



## TÉRMINOS Y CONDICIONES DE USO GENERALES

### A) INTRODUCCIÓN:

**PRIMERA.-** Desde la perspectiva de Prestador de Servicios de Confianza, SIA proporciona los siguientes servicios cualificados de expedición:

- Certificados cualificados de Empleado Público - Nivel medio
- Certificados cualificados de Ciudadano - Nivel medio
- Certificados cualificados de persona física vinculada a empresa - Nivel medio
- Certificados cualificados de Ciudadano – Nivel alto
- Certificados cualificados de persona física vinculada a empresa - Nivel alto
- Certificados cualificados de Empleado Público - Nivel alto
- Certificados cualificados de Empleado Público con seudónimo - Nivel medio
- Certificados cualificados de Empleado Público con seudónimo - Nivel alto
- Certificados cualificados de Empleado Público con seudónimo para el ámbito de Justicia- Nivel medio
- Certificados cualificados de Empleado Público con seudónimo para el ámbito de Justicia - Nivel alto
- Certificados cualificados de Persona Física Representante de Persona Jurídica - Nivel medio
- Certificados cualificados de Persona Física Representante de Persona Jurídica - Nivel alto
- Certificados cualificados de Sello Electrónico
- Certificados cualificados de Sello Electrónico AAPP
- Certificados cualificados de Sello Electrónico PSD2
- Certificados cualificados de Autenticación de Sitio Web – Nivel medio
- Certificados cualificados de Autenticación de Sitio Web PSD2 – Nivel medio
- Certificados cualificados de Sede Electrónica – Nivel alto
- Certificados cualificados de Sede Electrónica – Nivel medio
- Expedición de sellos electrónicos cualificados de tiempo

**SEGUNDA.-** SISTEMAS INFORMATICOS ABIERTOS S.A ha sometido sus servicios cualificados a la auditoría de un Organismo Evaluador de la Conformidad acreditado ante ENAC, tal como establece el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (eIDAS).

### B) CLAUSULAS:

**PRIMERA.-** Marco regulatorio aplicable.

La normativa aplicable es la siguiente:

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Orden ETD 465/2021 de 6 de mayo por la que se regulan los métodos de identificación remota por video para la expedición de certificados electrónicos cualificados
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre).
- Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público (LRJ)
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. (Norma derogada, con efectos de 2 de abril de 2021, por la disposición derogatoria única del Real Decreto 203/2021, de 30 de marzo).
- Resolución de 29 de noviembre de 2012 de la Secretaría de Estado de Administraciones Públicas, por la que publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. (Derogado por Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad).
- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.
- Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación

**SEGUNDA.-** Definición y funciones de las partes.

- El Solicitante es la persona física que, en su propio nombre, solicita la emisión de un certificado y es la persona que dispone del control exclusivo de los datos únicos que se utilizan para crear la firma electrónica (datos de creación de firma) y que actúa en nombre propio.
- El solicitante en el caso de certificados de componente, es la persona jurídica representada por el propio usuario con poderes de representación de la propia entidad, siendo ésta la que asuma la condición de titular/suscriptor.
- El Suscriptor es la entidad con personalidad jurídica que suscribe un contrato con la Autoridad de Certificación (en adelante AC) para la expedición de certificados.
- La Autoridad de Certificación (en adelante AC) es la entidad que actuando como Prestador Cualificado de Servicios de Confianza emitirá, a petición de la Autoridad de Registro, los Certificados que se precisen, de forma automatizada y previa confirmación de la Autoridad de Registro.
- La Autoridad de Registro (en adelante AR) que es la entidad encargada de gestionar el alta (así como las revocaciones y bajas) de los usuarios en una infraestructura de clave pública.
- El Operador, u Oficial de Registro, es la persona que realiza frente al Solicitante las labores de la AR.
- La Declaración de Prácticas de Certificación ("DPC") y la Política de Certificación ("PC") correspondientes al Certificado son los documentos que establecen la forma de funcionamiento de la AC y las características de los certificados emitidos.

**TERCERA.-** Obligaciones de las partes

#### Obligaciones de la AC:

- Actuar relacionando una determinada clave pública con su titular a través de la emisión de los certificados, de conformidad con los términos de la DPC.
- Prestar servicios, en el contexto de la DPC y PCs correspondientes, para la emisión, renovación y revocación de los certificados.
- Comunicar los cambios de la DPC y los presentes términos y condiciones de acuerdo con lo establecido en la DPC.
- Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libre de errores en la entrada de datos.
- Revocar los certificados en los términos recogidos en la DPC.
- Poner a disposición de los solicitantes los certificados correspondientes a la AC.
- Proteger la clave privada de la AC.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.



sia

siacert  
trusted services

- Responder por los daños y perjuicios que causen a cualquier ciudadano en el ejercicio de su actividad cuando incumpla las obligaciones que les impone el marco regulatorio.
- Conservar registrada toda la información y documentación relativa a los certificados reconocidos durante un mínimo de quince años.
- Colaborar con los procesos de auditoría que se realicen sobre la Infraestructura de Certificación.
- Operar de acuerdo con la legislación aplicable.
- En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ella emitidos y al organismo supervisor competente.
- Mantener un repositorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido extinguida.
- No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante

Para certificados de firma o sello electrónico en los casos en que aplique:

- Custodiar los datos de creación de firma del solicitante en un sistema de uso específico que permite la generación, almacenamiento y protección de la Clave Privada, garantizando el acceso exclusivo, con un alto nivel de confianza, a la misma por parte del firmante.
- Custodiar los datos de creación de firma en nombre del firmante protegiéndolos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante.
- No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se aplicarán los procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que ni la AC, ni la AR, ni cualquier otro tercero distintos del firmante tenga acceso a los datos de creación de firma del firmante.
- Solo los prestadores cualificados de servicios de confianza que expidan certificados cualificados que gestionen los datos de creación de firma electrónica en nombre del firmante podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No podrán duplicar los datos de creación de firma para ninguna otra finalidad.
- Utilizar sistemas fiables para almacenar los datos de creación de firma que permitan comprobar su autenticidad e impidan su alteración, facilitando la detección de cualquier cambio que afecte a estas condiciones de seguridad.

Para certificados de autenticación de sitio web y sede electrónica

- En caso de detectar directamente o por notificación de un tercero, cualquier anomalía en el certificado emitido, la AC deberá notificar esta circunstancia al suscriptor en el plazo de 24 horas y deberá investigar y corregir el problema en un plazo de 5 días. La AC podrá revocar unilateralmente el certificado en las primeras 24 horas en caso de detectar que el certificado ha sido mal emitido o en caso de incidente de seguridad grave.
- En caso de revocación del certificado, SIA sustituirá el certificado por uno válido siempre y cuando la anomalía haya podido ser corregida, sin que el suscriptor pueda reclamar ninguna indemnización.



#### • Obligaciones de la AR:

- Respetar lo dispuesto en la DPC y en la PC correspondiente al tipo de certificado que emita conforme a la diligencia de vida y conocimiento técnico experto.
- Respetar lo dispuesto en los contratos firmados con la AC.
- Comprobar la identidad de los solicitantes de certificados según lo descrito en la DPC y PC correspondiente o mediante otro procedimiento que haya sido aprobado por SIA.
- Verificar la exactitud y autenticidad de la información suministrada por el solicitante.
- Informar al solicitante, antes de la emisión de un certificado o el sello electrónico, de las obligaciones que asume, la forma en que debe custodiar el acceso a los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo, del método utilizado para comprobar la identidad del firmante u otros datos que figuren en el certificado, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, de las certificaciones que haya obtenido SIA y los procedimientos aplicables para la resolución extrajudicial de los conflictos que puedan surgir y de la página web donde puede consultar cualquier información de SIA, de la DPC y de la PC correspondiente al certificado.
- Tramitar y entregar los certificados conforme a lo estipulado en esta DPC y en la PC correspondiente.
- Formalizar el contrato de certificación con el firmante o suscriptor según lo establecido por la Política de Certificación aplicable.
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el suscriptor y el firmante de manera segura y totalmente disponible a favor de la AR.
- Informa a la AC las causas de revocación, siempre y cuando tomen conocimiento.
- Realizar las comunicaciones con los firmantes o suscriptores, por los medios que consideren adecuados, para la correcta gestión del ciclo de vida de los certificados. Concretamente realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las revocaciones de los mismos.
- Proporcionar al solicitante todas aquellas copias de documentos que firme, consienta y/o autorice.

#### • Obligaciones del Solicitante:

- Suministrar a las Autoridades de Registro información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de expedición o extinción del certificado.
- Notificar cualquier modificación de los datos suministrados en el proceso de registro o de cualquier modificación de las circunstancias reflejadas en el certificado o sello electrónico.
- Conocer y aceptar las condiciones de utilización de los certificados y sellos electrónicos.
- Utilizar de forma correcta el certificado o sello electrónico y sus claves y no utilizar los datos de creación de firma o clave privada cuando haya expirado el período de validez del certificado o sello electrónico o haya sido revocado.
- Comunicar a SIA a través de los mecanismos que se habilitan a tal efecto, cualquier mal funcionamiento del certificado o sello electrónico.
- Proteger sus datos de activación de firma, y los mecanismos de autenticación, tomando las precauciones razonables para evitar su pérdida, revelación o uso no autorizado.
- Cumplir las obligaciones y supuestos que se establecen para el usuario en la DPC y en el artículo 11 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- No superar los límites que figuren en el certificado o sello electrónico. El firmante o suscriptor asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado o sello electrónico.
- Así mismo, el firmante o suscriptor se responsabiliza de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios de confianza. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios de confianza deberán ser proporcionados por éste al firmante.
- Para certificados de autenticación web, aportar de forma fehaciente la información y documentación que se le requiere según el tipo de certificado de autenticación web solicitado (OV-EV) necesaria para acreditar la existencia de la entidad y su titularidad y control que tiene sobre el dominio, todo ello de acuerdo con los requisitos en cada momento determinen las políticas de la comunidad mundial CabForum en sus "Baseline Requirements" y "EV SSL Certificate guidelines". Por tanto, aceptar expresamente que las prácticas de SIA referidas al servicio de autenticación web y por tanto las condiciones contractuales aplicadas al servicio, puedan sufrir variaciones y cambios que afecten al certificado contratado durante su vigencia, sin que dichos cambios puedan ser motivos de resolución del contrato o indemnización alguna, siempre y cuando vengan motivados por una imposición de la comunidad Cabforum
- Solicitar sin demora la revocación del Certificado y dejar de usarlo y su clave privada asociada, si:
  - Hay algún uso o compromiso real o sospechoso de la clave privada del Suscriptor asociada con la Clave Pública incluida en el Certificado,
  - Si cualquier información del Certificado es o se vuelve incorrecta o inexacta
- Para certificados no remotos, tomar todas las medidas razonables para asegurar el control, mantener la confidencialidad y proteger adecuadamente en todo momento la clave privada que corresponde a la clave pública que se incluirá en el Certificado o Certificados solicitados (y cualquier dato o dispositivo de activación asociado, pines y contraseñas), tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
- Para certificados de servidor seguro, instalar el Certificado solo en servidores accesibles en el(los) subjectAltName(s) enumerado(s) en el Certificado, y de utilizar el certificado únicamente de conformidad con todas las leyes aplicables y únicamente de acuerdo con el Acuerdo de Suscriptor o términos de uso;

#### **CUARTA.- Vigencia de los certificados.**

Los certificados tienen un período de vigencia especificado en la PC. Los Certificados quedarán sin efecto en los siguientes casos:

- Expiración del período de validez del Certificado.
- Modificación de alguno de los datos contenidos en el certificado.
- Circunstancias que afectan a la seguridad de la clave privada, sus claves de acceso o del certificado:
- Compromiso de la clave privada de la AC.
- Compromiso de la claves de la infraestructura o sistemas de la AC, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado.
- Finalización de la relación jurídica entre la AC y el suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al firmante o suscriptor, incluyendo la inhabilitación temporal del firmante para el ejercicio profesional.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
- Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías establecidas en el instrumento jurídico correspondiente o en la DPC.
- Solicitud formulada por el firmante, suscriptor o un tercero autorizado.
- Por la concurrencia de cualquier otra causa especificada en la DPC, PC o legislación aplicable.

#### **QUINTA.- Responsabilidades.**

La AC y la AR responderán de las funciones asignadas respectivamente en estas Condiciones de uso.

Cualquiera que sea la causa por la que pudiera reclamarse responsabilidad a la AC la pretensión indemnizatoria no podrá exceder en conjunto, salvo en el supuesto de culpa grave o dolo, la cifra de 1.000 € y 2000€ para certificados de sitio web EV.

La AC y la AR no serán responsables de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del solicitante, de la entidad y/o Terceros usuarios, ni de la incorrecta utilización de los Certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada por la AC, en particular, el lucro cesante, la pérdida de ingresos o pedidos o pérdida de datos, no dando lugar a ningún tipo de derecho indemnizatorio.

La AC y la AR no será responsable en ningún caso cuando se encuentre ante cualquiera de las circunstancias establecidas en la delimitación de responsabilidades de la DPC

#### **SEXTA.- Protección de datos**



sia

siacert  
trusted services

- Responsable del tratamiento: SISTEMAS INFORMÁTICOS ABIERTOS, S.A (SIA) - NIF: A82733262; Dirección postal: Avenida de Europa nº 2, edificio B, Alcorcón (Madrid) CP 28922; Teléfono: 91 307 79 97; email: [dpo@sia.es](mailto:dpo@sia.es)
- El certificado contendrá el DNI, nombre, apellidos y correo electrónico del Solicitante y otros datos que figuren en la presente solicitud. Usted tiene derecho a acceder, rectificar y/o suprimir los datos, así como otros derechos, como se explica en la información adicional disponible en nuestra página web <https://psc.sia.es/protecciondedatos>.
- SIA tratará los datos que nos facilita en este formulario y las copias de su documento identificativo (anverso y reverso), para la emisión, renovación, suspensión o revocación del Certificado y para la prestación de los servicios de Firma Electrónica. La legitimación de SIA para el tratamiento se deriva del consentimiento otorgado y por obligación legal. Los destinatarios de los datos son la AC y la AR, pudiendo ser publicados y accedidos por terceros de acuerdo a la ley.
- Adicionalmente y cuando se siga un procedimiento autorizado conforme a la Orden ETD 465/2021 de 6 de mayo por la que se regulan los métodos de identificación remota por video para la expedición de certificados electrónicos cualificados:
  - SIA tratará su fotografía y sus datos biométricos de reconocimiento facial.
  - Que autorizo expresamente a la Autoridad de Certificación denominada SISTEMAS INFORMÁTICOS ABIERTOS, S.A. (SIA) para la grabación íntegra del video del proceso de solicitud del Certificado mediante identificación remota y para la toma de fotografías o capturas de pantalla del Solicitante y del documento de identidad utilizado en la identificación.
  - Que quedo informado que en el proceso de grabación del video de Solicitud de Certificado se recogen datos de identificación biométrica del Solicitante.
  - Que autorizo expresamente el tratamiento del video del proceso de solicitud del Certificado, el tratamiento de mis datos biométricos de reconocimiento facial y voz, el tratamiento de los datos personales que figuran en el Formulario y el tratamiento de las copias de mi documento identificativo (anverso y reverso), incluida mi fotografía con la finalidad abajo indicada.
  - Que se conservará durante un período mínimo de tiempo de quince años desde la extinción de la vigencia del certificado obtenido por este medio los siguientes elementos:
    - o Copia de la grabación del video.
    - o Fotos o capturas de la pantalla del Solicitante y del documento de identidad utilizado en las que será claramente reconocibles tanto la persona como el anverso y reverso del documento de identidad.
    - o Los datos extraídos del documento de identificación
    - o Número de teléfono móvil e email.
    - o Los resultados de la verificación automática del sistema
    - o Los resultados de la verificación del Oficial de Registro
    - o El contrato de aceptación de emisión del certificado cualificado
  - En el supuesto de que la AR considerase que existen indicios o sospecha de fraude en el proceso de identificación se conservaran las pruebas del proceso de identificación por el plazo de cinco años.
  - Conforme a lo dispuesto en el artículo 12.7 de la Orden de Identificación Remota la conservación se realizará mediante bloqueo de datos.

#### SEPTIMA.- Legislación y Fuero aplicable

Para la resolución de cualquier conflicto que pudiera surgir en relación con lo estipulado, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Tribunales de Madrid.

#### OCTAVA\_- Información de Contacto

Contacto	<a href="mailto:psc@sia.es">psc@sia.es</a>
Dirección correo	<a href="mailto:psc@sia.es">psc@sia.es</a>
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580
Sitio web:	<a href="https://psc.sia.es">https://psc.sia.es</a>

SIA AC dispone de un servicio 24X7 para atender revocaciones Las solicitudes de revocación pueden realizarse de la siguiente manera

Los suscriptores, los terceros que confían, los proveedores de software de aplicación y otros terceros pueden ponerse en contacto con AC SIA mediante [soc@sia.es](mailto:soc@sia.es) para denunciar incidentes de seguridad relacionados con los certificados proporcionados por el TSP, un supuesto compromiso de la clave privada, un uso incorrecto de certificados, otros tipos de fraude, compromiso, uso indebido o conducta inapropiada relacionada con los certificados o PKI de AC SIA.