correo electrónico que exprese y tenga directa relación con su nombre, y en caso de que no sea así otorgar declaración jurada ante notario sobre la cuenta que utilice;
c) custodiar adecuada y suficientemente los mecanismos de seguridad del funcionamiento del sistema de certificación proporcionado por el CERTIFICADOR;
d) dar aviso inmediato por los canales oficiales de comunicación al CERTIFICADOR sobre cualquier indicio serio de que la seguridad, autenticidad y uso seguro del certificado hayan sido vulnerados;
e) dar aviso inmediato al CERTIFICADOR y autoridades ante el hurto, robo o extravío de los elementos para la firma electrónica suministrados por el CERTIFICADOR;
f) deber de reserva sobre los datos y procesos del CERTIFICADOR que llegue a conocer en virtud del presente contrato de prestación de servicios.

RESPONSABILIDAD POR USO.

Desde entregado el certificado el CERTIFICADOR no es responsable de la forma en que este sea usado, siendo el USUARIO el único y exclusivo responsable civil, penal y administrativo por su uso, debiendo responder ante los daños o perjuicios causados por el uso indebido y fraudulento del certificado de firma electrónica o en contravención a las prohibiciones impuestas por este contrato. Sin perjuicio de lo anterior el CERTIFICADOR será

responsable de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas, a menos que demuestre haber actuado con la debida diligencia. El CERTIFICADOR es eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites de uso indicados en el certificado siempre y cuando los límites sean reconocibles por terceros.

PROHIBICIONES.

Es prohibido al USUARIO**:**

a) realizar ingeniería inversa a los elementos tecnológicos proporcionados por el CERTIFICADOR;
b) entregar o facilitar a cualquier título el certificado a terceros;
c) destinar el certificado a usos maliciosos, defraudatorios, contrarios a la ley, las buenas costumbres o al orden público;
d) divulgar con terceros los datos y procesos a que tenga acceso y conocimiento en virtud de este contrato de prestación de servicios. Cualquiera contravención a las prohibiciones antes señaladas da derecho al CERTIFICADOR a dar inmediata terminación al servicio pudiendo cancelar la certificación en cualquier momento desde tomado conocimiento de la contravención.

VIGENCIA.

Los certificados de firma electrónica quedarán sin efecto:

a) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;

b) Por revocación del prestador por:

b.1) haberlo solicitado el titular del certificado;

b.2) Por fallecimiento del titular o disolución de la persona jurídica que represente;

b.3) Por resolución judicial ejecutoriada;

b.4) Por incumplimiento de las obligaciones y prohibiciones del USUARIO establecidas en la ley y este contrato. La revocación de un certificado, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el CERTIFICADOR al USUARIO. El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.

RETRACTO.

Conforme a la ley vigente.

IUS VARIANDI:

Por cambios legales o instrucciones de la autoridad pública; cambios tecnológicos o variables de mercado, TSHC podrá introducir variaciones al presente, pudiendo el USUARIO rechazarlas dentro del plazo de 15 días corridos desde comunicadas al correo electrónico, en cuyo caso cualquiera de las partes podrá dar término unilateral a la prestación de servicios sin indemnización de ninguna clase.

CONSTANCIA.

Las partes dejan constancia de que los datos, procesos, mecanismos y demás elementos técnicos y de ingeniería que conforman el servicio prestado por este contrato son de entera y exclusiva propiedad del CERTIFICADOR.

CANALES DE COMUNICACIÓN.

Para todos los efectos de avisos y comunicaciones relativas a la ejecución de este contrato, el uso del servicio contratado y las relaciones de las partes, estas fijan como medio de comunicación oficial, sin perjuicio de otros, las siguientes:

soporte.cl@thsigne.com

Teléfono: +56 2 3259 7822;

Toda la documentación y comunicaciones en formato físico deben ser remitidas por el USUARIO al CERTIFICADOR a **Avenida Presidente Kennedy 5600 oficina 806, comuna de Vitacura, Santiago, Región Metropolitana.**

JURISDICCIÓN.

El presente acuerdo se rige por la ley chilena vigente y aplicable a la materia. Las partes fijan su domicilio civil especial en la provincia de Santiago, Región Metropolitana y someten toda controversia derivada de la interpretación o ejecución de este contrato y sus efectos al conocimiento de los Tribunales ordinarios de justicia con competencia en este territorio jurisdiccional.

MANUAL DEL USUARIO TSCH S.A.

El presente manual se entrega en cumplimiento del deber del CERTIFICADOR de informar al USUARIO previamente a la entrega del certificado de firma electrónica sobre las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, y que son las siguientes:

1. Desde aceptada la solicitud de certificación por el Acreditador, el uso del Certificado se rige por las normas del contrato y de la ley 19.799 y su Reglamento.
2. La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales. Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel; reputándose legalmente como documentos escritos en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.
3. Lo anterior no es aplicable a los siguientes actos o contratos: a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y c) Aquellos relativos al derecho de familia.
4. Los documentos electrónicos que tengan la calidad de instrumento público deberán suscribirse mediante firma electrónica avanzada.
5. Los Usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas, así como a informar cualquier modificación.
6. El CERTIFICADOR y el USUARIO deben guardar confidencialidad de la información proporcionada a cada uno por el otro en razón de la relación contractual que los liga.
7. Los precios de los servicios de certificación, incluidos cargos adicionales y formas de pago; las condiciones precisas para la utilización del certificado, sus limitaciones de uso y procedimientos de reclamación y de resolución de litigios están publicados en el sitio de internet www.thomas-signe.cl

2.2. PROCESO DE COMPRA ONLINE DE FIRMA ELECTRÓNICA AVANZADA A TRAVÉS DE AGENTE COMERCIAL Y SISTEMA DE AUTORIDAD DE REGISTRO (SAR)

Se explica a continuación el flujo de adquisición de FEA por parte del Solicitante mediante solicitud al Departamento Comercial de Thomas Signe por los canales de comunicación de Thomas Signe:

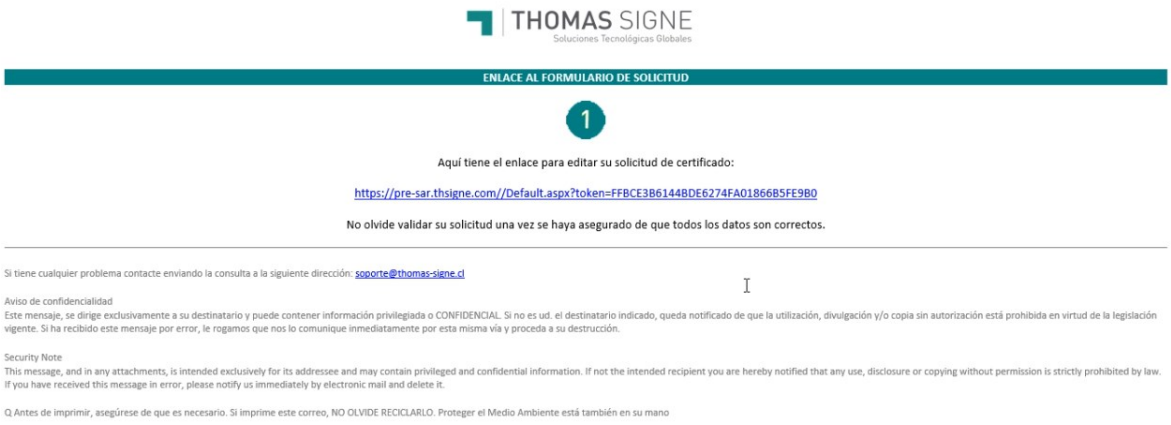
Correo electrónico: comercial@thomas-signe.cl

Teléfono: +562 232597821

Aunque este proceso se inicia a través de un agente comercial, el proceso de validación fehaciente de identidad, según Decreto 24, y la emisión del certificado de FEA se realiza a través de un proceso online.

1- **Contactar a Personal Comercial de Thomas Signe:** El solicitante deberá contactar con el personal comercial de Thomas Signe mediante el correo electrónico que usara para la emisión del certificado para poder adquirir un Certificado de Firma Electrónica Avanzada.
2- **Envío de información:** El departamento comercial de Thomas Signe contactará con el solicitante y enviará al correo indicado por el solicitante la información y condiciones para la emisión del certificado. Tarifas de certificado, tipos de soporte, condiciones generales y tarifas en caso de necesitar verificación presencial. Este proceso asegura la verificación del correo electrónico del solicitante.

3- **Confirmación de la solicitud:** Si el solicitante aprueba la solicitud al departamento comercial de Thomas Signe, éste enviará la solicitud al Operador de Registro de Thomas Signe. La aprobación de la solicitud y el envío de la evidencia del pago realizado mediante transferencia bancaria por medio del correo indicado garantiza que este tiene el control de la cuenta de correo a la que se ha enviado la información comercial. Además, se hace una validación de la transferencia.
4- **Creación de Solicitud:** El Operador de Registro de Thomas Signe debe crear la Solicitud en el sistema SAR. Incluir vigencia del certificado y evidencia de pago según indicaciones del departamento comercial.
5- **Correo Confirmación Datos Solicitante:** El Operador de Registro envía un enlace al correo previamente validado del Solicitante, el cual deberá ingresar para poder confirmar los datos personales. Este correo ya viene confirmado por el departamento comercial.


THOMAS SIGNE
Soluciones Tecnológicas Globales

ENLACE AL FORMULARIO DE SOLICITUD

1

Aquí tiene el enlace para editar su solicitud de certificado:

https://pre-sar.thsigne.com//Default.aspx?token=FFBCE3B6144BDE6274FA01866B5FE9B0

No olvide validar su solicitud una vez se haya asegurado de que todos los datos son correctos.

Si tiene cualquier problema contacte enviando la consulta a la siguiente dirección: soporte@thomas-signe.cl

Aviso de confidencialidad
Este mensaje, se dirige exclusivamente a su destinatario y puede contener información privilegiada o CONFIDENCIAL. Si no es ud. el destinatario indicado, queda notificado de que la utilización, divulgación y/o copia sin autorización está prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción.

Security Note
This message, and in any attachments, is intended exclusively for its addressee and may contain privileged and confidential information. If not the intended recipient you are hereby notified that any use, disclosure or copying without permission is strictly prohibited by law. If you have received this message in error, please notify us immediately by electronic mail and delete it.

Q Antes de imprimir, asegúrese de que es necesario. Si imprime este correo, NO OLVIDE RECICLARLO. Proteger el Medio Ambiente está también en su mano

6- **Ingresar RUN, Serie, Fecha de nacimiento, Teléfono:** el solicitante debe ingresar los datos requeridos para registro del proceso y poder iniciar el proceso de validación fehaciente de identidad con Clave Única más mecanismo complementario según Decreto 24. El campo de email aparece bloqueado, es decir, no se puede modificar, porque ha sido confirmado por el departamento comercial.

7- **Aceptar términos y condiciones:** el solicitante debe aceptar términos y condiciones, según Anexo I incluido en este documento. Puede ver y/o descargar este documento de Términos y condiciones en el enlace del Check.

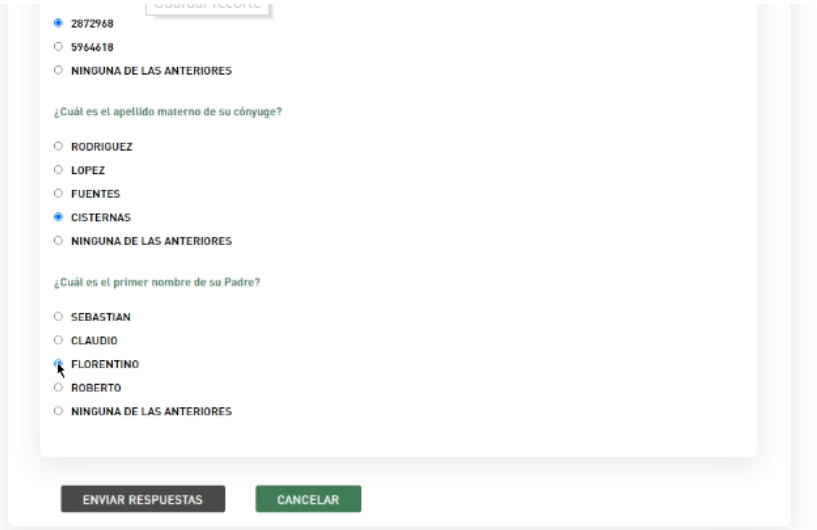
8- **Iniciando el proceso de validación de identidad**. Los siguientes pasos se corresponden con el proceso de verificación fehaciente de identidad más mecanismo complementario para emitir un Certificado de Firma Electrónica Avanzada (FEA) según el Decreto 24.

9- **Validación de Clave Única:** Se debe ingresar el primer factor de Autenticación que es Clave Única. Si no tiene, el proceso de enrolamiento en línea termina sin poder emitir el certificado FEA y se actuará como se describe en el párrafo *2.2.1 Validación de identidad no completada o no exitosa.*

10- **Clave Única retorna RUN, Nombre y Apellidos: Si la clave Única ingresada por el** solicitante es correcta, el sistema Clave Única retorna el RUN, Nombre y Apellidos. Al superar la validación de Clave Única, la plataforma habilita el Desafío de Preguntas que es **el mecanismo complementario de verificación fehaciente de identidad**, según el Decreto 24.

11- **Valida Serie OK, CI Vigente / No Vigente:** Buro Valida el estado de vigencia de la Cedula de identidad

12- **Desafío Preguntas y Respuestas:** si la cedula está vigente, se procede al desafío de preguntas y respuesta efectuadas por BURO, (actualmente EQUIFAX). Este es el mecanismo complementario de verificación fehaciente de identidad según el Decreto 24

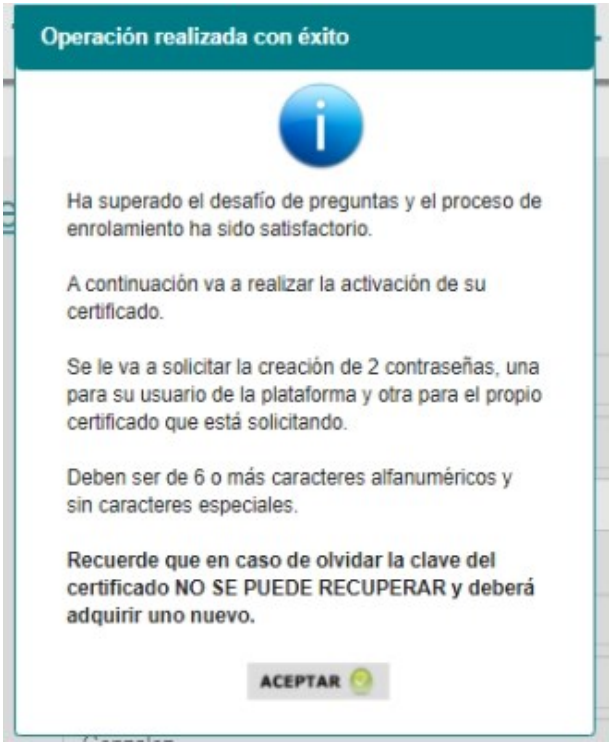


13- **Validar Score Desafío Preguntas:** Se valida el score de respuestas del solicitante, si estas son 4 de 5 correctas el proceso continúa, en caso contrario, el proceso finaliza sin emisión del certificado y se marca para verificación presencial de identidad. Un agente comercial u operador de registro de la Autoridad de Certificación se pondrá en contacto con el solicitante para programar una visita presencial y poder realizar una validación fehaciente de identidad in-situ, según el proceso descrito en el punto *2.2.1. Verificación de identidad no completada o no exitosa*.

14- **Finalizar Solicitud:** Este proceso de validación fehaciente de identidad garantiza que el control de la cuenta de correo la tiene el propio solicitante. El Sistema SAR realiza las validaciones pertinentes del proceso y finaliza la solicitud.

15- Generación del certificado: el certificado se genera en un sistema criptográfico FIPS 140 nivel 3, llamado HSM Centralizado. (Hardware Security Module) y el acceso al certificado es de control exclusivo a su titular, según Artículo 5 del Decreto 24 y cumpliendo con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).

16- Activación del certificado.



17- **Generar Contraseñas de Fortress y Certificado FEA:** el solicitante del certificado debe crear sus Claves de Usuario y Clave de su Certificado del Sistema HSM Centralizado.

CONTRASEÑA DE ACCESO AL HSM CENTRALIZADO

CONTRASEÑA DEL CERTIFICADO

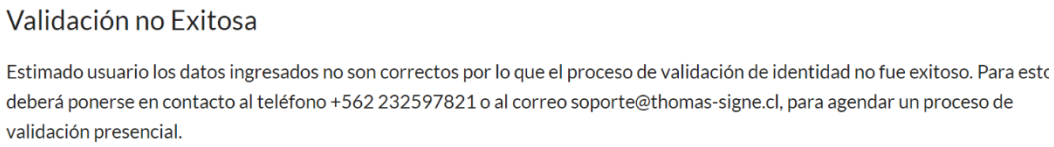
18- **Envío de información:** el solicitante recibirá en su correo (verificado por el Dpto. Comercial en el proceso de contratación) toda la información de la emisión del certificado y las instrucciones de uso. Se incluirá el documento de términos y condiciones aceptado en los pasos anteriores según Anexo I, incluido en este documento y el enlace a las instrucciones de uso del certificado custodiado en el HSM centralizado, en la sección de Soporte – Manuales de la página web de Thomas Signe.

Soporte (thomas-signe.cl)

Para poder usar el certificado FEA en HSM Centralizado ver el apartado 3.

2.2.1. VALIDACIÓN DE IDENTIDAD NO COMPLETADA O NO EXITOSA

En cualesquiera de las validaciones realizadas durante la emisión del certificado y no se haya completado exitosamente, se le mostrará un mensaje como el que sigue, para realizar una validación de identidad presencial y continuar con el proceso de emisión del certificado. Realizada la verificación fehaciente de identidad in-situ, recibirá un enlace en su correo electrónico para continuar con el proceso en el paso 17.



Una vez concretada la cita, Thomas Signe será visitado o visitará en el domicilio u oficina o por el Solicitante para realizar la validación de identidad, llevando a cabo las siguientes actividades:

- Validar presencialmente la identidad del Solicitante según el articulo 12 letra e) de la ley No 19.799
- Validación física del carné, Tomar firma, huella dactilar y confirmar el correo del Solicitante en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.
- Tomar una fotografía del Solicitante
- Mediante la conexión de internet exclusiva del Operador de registro este deberá ingresar mediante enlace seguro https las evidencias físicas digitalizadas al sistema SAR, para efectos de custodia digital y prueba de los actos de validación realizados. **Nunca haciendo uso de redes públicas o enlaces privados no seguros. El acceso al Sistema de Gestión de la Autoridad de Registro se realiza con dos factores, usuario y clave (con política de contraseñas) más el certificado de firma electrónica avanzada.**

2.2.2.VALIDACIONES REALIZADAS EN BACKEND DURANTE EL PROCESO

Para la emisión del certificado a través del Sistema SAR se realizan las siguientes validaciones antes de la generación del certificado. Estas validaciones son un proceso automatizado de backend del sistema.

1) Email validado por la información recibida desde el departamento comercial.
2) RUN válido, validando formato.
3) Informado el número serie y fecha de nacimiento de la cédula de identidad
4) Existencia de evidencia de pago
5) Evidencia de clave única OK
6) Recuperación de datos de nombre y apellidos del sistema de clave única.
7) Mecanismo complementario de verificación fehaciente de identidad:
    a. Evidencia de Buró de la vigencia de la cédula de identidad
    b. Evidencia del score del Buró (4 preguntas de 5 correctas al menos)
8) Evidencia de aceptación de condiciones y lectura de estas.

En caso de cumplir las condiciones anteriores se procede a la emisión del certificado online y se procede a la activación del certificado con usuario de HSM Centralizado y Contraseña del certificado.

El certificado se genera en un sistema criptográfico FIPS 140 nivel 3, llamado HSM Centralizado. (Hardware Security Module) y el acceso al certificado es de control exclusivo a su titular, según Artículo 5 del Decreto 24 y cumpliendo con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).

2.2.3.ANEXO II: REGISTRO DE VERIFICACIÓN PRESENCIAL Y TÉRMINOS Y CONDICIONES DEL SERVICIO

REGISTRO DE HUELLA DACTILAR Y CÉDULA NACIONAL DE IDENTIDAD.

PRIMERO**. Registro de firma manuscrita**. La siguiente es el registro de mi firma manual:

SEGUNDO**. Registro de impresiones dactilares**. Las siguientes son las impresiones de mis huellas dactilares que se indican:

DEDO ÍNDICE DERECHO DEDO PULGAR DERECHO

TERCERO**: Correo Electrónico**. La siguiente es la cuenta de correo electrónico que utilizo personalmente para todos los efectos legales:

CUARTO. **Autorización.** Respecto de las copias y registros señalados anteriormente, autorizo al Certificador de Firma Electrónica THOMAS SIGNE CHILE SA para que las almacene y use en todo lo que sea pertinente y necesario para la certificación de mi firma electrónica, autorización que tendrá vigencia por toda la vigencia de la prestación de dicho servicio.

QUINTO. **Constancia.** Dejo constancia de que las copias y registros señalados anteriormente las entrego para los fines señalados libre y voluntariamente en pleno conocimientos de los derechos que me asisten por la ley 19.628 sobre protección de datos y 19.496 sobre derechos del consumidor.

NOMBRES: _____
APELLIDOS: _____
CÉDULA NACIONAL DE IDENTIDAD _____
ESTADO CIVIL: _____ NACIONALIDAD: _____
FECHA DE NACIMIENTO: _____
OCUPACIÓN/PROFESIÓN: _____
DOMICILIO: PASAJE/CALLE/AVENIDA: _____
NÚMERO: _____ COMUNA: _____
CIUDAD: _____ REGIÓN: _____
MÓVIL: _____ FIJO: _____
CORREO ELECTRÓNICO: _____

TERMINOS Y CONDICIONES DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA

EN SU CALIDAD DE SUSCRIPTOR DE CERTIFICADO DE FIRMA ELECTRONICA USTED DEBERA DAR LECTURA DETALLADA AL SIGUIENTE ACUERDO EN FIN DE SOLICITAR, RENOVAR O REVOCAR SU SOLICITUD DE CERTIFICADO DE FIRMA ELECTRONICA. LA ACEPTACION DEL SIGUIENTE ACUERDO ESTA SUJETO A LOS SIGUIENTES TÉRMINOS Y CONDICIONES

El USUARIO DECLARA:

a) que los datos personales antes señalados son completamente verídicos y están actualizados a la fecha de este instrumento;

b) que solicita el servicio de certificación de firma electrónica por y para sí;

c) haber sido informado sobre los contenidos de este contrato los que conoce y acepta completa y plenamente.

OBLIGACIONES DEL CERTIFICADOR.

Son principales obligaciones del Certificador las siguientes:

l) Mantener un Registro de Acceso Público de Certificados;
Tratar los datos proporcionados por el titular del certificado única y exclusivamente para efectos de la certificación contratada teniendo prohibido utilizarlos para otros fines diferentes;

m) Conservar los datos proporcionados por el titular del certificado por a lo menos seis años desde la emisión inicial de los certificados;

n) Publicar en su sitio de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten y las normas legales y reglamentarias vigentes y aplicables en la materia;

o) Comprobar fehacientemente la identidad del solicitante;

p) En caso de cancelación de la inscripción en el registro de prestadores acreditados, o cese voluntario de actividad, comunicar inmediatamente esta circunstancia a cada uno de los USUARIOS y transferir los datos de sus certificados a otro prestador de servicios de certificación o dejarlos sin efecto en caso de oposición a la transferencia comunicada oportunamente por el USUARIO;

q) Mantener contratado un seguro por responsabilidad civil conforme a lo establecido en el artículo 14° de la ley 19.799;

r) Guardar reserva de los datos del USUARIO no divulgándolos con terceros excepto en los casos permitido por la ley y a propósito de la funcionalidad del servicio contratado;

s) Informar al USUARIO de los cambios en las condiciones de este contrato, teniendo el USUARIO 15 días corridos para rechazar dichas modificaciones y en caso de expirar dicho plazo sin hacerlo se entenderán por aceptadas;

t) Respetar en todos sus actos y procesos las disposiciones de la ley 19.628, sobre Protección de la Vida Privada y 19.496 sobre derechos del consumidor y 19.799 sobre documentos y firma electrónica y su Reglamento.

u) Para los casos de usos que corresponda, tomar todas las medidas de seguridad y control de acceso según lo dispuesto en el Decreto Supremo N°24 de 2019, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada con custodia de Certificados en HSM. Asegurando el control de acceso exclusivo por parte del suscriptor al uso del certificado digital en custodia exclusiva del CERTIFICADOR.

OBLIGACIONES DEL USUARIO.

Son obligaciones del USUARIO las siguientes:

g) mantener actualizados sus datos personales proporcionados al CERTIFICADOR;

h) proporcionar una dirección de cuenta de correo electrónico que exprese y tenga directa relación con su nombre, y en caso de que no sea así otorgar declaración jurada ante notario sobre la cuenta que utilice;

i) custodiar adecuada y suficientemente los mecanismos de seguridad del funcionamiento del sistema de certificación proporcionado por el CERTIFICADOR;

j) dar aviso inmediato por los canales oficiales de comunicación al CERTIFICADOR sobre cualquier indicio serio de que la seguridad, autenticidad y uso seguro del certificado hayan sido vulnerados;

k) dar aviso inmediato al CERTIFICADOR y autoridades ante el hurto, robo o extravío de los elementos para la firma electrónica suministrados por el CERTIFICADOR;

l) deber de reserva sobre los datos y procesos del CERTIFICADOR que llegue a conocer en virtud del presente contrato de prestación de servicios.

RESPONSABILIDAD POR USO.

Desde entregado el certificado el CERTIFICADOR no es responsable de la forma en que este sea usado, siendo el USUARIO el único y exclusivo responsable civil, penal y administrativo por su uso, debiendo responder ante los daños o perjuicios causados por el uso indebido y fraudulento del certificado de firma electrónica o en contravención a las prohibiciones impuestas por este contrato. Sin perjuicio de lo anterior el CERTIFICADOR será responsable de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas, a menos que demuestre haber actuado con la debida

diligencia. El CERTIFICADOR es eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites de uso indicados en el certificado siempre y cuando los límites sean reconocibles por terceros.

PROHIBICIONES.

Es prohibido al USUARIO**:**

e) realizar ingeniería inversa a los elementos tecnológicos proporcionados por el CERTIFICADOR;
f) entregar o facilitar a cualquier título el certificado a terceros;
g) destinar el certificado a usos maliciosos, defraudatorios, contrarios a la ley, las buenas costumbres o al orden público;
h) divulgar con terceros los datos y procesos a que tenga acceso y conocimiento en virtud de este contrato de prestación de servicios. Cualquiera contravención a las prohibiciones antes señaladas da derecho al CERTIFICADOR a dar inmediata terminación al servicio pudiendo cancelar la certificación en cualquier momento desde tomado conocimiento de la contravención.

VIGENCIA.

Los certificados de firma electrónica quedarán sin efecto:

a) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;

b) Por revocación del prestador por:

b.1) haberlo solicitado el titular del certificado;

b.2) Por fallecimiento del titular o disolución de la persona jurídica que represente;

b.3) Por resolución judicial ejecutoriada;

b.4) Por incumplimiento de las obligaciones y prohibiciones del USUARIO establecidas en la ley y este contrato. La revocación de un certificado, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el CERTIFICADOR al USUARIO. El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.

RETRACTO.

Conforme a la ley vigente.

IUS VARIANDI:

Por cambios legales o instrucciones de la autoridad pública; cambios tecnológicos o variables de mercado, TSHC podrá introducir variaciones al presente, pudiendo el USUARIO rechazarlas dentro del plazo de 15 días corridos desde comunicadas al correo electrónico, en cuyo caso cualquiera de las partes podrá dar término unilateral a la prestación de servicios sin indemnización de ninguna clase.

CONSTANCIA.

Las partes dejan constancia de que los datos, procesos, mecanismos y demás elementos técnicos y de ingeniería que conforman el servicio prestado por este contrato son de entera y exclusiva propiedad del CERTIFICADOR.

CANALES DE COMUNICACIÓN.

Para todos los efectos de avisos y comunicaciones relativas a la ejecución de este contrato, el uso del servicio contratado y las relaciones de las partes, estas fijan como medio de comunicación oficial, sin perjuicio de otros, las siguientes:

soporte.cl@thsigne.com

Teléfono: +56 2 3259 7822;

Toda la documentación y comunicaciones en formato físico deben ser remitidas por el USUARIO al CERTIFICADOR a **Avenida Presidente Kennedy 5600 oficina 806, comuna de Vitacura, Santiago, Región Metropolitana.**

JURISDICCIÓN.

El presente acuerdo se rige por la ley chilena vigente y aplicable a la materia. Las partes fijan su domicilio civil especial en la provincia de Santiago, Región Metropolitana y someten toda controversia derivada de la interpretación o ejecución de este contrato y sus efectos al conocimiento de los Tribunales ordinarios de justicia con competencia en este territorio jurisdiccional.

MANUAL DEL USUARIO TSCH S.A.

El presente manual se entrega en cumplimiento del deber del CERTIFICADOR de informar al USUARIO previamente a la entrega del certificado de firma electrónica sobre las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, y que son las siguientes:

8. Desde aceptada la solicitud de certificación por el Acreditador, el uso del Certificado se rige por las normas del contrato y de la ley 19.799 y su Reglamento.

9. La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales. Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel; reputándose legalmente como documentos escritos en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

10. Lo anterior no es aplicable a los siguientes actos o contratos: a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y c) Aquellos relativos al derecho de familia.

11. Los documentos electrónicos que tengan la calidad de instrumento público deberán suscribirse mediante firma electrónica avanzada.

12. Los Usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas, así como a informar cualquier modificación.

13. El CERTIFICADOR y el USUARIO deben guardar confidencialidad de la información proporcionada a cada uno por el otro en razón de la relación contractual que los liga.

14. Los precios de los servicios de certificación, incluidos cargos adicionales y formas de pago; las condiciones precisas para la utilización del certificado, sus limitaciones de uso y procedimientos de reclamación y de resolución de litigios están publicados en el sitio de internet www.thomas-signe.cl

3. USO DEL CERTIFICADO EN HSM CENTRALIZADO

Una vez emitido el certificado, puede usar nuestras plataformas de firma y no será necesario instalar ningún componente. Para el uso de nuestras plataformas de firma, contacte con el departamento comercial. Para usar el certificado FEA en cualquier otra herramienta de firma o autenticación, es necesario instalar en su ordenador una aplicación para poder usar el certificado como si estuviera instalado localmente.

3.1. INSTALACIÓN DEL COMPONENTE PARA EL USO DEL CERTIFICADO

Se podrá hacer uso del certificado digital en cualquier sitio web o aplicación que lo requiera, instalando en el PC el programa Thomas Signe HSM Centralizado Desktop que se puede descargar en este mismo enlace en la sección ***Soporte HSM***.

INSTALACIÓN Y USO DE LOS CERTIFICADOS

Según el soporte, los tipos de certificados que puede obtener son básicamente dos:

Soporte eToken

El certificado electrónico se encuentra en un dispositivo criptográfico. El uso de un dispositivo externo para manipulaciones, lo que garantiza que las operaciones criptográficas ahora permanecen aisladas y no son s

Para proteger tu identidad al tiempo que se mantienen las normas de seguridad y privacidad nuestra comp drivers para utilizarlo. Para poder descargar el certificado debe tener instalado el Thomas Signe RA Deskto

- Drivers para Windows
- Drivers para Mac
- Drivers para Linux

En el Manual de Usuario de eToken puede resolver sus dudas sobre la instalación y uso de este soporte

Soporte HSM

HSM son las siglas de "Hardware Security Module" (Módulo de Seguridad de Hardware). Ideal si desea rec

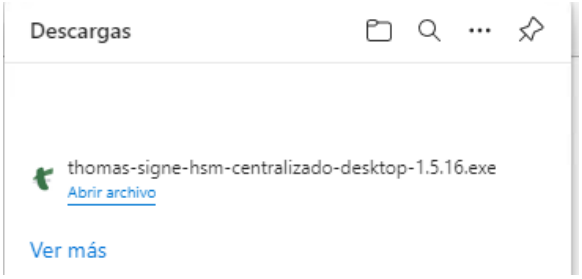
Para poder firmar a través de HSM es requisito INDISPENSABLE descargar el HSM Desktop. Thomas Signe tus certificados centralizados en Thomas Signe HSM Centralizado de forma universal con cualquier otro sit

- Windows
- MAC/iOS
  - macOs
  - Extensión
    - Crome
    - Firefox
  - Componente PKCS#11

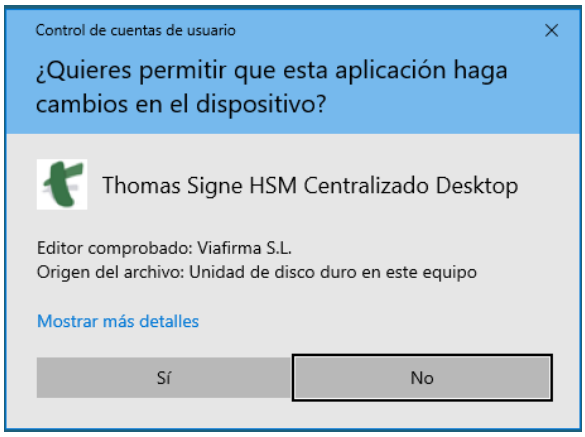
Si tiene alguna duda sobre las funcionalidades y uso del soporte HSM puede consultar, dependiendo del s

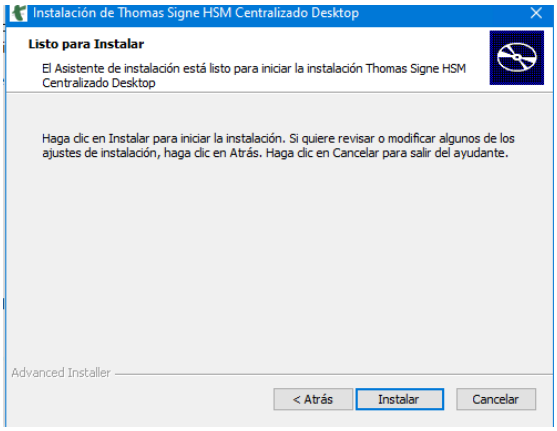
- Windows: Manual de Usuario para HSM Centralizado
- MAC/iOS: Manual de usuario para HSM centralizado MAC

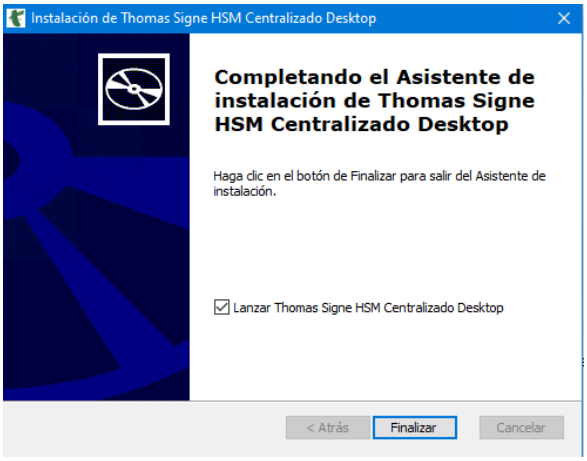
Descargue el componente para instalar en su computador.



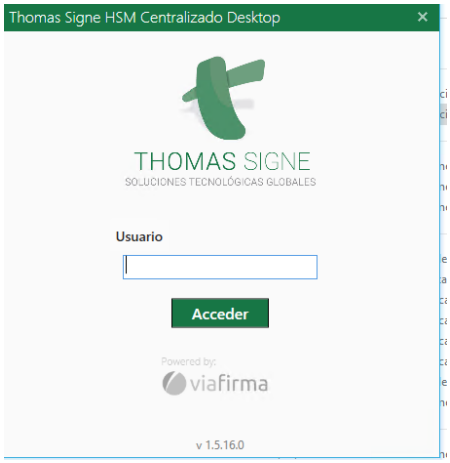
Esta aplicación es un componente que enlaza directamente con el certificado custodiado en el HSM Centralizado.



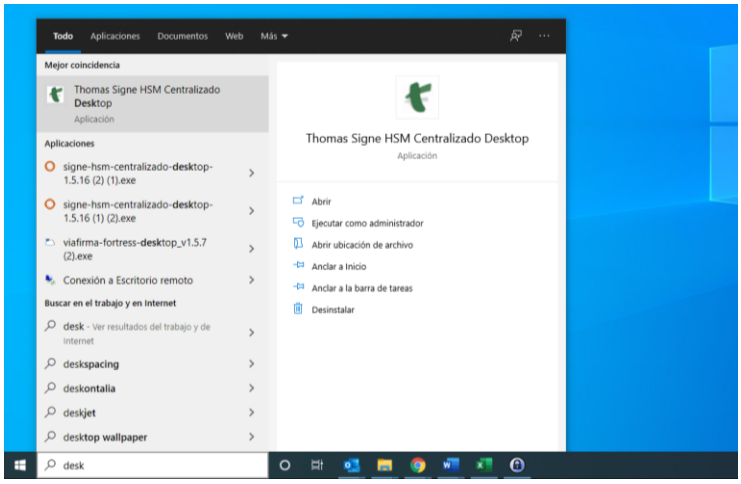




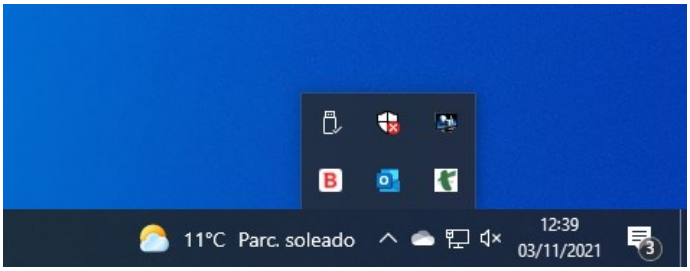
Una vez que se haya instalado el ejecutable, se debe iniciar sesión en la aplicación.



Si la ventana anterior no se ha lanzado automáticamente podrá encontrarse en el buscador del ordenador.



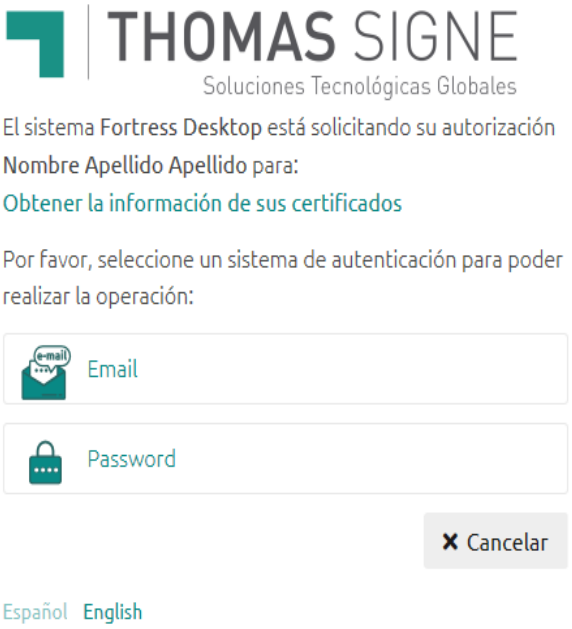
O bien pulsando en mostrar aplicaciones ocultas en la parte inferior derecha de la pantalla.



3.2. USO DEL CERTIFICADO

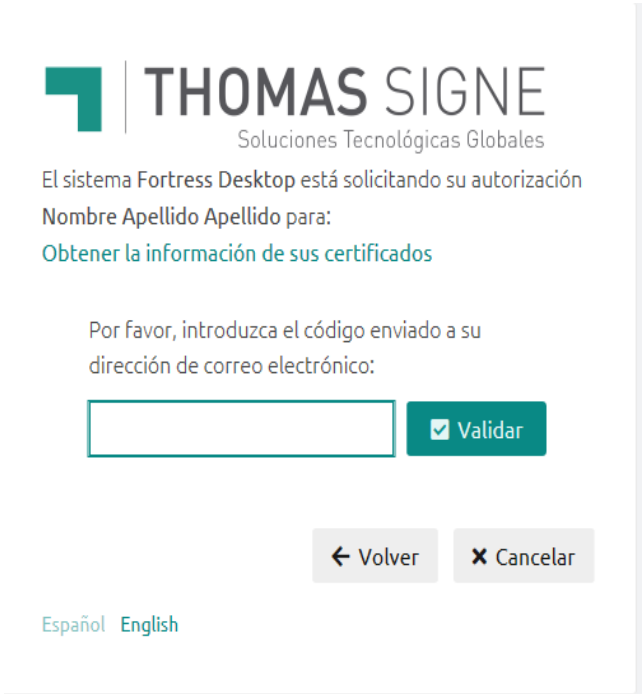
Se debe iniciar sesión cuando se inicia el ordenador o cuando se vaya a utilizar el certificado. Recuerda que el usuario es tu número de documento de identidad.

Para que el certificado esté bajo el control exclusivo del titular, existe un segundo factor de autenticación para el acceso y uso del certificado en el HSM Centralizado. Se solicita un OTP (código de un solo uso) que recibirás en tu email.



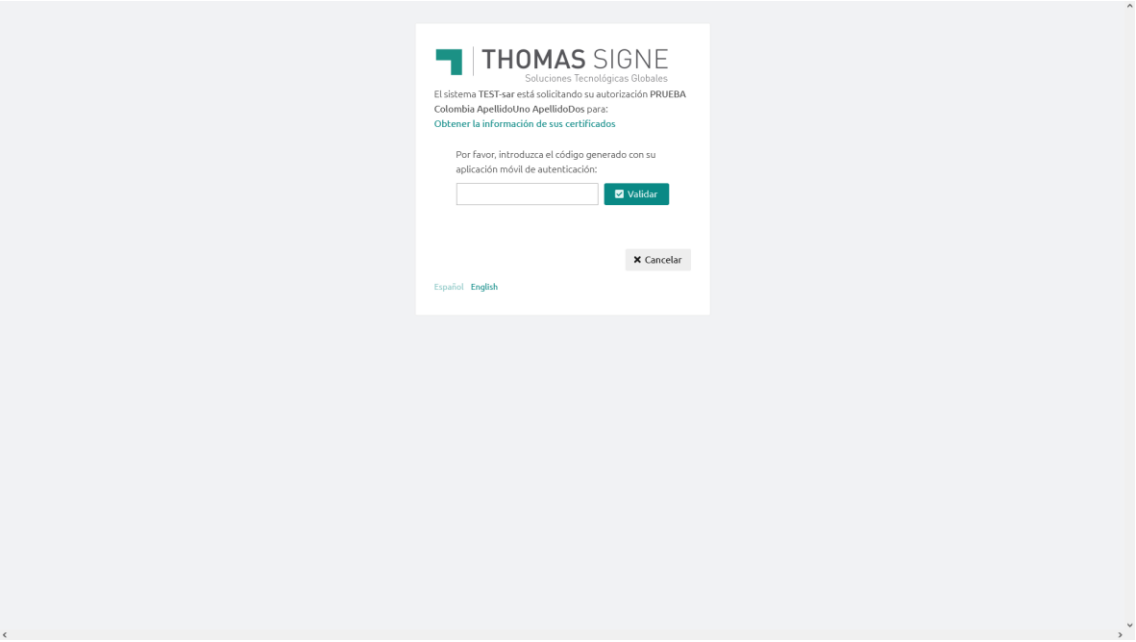
Se recibirá un correo como el que sigue en el correo electrónico asociado al certificado.

El OTP enviado en el correo es el que tiene que introducir en el sistema para poder acceder al uso del certificado.



Ya está el certificado FEA listo para usarlo en cualquiera de las herramientas de firma o de autenticación. En el momento de usarlo para firmar o autenticar, además se solicitará la contraseña del certificado.

Como se indica en las instrucciones durante la emisión del certificado, la contraseña del certificado no se puede recuperar. Si no se dispone de esta contraseña, el certificado tendrá que revocarse y emitirse uno nuevo.

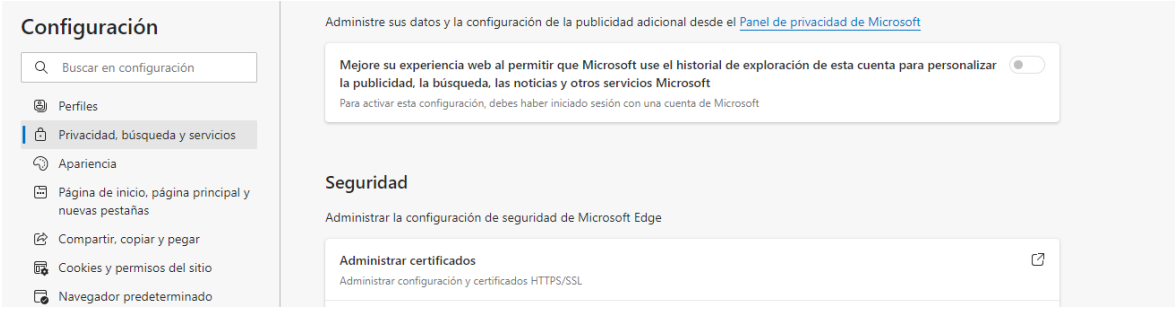


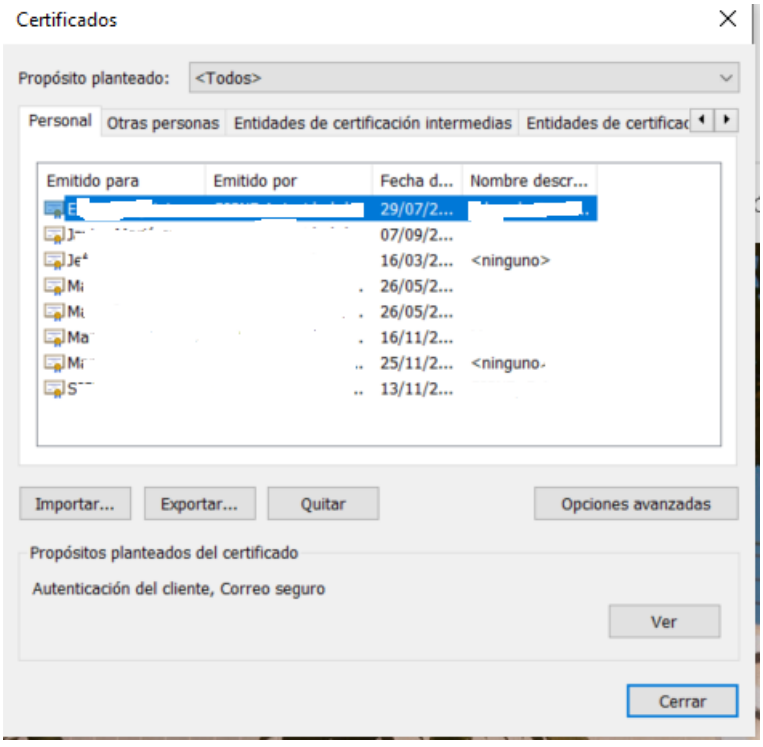
Si quiere comprobar que el certificado está disponible como si fuera local, es necesario abrir cualquier navegador en las opciones de configuración y listar los certificados disponibles.

A continuación, hacemos una breve descripción de la comprobación en algunos de los navegadores más usados. Si necesita más información consulte la ayuda de su navegador.

3.2.1. EDGE

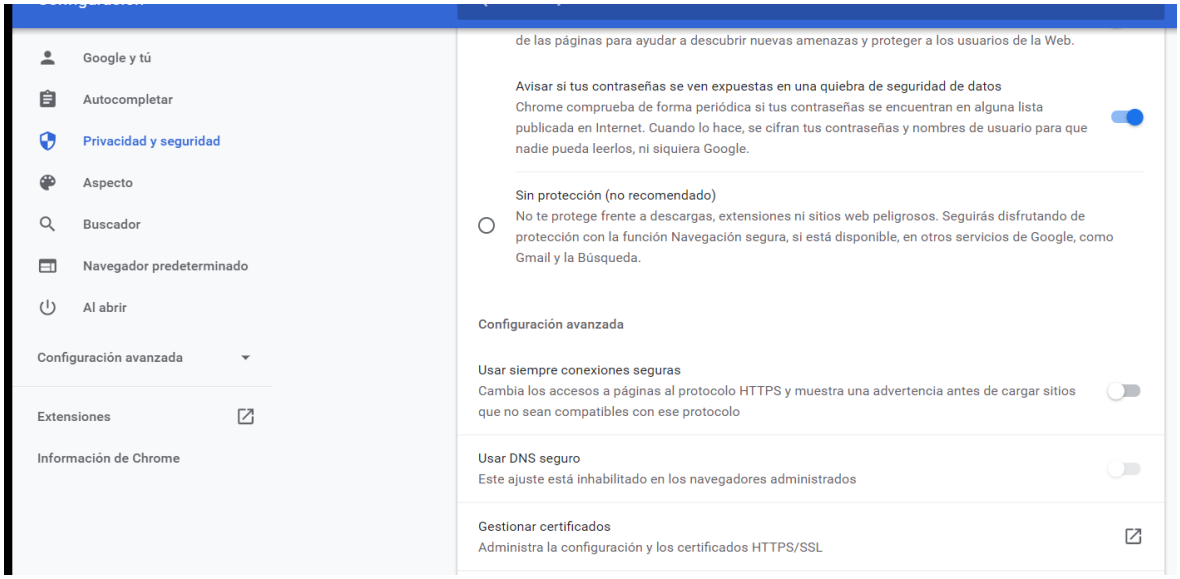
Opciones de configuración / Privacidad búsqueda y servicios / Seguridad / Administrar certificados

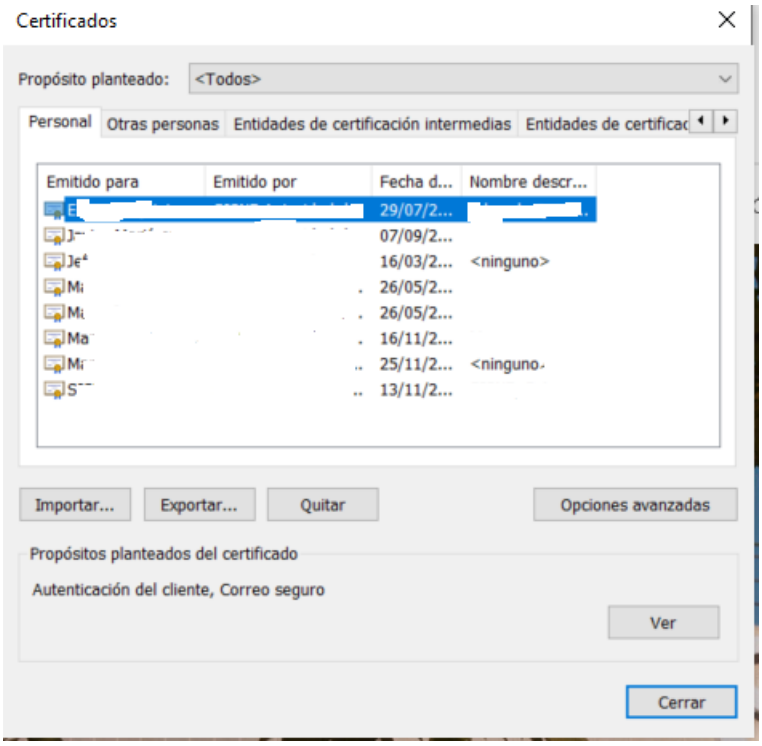




3.2.2. CHROME

Configuración / Privacidad y Seguridad / Gestionar Certificados

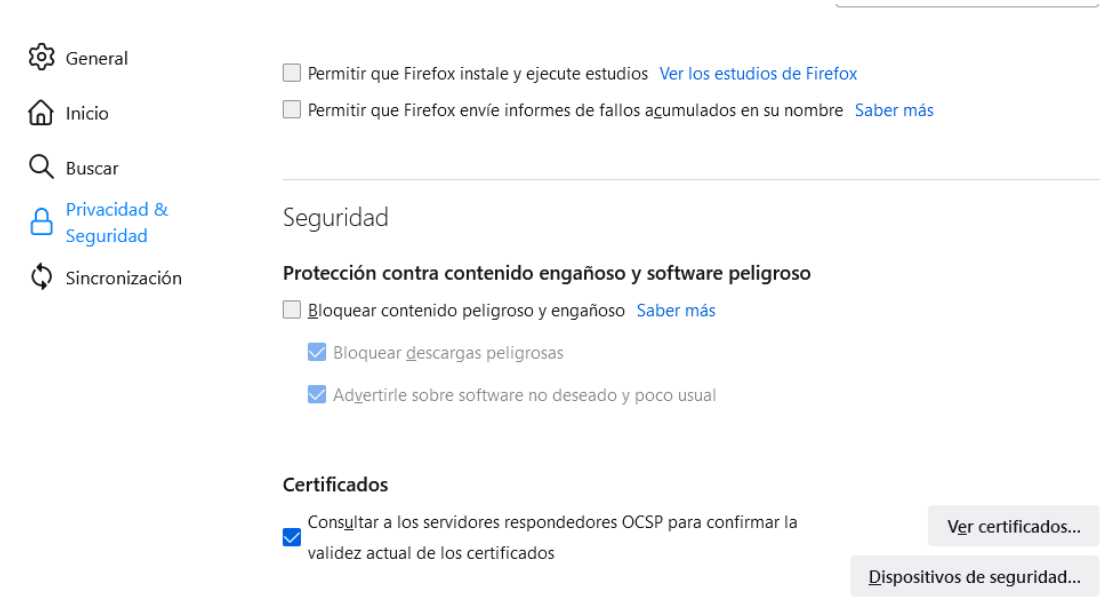


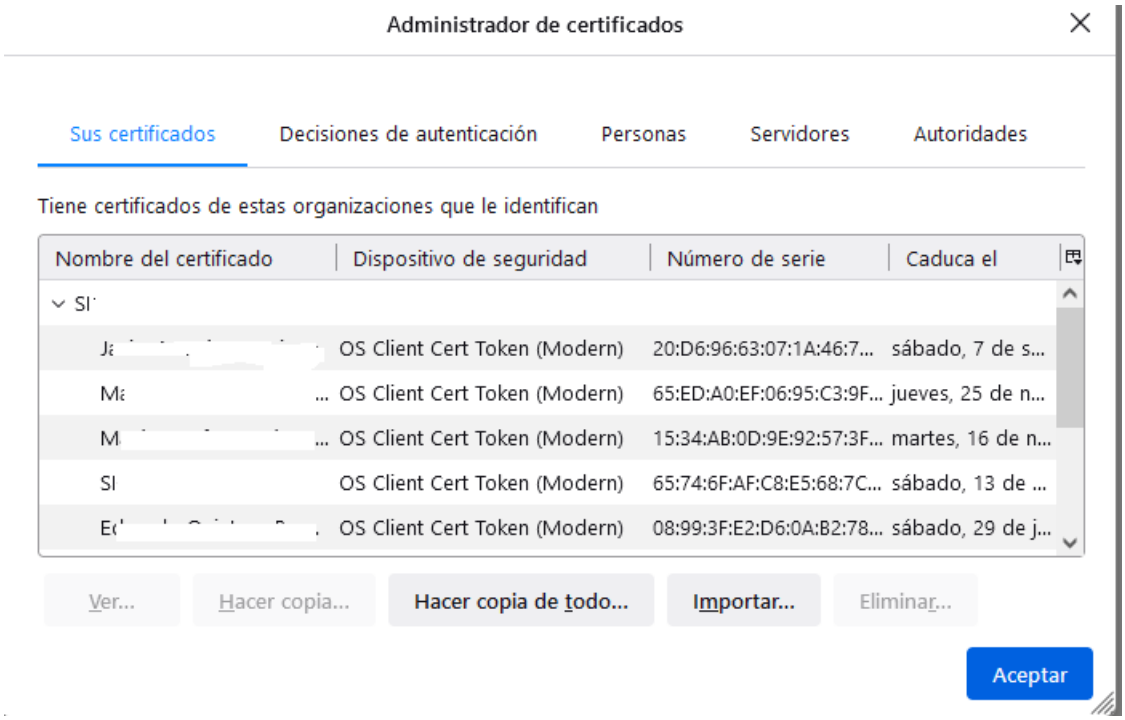


3.2.3. FIREFOX

Ajustes / Privacidad & Seguridad / Certificados

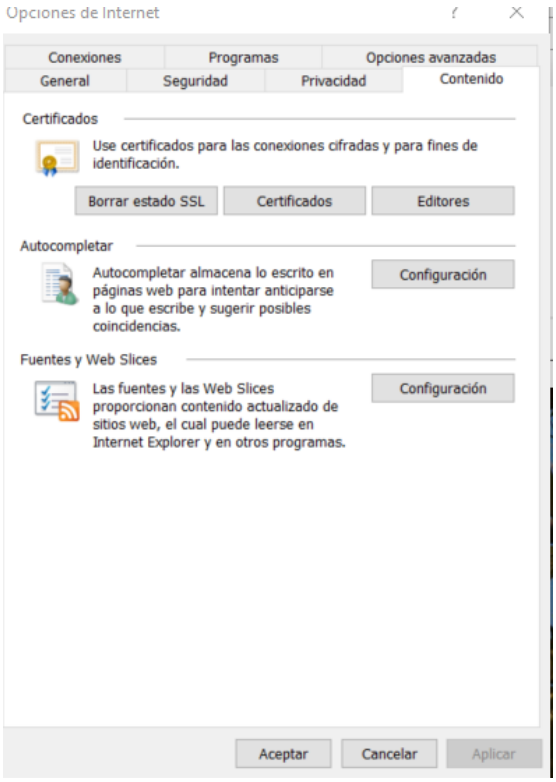
Ver Certificados (Sus Certificados)

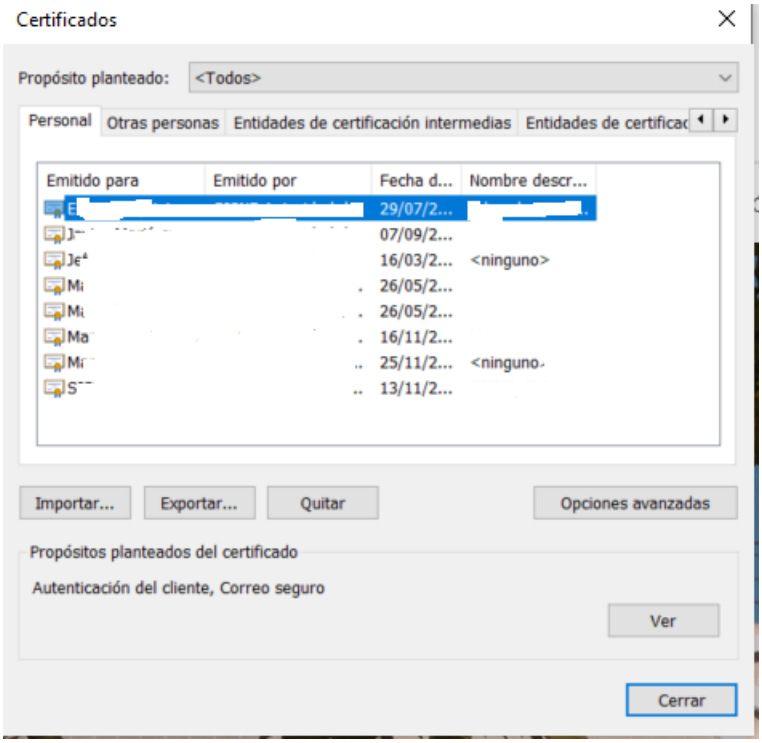




3.2.4. INTERNET EXPLORER

Opciones de Internet / Contenido / Certificados





3.3. RESUMEN

Si el certificado aparece en la lista de certificados en cualquiera de los navegadores, está listo para usarlo en cualquier herramienta de firma o autenticación.

El componente HSM Desktop se iniciará siempre cuando arranque el computador. El proceso descrito en el punto 3.1 sólo debe realizarse una única vez al finalizar la emisión del certificado y en el caso que vaya a usar herramientas de firma y autenticación de otros proveedores que no sean Thomas Signe.

Si usa herramientas de Thomas Signe, no es necesario realizarlo. Las herramientas de Thomas Signe conectan directamente con el HSM Centralizado y no es necesario instalar ningún componente en el computador personal.

El proceso descrito en el punto 3.2 será necesario realizarlo siempre que use el certificado.