An Indra company

PDS – SIA TSP

Texto divulgativo del Prestador de Servicios de Confianza SIA

28 de mayo de 2025

AVISO LEGAL

Toda la información contenida en el presente documento y sus anexos, tiene carácter confidencial, y sólo puede ser utilizada con el fin de ser evaluada por el destinatario (sea cliente, proveedor, colaborador, partner, etc.) de la misma y a los solos efectos de conducir los tratos comerciales, o de otra naturaleza, que motivan el envío del documento (en lo sucesivo, el "Propósito").

La información aquí presentada es elaborada por SISTEMAS INFORMATICOS ABIERTOS, S.A.U., (en adelante SIA) sociedad perteneciente al Grupo Indra, con C.I.F. A82733262 y domicilio en Av. de Bruselas, 35, 28108 Alcobendas (Madrid), España y anula y sustituye a las anteriores, y es constitutiva de secreto empresarial (también denominado en determinadas jurisdicciones, secreto comercial), y además, puede estar protegida por derechos de autor, derechos afines, patente, modelo de utilidad y/o diseño industrial por lo que queda terminantemente prohibida su divulgación y/o transmisión a terceros sin el permiso previo, expreso y por escrito de SIA.

Se limitará al máximo el acceso a la información confidencial por parte del personal del destinatario de la misma, o del personal de aquellos terceros a los que SIA haya autorizado a acceder a la información confidencial, limitándose únicamente a aquellas personas cuyo acceso resulte estrictamente necesario, y debiendo el destinatario de la información confidencial garantizar que informa a dichas personas del carácter confidencial y propietario de la información así como del Propósito, asegurando que dicho personal trata la información confidencial única y exclusivamente para el Propósito, y absteniéndose de toda divulgación. Una vez finalizado o concluido el Propósito, el cliente debe restituir a SIA toda la información confidencial sin conservar ninguna copia de la misma, no pudiendo utilizar de ninguna manera, ni para ningún fin la información confidencial y/o propietaria facilitada por SIA salvo que haya sido autorizado para ello previa y expresamente por escrito por SIA.

El destinatario de la información confidencial, después de finalizado el Propósito, no podrá utilizar de ninguna manera ni para ningún fin la información confidencial y/o propietaria facilitada por SIA.

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Descripción
1.0	Abril de 2018	Primera versión.
1.1	Diciembre de 2019	Revisión del documento.
1.2	Junio de 2020	Revisión del documento.
1.3	Noviembre de 2020	Revisión del documento.
1.4	Junio de 2021	Revisión del documento.
1.5	Mayo de 2022	Revisión del documento.
1.6	Enero de 2023	Revisión del documento.
1.7	Mayo de 2025	Revisión documento y adecuación a eIDAS2.

Tabla de contenido

1. INFORMACIÓN DEL TSP

El presente documento recoge, a un alto nivel, la información relativa al Servicio de expedición de Certificados Cualificados Electrónicos, prestado por SIA en su calidad de Proveedor de Servicios de Confianza (TSP).

La elaboración de este documento se ha realizado conforme a las directrices establecidas en la norma ETSI EN 319 411, específicamente en su anexo A, garantizando así su alineación con los estándares europeos aplicables a los servicios de certificación digital.

Este documento tiene un carácter divulgativo y no sustituye en ningún caso a las Políticas del Servicio de Expedición de Certificados Electrónicos Cualificados (PC) ni a la Declaración de Prácticas de Certificación (DPC) de SIA. Ambos documentos, que contienen información detallada sobre los procedimientos, responsabilidades y condiciones del servicio, están disponibles en el sitio web del Proveedor de Servicios de Confianza (TSP).

1.1 Organización responsable del TSP

Contacto	SIA
Entidad	SISTEMAS INFORMATICOS ABIERTOS, S.A.U.
C.I.F.	A82733262
Dirección postal	Avenida de Bruselas, 35 28108 Alcobendas - Madrid (España)
Dirección de correo electrónico	psc@sia.es
Dirección web	https://psc.sia.es
Teléfono	+34 91 307 79 97

Tabla 1: Organización responsable

1.2 Datos de contacto del TSP

Contacto	SIA
Dirección de correo electrónico	psc@sia.es
Dirección postal	Avenida de Bruselas, 35 28108 Alcobendas - Madrid (España)
Teléfono	+34 91 307 79 97
URL	https://psc.sia.es

Tabla 2: Persona de contacto

2. TIPOS DE SERVICIOS

2.1 Tipos de Certificados Emitidos

SIA, como Prestador de Servicios de Confianza (TSP) emite los siguientes tipos de certificados y sellos electrónicos cualificados, cumpliendo con los requisitos establecidos en el Reglamento (UE) 2024/1183, que modifica el Reglamento (UE) nº 910/2014 (eIDAS) en el marco del Marco Europeo de Identidad Digital:

- Certificados cualificados de persona física vinculada a empresa – Nivel medio
- Certificados cualificados de persona física vinculada a empresa – Nivel alto
- Certificados cualificados de ciudadano – Nivel medio
- Certificados cualificados de ciudadano – Nivel alto
- Certificados cualificados de Empleado Público – Nivel medio
- 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 Persona Física Representante de Entidad sin Personalidad Jurídica – Nivel medio
- Certificados cualificados de Persona Física Representante de Entidad sin Personalidad Jurídica – Nivel alto
- Certificados cualificados de Sello Electrónico – Nivel medio
- Certificados cualificados de Sello Electrónico – Nivel alto
- Certificados cualificados de Sello Electrónico AAPP – Nivel medio
- Certificados cualificados de Sello Electrónico AAPP – Nivel alto
- Certificados cualificados de Sello Electrónico PSD2 – Nivel medio
- Certificados cualificados de Sello Electrónico PSD2 – Nivel alto

2.2 Procedimientos de validación

Las terceras partes que confíen en los certificados y sellos electrónicos cualificados emitidos por SIA deberán conocer y aceptar las condiciones establecidas en la Declaración de Prácticas de Certificación (DPC) y en la Política de Certificación (PC) aplicable a cada tipo de certificado.

Asimismo, será su responsabilidad verificar la validez y estado de los certificados a través de los mecanismos de validación habilitados, que incluyen:

- Protocolo OCSP (Online Certificate Status Protocol) para la consulta en tiempo real del estado de los certificados.

- Descarga de CRLs (Listas de Certificados Revocados), disponibles para su comprobación periódica.

Para obtener información detallada sobre los procedimientos de validación, se pueden consultar las Políticas de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC), disponibles en el sitio web del Prestador de Servicios de Confianza (TSP) y referenciadas en el siguiente apartado.

Los certificados emitidos por el Proveedor de Servicios de Confianza (TSP) SIA estarán sujetos a los términos y condiciones de uso definidos en las Políticas de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC) correspondientes.

Estos documentos establecen las condiciones de emisión, aplicación y restricciones de los certificados, garantizando su conformidad con la normativa vigente y su uso adecuado dentro del marco de los servicios de confianza.

2.3 Usos de los certificados

Los certificados emitidos por el Proveedor de Servicios de Confianza (TSP) SIA estarán sujetos a los términos y condiciones de uso definidos en las Políticas de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC) correspondientes.

Estos documentos establecen las condiciones de emisión, aplicación y restricciones de los certificados, garantizando su conformidad con la normativa vigente y su uso adecuado dentro del marco de los servicios de confianza.

Nombre identificativo de la Política	OID de la Política
Política de Certificación de Certificados cualificados de persona física vinculada a empresa – Nivel medio	1.3.6.1.4.1.39131.10.1.2
Política de Certificación de Certificados cualificados de persona física vinculada a empresa – Nivel alto	1.3.6.1.4.1.39131.10.1.15 (QSCD centralizado)
Política de certificación de certificados cualificados de ciudadano – Nivel medio	1.3.6.1.4.1.39131.10.1.3
Política de certificación de certificados cualificados de ciudadano – Nivel alto	1.3.6.1.4.1.39131.10.1.17 (QSCD centralizado)
Política de certificación de certificados cualificados de Empleado Público – Nivel medio	1.3.6.1.4.1.39131.10.1.4
Política de certificación de certificados cualificados de Empleado Público – Nivel alto	1.3.6.1.4.1.39131.10.1.16 (QSCD centralizado)
Política de certificación de certificados cualificados de Empleado Público con seudónimo – Nivel medio	1.3.6.1.4.1.39131.10.1.19
Política de certificación de certificados cualificados de Empleado Público con seudónimo para el ámbito de Justicia – Nivel medio	1.3.6.1.4.1.39131.10.1.19.1
Política de certificación de certificados cualificados de Empleado Público con seudónimo – Nivel alto	1.3.6.1.4.1.39131.10.1.20 (QSCD centralizado)

Política de certificación de certificados cualificados de Empleado Público con seudónimo para el ámbito de Justicia – Nivel alto	1.3.6.1.4.1.39131.10.1.20.1 (QSCD centralizado)
Política de Servicio expedición de sellos electrónicos cualificados de tiempo (TSA)	1.3.6.1.4.1.39131.10.1.6
Política de certificación de certificados cualificados de Persona Física representante de Persona Jurídica – Nivel medio	1.3.6.1.4.1.39131.10.1.8
Política de certificación de certificados cualificados de Persona Física representante de Persona Jurídica – Nivel alto	1.3.6.1.4.1.39131.10.1.18 (QSCD centralizado)
Política de certificación de Certificados cualificados de Persona Física Representante de Entidad sin Personalidad Jurídica – Nivel medio	1.3.6.1.4.1.39131.10.1.8.1
Política de certificación de Certificados cualificados de Persona Física Representante de Entidad sin Personalidad Jurídica – Nivel alto	1.3.6.1.4.1.39131.10.1.18.1 (QSCD)
Política de certificación de Certificados cualificados de Sello Electrónico– Nivel medio	1.3.6.1.4.1.39131.10.1.12
Política de certificación de Certificados cualificados de Sello Electrónico AAPP – Nivel medio	1.3.6.1.4.1.39131.10.1.12.1
Política de certificación de Certificados cualificados de Sello Electrónico PSD2 – Nivel medio	1.3.6.1.4.1.39131.10.1.12.2
Política de certificación de Certificados cualificados de Sello Electrónico – Nivel alto	1.3.6.1.4.1.39131.10.1.13 (QSCD)
Política de certificación de Certificados cualificados de Sello Electrónico AAPP – Nivel alto	1.3.6.1.4.1.39131.10.1.13.1 (QSCD)
Política de certificación de Certificados cualificados de Sello Electrónico PSD2 – Nivel alto	1.3.6.1.4.1.39131.10.1.13.2 (QSCD)

Tabla 3: OID políticas de certificación

3. LÍMITES DE CONFIANZA

Los certificados emitidos por la Autoridad de Certificación (AC) de SIA solo podrán utilizarse para los propósitos expresamente autorizados en la Declaración de Prácticas de Certificación (DPC) y en su correspondiente Política de Certificación (PC). Por tanto, su uso está sujeto a ciertas limitaciones y condiciones que deben ser estrictamente respetadas.

3.1 Restricciones en el uso de los certificados

Los certificados deben emplearse exclusivamente para los fines previstos y autorizados, sin que puedan destinarse a otros usos distintos a los establecidos en la normativa aplicable.

Su uso debe respetar la legislación vigente, incluyendo aquellas disposiciones relacionadas con la importación y exportación de tecnologías criptográficas, que pueden estar sujetas a restricciones en función del país o región.

Se deberá cumplir con los requisitos de archivo de registros y auditoría establecidos en la norma ETSI EN 319 411-1, en particular, en sus apartados 6.4.5 y 6.4.6, así como con las obligaciones derivadas de la normativa vigente en materia de certificación electrónica.

3.2 Exclusión de responsabilidad

La Autoridad de Certificación (AC) y la Autoridad de Registro (AR) no asumirán responsabilidad alguna por:

- Los daños y perjuicios derivados del incumplimiento o la ejecución defectuosa de las obligaciones por parte del solicitante, entidad usuaria o terceros.
- La utilización incorrecta de los certificados y de las claves asociadas.
- Cualquier daño indirecto, incluyendo, entre otros, lucro cesante, pérdida de ingresos, pérdida de pedidos o pérdida de datos que pueda derivarse del uso del certificado o de la información suministrada por la AC.
- Cualquier circunstancia contemplada en la delimitación de responsabilidades establecida en la DPC.

3.3 Verificación del estado del certificado

Si un tercero o usuario final confía en un certificado y sellos electrónicos cualificados sin haber verificado previamente su estado de validez mediante los mecanismos habilitados (OCSP o CRL), no estará cubierto por las garantías establecidas en la Declaración de Prácticas de Certificación (DPC). En consecuencia, no tendrá legitimidad para presentar reclamaciones o emprender acciones legales contra SIA por daños, perjuicios o conflictos derivados del uso o confianza en dicho certificado.

3.4 Solicitud de Revocación

La revocación de un certificado deberá solicitarse siguiendo los procedimientos establecidos en los apartados 4.9.3 y 1.5.2 de la Declaración de Prácticas de Certificación (DPC).

Para garantizar la trazabilidad y seguridad del proceso, el solicitante deberá proporcionar la información requerida y seguir los mecanismos de autenticación definidos en la DPC. La solicitud de revocación podrá realizarse a través de los canales oficiales de contacto indicados en el punto 1.

SIA gestionará la revocación conforme a los tiempos de respuesta definidos en la DPC, garantizando la retirada del certificado del servicio activo y su inclusión en la Lista de Certificados Revocados (CRL) y/o en las respuestas OCSP en el menor tiempo posible. La revocación de un certificado es irreversible. Una vez procesada, el certificado dejará de ser válido para su uso en autenticación de sitios web.

4. OBLIGACIONES DE LOS SUSCRIPTORES

Los suscriptores de los servicios de expedición de certificados y sellos electrónicos cualificados estarán sujetos a las obligaciones establecidas en los convenios o contratos formalizados con el Prestador de Servicios de Confianza (QTSP). Dichos acuerdos regularán las condiciones de uso, responsabilidades y compromisos asumidos por las personas o entidades que soliciten los servicios de expedición de Certificados Electrónicos.

Asimismo, se establece un canal de comunicación para la notificación de incidentes de seguridad relacionados con los certificados emitidos por AC SIA. Los suscriptores, terceros de confianza, proveedores de software de aplicación y otros interesados podrán ponerse en contacto con AC SIA a través del correo electrónico soc@sia.es para reportar, entre otros, los siguientes eventos:

- Compromiso de la clave privada asociada a un certificado.
- Uso indebido o incorrecto de certificados emitidos.
- Incidentes de seguridad relacionados con los servicios de certificación.
- Fraude, abuso o actividades sospechosas vinculadas a la infraestructura de clave pública (PKI) de AC SIA.
- Cualquier conducta inapropiada relacionada con el uso de certificados.

Para obtener información detallada sobre las obligaciones de los suscriptores, se podrá consultar la Política de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC) referenciadas en el apartado 1 del presente documento.

5. OBLIGACIONES DE VALIDACIÓN DE LAS PARTES DE CONFIANZA

Para la validación del estado de los certificados emitidos por TSP SIA, los usuarios y terceras partes aceptantes deberán utilizar los mecanismos especificados en el apartado 2.2 "Procedimientos de Validación" del presente documento.

Asimismo, deberán cumplir con los requisitos establecidos en la norma ETSI EN 319 411-1, en particular, lo dispuesto en los apartados 6.3.5 h) a j) y 6.3.5-03 a).

5.1 Obligaciones de las Terceras Partes Aceptantes

Las terceras partes aceptantes estarán obligadas a:

- Respetar los usos permitidos de los certificados, asegurando que cualquier operación basada en ellos se realice conforme a las restricciones establecidas en sus extensiones, así como en la DPC, PC y los términos y condiciones aplicables.
- Verificar la validez y el estado de revocación de los certificados en los que confían, asumiendo la responsabilidad de dicha comprobación antes de su uso.
- Conocer las garantías y responsabilidades derivadas de la aceptación de un certificado, así como las obligaciones que implica su uso dentro del marco regulatorio y contractual aplicable.
- Notificar cualquier incidente o irregularidad relacionada con un certificado que pueda constituir una causa de revocación, comunicándolo sin demora a TSP SIA.

6. LIMITACIONES DE RESPONSABILIDAD

Las limitaciones de responsabilidad aplicables a los suscriptores estarán sujetas a lo estipulado en los convenios o contratos suscritos entre el Prestador de Servicios de Confianza (QTSP) y las personas o entidades que soliciten los servicios de expedición de certificados y sellos electrónicos cualificados. Dichos acuerdos definirán el alcance de las responsabilidades, así como las condiciones y restricciones bajo las cuales se prestan los servicios.

Para obtener información detallada sobre este apartado, se podrá consultar la Política de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC) referenciadas en el apartado 1 del presente documento.

7. ACUERDOS APLICABLES, POLÍTICA DE CERTIFICACIÓN (PC) Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)

Los acuerdos aplicables en el marco de los servicios proporcionados de emisión de certificados y sellos electrónicos cualificados se encuentran detallados en la Política de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC), así como en los convenios o contratos suscritos entre el Prestador de Servicios de Confianza (TSP) y las personas o entidades que requieran estos servicios.

Para una información más detallada sobre estos acuerdos y las condiciones aplicables, se recomienda consultar la PC y DPC referenciadas en el apartado 1 del presente documento.

8. POLÍTICA DE PRIVACIDAD

El Prestador de Servicios de Confianza (TSP) SIA aplica estrictamente la normativa vigente en materia de protección de datos personales en España, garantizando el cumplimiento de los principios de seguridad, confidencialidad e integridad de la información tratada.

Los datos recopilados en el marco de la prestación de los servicios de emisión de certificados y sellos electrónicos cualificados se incorporan a un fichero registrado en la Agencia Española de Protección de Datos (AEPD), específico para el Proveedor de Servicios de Confianza (TSP).

Toda la información obtenida será almacenada y gestionada por el TSP conforme a los requisitos establecidos en la legislación vigente aplicable, asegurando su protección y uso exclusivo dentro de los límites legales y contractuales del servicio.

9. POLÍTICA DE DEVOLUCIÓN

Las condiciones de reembolso aplicables a los servicios proporcionados por la Autoridad de emisión de certificados y sellos electrónicos cualificados estarán sujetas a lo estipulado en los convenios o contratos formalizados entre el Prestador de Servicios de Confianza (TSP) y las personas o entidades que contraten dichos servicios. Estos acuerdos definirán los criterios, procedimientos y posibles causas para la solicitud de reembolsos, garantizando la transparencia en la gestión de devoluciones.

Para obtener información detallada sobre esta política, se podrá consultar la Política de Certificación (PC) y la Declaración de Prácticas de Certificación (DPC) referenciadas en el apartado 1 del presente documento.

10. LEGISLACIÓN APLICABLE Y RESOLUCIÓN DE CONFLICTOS

10.1 Legislación Aplicable

El presente documento, así como las distintas Políticas de Certificación (PC) y las operaciones derivadas de ellas, se rigen por la normativa vigente en materia de identificación electrónica y servicios de confianza en la Unión Europea y España. En particular, son de aplicación las siguientes disposiciones:

- Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del Marco Europeo de Identidad Digital, reforzando la confianza en las transacciones electrónicas dentro del mercado único digital.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en España.
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.
- Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021.

10.2 Resolución de Conflictos

Para la resolución de cualquier conflicto derivado del presente documento, de las Políticas de Certificación (PC) o de cualquier instrumento jurídico vinculante, las partes acuerdan someterse a la jurisdicción de los Tribunales de Justicia de Madrid, con renuncia expresa a cualquier otro fuero que pudiera corresponderles.

11. ACREDITACIONES DE CONFIANZA Y AUDITORÍAS DE CONFORMIDAD

En cumplimiento de lo establecido en el Reglamento (UE) 2024/1183, que modifica el Reglamento (UE) nº 910/2014 (eIDAS) en relación con el Marco Europeo de Identidad Digital, así como en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en España, el Prestador de Servicios de Confianza (TSP) SIA se encuentra debidamente acreditado e incluido en los siguientes registros oficiales:

- TSL (Trusted Service List): Lista de Prestadores de Confianza de Europa, garantizando su reconocimiento oficial como Prestador Cualificado de Servicios de Confianza.
- Portal de Prestadores de Servicios de Confianza del Organismo Supervisor, asegurando la trazabilidad y supervisión de su actividad conforme a la normativa vigente.

En conformidad con el Artículo 20 del Reglamento (UE) 2024/1183, los servicios proporcionados por la Autoridad de emisión de certificados y sellos electrónicos cualificados son auditados al menos cada 24 meses. Estas auditorías se realizan conforme a las normas diferentes normas ETSI de aplicación, asegurando el cumplimiento de los estándares de seguridad, operatividad y fiabilidad de los servicios.

Asimismo, SIA dispone de un Informe de Evaluación de la Conformidad, emitido por un organismo evaluador independiente, en el marco del Reglamento (UE) 2024/1183, que garantiza el cumplimiento de los requisitos establecidos para la prestación de servicios electrónicos de confianza en el mercado único digital.

An Indra company

SIACERT Trusted Services
psc@sia.es

Av. de Bruselas, 35
28108 Alcobendas, Madrid
T +34 91 307 79 97

sia.es