

Sistemas Informáticos Abiertos, S.A.
Avenida de Europa, 2
Alcor Plaza Edificio B
Parque Oeste, Alcorcón 28922
Alcorcón - Madrid (España)
Telf: (34) 902 480 580 Fax: (34) 91 641 95 13

www.sia.es



Servicio Cualificado de Entrega Electrónica Certificada

Declaración de Prácticas y Políticas

Versión: 1.0

Fecha: 30/01/2019



SI-0013/2006



STI-01/2008



ISO/IEC 15504



ISO 22301

ISO 9001
ISO 14001
BUREAU VERITAS
Certification





INDICE

1. INTRODUCCIÓN	8
1.1 Resumen.....	8
1.2 Nombre del documento e identificación.....	9
1.3 Entidades y personas intervinientes.....	10
1.4 Administración de Políticas	10
1.4.1 Organización responsable.....	10
1.4.2 Persona de contacto	11
1.4.3 Responsables de adecuación de la DPyP	11
1.4.4 Procedimientos de aprobación de esta DPyP	12
1.5 Definiciones y Acrónimos	12
1.5.1 Definiciones	12
1.5.2 Acrónimos.....	15
2. REPOSITARIOS DE PUBLICACIÓN DE LA INFORMACIÓN	16
2.1 Repositorios.....	16
2.2 Publicación de información de certificación.....	16
2.3 Temporalidad o frecuencia de publicación	16
2.4 Controles de acceso a los repositorios	16
3. REQUISITOS DEL SERVICIO	17
3.1 Prestación del servicio.....	17
3.2 Identificación y autenticación en el servicio.....	17
3.3 Tratamiento y procesado de los registros de eventos.....	18
4. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y DE OPERACIONES	19
4.1 Controles de seguridad física.....	19
4.1.1 Ubicación física y construcción	19
4.1.2 Acceso físico	19
4.1.3 Alimentación eléctrica y aire acondicionado	20
4.1.4 Exposición al agua.....	20



4.1.5 Protección y prevención de incendios	20
4.1.6 Sistema de almacenamiento.....	20
4.1.7 Eliminación de los soportes de información	21
4.1.8 Copias de seguridad fuera de las instalaciones.....	21
4.2 Controles de Procedimiento.....	21
4.2.1 Identificación y autenticación para cada usuario.....	21
4.3 Controles de Personal	21
4.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales.....	21
4.3.2 Procedimientos de comprobación de antecedentes	22
4.3.3 Requerimientos de formación	22
4.3.4 Requerimientos de frecuencia de actualización de la información.....	22
4.3.5 Sanciones por actuaciones no autorizadas	22
4.3.6 Requisitos de contratación de terceros	22
4.3.7 Documentación proporcionada al personal.....	22
4.4 Procedimientos de auditoría de seguridad.....	23
4.4.1 Tipos de eventos registrados	23
4.4.2 Periodo de conservación de los registros de auditoría	24
4.4.3 Protección de los registros de auditoría	24
4.4.4 Procedimientos de respaldo de los registros de auditoría.....	24
4.4.5 Sistema de recogida de información de auditoría	24
4.4.6 Notificación al sujeto causa del evento	25
4.4.7 Análisis de vulnerabilidades.....	25
4.5 Archivo de registros.....	25
4.5.1 Tipos de eventos archivados.....	25
4.5.2 Periodo de conservación de registros.....	25
4.5.3 Protección del archivo	26
4.5.4 Procedimientos de copia de respaldo del archivo	26
4.5.5 Requerimientos para el sellado de tiempo de los registros.....	26
4.5.6 Sistema de archivo de información de auditoría	26
4.5.7 Procedimientos para obtener y verificar información archivada	26
4.6 Recuperación en casos de desastre natural u otro tipo de catástrofe	27



4.6.1 Procedimientos de gestión de incidentes y vulnerabilidades	27
4.6.2 Continuidad de negocio después de un desastre natural u otro tipo de catástrofe	27
4.7 Cese del servicio	27
5. CONTROLES DE SEGURIDAD TÉCNICA.....	29
5.1 Controles de seguridad informática	29
5.1.1 Requerimientos técnicos de seguridad específicos	29
5.1.2 Evaluación de la seguridad informática	29
5.2 Controles de seguridad del ciclo de vida	29
5.2.1 Controles de desarrollo de sistemas.....	29
5.2.2 Controles de gestión de seguridad	30
5.2.3 Controles de seguridad del ciclo de vida.....	30
5.3 Controles de seguridad de la red.....	30
5.4 Fuentes de tiempo.....	30
6. AUDITORÍAS DE CUMPLIMIENTO Y CONTROLES.....	31
6.1 Frecuencia o circunstancias de los controles	31
6.2 Identificación / cualificación del auditor	31
6.3 Relación entre el auditor y el Prestador	31
6.4 Aspectos cubiertos por los controles	32
6.5 Acciones a emprender como resultado de la detección de deficiencias	32
6.6 Comunicación de resultados	32
7. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD.....	33
7.1 Tarifas.....	33
7.1.1 Tarifas de servicios de confianza	33
7.1.2 Tarifas de otros servicios tales como información de políticas	33
7.2 Responsabilidad Financiera	33
7.2.1 Seguro de responsabilidad civil.....	33
7.3 Confidencialidad de la información y protección de datos	33
7.3.1 Confidencialidad de la información	33
7.4 Protección de datos personales	35
7.5 Derechos de propiedad Intelectual	35



7.6 Obligaciones	35
7.6.1 Obligaciones del Prestador del servicio	35
7.6.2 Obligaciones del Suscriptor	37
7.6.3 Obligaciones del Emisor	37
7.6.4 Obligaciones de los Destinatarios	37
7.6.5 Obligaciones de terceros en el soporte de servicios del PSC	38
7.7 Renuncias de garantías	38
7.8 Responsabilidades	39
7.8.1 Limitaciones de responsabilidades	39
7.8.2 Responsabilidades del Prestador del servicio	39
7.8.3 Responsabilidades del Suscriptor	40
7.8.4 Responsabilidades del Emisor	40
7.8.5 Responsabilidades del Destinatario	40
7.8.6 Delimitación de responsabilidades	40
7.8.7 Alcance de la cobertura	41
7.9 Limitaciones de pérdidas	41
7.10 Periodo de validez	42
7.10.1 Plazo	42
7.10.2 Sustitución y derogación de la DPyP	42
7.10.3 Efectos de finalización	42
7.11 Notificaciones individuales y comunicaciones con participantes	42
7.12 Reclamaciones y jurisdicción	43
7.13 Legislación aplicable	43
7.14 Conformidad con la Ley aplicable	44
7.15 Clausulas diversas	44
7.15.1 Acuerdo integro	44
7.15.2 Subrogación	44
7.15.3 Divisibilidad	44
7.15.4 Fuerza Mayor	44



RELACION DE TABLAS

Tabla 1 – Datos identificación DPyP.....	10
Tabla 2 – Organización responsable.....	11
Tabla 3 – Persona de contacto.....	11
Tabla 4 – Responsable de adecuación de la DPyP.....	12
Tabla 5 – Repositorios de publicación.....	16



1. INTRODUCCIÓN

1.1 Resumen

Sistemas Informáticos Abiertos, S.A. (en adelante SIA) es un prestador cualificado de servicios de confianza según lo establecido en 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/CE¹.

De conformidad con los requisitos establecidos en el artículo 44 del citado Reglamento, SIA incorpora el Servicio Cualificado de Entrega Electrónica Certificada (en adelante SCEEC²) a la lista de servicios de confianza, fijando en este documento sus políticas y declaración de prácticas.

El marco legislativo en el que se basa lo establecido en esta Declaración de Prácticas y Políticas (en adelante también se referenciará como DPyP) es el siguiente:

- 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 (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- REGLAMENTO DE EJECUCIÓN (UE) 2015/1502 DE LA COMISIÓN de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)³.

¹ El Reglamento (EU) Nº 910/2014 también es conocido como Reglamento eIDAS.

² También conocido por sus siglas en inglés QERDS, Qualified Electronic Registered Delivery Service. Al proveedor de este tipo de servicios se les denomina Qualified Electronic Registered Delivery Service Provider (QERDSP).

³ RGPD o sus siglas en inglés GDPR, General Data Protection Regulation.



- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- DIRECTIVA (UE) 2017/1564 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de septiembre de 2017 sobre ciertos usos permitidos de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos, y por la que se modifica la Directiva 2001/29/CE relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

La DPyP incluye, entre otras, las obligaciones que las partes se comprometen a cumplir para la gestión de los datos de registro de los usuarios, todas las actividades encaminadas a la gestión de las evidencias y los documentos relativos a las notificaciones electrónicas, y sirve de guía en la relación entre SIA y los usuarios de sus servicios telemáticos.

Esta DPyP recoge la política del servicio, así como la declaración del nivel de garantía ofrecido, mediante la descripción de las medidas técnicas y organizativas establecidas para garantizar el nivel de seguridad del Servicio Cualificado de Entrega Electrónica Certificada. Concretamente, en el envío de las notificaciones electrónicas, recogida, sellado y custodia de las evidencias del proceso de entrega electrónico.

En consecuencia, todas las partes involucradas tienen la obligación de conocer la DPyP y ajustar su actividad a lo dispuesto en la misma.

Esta DPyP asume que el lector conoce los conceptos de infraestructura de clave pública, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

Todos los servicios Web publicados por el Prestador, contemplan las características de accesibilidad necesaria y posible, en función de los medios disponibles, y de la seguridad aplicable.

1.2 Nombre del documento e identificación

Nombre del documento	Servicio Cualificado de Entrega Electrónica Certificada. Declaración Prácticas y Políticas
Versión del documento	1.0



Estado del documento	Vigente
Fecha de emisión	30/01/2019
Fecha de caducidad	No aplicable
OID	No aplicable
Ubicación de la DPyP	https://psc.sia.es/

Tabla 1 – Datos identificación DPyP

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- SIA como órgano competente de la gestión del servicio y como Prestador Cualificado de Servicios de Confianza.
- El Suscriptor es la entidad con personalidad jurídica que suscribe un contrato con el proveedor del servicio para el envío de notificaciones electrónicas certificadas.
- El Emisor es la Unidad de Negocio o persona física ligada al Suscriptor que realiza el envío de las notificaciones electrónicas certificadas.
- El Destinatario es la persona física o jurídica a la que se realiza el envío de notificaciones electrónicas certificadas.

1.4 Administración de Políticas

1.4.1 Organización responsable

Esta Declaración de Prácticas y Políticas es propiedad de SIA.

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2



	Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 2 – Organización responsable

1.4.2 Persona de contacto

Contacto	psc@sia.es
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 3 – Persona de contacto

1.4.3 Responsables de adecuación de la DPyP

La autoridad con atribuciones para realizar y aprobar cambios sobre la Declaración de Prácticas y las Políticas de SIA es el responsable de la Administración de Políticas. Los datos de contacto vienen detallados en la siguiente tabla:

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B



	Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 4 – Responsable de adecuación de la DPyP

La Autoridad de Administración de Políticas también es responsable de definir las políticas, las condiciones de uso y los contratos correspondientes.

1.4.4 Procedimientos de aprobación de esta DPyP

El procedimiento de aprobación de la DPyP garantiza, mediante la adecuada validación por parte de la Autoridad de Administración, que las modificaciones a realizar cumplen con los requisitos reflejados en la declaración de prácticas y en las políticas.

En el caso de que el responsable de la Administración de Políticas juzgue que los cambios a la especificación puedan afectar a las condiciones del servicio se comunicará a los Suscriptores, Emisores, y Destinatarios las modificaciones que se han efectuado y que deben consultar la o las nuevas versiones en el repositorio establecido.

Se podrá notificar directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

1.5 Definiciones y Acrónimos

1.5.1 Definiciones

En el ámbito de esta DPyP se utilizan las siguientes definiciones:

- **Autoridad de Registro (AR):** la autoridad de registro es la entidad encargada de gestionar el alta (así como las revocaciones y bajas) de los usuarios en una infraestructura de clave pública. El usuario se debe dirigir a la autoridad de registro para solicitar un certificado de clave pública con la garantía de la autoridad certificadora asociada a la autoridad de registro.

En definitiva, realiza las tareas de identificación de los solicitantes, comprobación de la documentación acreditativa de las circunstancias que constan en los certificados así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los certificados.



- **Certificado de firma electrónica:** una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.
- **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I de eIDAS.
- **Confidencialidad:** la confidencialidad es la capacidad de mantener un documento electrónico inaccesible a todos los usuarios, salvo a una determinada lista de personas. De este modo, podemos conseguir que las comunicaciones no sean escuchadas por otros y enviar documentos que solo puedan ser leídos por el destinatario indicado.
- **Declaración de Prácticas de Certificación (DPC):** declaración que SIA pone a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita.

La DPC tendrá la consideración de documento de seguridad en el que se detallarán, en el marco de la Ley 59/2003 de firma electrónica y de sus disposiciones de desarrollo, las obligaciones que los Prestadores de Servicios de Certificación se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

- **Documento electrónico:** todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.
- **Firma electrónica:** los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- **Firma electrónica avanzada:** la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS.
- **Firma electrónica cualificada:** una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- **Infraestructura de Claves Públicas (PKI, Public Key Infrastructure):** una PKI determina qué entidades entran a formar parte del sistema de certificación, qué papel juegan dichas entidades, qué normas y protocolos se deben seguir para poder operar dentro del sistema, cómo se codifica y se transmite la información digital, y qué información contendrán los objetos y documentos gestionados por la infraestructura. Todo esto basado en la tecnología de Clave Pública (dos claves).
- **Identificación:** procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados.
- **Identificación electrónica:** el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física.



- **Política de Certificación:** es un documento anexo a la Declaración de Prácticas de Certificación que recoge el ámbito de aplicación, las características técnicas de los diferentes tipos de certificados, el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación, así como sus condiciones de uso.
- **Prestador de Servicios de Confianza (TSP):** una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas.
- **Prestador cualificado de servicios de confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.
- **Servicio de confianza:** el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:
 - a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o
 - b) la creación, verificación y validación de certificados para la autenticación de sitios web, o
 - c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;
- **Servicio de confianza cualificado:** un servicio de confianza que cumple los requisitos aplicables establecidos en el Reglamento eIDAS.
- **Sello electrónico:** datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.
- **Sello electrónico avanzado:** un sello electrónico que cumple los requisitos contemplados en el artículo 36 del Reglamento eIDAS.
- **Sello electrónico cualificado:** un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.
- **Certificado cualificado de sello electrónico:** un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento eIDAS.
- **Sello de tiempo electrónico:** datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.
- **Sello cualificado de tiempo electrónico:** un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 del Reglamento eIDAS.
- **Servicio de entrega electrónica certificada:** un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada.



- **Servicio cualificado de entrega electrónica certificada:** un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44 del Reglamento eIDAS.
- **Datos de validación:** los datos utilizados para validar una firma electrónica o un sello electrónico.
- **Validación:** el proceso de verificar y confirmar la validez de una firma o sello electrónicos.

1.5.2 Acrónimos

En el ámbito de esta DPC se utilizan los siguientes acrónimos:

AR: Autoridad de Registro.

DPC: Declaración de Prácticas de Certificación.

ETSI: European Telecommunications Standard Institute.

OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

PC: Política de Certificación.

TSP: Prestador de Servicios de Confianza, en inglés Trust Services Provider.

RFC: Request For Comments (recomendación emitida por la IETF).

SIA: Sistemas Informáticos Abiertos.



2. REPOSITARIOS DE PUBLICACIÓN DE LA INFORMACIÓN

2.1 Repositorios

Documento	Repositorio
Declaración de Prácticas y Políticas	https://psc.sia.es/QERDS_SIA_DPyP_v1.0.pdf
Términos y Condiciones	https://psc.sia.es/QERDS_SIA_TERMINOS_Y_CONDICIONES_v1.0.pdf

Tabla 5 – Repositorios de publicación

2.2 Publicación de información de certificación

El contenido de esta Declaración de Prácticas y Políticas estará disponible en forma de libre acceso en las direcciones indicadas en el apartado: 2.1 Repositorios.

Nuevas versiones del documento se publicaran en la dirección web indicada sustituyendo a la versión anterior. Se mantendrán publicadas las versiones anteriores de toda la documentación.

2.3 Temporalidad o frecuencia de publicación

La DPyP se publicará en el momento de su aprobación y se volverán a publicar en el momento en que se apruebe cualquier modificación sobre la misma. Las modificaciones se harán públicas en el sitio web indicado en el apartado 2.1 Repositorios.

2.4 Controles de acceso a los repositorios

SIA como Prestador de Servicios de Confianza tiene implantados controles para mantener la integridad de su repositorio interno, de forma tal que:

- Las personas no autorizadas no puedan alterar los datos y documentación publicada.
- Se detecta cualquier cambio técnico que afecte a los requisitos de seguridad.



3. REQUISITOS DEL SERVICIO

3.1 Prestación del servicio

El objetivo del Servicio Cualificado de Entrega Electrónica Certificada es proporcionar una entrega segura y fiable de mensajes electrónicos entre las partes. Se entiende por entrega segura el proceso que contempla las siguientes etapas:

- Carga o subida de la documentación por parte del Emisor al servicio. En este punto se le aplica un sello electrónico y un sellado cualificado de tiempo, con el fin de garantizar la integridad de la misma y el momento de la recepción en el servicio. Una vez subida la documentación al servicio no es posible llevar a cabo modificaciones de la misma por lo que no se realizan notificaciones de este tipo.
- Notificación desde el servicio al Destinatario para indicarle que tiene un mensaje pendiente.
- Acceso del Destinatario al servicio donde podrá descargar el mensaje/documento, aceptarlo, rechazarlo, etc.

Durante todas estas etapas se recopilan evidencias del proceso de notificación y entrega con el propósito de asegurar la responsabilidad legal, garantizando la integridad de los datos, que estos han sido enviados por el Emisor y recibidos por el Destinatario, en los momentos de tiempo registrados.

Las evidencias hacen referencia al conjunto de eventos registrados por SIA como Prestador del Servicio de Confianza en relación a la consecución de las distintas etapas del proceso de notificación y entrega. Estas evidencias serán selladas electrónicamente y custodiadas en un servicio independiente para permitir el acceso posterior a cualquiera de las partes interesadas. Con el fin de garantizar el momento en el que se generaron esas evidencias, también se les aplica un sello cualificado de tiempo.

El sellado electrónico se lleva a cabo con un sello cualificado y el sellado de tiempo se realiza por un servicio cualificado de sello de tiempo. En ambos casos, SIA es el proveedor de estos servicios y su uso se llevará a cabo tal y como está estipulado en la Declaración de Prácticas de Certificación y en las Políticas de Certificación de cada uno.

3.2 Identificación y autenticación en el servicio

Todos los usuarios del servicio están convenientemente identificados y autenticados con el fin de evitar accesos no autorizados a la información de la entrega.

Los usuarios emisores (usuarios del Suscriptor) dispondrán de un certificado cualificado emitido en las condiciones estipuladas en la Declaración de Prácticas de Certificación y en la correspondiente Política de Certificación. Este certificado lo usarán en el acceso al servicio, tanto para subir la documentación de la notificación como para el seguimiento del proceso de notificación.



Los usuarios destinatarios podrán acceder al servicio mediante certificado cualificado emitido por cualquier prestador que esté presente en la lista europea de prestadores de servicios de confianza para la emisión de certificados cualificados. El certificado ha de ser válido y no estar revocado.

En ambos casos, Emisor y Destinatario, el acceso se realiza sobre una conexión segura sobre protocolo TLS y autenticando al usuario que accede con su certificado cualificado.

3.3 Tratamiento y procesado de los registros de eventos

Como servicio cualificado, desde el momento que se produce la subida de la documentación al servicio por parte de un Emisor se comienzan a registrar, sellar y guardar los siguientes eventos:

- Datos de identificación y autenticación del Emisor y Destinatario en el proceso de acceso al servicio.
- Prueba de integridad del contenido que garantice que este no ha sido alterado durante la transmisión. Esto se lleva a cabo con el sello electrónico y el sellado de tiempo que se aplica sobre la documentación.
- Prueba con fecha y hora de:
 - La recepción de la documentación a notificar en la plataforma, enviada por el Emisor.
 - El envío de la notificación al Destinatario.
 - El acceso del Destinatario al servicio cualificado.
 - El acceso del Destinatario, dentro del servicio, al listado de notificaciones o documentos pendientes.
 - La acción o acciones realizadas por el usuario con la notificación o documento (descarga, aceptación, rechazo, etc.).

La información identificada para estos registros de eventos es la que posteriormente se recopila en un único documento descargable por las partes que se genera como informe de la entrega.



4. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y DE OPERACIONES

4.1 Controles de seguridad física

Los aspectos referentes a los controles de seguridad física se encuentran recogidos en detalle en la documentación que SIA ha desarrollado a tal efecto. En este apartado se van a recoger las medidas adoptadas más relevantes.

4.1.1 Ubicación física y construcción

Los edificios donde se encuentra ubicada la infraestructura del Prestador disponen de medidas de seguridad de control de acceso, de forma que solo se permite la entrada a los mismos a las personas debidamente autorizadas, los cuales cumplen los siguientes requisitos físicos:

- Ubicado en emplazamiento específico para evitar daños por posibles incendios.
- Ausencia de ventanas al exterior del edificio.
- Cámaras de vigilancia en las áreas de acceso restringido.
- Controles de acceso basados en tarjeta y contraseña.
- Sistemas de protección y prevención de incendios.
- Protección del cableado contra daños e interceptación de la transmisión de datos.

4.1.2 Acceso físico

El acceso físico a las dependencias del Prestador de Servicios de Confianza donde se llevan a cabo las tareas del servicio está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar, gestionado por un sistema informático que mantiene un registro de entradas y salidas automático.



4.1.3 Alimentación eléctrica y aire acondicionado

Los equipos informáticos del Prestador de Servicios de Confianza están convenientemente protegidos ante fluctuaciones o cortes de suministro eléctrico, que puedan dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener este suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas.

Los equipos informáticos están ubicados en un entorno donde se garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

Se realizan controles periódicos de los generadores y fuentes de energía para validar el correcto funcionamiento.

4.1.4 Exposición al agua

Las instalaciones de SIA donde se encuentran los equipos están protegidas para evitar las exposiciones al agua de los mismos, mediante detectores de humedad y otros mecanismos de seguridad.

Se realizan controles periódicos de estos elementos.

4.1.5 Protección y prevención de incendios

Las instalaciones donde se encuentran los equipos del Prestador cuentan con las medidas adecuadas de protección contra el fuego, tales como detectores de humo sensores iónicos, alarmas, extintores y gas HFC-227 en caso de incendio.

Se realizan controles periódicos de todos estos elementos.

4.1.6 Sistema de almacenamiento

SIA ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva. Las copias de respaldo se almacenan de forma segura.

SIA ha dispuesto planes de copia de respaldo, para toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.



4.1.7 Eliminación de los soportes de información

Se ha adoptado una política de gestión de residuos que garantiza la destrucción de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

4.1.8 Copias de seguridad fuera de las instalaciones

SIA dispone de copias de seguridad en ubicaciones distintas que reúnen las medidas precisas de seguridad y con una separación física adecuada.

4.2 Controles de Procedimiento

Por razones de seguridad, la información relativa a los controles de procedimiento se considera material confidencial. Asimismo, SIA garantiza que sus sistemas se operan y administran de forma segura, y para este propósito establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

4.2.1 Identificación y autenticación para cada usuario

Las personas asignadas para cada rol dentro del Prestador son identificadas para asegurar que solo realizan las operaciones para las que está asignado a través de un auditor.

El acceso a los activos viene definido por estos roles, aportando a la vez, acceso a los mismos por medio de dispositivos seguros.

En cualquier caso, el acceso a cualquier activo del Prestador de Servicios de Confianza requiere, al menos, de un doble factor de autenticación.

4.3 Controles de Personal

4.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

El personal que presta sus servicios en el ámbito del Servicio Cualificado de Entrega Electrónica Certificada posee el conocimiento, experiencia y formación suficientes para el correcto cometido de las funciones asignadas. Para ello, SIA lleva a cabo los procesos de selección de personal que estima necesarios con objeto de que el perfil profesional del empleado se adecúe lo más posible a las características propias de las tareas a desarrollar.



4.3.2 Procedimientos de comprobación de antecedentes

Los procesos de selección de personal son los ya definidos por SIA. Estas prácticas aseguran los requisitos de experiencia, cualificación e historial precisos para cada puesto, sean o no de un rol de confianza.

4.3.3 Requerimientos de formación

SIA provee al personal relacionado con la explotación del servicio de toda la información y documentación necesaria sobre los procedimientos operativos relativos a la misma.

4.3.4 Requerimientos de frecuencia de actualización de la información

SIA ejecuta planes de formación continua, prestando principal interés cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

4.3.5 Sanciones por actuaciones no autorizadas

Se consideran acciones no autorizadas las que contravengan la Declaración de Prácticas y Políticas pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, se suspenderá el acceso de las personas involucradas a todos los sistemas de información de SIA de forma inmediata al conocimiento del hecho.

SIA adoptará las medidas disciplinarias que puedan corresponder sobre la base del incumplimiento acaecido, la gravedad de los hechos y su intencionalidad. Al mismo tiempo SIA se reserva el ejercicio de derechos civiles y penales.

4.3.6 Requisitos de contratación de terceros

Los empleados contratados para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y de requerimientos operacionales empleados por SIA. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

4.3.7 Documentación proporcionada al personal

SIA proporcionará a sus empleados toda la documentación necesaria para el correcto desempeño de sus tareas, incluyendo la necesaria para las tareas descritas en la DPyP y la normativa de seguridad.



4.4 Procedimientos de auditoría de seguridad

4.4.1 Tipos de eventos registrados

Se registraran todos los eventos relacionados con la operación y gestión del sistema, así como los relacionados con la seguridad del mismo, entre otros:

- Arranque y parada de aplicaciones.
- Intentos exitosos o fallidos de inicio y fin de sesión.
- Intentos exitosos o fallidos de crear, modificar o borrar usuarios del sistema autorizados.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal.
- Registros de la destrucción de material que contenga información sensible.
- Informes de compromisos y discrepancias.
- Registros de acceso físico.

Las operaciones se dividen en eventos, por lo que se guarda información sobre uno o más eventos para cada operación relevante. Los eventos registrados poseen, como mínimo, la información siguiente:

- **Categoría:** Indica la importancia del evento.
 - Informativo: los eventos de esta categoría contienen información sobre operaciones realizadas con éxito.
 - Marca: cada vez que empieza y termina una sesión de administración, se registra un evento de esta categoría.
 - Advertencia: indica que se ha detectado un hecho inusual durante una operación, pero que no provocó que la operación fallara.
 - Error: indica el fallo de una operación debido a un error predecible.



- Error Fatal: indica que ha ocurrido una circunstancia excepcional durante una operación.
- **Fecha:** Fecha y hora en la que ocurrió el evento.
- **Autor:** Nombre distintivo de la Autoridad que generó el evento.
- **Rol:** Tipo de Autoridad que generó el evento.
- **Tipo de evento:** Identifica el tipo del evento, distinguiendo, entre otros, los eventos criptográficos, de interfaz de usuario, de librería.
- **Módulo:** Identifica el módulo que generó el evento.
- **Descripción:** Representación textual del evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyos valores variarán dependiendo de los datos sobre los que se ejecutó la operación.

4.4.2 Periodo de conservación de los registros de auditoría

La información generada por los registros de auditoría se mantiene en línea hasta que es archivada. Una vez archivados, los registros de auditoría se conservará, al menos, durante quince (15) años.

4.4.3 Protección de los registros de auditoría

Los ficheros de registros de auditoría, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

Los registros del servicio están protegidos por técnicas criptográficas, de modo que nadie, excepto la aplicación de visualización de eventos, con un adecuado control de acceso, puede acceder a ellos.

4.4.4 Procedimientos de respaldo de los registros de auditoría

SIA realiza copias de seguridad periódicas de los registros de auditoría generados por el servicio.

4.4.5 Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.



4.4.6 Notificación al sujeto causa del evento

No se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento.

4.4.7 Análisis de vulnerabilidades

SIA de acuerdo al procedimiento interno en su política de seguridad, realiza revisiones de discrepancias en la información de los logs y actividades sospechosas periódicamente.

4.5 Archivo de registros

SIA conserva toda la información relevante sobre las operaciones realizadas en el servicio durante los periodos de tiempo estipulados, manteniendo un registro de eventos.

4.5.1 Tipos de eventos archivados

Los tipos de eventos que se registran, entre otros, son:

- Todos los eventos llevan fecha y hora, pero estos, además un sellado de tiempo cualificado:
 - La recepción de la documentación a notificar en la plataforma, enviada por el Emisor.
 - El envío de un correo electrónico al Destinatario con la notificación y un enlace de acceso a la misma.
 - El acceso del Destinatario al servicio.
 - El acceso del Destinatario, dentro del servicio, al listado de notificaciones o documentos pendientes.
 - La acción o acciones realizadas por el usuario con la notificación o documento (descarga, aceptación, rechazo o ninguna acción).
- Logs de auditoría de la sección [Tipos de evento registrados](#).
- Eventos de error en los procesos realizados.

4.5.2 Periodo de conservación de registros

Toda la información y documentación relativa a las notificaciones se conservará durante un mínimo de cinco (5) años.



4.5.3 Protección del archivo

Los archivos de registro están protegidos mediante cifrado, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.

La destrucción de un archivo de registro solo se puede llevar a cabo con la autorización del administrador del sistema, el coordinador de seguridad y el administrador de auditorías de SIA. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres autoridades o del administrador del servicio auditado, y siempre que haya transcurrido el periodo mínimo de retención estipulado en la DPyP. Dicha destrucción requerirá la autorización expresa y por escrito.

4.5.4 Procedimientos de copia de respaldo del archivo

Las copias de respaldo de los archivos de registro se realizarán según las medidas estándar establecidas por SIA para las copias de respaldo del resto de sistemas de información. Esta copia de seguridad se ejecuta de forma automática y se envía al Centro de Respaldo.

4.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de información empleados por SIA garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. Todos los servidores que conforman la infraestructura del Servicio Cualificado de Entrega Electrónica Certificada están sincronizados en fecha y hora. Las fuentes de tiempo utilizadas, basadas en el protocolo NTP (Network Time Protocol), se sincronizan utilizando como referencia la del Real Instituto y Observatorio de la Armada.

4.5.6 Sistema de archivo de información de auditoría

El sistema de recogida de información es interno a la Autoridad y corresponde a SIA.

4.5.7 Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos puedan acceder a ellos. Solo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Administrador de Auditoría que debe tener acceso a las herramientas de verificación y control de integridad del registro del servicio.



4.6 Recuperación en casos de desastre natural u otro tipo de catástrofe

4.6.1 Procedimientos de gestión de incidentes y vulnerabilidades

SIA tiene establecido un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de confianza prestados.

El Plan de Contingencias contempla, entre otros aspectos, los siguientes:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.

En el caso de que se viera afectada la seguridad del servicio, SIA informará a los suscriptores, destinatarios y al organismo supervisor. Tan pronto como sea posible se procederá al restablecimiento del servicio.

4.6.2 Continuidad de negocio después de un desastre natural u otro tipo de catástrofe

SIA restablecerá los servicios críticos de acuerdo con esta DPyP dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencia y continuidad de negocio existente.

SIA dispone de un centro alternativo, en caso de ser necesario, para la puesta en funcionamiento de los sistemas del Servicio Cualificado de Entrega Electrónica Certificada.

4.7 Cese del servicio

En el caso de que SIA como Prestador de Servicios de Confianza cesara la actividad de su Servicio Cualificado de Entrega Electrónica Certificada se procedería a notificar a todos sus clientes, a los auditores, así como, al Organismo Regulador con una antelación de, al menos, dos meses.

Durante el periodo de aviso los clientes podrán solicitar los informes de evidencias, además de los documentos sellados (electrónicamente y con sello cualificado de tiempo) de las notificaciones que todavía tengan pendientes o estén cerrando durante ese periodo de tiempo. El cese de actividad también se publicará, con la antelación indicada, en el sitio web del Prestador.



En especial, se comunicará, en cuanto SIA tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra SIA. Igualmente, comunicará cualquier otra circunstancia relevante que pudiera impedir la continuidad de su actividad.

Una vez cesada la actividad del servicio, SIA archivará los registros y documentación relativa a éste por el periodo de tiempo indicado en la DPYP para el archivado de información y registros.



5. CONTROLES DE SEGURIDAD TÉCNICA

5.1 Controles de seguridad informática

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías tanto externas como internas e inspecciones.

5.1.1 Requerimientos técnicos de seguridad específicos

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionarán a quien acredite la necesidad de conocerlos.

No obstante, respecto a la gestión de la seguridad de la información, se sigue el esquema previsto en la UNE-ISO 27002 (anteriormente denominada ISO 17799), Código de Buenas Prácticas para la Seguridad de la Información.

5.1.2 Evaluación de la seguridad informática

SIA evalúa de forma continua su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así como, la realización continua de controles de seguridad.

5.2 Controles de seguridad del ciclo de vida

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías tanto externas como internas e inspecciones.

5.2.1 Controles de desarrollo de sistemas

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de SIA.



5.2.2 Controles de gestión de seguridad

SIA cuenta con una organización de seguridad encargada de su gestión sobre la base la norma UNE-ISO/IEC 27001:2007 sometida a auditorías periódicas por parte de AENOR.

5.2.3 Controles de seguridad del ciclo de vida

SIA tiene definidos controles de seguridad a los largo de todo el ciclo de vida de los sistemas con posibles impactos en la seguridad de la misma.

5.3 Controles de seguridad de la red

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías tanto externas como internas e inspecciones.

5.4 Fuentes de tiempo

La hora del sistema se encuentra sincronizada con el Real Observatorio de la Armada, siguiendo el protocolo NTP a través de internet. La descripción del protocolo NTP se puede encontrar en RFC5905. Network Time Protocol Version 4: Protocol and Algorithms Specification.



6. AUDITORÍAS DE CUMPLIMIENTO Y CONTROLES

6.1 Frecuencia o circunstancias de los controles

Se realizarán auditorías internas periódicas, generalmente con carácter anual. Asimismo, SIA realizará una auditoría externa cada dos años y llevada a cabo por una entidad reconocida y acreditada con objeto de confirmar que los servicios de confianza cumplen con los requisitos establecidos legalmente.

Con carácter extraordinario se podrán llevar a cabo auditorías específicas frente a posibles incidentes de seguridad y/o por cualesquiera otros motivos aprobados por el Responsable de Seguridad.

Por último, el Prestador de Servicios de Confianza será auditado, al menos cada 2 años por un organismo de evaluación de la conformidad según se establece en el Reglamento eIDAS. Así mismo, se llevará a cabo una revisión de carácter anual de la misma.

6.2 Identificación / cualificación del auditor

Las auditorías pueden ser de carácter tanto interno como externo. En este segundo caso se realizan por empresas de reconocido prestigio en el ámbito de las auditorías. El auditor tendrá cualificación y experiencia acreditadas para la realización de este tipo de tareas.

6.3 Relación entre el auditor y el Prestador

Al margen de la función de auditoría, el auditor externo y la parte auditada (SIA) no deberán tener relación alguna que pueda derivar en un conflicto de intereses. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría. Los auditores son independientes de la actividad que es auditada y están libres de sesgo y conflicto de intereses. Los auditores mantendrán una actitud objetiva a lo largo del proceso de auditoría para asegurarse de que los hallazgos y conclusiones de la auditoría estarán basados sólo en la evidencia de la auditoría.

El equipo auditor es plenamente independiente, habiéndose verificado con anterioridad a estos efectos:

- La falta de vinculación laboral, mercantil, o a favor de apoderamientos con la organización auditada.
- Ningún interés directo o indirecto con la entidad auditada.



- La inexistencia de vínculos de matrimonio, consanguinidad o afinidad hasta el primer grado o consanguinidad colateral hasta segundo grado, con los empresarios, administradores o los responsables del área de sistemas de información y/o seguridad de la información.
- Falta de familiaridad o confianza, por la influencia y proximidad excesiva con los administradores o directivos de la entidad auditada.
- La no ejecución previa de servicios relativos a la definición e implantación de medidas de seguridad en la organización auditada por parte del equipo auditor.
- Los honorarios ofertados, no suponen un porcentaje significativo de la facturación de la compañía.

6.4 Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de SIA con esta DPyP. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por este documento.

En general, serán de aplicación los requisitos establecidos en el artículo 44 del 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 la que se deroga la Directiva 1999/93/CE.

Los controles están en consonancia con los requisitos establecidos en el citado artículo, y es de aplicación la norma técnica ETSI EN 319 521. Además, también son aplicables los controles de las normas actualmente en vigor ETSI EN 319 401 y recomendaciones de las normas ISO/IEC 27002:2013 e ISO/IEC 27005, tal y como se referencia en las normas ETSI anteriormente citadas.

6.5 Acciones a emprender como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. El responsable de la aprobación de las Políticas, en colaboración con el auditor, será el encargado de tomar la determinación de las mismas con la máxima diligencia posible.

6.6 Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría al responsable de la aprobación de políticas de SIA, al gestor de seguridad del sistema, así como a los administradores de las infraestructuras y servicios en los que se detecten las incidencias.



7. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

7.1 Tarifas

7.1.1 Tarifas de servicios de confianza

Los precios de los servicios de confianza serán facilitados a los clientes o posibles clientes por el Departamento Comercial de SIA. Los precios no tendrán contemplado el IVA ni cualquier otro impuesto, tasa o cargo adicional que será por cuenta del cliente.

7.1.2 Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta DPyP, ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

7.2 Responsabilidad Financiera

7.2.1 Seguro de responsabilidad civil

SIA, en su actividad como Prestador de Servicios de Confianza, dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad de Prestador tal y como se define en la legislación española vigente.

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una compañía aseguradora de reconocido prestigio que garantizará la cobertura de los riesgos propios de esta prestación de servicios o aval bancario con una cobertura de 3.000.000 €.

7.3 Confidencialidad de la información y protección de datos

7.3.1 Confidencialidad de la información

SIA dispone de una adecuada política de tratamiento de la información, dentro de la cual se incluyen los modelos de acuerdo que deberán de firmarse por todas las personas que tengan acceso a la información confidencial.



Cumpliendo en todo caso con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

7.3.1.1 Ámbito de la información confidencial

SIA considerará confidencial toda la información que no esté catalogada expresamente como “no confidencial”. No se difundirá información declarada como confidencial sin el consentimiento expreso y por escrito de la entidad u organización que le haya otorgado tal carácter, a no ser que exista una obligación legal de hacerlo.

7.3.1.2 Información no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente DPyP.
- La información estipulada en la Declaración de Prácticas de Certificación y en la Política de Certificación del certificado cualificado, publicadas por SIA.
- Cualquier información cuya publicidad sea impuesta normativamente.

7.3.1.3 Deber de secreto profesional

Todo el personal encargado de la administración, operación y supervisión de los servicios de confianza de SIA mantiene la confidencialidad sobre la información a la que acceden en el ejercicio de sus funciones. Esta obligación se extiende al resto del personal, así como a los contratistas y proveedores a través de sus empleados, y colaboradores de SIA.

Esta obligación de deber de secreto subsistirá aun después de finalizar sus relaciones laborales y/o de prestación de servicios y/o ejecución de proyectos a/en SIA.



7.4 Protección de datos personales

A efectos del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa y pide consentimiento para que los datos personales que se facilitan como parte del registro o uso del Servicio Cualificado de Entrega Electrónica Certificada pasen a formar parte de un fichero responsabilidad del Prestador, cuya finalidad será la gestión de los envíos y notificaciones, de conformidad y con el alcance definido en las prácticas y políticas del servicio.

Este tratamiento es necesario para cumplir con la finalidad del servicio. Los usuarios podrán ejercitar sus derechos de acceso, rectificación, cancelación u oposición dirigiéndose a SISTEMAS INFORMATICOS ABIERTOS S.A. por comunicación postal al domicilio indicado en el [apartado para tal efecto](#).

7.5 Derechos de propiedad intelectual

En los términos establecidos en el Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017, SIA es titular en exclusiva de todos los derechos de propiedad intelectual relativos a los servicios de confianza que presta y al contenido de la presente Declaración de Prácticas y Políticas. Asimismo, SIA es titular de los derechos relativos a cualquier otro documento electrónico o de otro tipo, protocolos, programas de ordenador y hardware, archivos, directorios, bases de datos y servicio de consulta que sean generados y utilizados en el ámbito de actuación como Prestador de Servicios de Confianza.

7.6 Obligaciones

7.6.1 Obligaciones del Prestador del servicio

El servicio prestado por SIA en el contexto de esta DPyP es el Servicio Cualificado de Entrega Electrónica Certificada.

SIA, como Prestador del servicio, está obligado a:

- Comunicar los cambios de la DPyP de acuerdo con lo establecido en el propio documento;



- poner a disposición del público la presente declaración sobre las prácticas y políticas del servicio, en su sitio web, o disponible por cualquier otro medio electrónico, donde se recojan las prácticas y los procedimientos utilizados para cumplir los requisitos del servicio de notificaciones electrónicas cualificadas. No se publicarán elementos que puedan contener información sensible;
- presentar y recoger, aceptados y firmados por el Suscriptor, los términos y condiciones del contrato del servicio antes de iniciar el servicio;
- garantizar la disponibilidad, integridad y confidencialidad de los contenidos asociados a las notificaciones electrónicas mientras están siendo gestionados por el servicio, incluyendo el sello electrónico de los contenidos y las garantías de tiempo ofrecidas por los sellos electrónicos cualificados de tiempo;
- emitir informes que sean conformes con la información y evidencias conocidas en el momento de su emisión, y libre de errores en la entrada de datos;
- proteger la confidencialidad de la identidad de los emisores y destinatarios del servicio para todos aquellos elementos externos al propio servicio de notificación;
- verificar la identidad del Emisor y del Destinatario directamente o confiando en un tercero si es un Prestador de Servicios de Confianza emitiendo los certificados cualificados de los destinatarios;
- garantizar que solo aceptará el contenido de la notificación enviado desde el Emisor una vez que éste haya sido identificado y autenticado con éxito;
- garantizar que solo entregará el contenido de la notificación al Destinatario una vez que éste haya sido identificado y autenticado con éxito;
- garantizar la disponibilidad de la notificación de cara al Destinatario durante el período de tiempo de vigencia que se haya definido para ella;
- garantizar el momento temporal de las notificaciones electrónicas mediante el uso de sellos electrónicos cualificados de tiempo;
- recolectar y custodiar, durante la vigencia del contrato con el Suscriptor, las evidencias necesarias e identificadas en esta DPYP para cada proceso de entrega certificada;
- 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 usuario en el ejercicio de su actividad cuando incumpla las obligaciones que les impone la legislación aplicable;
- conservar registrada toda la información y documentación relativa al Servicio Cualificado de Entrega Electrónica Certificada durante un mínimo de cinco años;
- colaborar en los procesos de auditoría que se realicen sobre la infraestructura con la que se proveen los servicios de confianza;
- realizar revisiones periódicas, al menos de carácter anual, con el fin de verificar el cumplimiento de las políticas definidas en su Política de Seguridad, garantizando con ello la seguridad de sus infraestructuras;
- operar de acuerdo con la [legislación aplicable](#);
- comunicar con una antelación mínima de dos meses a los suscriptores del servicio, terceras partes interesadas y al organismo supervisor competente en el caso de cesar su actividad.



7.6.2 Obligaciones del Suscriptor

El Suscriptor también está obligado, en los términos definidos en la presente DPyP, principalmente a:

- Respetar lo dispuesto en esta DPyP;
- formalizar un contrato de prestación del Servicio Cualificado de Entrega Electrónica Certificada con SIA como proveedor del servicio;
- respetar lo dispuesto en los contratos firmados con el Prestador del servicio;
- cumplir las obligaciones y hacer uso correcto del Servicio Cualificado de Entrega Electrónica Certificada de acuerdo a lo definido en las prácticas y políticas publicadas por SIA;
- conocer y aceptar las condiciones de utilización de los envíos de notificaciones electrónicas;
- hacer un uso adecuado de los informes de evidencias, respetando las limitaciones establecidas en esta DPyP;
- notificar cualquier hecho o situación anómala que afecte a los servicios.

7.6.3 Obligaciones del Emisor

Según la presente DPyP, el Emisor está obligado a:

- Conocer y respetar lo dispuesto en esta DPyP;
- conocer y aceptar las condiciones de utilización de los envíos de notificaciones electrónicas;
- cumplir las obligaciones y hacer uso correcto del Servicio Cualificado de Entrega Electrónica Certificada de acuerdo a lo definido en las prácticas y políticas publicadas por SIA;
- suministrar al Prestador información exacta, completa y veraz en relación a los datos que éstas les soliciten para realizar el proceso de envío de las notificaciones electrónicas;
- utilizar de forma correcta el servicio de notificaciones electrónicas para el fin y dentro del ámbito para el que haya sido contratado;
- comunicar a SIA, a través de los mecanismos que se habilitan a tal efecto, cualquier mal funcionamiento del servicio de envío de notificaciones electrónicas que pueda detectar;
- cumplir con las obligaciones y responsabilidades establecidas en la Declaración de Prácticas de Certificación y en la Política de Certificación de los certificados cualificados.

7.6.4 Obligaciones de los Destinatarios

Es obligación de los terceros que acepten y confíen en los certificados emitidos por la AC de SIA:



- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y en esta DPC.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez y del estado de revocación de los certificados y sellos electrónicos en que confía.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados y sellos electrónicos en los que confía y asumir sus obligaciones.

Conocer y aceptar las condiciones de utilización de los envíos de notificaciones electrónicas

7.6.5 Obligaciones de terceros en el soporte de servicios del PSC

Las obligaciones de terceros en el soporte de los servicios que ofrece el Prestador deben proporcionar, en líneas generales, las siguientes garantías:

- Cumplir y facilitar el cumplimiento de todo lo estipulado en esta DPyP.
- Los servicios cuya infraestructura estén desplegados en terceros deben ofrecer los mismos niveles de seguridad y fiabilidad como si estuvieran desplegados en las infraestructuras del Prestador.
- El tercero deberá conocer y seguir lo establecido en esta DPyP, siendo de obligado cumplimiento como si del propio Prestador se tratara.
- En el caso en el que el tercero, además, tenga que archivar información y datos, lo hará en las mismas condiciones y plazos que marquen la DPyP.
- El tercero deberá de informar al Prestador de cualquier cambio que se vaya a llevar en la infraestructura o en los procedimientos con el fin de someterlo a evaluación por parte del PSC. En cualquier caso, dichos cambios deberán garantizar lo estipulado en esta DPyP.

7.7 Renuncias de garantías

El Prestador de Servicios de Confianza SIA podrá renunciar a todas las garantías de los servicios que presta y que no se encuentren vinculadas a las obligaciones establecidas por Ley y normas del Reglamento eIDAS.

Dichas renuncias serán previamente notificadas a las partes afectadas.



7.8 Responsabilidades

7.8.1 Limitaciones de responsabilidades

SIA como Prestador de Servicios de Confianza tiene atribuidas las competencias del Servicio Cualificado de Entrega Electrónica Certificada y las de emisión de certificados cualificados y responderá en caso de incumplimiento de las obligaciones contenidas en la legislación aplicable, en la presente Declaración de Prácticas y Políticas y en la Declaración de Prácticas de Certificación y las Políticas de Certificación para la emisión de los certificados cualificados.

7.8.2 Responsabilidades del Prestador del servicio

- SIA responderá por los daños y perjuicios que causen a cualquier usuario en el ejercicio de su actividad cuando incumpla las obligaciones que les impone la legislación aplicable y con las limitaciones establecidas en la presente DPyP.
- La responsabilidad del Prestador de Servicios de Confianza regulada en el Reglamento eIDAS será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al Prestador demostrar que actuó con la diligencia profesional que le es exigible.
- SIA como Prestador de Servicios de Confianza asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que delegue la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.
- SIA no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones de los usuarios finales (Suscriptor, Emisor y Destinatario).
- SIA no será responsable de la utilización incorrecta de los certificados ni las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del servicio.
- SIA no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado o el servicio.
- SIA no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta DPyP, si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.
- SIA no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guarda la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta DPyP y en la Ley.



7.8.3 Responsabilidades del Suscriptor

El Suscriptor en su función de Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los emisores y la validación de sus datos, con las mismas limitaciones y obligaciones que se establecen en la Declaración de Prácticas de Certificación y en las Políticas de Certificación del certificado cualificado

7.8.4 Responsabilidades del Emisor

Es responsabilidad del Emisor cumplir con las obligaciones estipuladas en la presente DPyP, así como velar por el correcto registro en el servicio de los datos de identificación de los destinatarios.

De la misma manera, como titular de un certificado cualificado, es también responsable de hacer un uso adecuado a lo establecido en la legislación aplicable, en la Declaración de Prácticas de Certificación y en las Políticas de Certificación de dicho tipo de certificado.

7.8.5 Responsabilidades del Destinatario

Es responsabilidad del Destinatario cumplir con las obligaciones estipuladas en la presente DPyP, así como facilitar información veraz en el proceso de registro con el Emisor.

También está dentro de sus responsabilidades el hacer un uso adecuado y conforme a la legislación aplicable, a la Declaración de Prácticas de Certificación y a las Políticas de Certificación del emisor del certificado cualificado que utiliza para acceder al servicio.

7.8.6 Delimitación de responsabilidades

SIA no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Por el incumplimiento de las obligaciones contenidas en la legislación aplicable y la presente Declaración de Prácticas y Políticas.
- Por el uso indebido o fraudulento de las evidencias emitidas por el servicio.
- Por el uso indebido o fraudulento del contenido de los mensajes o documentos a los que se aplique el servicio.



- En relación a acciones u omisiones del Emisor, aplicaría las delimitaciones establecidas en la Declaración de Prácticas de Certificación de SIA y la Política de Certificación correspondiente al certificado cualificado, ambos documentos publicados en la web del Prestador.
- En relación a acciones u omisiones del Destinatario:
 - Falta de veracidad de la información suministrada para emitir el certificado cualificado de acceso a los servicios.
 - Falta de comunicación de cualquier modificación de las circunstancias reflejadas en el certificado.
 - Retraso en la comunicación de las causas de suspensión o revocación del certificado.
 - Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
 - Uso del certificado fuera de su periodo de vigencia, o cuando el Prestador de Servicios de Confianza que emitió el certificado le notifique la revocación del mismo.
 - Cualquier uso indebido del certificado que contravenga las Políticas de Certificación y la Declaración de Prácticas de Certificación del Prestador que ha emitido el certificado del Destinatario.

7.8.7 Alcance de la cobertura

El seguro se hará cargo de todas las cantidades que SIA resulte legalmente obligado a pagar, hasta el límite de la cobertura contratada, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error o incumplimiento no intencionado de la legislación vigente entre otros.

7.9 Limitaciones de pérdidas

En el proceso de formalización del instrumento jurídico vinculante, el Solicitante podrá establecer, si lo desea, un límite concreto, asumiendo los costes adicionales que en su caso se establezcan. Además, el Solicitante y terceras partes podrán acordar bilateralmente pactos o coberturas específicas para transacciones de valor superior, manteniéndose en este caso el límite de responsabilidad del Prestador citado en los párrafos anteriores, según la Declaración de Prácticas y Políticas aplicable.



7.10 Periodo de validez

7.10.1 Plazo

La Declaración de Prácticas y Políticas del Servicio Cualificado de Entrega Electrónica Certificada de SIA entrarán en vigor en el momento de su publicación.

Su publicación se llevará a cabo con la autorización y bajo la supervisión del organismo Regulador.

7.10.2 Sustitución y derogación de la DPyP

La presente Declaración de Prácticas y Políticas será derogada en el momento en que una nueva versión del documento sea publicada.

La nueva versión suplirá íntegramente el documento anterior. No obstante, se conservará un histórico de versiones durante, al menos, cinco (5) años.

7.10.3 Efectos de finalización

Para los Suscriptores vigentes cuyo acuerdo se firmara bajo una DPyP anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

7.11 Notificaciones individuales y comunicaciones con participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPyP se realizará mediante mensaje electrónico o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto [1.4 Administración de las Políticas](#). Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.



7.12 Reclamaciones y jurisdicción

Para la resolución de cualquier conflicto que pudiera surgir en relación con este documento o el instrumento jurídico vinculante, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Tribunales de Justicia de Madrid.

7.13 Legislación aplicable

La normativa aplicable al presente documento de declaración de prácticas y políticas, y a las operaciones que derivan de ellas, es la siguiente:

- 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 (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- REGLAMENTO DE EJECUCIÓN (UE) 2015/1502 DE LA COMISIÓN de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- DIRECTIVA (UE) 2017/1564 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de septiembre de 2017 sobre ciertos usos permitidos de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos, y por la que se modifica la Directiva 2001/29/CE relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.



7.14 Conformidad con la Ley aplicable

Es responsabilidad de todos los intervinientes en el Servicio Cualificado de Entrega Electrónica Certificada de SIA velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

7.15 Clausulas diversas

7.15.1 Acuerdo integro

Todos los Terceros Aceptantes asumen en su totalidad el contenido de la última versión de esta Declaración de Prácticas y Políticas.

7.15.2 Subrogación

Los derechos, deberes y obligaciones asociados al Servicio Cualificado de Entrega Electrónica Certificada de SIA no podrán ser objeto de cesión a terceros. En el caso de subrogación del servicio, se procederá a la finalización del servicio.

7.15.3 Divisibilidad

En el caso que una o más cláusulas de esta Declaración de Prácticas y Políticas sea o llegase a ser inválida, ilegal o inexigible legalmente, tal inaplicabilidad no afectará a ninguna otra clausula, sino que se actuará entonces como si las cláusula o cláusulas inaplicables nunca hubieran sido contenidas por este documento, y en tal grado como sea posible se interpretará la DPyP para mantener la voluntad original de la misma.

7.15.4 Fuerza Mayor

En caso de fuerza mayor se atenderá a lo establecido en la cláusula 9.8 Limitaciones de Responsabilidad.