



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 Firma Centralizada
- 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 Persona Física Representante de Persona Jurídica - Nivel medio
- Certificados cualificados de Persona Física Representante de Persona Jurídica - Nivel alto
- Certificados cualificados de Sello Electrónico
- 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) N° 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 59/2003, de 19 de diciembre, de firma electrónica. (Texto consolidado, última modificación: 2 de Octubre de 2015).
- Reglamento (UE) N° 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.
- 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).
- 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.
- 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.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- 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.

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 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, para la emisión, renovación y revocación de los certificados.
- Comunicar los cambios de la DPC de acuerdo con lo establecido en el propio documento.
- 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.
- 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.
- 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.



sia

siacert
trusted services

• 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 esta DPC 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 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.
- Informar a la AC las causas de revocación, siempre y cuando tomen conocimiento.
- Realizar las comunicaciones con los firmantes, 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 en 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 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 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- No superar los límites que figuren en el certificado o sello electrónico. El firmante 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 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.

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 del firmante.
- 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, 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 €.

SEXTA.- Protección de datos

A los efectos de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante "LOPD"), artículos 5 y 6, en correlación con el artículo 17 LFE, que he sido informado de y consiento que los datos personales que estoy facilitando en este Formulario así como aquellos otros que facilite en la documentación que se haya de aportar a lo largo del proceso de generación del Certificado, así como a lo largo del ciclo de vida del mismo, pasen a formar parte de un fichero responsabilidad de la AC (actuando la AR a estos efectos como encargado del tratamiento), cuya finalidad será la emisión de Certificados Electrónicos y la prestación de servicios de Firma Electrónica, de conformidad y con el alcance en su difusión que establece la LFE, incluyendo a título meramente enunciativo, la publicación de datos personales en un directorio de certificados electrónicos vigentes, de acceso público (sobre cuyo uso posterior por terceros la AC no puede establecer control alguno y de cuyo uso indebido la AC queda expresamente exonerada). Este tratamiento es necesario para cumplir con la finalidad de mi solicitud. Podré ejercitar mis derechos de acceso, rectificación, cancelación u oposición dirigiéndome a SISTEMAS INFORMATICOS ABIERTOS S.A. por comunicación postal al domicilio indicado en el encabezado.

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.