

SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Avenida de Europa, 2

Alcor Plaza Edificio B

Parque Oeste Alcorcón

28922 Alcorcón - Madrid (España)

Tel: (34) 902 480 580 Fax: (34) 91 641 95 13

psc.sia.es



DPC - SIA

Declaración de Practicas de Certificación

OID: 1.3.6.1.4.1.39131.10.1.1.1.0

Versión: 1.0



ISO 9001
ISO 14001
BUREAU VERITAS
Certification



INDICE

1. INTRODUCCIÓN	14
1.1 Resumen.....	14
1.2 Nombre del documento e identificación.....	16
1.3 Entidades y personas intervinientes.....	16
1.3.1 Autoridad de Certificación	16
1.3.2 Autoridades de Registro	18
1.3.3 Solicitante	18
1.3.4 Firmante	19
1.3.5 Suscriptor.....	19
1.3.6 Terceras Partes Aceptantes	19
1.3.7 Otros intervinientes	19
1.4 Uso de los certificados.....	19
1.4.1 Usos apropiados / permitidos de los certificados	19
1.4.2 Limitaciones y restricciones en el uso de los certificados	20
1.5 Administración de Políticas	20
1.5.1 Organización responsable.....	20
1.5.2 Persona de contacto	20
1.5.3 Responsables de adecuación de la DPC	21
1.5.4 Procedimientos de aprobación de esta DPC	21
1.6 Definiciones y Acrónimos	22
1.6.1 Definiciones	22
1.6.2 Acrónimos.....	24
2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN	26
2.1 Repositorios.....	26
2.2 Publicación de información de certificación.....	26
2.3 Temporalidad o frecuencia de publicación	26
2.4 Controles de acceso a los repositorios	27
3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS.....	28

3.1 Nombres	28
3.1.1 Tipos de nombres	28
3.1.2 Necesidad de que los nombres sean significativos	28
3.1.3 Uso de seudónimos	28
3.1.4 Reglas para interpretar varios formatos de nombres	29
3.1.5 Unicidad de los nombres	29
3.1.6 Procedimientos de resolución de conflictos sobre nombres	29
3.1.7 Reconocimiento, autenticación y papel de las marcas registradas	29
3.2 Validación de la identidad inicial	29
3.2.1 Métodos para probar la posesión de la clave privada	29
3.2.2 Autenticación de la identidad de una persona jurídica	30
3.2.3 Autenticación de la identidad de una persona física	30
3.2.4 Información no verificada sobre el solicitante	30
3.2.5 Comprobación de las facultades de representación	30
3.3 Identificación y autenticación para peticiones de renovación de claves	30
4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS	31
4.1 Solicitud de certificados	31
4.1.1 Quien puede efectuar una solicitud	31
4.1.2 Registro de las solicitudes de certificados	31
4.2 Tramitación de las solicitudes de certificados	31
4.2.1 Realización de las funciones de identificación y autenticación	31
4.2.2 Aprobación o negación de las solicitudes de certificados	32
4.2.3 Plazo para la tramitación de las solicitudes de certificados	32
4.3 Emisión de certificados	32
4.3.1 Actuaciones de la AC durante la emisión de los certificados	32
4.3.2 Notificación al solicitante de la emisión por la AC del certificado	32
4.4 Aceptación del certificado	32
4.4.1 Forma en la que se acepta el certificado	32
4.4.2 Publicación del certificado por la AC	33
4.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades	33
4.5 Par de claves y uso del certificado	33

4.5.1	Uso de la clave privada del certificados por el titular	33
4.5.2	Uso de la clave pública y del certificado por los terceros aceptantes	33
4.6	Renovación de certificados sin cambio de claves	33
4.6.1	Circunstancias para la renovación de certificados sin cambio de claves	33
4.7	Renovación de certificados con cambio de claves	34
4.8	Modificación de certificados	34
4.9	Revocación y suspensión de certificados	34
4.9.1	Causas para la revocación	34
4.9.2	Quien puede solicitar la revocación	36
4.9.3	Procedimiento de solicitud de revocación	36
4.9.4	Periodo de gracia de la solicitud de revocación	37
4.9.5	Plazo en que la AC debe resolver la solicitud de revocación	37
4.9.6	Requisitos de verificación de las revocaciones por los terceros aceptantes	37
4.9.7	Frecuencia de emisión de CRLs	37
4.9.8	Tiempo máximo entre la generación y la publicación de las CRLs	37
4.9.9	Disponibilidad de un sistema en línea de verificación del estado de los certificados	37
4.9.10	Requisitos de comprobación en línea de la revocación	38
4.9.11	Otras formas de divulgación de información de revocación	38
4.9.12	Requisitos especiales de renovación de claves comprometidas	38
4.9.13	Circunstancias para la suspensión	38
4.9.14	Quién puede solicitar la suspensión	39
4.9.15	Procedimiento para la solicitud de suspensión	39
4.9.16	Límites del periodo de suspensión	39
4.10	Servicios de información del estado de certificados	39
4.10.1	Características operativas	39
4.10.2	Disponibilidad del servicio	39
4.10.3	Características adicionales	39
4.11	Finalización de la suscripción	39
4.12	Custodia y recuperación de claves	40
4.12.1	Prácticas y políticas de custodia y recuperación de claves	40
4.12.2	Prácticas y políticas de protección y recuperación de la clave de sesión	40

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y DE OPERACIONES	41
5.1 Controles de seguridad física.....	41
5.1.1 Ubicación física y construcción	41
5.1.2 Acceso físico	41
5.1.3 Alimentación eléctrica y aire acondicionado	42
5.1.4 Exposición al agua.....	42
5.1.5 Protección y prevención de incendios	42
5.1.6 Sistema de almacenamiento.....	42
5.1.7 Eliminación de los soportes de información	43
5.1.8 Copias de seguridad fuera de las instalaciones.....	43
5.2 Controles de Procedimiento.....	43
5.2.1 Roles responsables del control y gestión.....	43
5.2.2 Número de personas requeridas por tarea.....	44
5.2.3 Identificación y autenticación para cada usuario.....	45
5.2.4 Roles que requieren segregación de funciones	45
5.3 Controles de Personal	45
5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales.....	45
5.3.2 Procedimientos de comprobación de antecedentes	45
5.3.3 Requerimientos de formación	46
5.3.4 Requerimientos de frecuencia de actualización de la información.....	46
5.3.5 Frecuencia y secuencia de rotación de tareas	46
5.3.6 Sanciones por actuaciones no autorizadas	46
5.3.7 Requisitos de contratación de terceros	46
5.3.8 Documentación proporcionada al personal.....	46
5.4 Procedimientos de auditoria de seguridad.....	47
5.4.1 Tipos de eventos registrados.....	47
5.4.2 Frecuencia de procesado de registros de auditoria	48
5.4.3 Periodo de conservación de los registros de auditoria	49
5.4.4 Protección de los registros de auditoria	49
5.4.5 Procedimientos de respaldo de los registros de auditoria.....	49
5.4.6 Sistema de recogida de información de auditoria	49

5.4.7 Notificación al sujeto causa del evento	49
5.4.8 Análisis de vulnerabilidades.....	49
5.5 Archivo de registros.....	49
5.5.1 Tipos de eventos archivados.....	50
5.5.2 Periodo de conservación de registros.....	50
5.5.3 Protección del archivo	50
5.5.4 Procedimientos de copia de respaldo del archivo	50
5.5.5 Requerimientos para el sellado de tiempo de los registros.....	51
5.5.6 Sistema de archivo de información de auditoría	51
5.5.7 Procedimientos para obtener y verificar información archivada	51
5.6 Cambio de claves de una AC.....	51
5.7 Recuperación en casos de vulneración de una clave y de desastre natural u otro tipo de catástrofe	51
5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades	51
5.7.2 Alteración de los recursos hardware, software y/o datos	52
5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad.....	52
5.7.4 Continuidad de negocio después de un desastre natural u otro tipo de catástrofe	53
5.8 Cese de una AC o AR.....	53
5.8.1 Autoridad de Certificación.....	53
5.8.2 Autoridad de Registro.....	54
6. CONTROLES DE SEGURIDAD TÉCNICA.....	55
6.1 Generación e instalación del par de claves	55
6.1.1 Generación del par de claves.....	55
6.1.2 Entrega de la clave privada al titular.....	55
6.1.3 Entrega de la clave pública al emisor del certificado	55
6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes.....	55
6.1.5 Tamaño de las claves	55
6.1.6 Parámetros de generación de la clave pública y verificación de la calidad	56
6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3).....	56
6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos	56
6.2.1 Estándares para los módulos criptográficos	56
6.2.2 Control multi-persona (n de m) de la clave privada.....	57

6.2.3 Custodia de la clave privada	57
6.2.4 Copia de seguridad de la clave privada.....	57
6.2.5 Archivo de la clave privada	57
6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico	57
6.2.7 Almacenamiento de la clave privada en un módulo criptográfico.....	57
6.2.8 Método de activación de la clave privada.....	58
6.2.9 Método de desactivación de la clave privada	58
6.2.10 Método de destrucción de la clave privada	58
6.2.11 Clasificación de los módulos criptográficos	58
6.3 Otros aspectos de la gestión del par de claves.....	58
6.3.1 Archivo de la clave pública.....	58
6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves	58
6.4 Datos de activación	59
6.4.1 Generación e instalación de los datos de activación.....	59
6.4.2 Protección de los datos de activación.....	59
6.4.3 Otros aspectos de los datos de activación	59
6.5 Controles de seguridad informática	59
6.5.1 Requerimientos técnicos de seguridad específicos	59
6.5.2 Evaluación de la seguridad informática	60
6.6 Controles de seguridad del ciclo de vida	60
6.6.1 Controles de desarrollo de sistemas.....	60
6.6.2 Controles de gestión de seguridad	60
6.6.3 Controles de seguridad del ciclo de vida.....	60
6.7 Controles de seguridad de la red.....	60
6.8 Fuentes de tiempo.....	61
7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP	62
7.1 Perfil de certificado	62
7.1.1 Número de versión	62
7.1.2 Extensiones del certificado	62
7.1.3 Identificadores de objeto (OID) de los algoritmos	64
7.1.4 Formatos de nombre	64

7.1.5 Restricciones de nombre	64
7.1.6 Identificador de objeto (OID) de la Política de Certificación	64
7.1.7 Uso de la extensión "PolicyConstraints"	64
7.1.8 Sintaxis y semántica de los "PolicyQualifier"	65
7.1.9 Tratamiento semántico para la extensión "Certificate Policy"	65
7.2 Perfil de CRL	65
7.2.1 Numero de versión	65
7.2.2 CRL y extensiones	65
7.3 Perfil de OCSP	66
7.3.1 Número de versión	66
7.3.2 Extensiones del OCSP	66
8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES	68
8.1 Frecuencia o circunstancias de los controles para cada autoridad	68
8.2 Identificación / cualificación del auditor	68
8.3 Relación entre el auditor y la Autoridad auditada	68
8.4 Aspectos cubiertos por los controles	69
8.5 Acciones a emprender como resultado de la detección de deficiencias	69
8.6 Comunicación de resultados	69
9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD	70
9.1 Tarifas	70
9.1.1 Tarifas de emisión de certificado o renovación	70
9.1.2 Tarifas de acceso a los certificados	70
9.1.3 Tarifas de acceso a la información de estado o revocación	70
9.1.4 Tarifas de otros servicios tales como información de políticas	70
9.1.5 Política de reembolso	70
9.2 Responsabilidad Financiera	71
9.2.1 Seguro de responsabilidad civil	71
9.3 Confidencialidad de la información y protección de datos	71
9.3.1 Confidencialidad de la información	71
9.3.2 Información no calificada como privada	72

9.4 Protección de datos personales	73
9.4.1 Política de protección de datos de carácter personal	73
9.4.2 Documento de seguridad LOPD	74
9.5 Derechos de propiedad Intelectual	78
9.6 Obligaciones	79
9.6.1 Obligaciones de la AC	79
9.6.2 Obligaciones de la AR	80
9.6.3 Obligaciones de los firmantes	80
9.6.4 Obligaciones de los terceros aceptantes	81
9.6.5 Obligaciones de otros participantes	81
9.7 Renuncias de garantías	82
9.8 Limitaciones de responsabilidad	82
9.9 Responsabilidades	82
9.9.1 Limitaciones de responsabilidades	82
9.9.2 Responsabilidades de la Autoridad de Certificación	82
9.9.3 Responsabilidades de la Autoridad de Registro	83
9.9.4 Responsabilidad del titular	83
9.9.5 Delimitación de responsabilidades	83
9.9.6 Alcance de la cobertura	84
9.9.7 Cobertura de seguro u otras garantías para los terceros aceptantes	84
9.10 Limitaciones de pérdidas	85
9.11 Periodo de validez	85
9.11.1 Plazo	85
9.11.2 Sustitución y derogación de la DPC	85
9.11.3 Efectos de finalización	85
9.12 Notificaciones individuales y comunicaciones con participantes	86
9.13 Reclamaciones y jurisdicción	86
9.14 Legislación aplicable	86
9.15 Conformidad con la Ley aplicable	87
9.16 Clausulas diversas	87

9.16.1 Acuerdo integro.....	87
9.16.2 Subrogación.....	87
9.16.3 Divisibilidad	87
9.16.4 Fuerza Mayor.....	87
9.17 Otras estipulaciones	88

RELACION DE TABLAS

Tabla 1 – Datos identificación DPC.....	16
Tabla 2 – Datos AC ROOT	17
Tabla 3 – Datos AC SUB01	17
Tabla 4 – Organización responsable.....	20
Tabla 5 – Persona de contacto	21
Tabla 6 – Responsable de adecuación de la DPC	21
Tabla 7 – Repositorios de publicación.....	26
Tabla 8 – Roles de gestión del sistema.....	44
Tabla 9 – Roles de gestión del HSM	44
Tabla 10 – Definición extensión SubjectAltName	63
Tabla 11 – OID políticas de certificación	64
Tabla 12 – Perfil CRL y extensiones.....	66
Tabla 13 – Extensiones del certificado de OCSP.....	67
Tabla 14 – Datos de carácter personal tratados	75

RELACION DE ILUSTRACIONES

Ilustración 1: Diagrama de componentes lógicos	15
--	----

1. INTRODUCCIÓN

1.1 Resumen

El presente documento recoge la Declaración de Prácticas de Certificación de la Autoridad de Certificación SIA, en adelante AC de SIA, que define los mecanismos y procedimientos para la solicitud, expedición, uso, gestión, extinción, renovación y cualquier otro proceso que afecte al ciclo de vida de los certificados electrónicos emitidos por la AC de SIA. La Declaración de Prácticas de Certificación (en adelante DPC) se ha estructurado conforme al documento RFC-3647 “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”, y se alinea con lo establecido en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC-3647. Cuando no se haya previsto nada en alguna sección aparecerá la frase “No Estipulado” o “No Aplica”.

En cuanto al marco legislativo, se han seguido estas normativas:

- 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.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Resolución de 29 de noviembre de 2012 de la Secretaría de Estado de Administraciones Públicas, por la que publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

La DPC incluye, entre otras, las obligaciones que las partes se comprometen a cumplir para la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida y sus condiciones aplicables, y sirve de guía en la relación entre SIA y los usuarios de sus servicios telemáticos.

Esta DPC recoge la política de servicios, 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 de la Infraestructura de Clave Pública. Concretamente 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 mecanismos de información sobre la vigencia de los certificados. A este respecto recomendamos la consulta en la dirección de internet del organismo competente.

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

Esta DPC 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.

La arquitectura general, a nivel jerárquico, de la PKI de SIA es la siguiente:

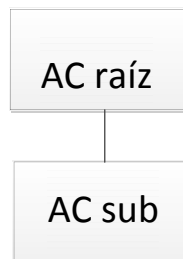


Ilustración 1: Diagrama de componentes lógicos

- Un primer nivel en el que se ubica la AC raíz que representa el punto de confianza de todo el sistema y que permitirá que todas las personas físicas o jurídicas, públicas o privadas, reconozcan la validez del mismo para su acreditación.
- Un segundo nivel, constituido por la AC subordinada de la AC Raíz que emitirá los diferentes tipos de certificados.

Todas las partes involucradas tienen la obligación de conocer esta DPC y ajustar su actividad a lo dispuesto en la misma.

1.2 Nombre del documento e identificación

Nombre del documento	Declaración Prácticas Certificación
Versión del documento	1.0
Estado del documento	Vigente
Fecha de emisión	30/01/2015
Fecha de caducidad	No aplicable
OID	1.3.6.1.4.1.39131.10.1.1.1.0
Ubicación de la DPC	https://psc.sia.es/

Tabla 1 – Datos identificación DPC

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- SIA como órgano competente de la expedición y gestión de la Autoridad de Certificación.
- Las Autoridades de Registro.
- Los Firmantes/Titulares
- Los Suscriptores.
- Las Terceras partes aceptantes de los certificados emitidos.

1.3.1 Autoridad de Certificación

SIA actúa como Autoridad de Certificación (AC) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de certificados digitales.

Las Autoridades de Certificación que componen la PKI de SIA son:

- **“AC raíz”** Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. Esta es la información más relevante del certificado:

Nombre Distintivo	CN = SIA ROOT, SERIALNUMBER = A82733262, O = SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA, C = ES
Número de serie	54 ca 01 89
Periodo de validez	Desde jueves, 29 de enero de 2015 10:17:03 Hasta martes, 29 de diciembre de 2037 10:47:03
Huella Digital (SHA1)	3524e8ebb8643f1c744522848925c7b10e4c2e32
Huella Digital (SHA256)	4c8cb897fed5ffceb8796cdfef70c1d34044f2c5085e85de7ce9c86798a29e2c
Huella Digital (SHA512)	9b7502485f12e41f0da43ade533e7133b941a5fc2793079d57e0f944b4a76b600c347a2685c0b2581296a9dbc05da6c87a89c005929683882d047cdffea24db8

Tabla 2 – Datos AC ROOT

- **“AC subordinada”**. Autoridad de Certificación subordinada de “SIA ROOT”, para la emisión de certificados finales. Esta es la información más relevante:

Nombre Distintivo	CN = SIA SUB01, SERIALNUMBER = A82733262, OU = QUALIFIED CA, O = SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA, C=ES
Número de serie	54 ca 01 dc
Periodo de validez	Desde jueves, 29 de enero de 2015 10:56:43 Hasta viernes, 29 de diciembre de 2030 11:26:43
Huella Digital (SHA1)	9bf08f93b873e4cdc0acf2bd32f48744fcf9681b
Huella Digital (SHA256)	68690054b917c0e4a96092c4b359f7418098b64ef149a70b785a389c45515d10
Huella Digital (SHA512)	2d45cca297f615f996fb15aac1624faac3fdb0d135270131cf69683630659324de61d922785829c28caaa81be18093adac33fe4cd055491aa80654f3a52c4ed0

Tabla 3 – Datos AC SUB01

El cese de operación o la incorporación de una nueva AC al dominio serán causa de modificación de la presente DPC y de notificación a través de los mecanismos habilitados a tal efecto.

1.3.2 Autoridades de Registro

La Autoridad de Registro (en adelante AR) de SIA es la entidad encargada de:

- Identificar y comprobar la identidad de los solicitantes y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que contará como firmante del certificado.
- Realizar la tramitación de las solicitudes de certificados.
- Proporcionar al solicitante antes de la expedición del certificado la información mínima necesaria.
- Facilitar al firmante y suscriptor la usabilidad del certificado.

Actuarán como entidades de registro de SIA:

- Corporaciones que sean clientes de SIA, para la emisión de certificados a nombre de la corporación o a miembros de la propia corporación, previo acuerdo de prestación de servicios.
- Cualquier entidad de confianza que llegue a un acuerdo con SIA para actuar como intermediario en nombre del prestador.
- La propia SIA directamente.

El PSC formalizará contractualmente las relaciones entre él y cada una de las entidades clientes que realicen actuaciones de comprobación de la identidad y otras circunstancias personales. La entidad que actúe como AR podrá autorizar a una o varias personas como operadores con el fin de manejar los sistemas informáticos para la emisión de certificados.

Allí donde la ubicación geográfica de los solicitantes represente un problema logístico para su identificación, la AR podrá delegar la función de comprobación en otra entidad de confianza. Dicha entidad deberá tener una especial vinculación con la AR y una relación de proximidad con los solicitantes de los certificados que justifique la delegación. La entidad de confianza deberá firmar un acuerdo de colaboración con la AR en el que se acepte la delegación de estas funciones. SIA deberá conocer y autorizar de manera expresa el acuerdo, asegurando las obligaciones en la comprobación de identidad y asumiendo la responsabilidad frente a terceros por la actuación de estas entidades de confianza.

1.3.3 Solicitante

Solicitante es aquella persona que, en su propio nombre o en nombre de una organización, solicita la emisión de un certificado.

1.3.4 Firmante

Se entiende por firmante a la persona o titular del certificado que realiza y crea la firma electrónica.

1.3.5 Suscriptor

En el caso de una vinculación entre el firmante y una entidad mediante una relación laboral o contractual. El suscriptor es la entidad con personalidad jurídica que suscribe un contrato con SIA para la expedición de certificados a sus usuarios o terceros con vinculación a la empresa. Asimismo, podrá solicitar la revocación del certificado cuando cese la vinculación del firmante con el suscriptor.

1.3.6 Terceras Partes Aceptantes

Las terceras partes aceptantes, son las personas físicas o jurídicas diferentes al titular que deciden aceptar y confiar en un certificado emitido por SIA. Y como tales, les es de aplicación lo establecido por la presente Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados.

1.3.7 Otros intervinientes

No estipulado.

1.4 Uso de los certificados

1.4.1 Usos apropiados / permitidos de los certificados

Un certificado emitido por la AC de SIA sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta DPC y en su correspondiente Política de Certificación, por lo que existen ciertas limitaciones en el uso de los certificados de SIA.

Los certificados deben emplearse únicamente de conformidad con la legislación que les sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia criptográfica existentes en cada momento.

1.4.2 Limitaciones y restricciones en el uso de los certificados

Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades de las descritas para cada uno de ellos en el apartado 1.4.1 Usos apropiados / permitidos de los certificados.

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta Declaración de Prácticas de Certificación y las Políticas de Certificación son propiedad de SIA.

Nombre	SIA
Dirección correo	info@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 – Organización responsable

1.5.2 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 5 – Persona de contacto

1.5.3 Responsables de adecuación de la DPC

La autoridad con atribuciones para realizar y aprobar cambios sobre la DPC y las PC 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 6 – Responsable de adecuación de la DPC

La Autoridad de Administración de Política también es responsables de definir las políticas de certificación y los contratos correspondientes.

1.5.4 Procedimientos de aprobación de esta DPC

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

En el caso de que el responsable de la Administración de Políticas juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se comunicará a los suscriptores, firmantes, usuarios de los certificados o terceros dichas modificaciones que se han efectuado y que deben consultar la o las nuevas versiones en el repositorio establecido.

Las AR podrán ser notificadas directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

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

- **Autoridad de Certificación (AC):** la Autoridad de Certificación es la entidad que emitirá, a petición de la Autoridad de Registro, los Certificados que se precisen, de forma automatizada y previa confirmación de la Autoridad de Registro.
- **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 Electrónico:** es un documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- **Certificado reconocido:** certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- **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.
- **Criptografía:** la criptografía es una rama de las Matemáticas que estudia la transformación de información legible en información que no se puede leer directamente, es decir, que tiene que ser descifrada para ser leída.
- **Datos de creación de firma (Clave Privada):** datos únicos, como códigos o claves criptográficas privadas que el firmante utiliza para crear la firma electrónica.
- **Datos de Verificación de firma (Clave Pública):** Datos como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.
- **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.

• **Dispositivo de creación de firma:** programa o sistema informático que sirve para aplicar los datos de creación de firma.

Dispositivo Seguro de creación de firma: es el dispositivo que sirve para aplicar los datos de creación de firma, que se alinea a los requisitos establecidos en las normas específicas de aplicación en España, así como las recogidas en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se instaure un marco común para la firma electrónica.

• **Firma electrónica:** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

• **Firma electrónica avanzada:** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

• **Firma electrónica reconocida:** se considera firma electrónica reconocida, la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

• **Firmante:** es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

• **Solicitante del certificado:** es aquella persona que, en su propio nombre o en nombre de una organización, solicita la emisión de un certificado.

• **Poseedores de claves:** son las personas físicas que poseen o responden de la custodia de las claves de firma digital.

• **Terceros que confían en terceros:** son las personas físicas o jurídicas que reciben certificados expedidos por SIA. Son terceros que confían en certificados y, como tales, les es de aplicación lo establecido por la Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados.

• **Función hash:** es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

• **Hash o huella digital:** resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que se encuentra asociado unívocamente a los datos iniciales.

- **HSM (Módulo de seguridad criptográfico):** es un dispositivo de seguridad que genera y protege claves criptográficas.
- **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).
- **Lista de Certificados Revocados (CRL):** es aquella lista donde figura la relación de certificados revocados que SIA emite desde el momento en que se produce una revocación con carácter inmediato.
- **Número de serie del Certificado:** es un valor entero y único asociado inequívocamente con un certificado expedido por cualquier Prestador de Servicios de Certificación.
- **OCSP (Online Certificate Status Protocol):** es un protocolo informático que permite la comprobación de la vigencia de un certificado electrónico.
- **OID (Object Identifier):** valor que comprende una secuencia de componentes variables constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que poseen la propiedad de ser únicos entre el resto de OID.
- **PKCS (Public-Key Cryptography Standards):** es el estándar de facto más popular para codificar los diferentes tipos de información, como certificados o archivos firmados. Los programadores o analistas se refieren a estas convenciones o estándares como “formatos” o “lay-out”. PKCS responde a “Public Key Cryptography Standards”.
- **PKCS#10 (Certification Request Syntax Standard):** estándar de facto para solicitud de certificación. Define el formato de los mensajes enviados a una Autoridad de Certificación para solicitar la certificación de una clave pública.
- **Política de Certificación:** es un documento anexo a la Declaración de Prácticas de Certificación que recoge el ámbito de aplicación, los caracteres técnicos 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 Certificación (PSC):** es la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

1.6.2 Acrónimos

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

AC: Autoridad de Certificación.

AR: Autoridad de Registro.

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CDP: CRL Distribution Point (Punto de Distribución de CRLs).

CEN: Comité Europeo de Normalización.

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CRL: Certificate Revocation List (Lista de Revocación de Certificados).

CWA: CEN Workshop Agreement.

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

DPC: Declaración de Prácticas de Certificación.

ETSI: European Telecommunications Standard Institute.

FIPS: Federal Information Processing Standard (Estándar USA de procesamiento de información).

HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

IETF: Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet).

LDAP: Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio).

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

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

OID: Object identifier (Identificador de objeto único).

OU: Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PC: Política de Certificación.

PKCS: Public Key Infrastructure Standards. Estándares de PKI desarrollados por "RSA Laboratories" y aceptados internacionalmente.

PKI: Public Key Infrastructure (Infraestructura de Clave Pública).

PKIX: Grupo de trabajo dentro del IETF (Internet Engineering Task Group) constituido con el objeto de desarrollar las especificaciones relacionadas con PKI e Internet.

PSC: Prestador de Servicios de Certificación.

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

SIA: Sistemas Informáticos Abiertos.

2. REPOSITARIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 Repositorios

Documento	Repositorio
Certificado de la AC raíz	https://psc.sia.es/ac_raiz.crt
Certificado de la AC subordinadas	https://psc.sia.es/ac_sub01.crt
Lista de AC revocadas (ARL)	https://psc.sia.es/ar1.crl
Lista de revocación de usuarios (CRL)	https://psc.sia.es/ac_sub01.crl
Declaración de Prácticas de Certificación	https://psc.sia.es/AC_SIA_DPC.pdf
Política de Certificación de persona física vinculada a empresa	https://psc.sia.es/AC_SIA_PC_PFVE.pdf
Política de certificación de ciudadano	https://psc.sia.es/AC_SIA_PC_CIU.pdf

Tabla 7 – Repositorios de publicación

2.2 Publicación de información de certificación

El contenido de esta DPC, junto con las Políticas de Certificación para cada tipo de certificado, 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 DPC y las PC se publicaran 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. La AC añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el apartado 4.9.7 Frecuencia de emisión de CRLs.

2.4 Controles de acceso a los repositorios

La AC de SIA tiene implantados controles para mantener la integridad de su repositorio interno, de forma tal que:

- Se pueda comprobar la autenticidad de los certificados.
- Las personas no autorizadas no puedan alterar los datos.
- Los certificados solamente están accesibles en los supuestos o a las personas que el firmante indique.
- Detecte cualquier cambio técnico que afecte a los requisitos de seguridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

3.1 Nombres

3.1.1 Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o Distinguished Name) conforme al estándar X.500. Adicionalmente, todos los nombres de los certificados reconocidos son coherentes con lo dispuesto en las normas:

- ETSI TS 101 862 “Qualified Certificate profile” conocida como “European profile for Qualified Certificates”.
- ETSI TS 102 280 “X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons”
- RFC 5280 “Internet x509 Public Key Infrastructure. Certificate and CRL Profile” y su actualización RFC 6818.
- RFC 3739 “Internet x509 Public Key Infrastructure. Qualifies Certificates Profile”.

Y alineado con:

- Perfiles de Certificados Electrónicos según Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

3.1.2 Necesidad de que los nombres sean significativos

Los campos del DN referentes a Nombre y Apellidos corresponderán con los datos registrados legalmente del solicitante, expresados exactamente en el formato que conste en el Documento Nacional de Identidad, tarjeta de residencia, pasaporte u otro medio admitido en derecho.

En el caso de que los datos consignados en el DN fueran ficticios o se indique expresamente su invalidez (ej. “PRUEBAS” o “DESARROLLO”), se considera al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad.

3.1.3 Uso de seudónimos

No se permite la utilización de seudónimos en ningún caso.

3.1.4 Reglas para interpretar varios formatos de nombres

Las reglas utilizadas por SIA para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (x.500) Distinguished Name (DN) y ISO/IEC 9594-8 (X.509).

Los certificados expedidos por la Autoridad de Certificación SIA cumple las recomendaciones de la RFC 5280 (“Internet X.509 Public Key Infrastructure. Certificate and CRL Profile”) respecto a la utilización de la codificación de los atributos de los campos Issuer (Emisor) y Subject (Sujeto). En concreto, por medio de la codificación en formato UTF8String.

3.1.5 Unicidad de los nombres

El nombre distintivo de los certificados emitidos por la AC de SIA será único e inequívoco.

3.1.6 Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el apartado, 9.14 Reclamaciones y jurisdicción, de esta DPC.

SIA se reserva el derecho de rechazar una solicitud de certificado debido a un conflicto sobre nombres.

3.1.7 Reconocimiento, autenticación y papel de las marcas registradas

SIA no asume compromisos respecto al uso de marcas comerciales en los certificados ni determina si el firmante tiene derecho sobre la marca. Asimismo, se reserva el derecho de rechazar una solicitud de certificado debido a un conflicto de marcas registradas.

3.2 Validación de la identidad inicial

3.2.1 Métodos para probar la posesión de la clave privada

Debido a que el procedimiento de generación del par de claves depende del tipo de certificado emitido, la prueba de posesión de la clave privada se describirá en cada política de certificación específica.

La clave privada tanto de la AC Raíz como de la AC Subordinada se genera de forma segura en un módulo hardware criptográfico (HSM) y en ningún momento saldrá del mismo.

3.2.2 Autenticación de la identidad de una persona jurídica

No estipulado

3.2.3 Autenticación de la identidad de una persona física

La autenticación de la identidad para los certificados de cliente se especifica en la correspondiente Política de Certificación.

3.2.4 Información no verificada sobre el solicitante

Cada Política de Certificación establecerá qué parte de la información suministrada en la solicitud de un certificado no se verificará necesariamente.

3.2.5 Comprobación de las facultades de representación

Cada Política de Certificación establecerá el procedimiento de comprobación de las facultades que se reclamen para cada caso.

3.3 Identificación y autenticación para peticiones de renovación de claves

Este apartado es dependiente del tipo de certificado en particular, y está recogido en su correspondiente Política de Certificación.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 Solicitud de certificados

4.1.1 Quien puede efectuar una solicitud

Este apartado es dependiente del tipo de certificado en particular y está recogido en su correspondiente Política de Certificación. Asimismo, la PC establece los pasos que deben seguirse en su tramitación.

4.1.2 Registro de las solicitudes de certificados

SIA o un intermediario de SIA que actúe como AR para gestionar la solicitud del certificado, es el responsable de realizar el procedimiento de alta de la misma. Esta información será dada de alta en la base de datos de la autoridad de registro con el fin de realizar consultas posteriores, sobre el estado de la solicitud del solicitante o de los certificados solicitados para un suscriptor particular.

4.2 Tramitación de las solicitudes de certificados

En el momento en que SIA o un intermediario de SIA que actúe como AR recibe una solicitud de certificado, se procede al registro de la misma mediante la aplicación de registro correspondiente asociada a la Autoridad de Certificación.

Durante el proceso de solicitud existe una comprobación de que el usuario realmente pertenece al sistema, dicha comprobación es llevada a cabo mediante consulta al repositorio de SIA, donde necesariamente debe encontrarse la información del solicitante.

4.2.1 Realización de las funciones de identificación y autenticación

Es responsabilidad de la AR realizar de forma fehaciente la identificación y autenticación del solicitante. Este proceso deberá ser realizando previamente a la emisión del certificado.

4.2.2 Aprobación o negación de las solicitudes de certificados

En el momento de la personación, la AR verifica la información proporcionada por el solicitante, incluyendo la validación de la identidad del firmante. Si esta información es correcta, se procede a la firma del instrumento jurídico vinculante entre el firmante y SIA.

Se podrá entonces proceder a la emisión del certificado.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

No estipulado.

4.3 Emisión de certificados

4.3.1 Actuaciones de la AC durante la emisión de los certificados

Esta información se especifica en la Política de Certificación correspondiente.

4.3.2 Notificación al solicitante de la emisión por la AC del certificado

Esta información se especifica en la Política de Certificación correspondiente.

4.4 Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto al prestador SIA. El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el solicitante y SIA haya sido firmado y el certificado esté en posesión del firmante.

Como evidencia de la aceptación deberá quedar una hoja de aceptación firmada por el firmante. Se podrá comenzar a utilizar el certificado a partir de la fecha en que se firmó la hoja de aceptación.

Desde el momento de la aceptación, la presente DPC con relación al firmante despliega todos sus efectos.

4.4.2 Publicación del certificado por la AC

Los certificados no se publicarán en ningún repositorio de acceso libre.

4.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades

No se efectúan notificaciones a terceros.

4.5 Par de claves y uso del certificado

4.5.1 Uso de la clave privada del certificados por el titular

Las responsabilidades y limitaciones de uso del par de claves y del certificado se establecerán en la correspondiente PC. El titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la DPC y PC, el documento de aceptación medios y de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas de terceros, quedando su regulación fuera del alcance de este documento.

Tras la extinción de la vigencia o la revocación del certificado, el titular deberá dejar de utilizar la clave privada asociada y los correspondientes certificados.

4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente DPC y la PC correspondiente, y con lo establecido en los campos “Key Usage” y “Extended Key Usage” del certificado.

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por SIA concretamente para ello y especificados en el presente documento.

4.6 Renovación de certificados sin cambio de claves

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

En el ámbito de la AC de SIA no se realizara la renovación de certificados sin cambio de claves.

4.7 Renovación de certificados con cambio de claves

Las condiciones particulares de renovación se especifican en la correspondiente Política de Certificación.

4.8 Modificación de certificados

En caso de modificar algún dato, la AR deberá proceder a la revocación y a la emisión de un nuevo certificado.

4.9 Revocación y suspensión de certificados

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible.

La suspensión supone la pérdida temporal de validez de un certificado, y es reversible.

Las revocaciones y suspensiones tienen efecto desde el momento en que la indicación de dicha revocación o suspensión se incluya en el servicio de consulta sobre la vigencia de los certificados de SIA.

4.9.1 Causas para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

- a) Circunstancias que afectan a la información contenida en el certificado:
 - Modificación de alguno de los datos contenidos en el certificado.
 - Descubrimiento de que alguno de los datos contenidos en la solicitud del certificado es incorrecto.
 - Pérdida o cambio de la vinculación del firmante con la Corporación.
- b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:
 - Compromiso de la clave privada de la AC.
 - Compromiso de las claves de la infraestructura o sistemas de la CA, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
 - Infracción, por parte de la CA o de la RA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la DPC.
 - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del firmante.
 - Acceso o utilización no autorizados, por un tercero, de la clave privada del firmante.
 - La utilización indebida de los datos de creación de firma por un tercero.

- El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre SIA y el firmante o el suscriptor.
- c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:
- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
 - Acceso no autorizado, por un tercero, a los datos de activación del firmante.
- d) Circunstancias que afectan al suscriptor:
- Finalización de la relación jurídica entre la AC SIA y el suscriptor.
 - Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al firmante, incluyendo la inhabilitación temporal del firmante para el ejercicio profesional.
 - Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
 - Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías establecidas en el instrumento jurídico correspondiente o en la DPC.
 - Por extinción de la capacidad jurídica del suscriptor.
- e) Circunstancias que afectan al firmante
- La incapacidad sobrevenida, total o parcial.
 - Por el fallecimiento del firmante.
 - Modificación de la relación jurídica entre el firmante y SIA.
 - Infracción por el firmante, de sus obligaciones, responsabilidad y garantías establecidas en el instrumento jurídico correspondiente o en la DPC.
 - El uso irregular del certificado por el firmante.
- f) Otras circunstancias:
- Por resolución judicial o administrativa con competencias sobre ello que lo ordene.
 - Cese en la actividad de SIA salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos sean transferidos a otro Prestador de Servicios de Certificación. En tal caso SIA lo comunicará con dos meses de antelación y remitirá al firmante las características del prestador al que se propone las transferencias para que éste en su caso lo autorice mediante el consentimiento que reúna los requisitos exigibles por la normativa; libre, específico, previo e informado.
 - Solicitud formulada por el firmante, suscriptor o un tercero autorizado.
 - Por la concurrencia de cualquier otra causa especificada en la DPC.

4.9.2 Quien puede solicitar la revocación

En el ámbito de la AC de SIA pueden solicitar la revocación de un certificado:

- El firmante titular a nombre del cual fue expedido el certificado.
- Las personas físicas autorizadas por el suscriptor.
- La Entidad de Registro que intervino en la emisión.
- La propia AC de SIA cuando tenga conocimiento de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.
- Cualquier otra persona autorizada por el firmante si tiene conocimiento de algunas de las circunstancias indicadas en el punto anterior.

4.9.3 Procedimiento de solicitud de revocación

Por medio del buzón de correo y con una disponibilidad de 24x7, las solicitudes de revocación de certificados deberán ser efectuadas según lo descrito a continuación:

- El firmante deberá enviar un correo electrónico con la solicitud de revocación con:
 - Remitente. Debe ser enviado desde la cuenta de correo con la que se registró.
 - Asunto. Solicitud de revocación de certificado electrónico.
 - Cuerpo. Indicará el motivo por el cual se solicita la revocación.
- El PSC se pondrá en contacto con el firmante, para validar y confirmar la solicitud a través del número de teléfono de contacto con el que se registró. Si hubiera cambiado, sin ser notificado y no fuera posible contactar con el titular, se solicitará al titular el nuevo número de teléfono.
 - Se validará la información del titular: NIF, Nombre, Apellidos y fecha de nacimiento.
 - Se confirmará el motivo de la solicitud de revocación.
- Validados estos datos y aceptada la solicitud de revocación, se procederá de carácter inmediato a la revocación del certificado.
- Una vez revocado el certificado, se confirmará al firmante mediante el envío de un correo electrónico desde el buzón de correo del PSC, que este ha sido revocado, al igual que la fecha desde la que ha dejado de ser efectivo y el motivo por el cual se ha revocado.

4.9.4 Periodo de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

4.9.5 Plazo en que la AC debe resolver la solicitud de revocación

Una vez la identidad del solicitante de la revocación haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por la AR, la revocación se hará efectiva inmediatamente.

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes

Los terceros que aceptan certificados de SIA podrán verificar el estado de los mismos accediendo a los servicios de consulta sobre la vigencia de los certificados establecidos por SIA, dicha información de localización se encuentra en el propio certificado que se pretende verificar, al igual que en esta DPC.

4.9.7 Frecuencia de emisión de CRLs

La AC SIA, generara una nueva CRL cada 24 horas como máximo, o en su defecto, en el momento en que se produzca una revocación de un certificado.

4.9.8 Tiempo máximo entre la generación y la publicación de las CRLs

SIA publicara de carácter inmediato la CRL que se haya generado en cualquiera de los casos indicados en el apartado 4.9.7, por medio de un proceso automatizado.

4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la CA, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

Este plazo no será de aplicación para supuestos de fuerza mayor en los términos del artículo 1105 del Código Civil. Tampoco será de aplicación bajo los supuestos donde SIA no sea responsable incluyendo fuentes de alimentación

eléctrica, comunicaciones, componentes de hardware y software del que SIA no sea titular o cualesquiera otras análogas.

4.9.10 Requisitos de comprobación en línea de la revocación

Para el uso del servicio de CRLs, que es de acceso libre, deberá considerarse que:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión “CRL Distribution Point” o en esta misma DPC.
- El usuario deberá comprobar, adicionalmente, las CRLs pendientes de la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren no serán retirados de la CRL.

En el caso de que la política de certificación del certificado incluya el servicio de OCSP, este servicio será de acceso libre y debe considerar:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del certificado.
- Comprobar que la respuesta OCSP está firmada.

4.9.11 Otras formas de divulgación de información de revocación

No estipulado.

4.9.12 Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.9.13 Circunstancias para la suspensión

En el ámbito de la AC de SIA, no se contempla la suspensión (revocación temporal) de certificados. En todos los casos en los que sea necesario suspender un certificado, este se revocará de forma permanente.

4.9.14 Quién puede solicitar la suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del periodo de suspensión

No aplica.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

SIA ofrece un servicio gratuito de publicación en la web de Listas de Certificados Revocados (CRL) sin restricciones de acceso. Asimismo, puede ofrecer servicio mediante protocolo OCSP en las políticas de certificación que lo establezcan.

4.10.2 Disponibilidad del servicio

Los servicios de la consulta del estado de los certificados de SIA funcionarán 24 horas al día, 7 días a la semana y todos los días del año. SIA dispone de un CPD (Centro de Proceso de Datos) replicado, donde en caso de caída del nodo principal, este asumirá dicho servicio.

4.10.3 Características adicionales

No aplica.

4.11 Finalización de la suscripción

La suscripción finalizará en el momento de extinción de la vigencia de un certificado electrónico. La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas recogidas en el apartado 4.9.1.
- Expiración del período de validez que figura en el certificado.

Si no se solicita la renovación del certificado la extinción de su validez supondrá la extinción de la relación entre el titular y la AC.

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de custodia y recuperación de claves

La clave privada de la AC raíz como las de las AC Subordinadas de SIA, han sido generadas sobre módulos de seguridad criptográficos, cumpliendo con niveles de seguridad necesarios.

El PSC en ningún momento custodiara ni copiara la clave privada emitida a los usuarios. Por lo tanto el PSC en ningún momento podrá recuperar la clave de los usuarios. En caso de pérdida de la misma, se deberá revocar el certificado y emitir uno nuevo.

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión

No estipulado.

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

5.1 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.

5.1.1 Ubicación física y construcción

Los edificios donde se encuentra ubicada la infraestructura de la AC de SIA 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 específicos para evitar daños por posibles incendios.
- Ausencia de ventanas al exterior del edificio.
- Cámaras de vigilancia en las áreas de acceso restringido.
- Controles de accesos basados en tarjeta y contraseña.
- Sistemas de protección y prevención de incendios.
- Protección del cableado contra daños e interceptación de la transmisión de datos.

5.1.2 Acceso físico

El acceso físico a las dependencias del PSC donde se llevan a cabo procesos de certificación 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.

5.1.3 Alimentación eléctrica y aire acondicionado

Los equipos informáticos de la AC de SIA 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.

5.1.4 Exposición al agua

Las instalaciones del 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.

5.1.5 Protección y prevención de incendios

Las instalaciones donde se encuentran los equipos de la AC de SIA, 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.

5.1.6 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.

5.1.7 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.

5.1.8 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.

5.2 Controles de Procedimiento

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se incluye una parte de la misma. 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.

5.2.1 Roles responsables del control y gestión

De acuerdo a la norma CWA 14167-1, el conjunto de productos que implementan la AC de SIA permite el establecimiento de los siguientes roles indispensables para:

- La gestión del sistema

ROLES	RESPONSABILIDADES
Oficial de seguridad (Security Officer)	Responsable global de la administración e implementación de las políticas y procedimientos de seguridad.
Administrador de sistema de certificación (System Administrator)	Autorizado para la realización de cambios en la configuración de sistemas, pero sin acceso a datos del mismo.
Operadores de sistema (System Operator)	Responsable de la gestión del día a día del sistema (Monitorización, backup, recovery...).

Auditor de sistema (System Auditor)	Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
Operador de AC	Responsable de activar las claves de la AC en el entorno Online, o de los procesos de firma de certificados y CRLs en el entorno raíz offline.
Operador de AR (Registration Officer)	Responsable de aprobar, emitir y revocar los certificados de usuario.

Tabla 8 – Roles de gestión del sistema

- La gestión del HSM

ROLES	RESPONSABILIDADES
Administrador HSM	Custodio del acceso, mediante dispositivo seguro (token), a las tareas administrativas del HSM.
Operador HSM	Acceso a la consola del HSM y de la habilitación del mecanismo de accesos mediante dispositivos seguros (token).
Usuario HSM	Custodio del acceso mediante dispositivo seguro (token) a la partición donde se aloja la clave privada de la AC raíz.

Tabla 9 – Roles de gestión del HSM

5.2.2 Número de personas requeridas por tarea

La AC SIA garantiza al menos tres personas, para realizar las tareas que requieran un control multi-persona detalladas a continuación:

- Generación de la clave de las ACs.
- Recuperación y backup de la clave privada de las ACs
- Emisión de certificados de las ACs.
- Activación de la clave privada de las ACs.
- Cualquier otra actividad realizada sobre los recursos hardware y software que dan soporte a la AC raíz.

5.2.3 Identificación y autenticación para cada usuario

Las personas asignadas para cada rol son identificadas para asegurar que solo realiza 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.

5.2.4 Roles que requieren segregación de funciones

La norma CWA 14167-1 establece las siguientes incompatibilidades entre roles:

- Incompatibilidad entre oficial de seguridad y operador del HSM.
- Incompatibilidad entre los roles administrativos (administrador de sistema y operador de la AR).
- Incompatibilidad entre los administradores y los operadores del HSM.
- Incompatibilidad entre el rol auditor de sistema y cualquier otro rol.

5.3 Controles de Personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

El personal que presta sus servicios en el ámbito de la Autoridad de Certificación de SIA 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 adecue lo más posible a las características propias de las tareas a desarrollar.

5.3.2 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.

5.3.3 Requerimientos de formación

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

5.3.4 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.

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6 Sanciones por actuaciones no autorizadas

Se consideran acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación 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.

5.3.7 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.

5.3.8 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 Declaración de Prácticas de Certificación y la normativa de seguridad.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

Se registrarán 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 fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs.
- 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.
- Cambios en las claves de la Autoridad de Certificación.
- Cambios en las políticas de emisión de certificados y en la presente DPC.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor.
- Informes de compromisos y discrepancias.
- Registros de acceso físico.
- Acontecimientos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.

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 otro, los eventos criptográficos, de interface de usuario, de librería.
- **Módulo:** Identifica el módulo que generó el evento. Los posibles módulos son:
 - AC
 - AR
 - Repositorio de información
 - Librerías de control de almacenamiento de información.
- **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. Algunos ejemplos de los parámetros que se incluyen para la descripción del evento “Certificado generado” son: el número de serie, el nombre distintivo del titular del certificado emitido y la plantilla de certificación que se ha aplicado.

5.4.2 Frecuencia de procesamiento de registros de auditoría

Los registros se analizarán de manera manual cuando sea necesario, por ejemplo en caso de que se produzca una alerta del sistema motivada por la existencia de algún incidente, no existiendo una frecuencia definida para dicho proceso.

5.4.3 Periodo de conservación de los registros de auditoria

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

5.4.4 Protección de los registros de auditoria

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

Los registros de software de la AC 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.

5.4.5 Procedimientos de respaldo de los registros de auditoria

SIA realiza copias de seguridad periódicas de los registros de auditoria generados por la AC.

5.4.6 Sistema de recogida de información de auditoria

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

5.4.7 Notificación al sujeto causa del evento

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

5.4.8 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.

5.5 Archivo de registros

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

5.5.1 Tipos de eventos archivados

Los tipos de eventos que se registran en el archivo son:

- Certificados y listas de revocación.
- Datos relacionados con el proceso de solicitud y registro de certificados.
- Las Prácticas y Políticas de Certificación y su histórico.
- Logs de auditoría de la sección 5.4.1 Tipos de evento.
- Eventos de error en los procesos realizados.

5.5.2 Periodo de conservación de registros

Toda la información y documentación relativa a los certificados se conservará durante un mínimo de quince (15) años.

Para los registros de auditoria se contempla lo especificado en el apartado 5.4.3, siempre atendiendo a cualquier particularidad especifica en la Política de Certificación del Certificado correspondiente a los datos involucrados.

5.5.3 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 de quince (15) años. Dicha destrucción requerirá la autorización expresa y por escrito.

5.5.4 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 al Centro de Respaldo.

5.5.5 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 de Certificación Electrónica 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.

5.5.6 Sistema de archivo de información de auditoría

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

5.5.7 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 pueda 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 de eventos de la PKI.

5.6 Cambio de claves de una AC

Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de AC a los titulares y terceros aceptantes de los certificados de la misma, son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicara en el repositorio de SIA (ver apartado 2.1 Repositorios).

5.7 Recuperación en casos de vulneración de una clave y de desastre natural u otro tipo de catástrofe

5.7.1 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 certificación prestados.

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

- La redundancia de los componentes más críticos.
- La respuesta 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 de los datos de creación de firma de alguna Autoridad de Certificación, SIA informará a todos los titulares de certificados, organismo supervisor y terceros aceptantes conocidos que todos los certificados y listas de revocación firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio.

5.7.2 Alteración de los recursos hardware, software y/o datos

Cuando tenga lugar un acontecimiento de anomalías de recursos hardware, software y/o datos, SIA procederá a detener los servicios de la AC hasta que se pueda verificar la seguridad del entorno, si es necesario sustituyendo los componentes afectados por otros cuya integridad sea debidamente verificada. A su vez, se realizará una auditoria para identificar la causa de la alteración y asegurar su no reproducción.

En el caso de verse afectados los certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad

SIA considera el compromiso o la sospecha de compromiso de la clave privada de la AC como un desastre. En caso de verse comprometida la seguridad de la clave privada de la AC, SIA procederá a realizar las siguientes acciones:

- Revocar el certificado de la AC actual, de tal forma que los certificados emitidos por esa AC dejen de tener validez.
- Informar a todos los titulares y suscriptores de certificados que todos los certificados emitidos por esa AC ya no son válidos. Asimismo, notificará al organismo supervisor este hecho.
- Revocar el certificado de la AC subordinada y de todos los certificados vigentes y expedidos por esa AC. Si el certificado revocado es la AC raíz, eliminará el certificado del repositorio y avisará de este hecho en la página web del prestador.
- Publicar la ARL correspondiente.
- Generar una nueva AC con una clave de firma y certificados nuevos.
- Restablecer, tan pronto como sea posible, el servicio.

- Dar conocimiento a los cuerpos y fuerzas de seguridad del estado y/o Fiscalía General del Estado y/o Autoridad Judicial por si pudiese haber actividades constitutivas de delito.

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

SIA restablecerá los servicios críticos (revocación y publicación de certificados revocados) de acuerdo con esta DPC 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 de certificación.

5.8 Cese de una AC o AR

5.8.1 Autoridad de Certificación

En el caso del cese de actividad de la AC, se adoptarán las medidas necesarias para que los potenciales problemas para los titulares de sus certificados y los terceros aceptantes sean los mínimos, así como el mantenimiento de los registros requeridos para proporcionar prueba cierta de la certificación a efectos legales.

En caso de cese de actividad, se comunicará a los titulares de sus certificados, a través del sitio web indicado en el apartado 2.1 Repositorios, con un plazo mínimo de antelación de dos meses al citado cese de actividad, su intención de que la AC correspondiente cese en la actividad como PSC.

En el caso de que SIA decidiera transferir la actividad de PSC a otro organismo, comunicará a los titulares de sus certificados los acuerdos de transferencia. A tal efecto, SIA enviará un documento explicativo de la transferencia de la gestión de los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de dos meses al cese efectivo de su actividad. SIA podrá transferir, con el consentimiento expreso del firmante, la gestión de los certificados que sigan siendo válidos en la fecha del cese. Si no consiguiese el consentimiento del firmante, el certificado correspondiente quedará revocado.

SIA comunicará al organismo supervisor, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados especificando si va a transferir la gestión y a quién o si se extinguirá su vigencia. En especial, 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.

SIA remitirá al organismo supervisor, con carácter previo al cese definitivo de su actividad, la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos previstos en el artículo 20.1.f) de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

5.8.2 Autoridad de Registro

Una vez que la AR cese en el ejercicio de las funciones, transferirá los registros que mantenga a SIA, mientras exista la obligación de mantener archivada la información, y de no ser así, ésta será destruida de manera segura y acreditándolo de manera fehaciente.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de la AC raíz como de la AC subordinada de SIA, se generan y almacenan en un módulo de hardware criptográfico seguro (HSM), que cumple los requisitos de seguridad necesarios.

Las claves y certificados de entidades se emiten según lo dispuesto en la Política de Certificación correspondiente al tipo de certificado.

6.1.2 Entrega de la clave privada al titular

El envío de la clave privada al titular se realizará de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

6.1.3 Entrega de la clave pública al emisor del certificado

La entrega de la clave pública se realizará de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes

Tanto el certificado de la AC raíz como el de la AC subordinada, se publican en los repositorios indicados en el apartado 2.1 Repositorios de esta misma DPC.

6.1.5 Tamaño de las claves

Las claves de la AC raíz de SIA son de 4096 bits.

Las claves de la AC subordinada de SIA son de 4096 bits.

La longitud de las claves de los titulares de certificados, se especifica en la correspondiente Política de Certificación.

6.1.6 Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de la AC raíz y de la AC subordinada está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es RSA.

Los parámetros de generación de claves para cada tipo de certificado emitido, se especifica en la correspondiente Política de Certificación.

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido, se especifica en la correspondiente Política de Certificación.

6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave vienen definidos de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

Todos los certificados emitidos por SIA contienen la extensión “Key Usage” definida por el estándar X.509 v3, la cual se califica como crítica. Asimismo, pueden establecerse limitaciones adicionales mediante la extensión “Extended Key Usage”.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en las extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido creadas ni controladas por SIA.

6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos

6.2.1 Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves de la AC raíz y la AC subordinada, cumplen con los requisitos de seguridad necesarios y garantizan la protección de las mismas.

La puesta en marcha de cada una de las AC, teniendo en cuenta que se emplean módulos criptográficos de seguridad (HSM), conlleva las siguientes tareas:

- Inicialización del HSM.
- Creación de los medios de acceso para los roles de administración y operador.
- Generación de las claves de la AC.

Las medidas desempeñadas para la custodia de las claves de los firmantes, vienen detalladas en su correspondiente Política de Certificación.

6.2.2 Control multi-persona (n de m) de la clave privada

El acceso a la clave privada, requiere de la presencia de un mínimo de tres personas con los roles específicos para poder acceder a la misma, siendo estos roles tanto de controles físicos como controles lógicos.

6.2.3 Custodia de la clave privada

Las claves privadas tanto de la AC raíz como de la AC subordinada, se encuentran almacenadas y protegidas en el HSM, y nunca sale del mismo.

6.2.4 Copia de seguridad de la clave privada

Se realizan copias de seguridad de la clave privada de la AC durante el proceso de generación de las mismas.

Estas copias se realizan a efectos de continuidad de negocio para la recuperación ante desastres. Las copias de seguridad, tienen el mismo nivel de seguridad que la clave original, dado que forma parte del propio módulo de seguridad criptográfico.

Las copias de la clave se guardan en una localización diferente a aquella donde está ubicada la AC.

6.2.5 Archivo de la clave privada

Las claves privadas de los certificados reconocidos de los firmantes nunca serán archivadas por la AC.

6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico

La transferencia de la clave privada solo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de tres personas con roles distintos.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en el módulo criptográfico en el momento de activación de cada una de las AC que hacen uso de dichos módulos.

6.2.8 Método de activación de la clave privada

Tal y como se estipula en el apartado 6.2.2 Control multi-persona de la clave privada, la clave privada tanto de la AC raíz como de la AC subordinada, se activa mediante la inicialización del software de AC por medio de la personación mínima de tres personas con roles específicos. Este es el único método de activación de dicha clave privada.

6.2.9 Método de desactivación de la clave privada

Un administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación mediante la detención del software de la AC. Para su reactivación es necesaria la intervención mínima de los roles descritos en apartados anteriores.

6.2.10 Método de destrucción de la clave privada

Cuando sea necesario, SIA destruirá la clave privada de la AC y su copia de seguridad para garantizar que no se mantiene información residual que se pueda utilizar para reconstruir la clave privada.

En términos general la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.

6.2.11 Clasificación de los módulos criptográficos

Los dispositivos criptográficos utilizados por las autoridades de certificación cumplen con los requisitos de seguridad necesarios para garantizar la protección de las claves de las Autoridades de Certificación.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

SIA conservará todas las claves públicas durante el periodo exigido por la legislación vigente y de acuerdo con lo establecido en este documento.

6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves

El certificado y el par de claves de la AC raíz de SIA tienen una validez de veintidós (22) años y los de la AC subordinada de SIA de quince (15) años.

El periodo de validez del resto de certificados vendrá establecido por la Política de Certificación aplicable a cada uno.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Para la activación de las claves privadas de la AC, es necesaria la intervención mínima del administrador de sistemas, operadores de la AC y administradores del HSM. Este es el único método de activación de dicha clave privada.

En el caso de las claves de los certificados de entidad final, la generación de datos de activación se indica en la correspondiente Política de Certificación.

6.4.2 Protección de los datos de activación

Solo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la AC raíz y AC subordinada.

Para los certificados de entidad final se detallará en su correspondiente política de certificación.

6.4.3 Otros aspectos de los datos de activación

No aplica.

6.5 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.

6.5.1 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.

6.5.2 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.

Los productos utilizados para la prestación de servicios de certificación disponen de certificación Common Criteria y/o FIPS 140-2.

6.6 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.

6.6.1 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.

6.6.2 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.

6.6.3 Controles de seguridad del ciclo de vida

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

6.7 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.

6.8 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.

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 Perfil de certificado

Los certificados emitidos por los sistemas de SIA, serán conformes con lo dispuesto en las siguientes normas y especificaciones técnicas:

- ETSI TS 101 862 “Qualified Certificate profile” conocida como “European profile for Qualified Certificates”.
- RFC 5280 “Internet X.509 Public Key Infrastructure. Certificate and CRL Profile”.
- RFC 3739 “Internet x509 Public Key Infrastructure. Qualified Certificates Profile”.
- Perfiles de Certificados Electrónicos para la Administración General del Estado según Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos Los perfiles están definidos en el Anexo II de la Resolución de 29 de noviembre de 2012 de la Secretaría de Estado de Administraciones Públicas.
- ETSI TS 102 280 “X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons”.

7.1.1 Número de versión

Los certificados siguen el estándar definido X.509 versión 3.

7.1.2 Extensiones del certificado

Los certificados emitidos por SIA de usuario vinculan la identidad de una persona a una determinada clave pública. Para garantizar la autenticidad y no repudio, toda esta información estará firmada electrónicamente por SIA, entidad encargada de la emisión.

Las extensiones utilizadas en los certificados son:

- Authority Key Identifier.
- Subject Key Identifier.
- KeyUsage. Calificada como crítica.
- ExtKeyUsage.
- CRL Distribution Point.
- Authority Information Access.
- Qualified Certificate Statements.

- CertificatePolicies.
- Subject Alternative Name.

Los certificados emitidos con la consideración de reconocidos incorporan adicionalmente el identificador de declaración representado por un OID definido por el TS 101 862, sobre perfiles de certificados reconocidos: 0.4.0.1862.1.1.

Los certificados que son expedidos con la calificación de reconocidos están identificados en la extensión QcStatements (OID 1.3.6.1.5.5.7.1.3) que indica la existencia de una lista de declaraciones conforme a la especificación técnica TS 101 862, concretamente los certificados reconocidos expedidos por SIA incluirán como mínimo las declaraciones:

- QcCompliance, establece la calificación con la que se ha realizado la emisión del “Certificado reconocido”.
- QcEuRetentionPeriod, determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de SIA, es de quince (15) años.

SIA tiene definida una política de asignación de OIDs dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de SIA comienza por el prefijo 1.3.6.1.4.1.39131.10.3.

Por otro lado, el certificado contiene más información sobre el firmante en la extensión SubjectAltName. En esta extensión se utilizará el sub-campo DirectoryName que incluye atributos definidos por SIA con la información del firmante con objeto de proporcionar una forma sencilla de obtener los datos personales del firmante y el suscriptor.

Los OIDs de los atributos definidos por SIA en el sub-campo DirectoryName de la extensión SubjectAltName comienzan por el prefijo 1.3.6.1.4.1.39131.10.2 y se describen en el cuadro siguiente.

OID	Concepto	Descripción
1.3.6.1.4.1.39131.10.2.1	Tipo de certificado	Tipo de certificado
1.3.6.1.4.1.39131.10.2.2	Nombre	Nombre del usuario
1.3.6.1.4.1.39131.10.2.3	Apellido1	Primer apellido del usuario
1.3.6.1.4.1.39131.10.2.4	Apellido2	Segundo apellido del usuario
1.3.6.1.4.1.39131.10.2.5	DNI	DNI del usuario

Tabla 10 – Definición extensión SubjectAltName

En la política de certificación de cada tipo de certificado se especificará con más detalle las extensiones requeridas y el perfil del certificado.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

7.1.4 Formatos de nombre

Los certificados emitidos por SIA contienen el “distinguished name X.500” del emisor y del titular del certificado en los campos “issuer” y “subject” respectivamente.

7.1.5 Restricciones de nombre

No se emplean restricciones de nombres.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente DPC es 1.3.6.1.4.1.39131.10.1.0. Se le añade una extensión con formato X.Y que recoge la versión.

De esta forma el OID 1.3.6.1.4.1.39131.10.1.1.X.Y correspondería a la subversión Y de la versión X de esta DPC.

Los identificadores de las Políticas de Certificación asociadas bajo las que se emiten los certificados de Identidad Pública son los siguientes:

Política de Certificados de persona física vinculada a empresa	1.3.6.1.4.1.39131.10.1.2
Política de Certificados de Ciudadano	1.3.6.1.4.1.39131.10.1.3

Tabla 11 – OID políticas de certificación

7.1.7 Uso de la extensión “PolicyConstraints”

No estipulado.

7.1.8 Sintaxis y semántica de los “PolicyQualifier”

La extensión “Certificate Policies” contiene los siguientes “Policy Qualifiers”:

- URL DPC: contiene la URL donde puede obtener la última versión de la DPC y de las Políticas de Certificación asociadas.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

7.1.9 Tratamiento semántico para la extensión “Certificate Policy”

Teniendo en cuenta los matices introducidos por la RFC 5280 respecto al uso de esta extensión se decide incluir el valor 2.5.29.32.0 en los certificados de las ACs. Partiendo de un OID común de la AC reconocida, se especificarán OIDs diferentes para cada una de las políticas de certificación de cada tipo de certificado.

7.2 Perfil de CRL

7.2.1 Numero de versión

La infraestructura del SIA soporta y utiliza CRLs X.509 versión 2 (v2).

7.2.2 CRL y extensiones

Las CRLs emitidas por SIA serán conformes con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, April 2002.
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework.

CAMPOS Y EXTENSIONES	VALORES
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption

Numero de CRL	Número incremental
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
Fecha de próxima actualización	Fecha efectiva de emisión + 24 horas
Identificador de la clave de autoridad	Hash de la clave del emisor

Tabla 12 – Perfil CRL y extensiones

7.3 Perfil de OCSP

Los certificados emitidos por AC SIA son conformes a la norma:

RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”.

7.3.1 Número de versión

Los certificados de OCSP Responder utilizarán el estándar X.509 versión 3 (X.509 v3).

7.3.2 Extensiones del OCSP

Las principales extensiones para OCSP son las que se muestran en la siguiente tabla:

Campo	Obligatorio	Crítico
1. Issuer Alternative Name	No	No
2. Authority/Subject key Identifier	No	No
3. CRL Distribution Point	No	No
4. Key usage	Si	Si

5. Enhanced Key usage	SI	No
-----------------------	----	----

Tabla 13 – Extensiones del certificado de OCSP

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia o circunstancias de los controles para cada autoridad

Se realizarán auditorías internas periódicas, generalmente con carácter anual. Asimismo, SIA podrá realizar una auditoría externa cada dos años y realizada por una entidad reconocida y acreditada con objeto de confirmar que los servicios de expedición de certificados 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.

8.2 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.

8.3 Relación entre el auditor y la Autoridad auditada

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.

8.4 Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de SIA con esta DPC. También determinara los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

En general los criterios establecidos en la sección 3.3 (“Introduction to conformity assessment of Certification Authorities”) y 3.5 (“Guidance on the conformity assessment process”) de la CWA 14172-2.

8.5 Acciones a emprender como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoria 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.

8.6 Comunicación de resultados

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

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

Los precios de los servicios de certificación o cualquier otro servicio 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.

9.1.2 Tarifas de acceso a los certificados

No estipulado.

9.1.3 Tarifas de acceso a la información de estado o revocación

SIA provee un acceso a la información relativa al estado de los certificados o de los certificados revocados de manera gratuita, por medio de la publicación de las correspondientes CRLs o de un servicio en línea OCSP cuando aplique al tipo de certificado.

9.1.4 Tarifas de otros servicios tales como información de políticas

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

9.1.5 Política de reembolso

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de SIA para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente.

9.2 Responsabilidad Financiera

9.2.1 Seguro de responsabilidad civil

SIA, en su actividad como Prestador de Servicios de Certificación 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 PSC tal 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 €.

Dichas garantías no son aplicables a los certificados que no sean reconocidos, por lo que la cuantía que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial se limita a un máximo de 6.000 €.

9.3 Confidencialidad de la información y protección de datos

9.3.1 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 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

9.3.1.1 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.

9.3.1.2 Información no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.
- La contenida en las distintas Políticas de Certificación.

- La información contenida en los certificados, puesto que para su emisión el solicitante otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de revocación de certificados (CRLs) y otros servicios con información del estado de los certificados.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

SIA pone a disposición de los Terceros Aceptantes las listas de revocación de certificados (que no contienen datos de carácter personal) para el cumplimiento diligente de los servicios de certificación. El Tercero Aceptante, como cesionario de la información contenida en dichas listas, únicamente podrá utilizarla a tal fin.

9.3.2 Información no calificada como privada

Es considerada no confidencial la siguiente información:

- Los certificados.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados, así como el resto de informaciones de estado de revocación.

9.3.2.1 Deber de secreto profesional

Todo el personal encargado de la administración, operación y supervisión de la AC 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.

9.4 Protección de datos personales

9.4.1 Política de protección de datos de carácter personal

SIA mantiene un plan alineado con el cumplimiento de los requisitos establecidos en la normativa aplicable sobre protección de datos de carácter personal, concretamente con lo dispuesto por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante, LOPD) y su reglamento de desarrollo.

Sin menoscabo de otras obligaciones, las Autoridades de Registro que se constituyan en SIA verificarán que el solicitante de un certificado presta su consentimiento al tratamiento de sus datos de carácter personal, previa información sobre la finalidad a la que se van a destinar, su inclusión en el fichero declarado al efecto por SIA ante la Agencia Española de protección de Datos, (en adelante, el Fichero) así como el resto de aspectos a que se refiere el artículo 5 de la LOPD.

En los casos en que los datos no hayan sido recabados directamente de los interesados, SIA, o su representante, informarán de forma expresa, precisa e inequívoca a estos, dentro de los tres meses siguientes al momento del registro de los datos, de lo indicado en el párrafo anterior.

El titular de los datos podrá, en cualquier momento, ejercitar los derechos de acceso, rectificación, cancelación y oposición, dirigiéndose para ello al domicilio social de SIA, identificado en varios de los epígrafes de la presente DPC.

Los datos contenidos en el Directorio seguro de Certificados que tengan la consideración de datos de carácter personal a efectos de lo dispuesto en la LOPD, no serán accesibles a terceros diferentes de los titulares de los mismos, salvo con el consentimiento del titular o en los casos en los que concurra alguna de las excepciones previstas en la LOPD y su normativa de desarrollo.

SIA ha creado un fichero de datos de carácter personal cuya finalidad es la gestión y uso de los certificados electrónicos, al cual se le aplican las medidas de seguridad correspondientes al nivel básico, de acuerdo a lo dispuesto en el Título VIII del Reglamento de desarrollo de la LOPD. En dicho fichero se recogen, en concreto, los datos de carácter personal contenidos en:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por los firmantes.
- Cualquier otro dato de carácter personal recogido con la finalidad del fichero.

En cumplimiento de lo dispuesto en el artículo 19.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, esta DPC tiene la consideración de “Documento de Seguridad”, a los efectos previstos en la legislación en materia de protección de datos de carácter personal, y contiene todos los requisitos exigidos para dicho documento en la mencionada legislación, siendo los datos de carácter personal protegidos frente a su posible pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en Reglamento de desarrollo de la LOPD, aprobado en virtud de Real Decreto 1720/2007, de 21 de diciembre.

9.4.2 Documento de seguridad LOPD

9.4.2.1 Aspectos cubiertos

La presente DPC, tal como se señala en el punto 1.1, se ha hecho de acuerdo a la especificación RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” del Internet Engineering Task Force (IETF) para este tipo de documentos.

No obstante lo anterior y teniendo en cuenta lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, que considera la DPC como documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal, resulta obligado añadir el presente apartado con objeto de recoger todos los requisitos contemplados en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 diciembre, de protección de datos de carácter personal.

A tal fin se tratan los siguientes aspectos:

- Funciones y obligaciones del personal.
- Estructura básica de datos de carácter personal.
- Nivel de seguridad aplicable.
- Sistemas de información que soportan el fichero.
- Relación de usuarios.
- Notificación y Gestión de Incidencias.
- Copias de respaldo y recuperación.
- Control de Accesos.
- Ficheros Temporales.
- Gestión de Soportes.
- Utilización de datos reales en pruebas.

9.4.2.2 Funciones y obligaciones del personal

Esta DPC, así como futuras versiones de la misma, es conocida por todas las personas con acceso autorizado a los datos de carácter personal contenidos en el Fichero, siendo de obligado cumplimiento para las mismas las funciones y obligaciones establecidas, tanto en la presente DPC, como en los procedimientos internos que desarrollan el documento de seguridad en ella contenido.

9.4.2.3 Estructuras de datos de carácter personal

En la siguiente tabla se recoge la estructura de los datos de carácter personal incorporados en el Fichero, utilizando las denominaciones previstas en el formulario de notificación de ficheros ante la Agencia Española de Protección de Datos:

DATOS TRATADOS	
Datos de carácter Identificativo	DNI / NIF
	Nombre y apellidos
	Dirección electrónica
	Nº registro Personal
	Firma electrónica
Datos de detalles de empleo	Otros: Empresa

Tabla 14 – Datos de carácter personal tratados

En el apartado 7 se recoge la estructura detallada del perfil del certificado al igual que en la PC.

9.4.2.4 Nivel de seguridad

Los datos de carácter personal tratados exigen el nivel de seguridad básico, sin perjuicio de que, dadas las especiales características de seguridad que ha de tener una PKI y el nivel de seguridad que establece esta DPC, se proporciona un nivel de seguridad superior.

9.4.2.5 Sistema de información

Dentro de la estructura de sistemas de información que constituye SIA se pueden distinguir tres subsistemas con alguna implicación en el tratamiento de datos de carácter personal. A continuación se relacionan y describen de forma sintética:

- **Subsistema de gestión de certificados:** Se encarga de la creación de los certificados conforme al estándar X.509v3, donde se introducen las claves generadas por el subsistema de generación de claves y otros datos identificativos que se definen en la correspondiente PC.
- **Subsistema de Autoridad de Registro:** Se encarga de la identificación del solicitante del certificado del certificado para proceder a la emisión posterior del certificado por SIA.
- **Subsistema de publicación:** Se encarga de la gestión de la publicación de las listas de revocación de certificados (CRL).

9.4.2.6 Relación de usuarios

El Coordinador de Seguridad mantiene una relación de los usuarios con acceso a los datos de carácter personal tratados por la PKI en la que se indica su rol y nivel de acceso. Dicha relación de usuarios tiene carácter confidencial por motivos de seguridad, por lo que será precisa una petición motivada al Coordinador de Seguridad para tener acceso a la misma.

No se incluyen en esa relación los usuarios con acceso a los certificados electrónicos a efectos de hacer uso de los mismos para el envío de información cifrada ni los usuarios con acceso a las CRL.

9.4.2.7 Notificación y gestión de incidencias

Los procedimientos internos del Departamento de Sistemas de Información asociados a la gestión de problemas aseguran que todas las incidencias se registran y documentan, realizándose un seguimiento de las mismas. Se registra información relativa a: fecha, hora, tipo de incidencia, persona que comunica la misma, persona a quien se asigna la resolución de la incidencia, documentación sobre la causa y sus efectos.

9.4.2.8 Copias de respaldo y recuperación

Las copias de respaldo se realizan de forma diaria conforme a la normativa en vigor de SIA para sus ordenadores centrales.

Las recuperaciones de datos se hacen con la autorización del responsable del fichero:

- Incidencia en el sistema informático: Se comunica al responsable informático del sistema, quien deberá obtener la autorización del propietario mediante los procedimientos establecidos al efecto.
- Incidencias en la infraestructura del sistema informático: Se siguen los procedimientos establecidos en los planes de respaldo del Departamento de Sistemas de Información para cada contingencia.

9.4.2.9 Control de accesos

Las autorizaciones de acceso a los sistemas de información estarán basadas exclusivamente en el principio de necesidad para el trabajo. Los administradores de usuarios y de elementos se encargarán de validar siempre esta necesidad antes de conceder el acceso a los datos.

Asimismo, todos los elementos que permitan acceder a datos personales estarán catalogados como de uso restringido.

9.4.2.10 Ficheros temporales

El software utilizado para generar un certificado electrónico conforme al estándar X.509 v3 genera ficheros temporales, ficheros de registros de auditoria, que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.4.2.11 Gestión de soportes

Los soportes internos están correctamente identificados por su código de barras o incluyen su correspondiente etiqueta identificativa.

Los soportes están ubicados en las salas de ordenadores. El acceso a estas salas está restringido, las autorizaciones permanentes son validadas por el Jefe del Departamento de Sistemas de la Información y el acceso provisional solo podrá ser autorizado por el Jefe de Explotación o el Jefe de Operación.

Toda salida de soportes fuera del hosting de SIA deberá ser autorizada por el Administrador de la PKI. El departamento de Sistemas de la Información mantiene un registro en papel de la entrada / salida de soportes.

Los soportes que hubieran contenido datos personales se borrarán utilizando un borrado físico o procedimiento similar. Este proceso se realiza siempre que se reutilizan soporte que van a ser enviados al exterior; en otros casos no existe manipulación de soportes, ya que la gestión es realizada directamente por los robots que gestionan cartuchos.

Antes de autorizar la salida de soportes que contengan datos personales para operaciones de mantenimiento, se procederá a su borrado físico o a su des-magnetización. La salida de soportes por mantenimiento sólo se daría en el caso de discos.

9.4.2.12 Utilización de datos reales en pruebas

No se utilizarán datos personales reales para la realización de pruebas, salvo que se aseguren los mismos niveles de seguridad que establece la presente DPC.

Los procedimientos de pruebas utilizados en el Departamento de Sistemas de Información aseguran el cumplimiento del nivel de seguridad requerido para la utilización de datos reales en pruebas.

9.5 Derechos de propiedad Intelectual

En los términos establecidos en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, SIA es titular en exclusiva de todos los derechos de propiedad intelectual relativos a los certificados electrónicos emitidos por esta AC para personas y componentes informáticos, a las listas de revocación de certificados y otros servicios de consulta implementados, al contenido de la presente Declaración de Practicad de Certificación y a las Políticas de Certificación. 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 de la misma AC.

Los identificadores de objeto (OIDs) utilizados son propiedad de SIA y han sido registrados en Internet Assigned Number Authority (IANA) bajo la rama iso.org.dod.internet.private.enterprise.1.3.6.1.4.1.39131 (SIA). Esto puede ser consultado y comprobado en <http://www.iana.org/assignments/enterprise-numbers>.

Queda prohibido, salvo acuerdo expreso en contrato celebrado con SIA, el uso total o parcial de cualquiera de los OID asignados a SIA, salvo para los usos específicos con que se incluyeron en el Certificado o en el Directorio.

9.6 Obligaciones

9.6.1 Obligaciones de la AC

Los servicios prestados por la AC de SIA en el contexto de esta DPC son los servicios de emisión y revocación de certificados, y emisión de listas de revocación de acuerdo con esta DPC.

SIA, como prestador de servicios de certificación:

- Actuará relacionando una determinada clave pública con su titular a través de la emisión de los certificados, de conformidad con los términos de la DPC.
- Prestará servicios, en el contexto de la DPC, para la emisión, renovación y revocación de los certificados.
- Comunicará los cambios de la DPC de acuerdo con lo establecido en el propio documento.
- Emitirá certificados que sean conformes con la información conocida en el momento de su emisión, y libre de errores en la entrada de datos.
- Revocará los certificados en los términos recogidos en la DPC.
- Pondrá a disposición de los ciudadanos los certificados correspondientes a la AC de SIA.
- Protegerá la clave privada de la AC de SIA.
- Utilizará 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.
- 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 Ley 59/2003, de 19 de Diciembre, de firma electrónica.
- Conservar registrada toda la información y documentación relativa a los certificados reconocidos durante un mínimo de quince años.
- Colaborar con los procesos de auditoría que se realicen sobre la Infraestructura de Certificación.
- Operar de acuerdo con la legislación aplicable. En concreto con:
 - Directiva 1999/93/CE del parlamento Europeo y del consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
 - Ley 59/2003, 19 de diciembre, de firma electrónica.
 - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ella emitidos y al organismo supervisor competente.
- No almacenar ni copiar los datos de creación de firma de la persona a la que haya prestado sus servicios.
- Mantener un repositorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido extinguida.
- Utilizar sistemas fiables para almacenar certificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

9.6.2 Obligaciones de la AR

Las Autoridades de Registro también se obligan en los términos definidos en la presente DPC para la emisión de certificados, principalmente a:

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

9.6.3 Obligaciones de los firmantes

Es obligación de los titulares de los certificados emitidos bajo la presente DPC:

- Suministrar a las Autoridades de Registro información exacta, completa y veraz en relación a los datos que estas les soliciten para realizar el proceso de expedición o extinción del certificado.
- Notificar cualquier modificación de los datos suministrados en el proceso de registro o de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.
- Conocer y aceptar las condiciones de utilización de los certificados
- Utilizar de forma correcta el certificado electrónico y sus claves y no utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o haya sido revocado.
- Comunicar a SIA a través de los mecanismos que se habilitan a tal efecto, cualquier mal funcionamiento del certificado.
- Proteger sus datos de activación de firma, y los mecanismos de autenticación, tomando las precauciones razonables para evitar su pérdida, revelación o uso no autorizado.
- Cumplir las obligaciones y supuestos que se establecen para el usuario en la DPC y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- No superar los límites que figuren en el certificado electrónico. El firmante asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.
- Así mismo, el firmante se responsabiliza de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al firmante.

9.6.4 Obligaciones de los terceros aceptantes

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 en que confía.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.

9.6.5 Obligaciones de otros participantes

Sin estipulación adicional.

9.7 Renuncias de garantías

La infraestructura de clave pública de SIA podrá renunciar a todas las garantías del servicio que presta y que no se encuentren vinculadas a las obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Dichas renuncias serán previamente notificadas a las partes afectadas.

9.8 Limitaciones de responsabilidad

Subsumido en el siguiente apartado.

9.9 Responsabilidades

9.9.1 Limitaciones de responsabilidades

SIA, que actúa como órgano al que se le atribuyen las competencias de AC, responderá en caso de incumplimiento de las obligaciones contenidas en la Ley 59/2003, de 19 de diciembre, de firma electrónica y normativa de desarrollo, y en la presente DPC.

9.9.2 Responsabilidades de la Autoridad de Certificación

- 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 Ley 59/2003, de 19 de diciembre, de firma electrónica.
- La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al PSC demostrar que actuó con la diligencia profesional que le es exigible.
- De manera particular, SIA responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.
- SIA como PSC asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

- SIA no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del ciudadano y/o del prestador de servicio telemático.
- SIA no será responsable de la utilización incorrecta de los certificados ni las claves, ni cualquier daño indirecto que pueda resultar de la utilización del certificado.
- SIA no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado.
- SIA no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta DPC, 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 DPC y en la Ley.

9.9.3 Responsabilidades de la Autoridad de Registro

La autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los solicitantes y la validación de sus datos, con las mismas limitaciones que se establecen en el anterior apartado para la Autoridad de Certificación.

9.9.4 Responsabilidad del titular

Es responsabilidad del suscriptor y el firmante cumplir con las obligaciones estipuladas en el presente documento y en la PC correspondiente, y en el instrumento jurídico vinculante.

9.9.5 Delimitación de responsabilidades

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

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos utilizados por el suscriptor o por los terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento del directorio de certificados y CRLs emitidos por la Autoridad de Certificación.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.