Carrer d'Avila nº29 Pta 1 – 08005 Barcelona
www.signaturit.com - Tel. 960 031 203

DECLARACIÓN DE PRÁCTICAS Y POLITICAS DE CERTIFICACION DE

SIGNATURIT GLOBAL CA

1.3.6.1.4.1.50646.5.1

SIGNATURIT SOLUTIONS, S.L.U. - PRESTADOR DE SERVICIOS ELECTRÓNICOS DE CONFIANZA

Signaturit Solutions, S.L.U.

Fecha del documento: 01/05/2023

CONTROL DE VERSIONES

Revisión	Fecha	Descripción
0	01/04/2023	Versión inicial (borrador)
1	01/05/2023	Se precisa que bajo esta versión 1 de la DPC solo se incluye el perfil de certificado de tipo “Ciudadano” en soporte Software. No obstante, se contemplan practicas aplicables a perfiles de certificados centralizados y de atributo por si se incorporasen posteriormente.

Intervinientes

Versión	Fecha	Autor	Revisado por	Aprobado por
0	01/04/2023	France Vidal (Compliance)	Sergio Serrano (PKI)	Felix Esteban (CTO)
1	01/05/2023	France Vidal (Compliance)	Sergio Serrano (PKI)	Felix Esteban (CTO)

CONTENIDOS

1 INTRODUCCIÓN

1.1 VISTA GENERAL

El presente documento constituye la Declaración de Prácticas de Certificación (en adelante CPS, Certification Practice Statement) de “**Signaturit Global CA”,** Autoridad de Certificación titularidad del Prestador Signaturit Solutions, S.L.U. (en adelante, Signaturit), para la prestación del **SERVICIO DE EXPEDICIÓN DE CERTIFICADOS ELECTRÓNICOS CUALIFICADOS.**

Signaturit Global CA es una Autoridad de Certificación Subordinada externa (en adelante SubCA) bajo la CA raíz “**IvSign Root CA”** que es una Jerarquía de Certificación gestionada y propiedad de Ivnosys Soluciones, S.L.U. (en adelante Ivnosys Soluciones) con NIF B-98333362 y domicilio en C/ Acceso Ademuz nº12, 1º1 – 46980 Paterna (Valencia).

Por tanto, esta CPS se encuentra en conformidad con la CPS de IvSign Root CA de Ivnosys Soluciones y sus políticas de certificación y, especialmente, en lo referente a las disposiciones sobre Autoridades de Certificación Subordinadas Externas.

Ambas entidades mercantiles, Signaturit y Ivnosys Soluciones, pertenecen al “Grupo Signaturit”.

La prestación de este servicio se realiza de acuerdo con el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (de ahora en adelante, eIDAS) y la Ley Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Los certificados digitales emitidos según esta CPS podrán emitirse en los siguientes modos o formatos a medida que vaya incorporando nuevos perfiles en la tabla que figura al final del presente apartado:

- En modo software (formato PKCS#12) utilizando la infraestructura técnica de la PKI de Ivnosys Soluciones.
- Centralizados en el sistema de gestión de claves **IvSign** de Ivnosys Soluciones en cual se encuentra integrado de forma confiable con la PKI IvSign Root CA. (no disponible en la versión 1 de esta CPS)
- Opcionalmente, para algunos perfiles está soportada su emisión en dispositivos Hardware (HSM o Smartcard) (no disponible en la versión 1 de esta CPS)

Para los servicios centralizados (no disponible bajo la versión 1 de esta CPS), Signaturit utilizará el **Servicio IvSign** desarrollado por Ivnosys Soluciones con el objetivo de permitir la realización de firmas y sellos electrónicos a distancia, conforme posibilita e incentiva el Reglamento eIDAS. Por este motivo, las Autoridades de Certificación dependientes **IvSign Root CA,** pueden utilizar el Sistema de Firma a Distancia IvSign como formato preferente para la expedición de certificados, como es el caso de Signaturit Global CA.

De acuerdo con el Reglamento eIDAS, para garantizar que un sistema de gestión de firmas electrónicas a distancia, gestionado por el prestador de servicios de confianza en nombre del titular tenga el mismo reconocimiento jurídico que los que utilizan un entorno completamente

gestionado por el usuario, se deben aplicar unos sistemas y procedimientos de seguridad específicos que permitan garantizar que el entorno es fiable y se utiliza bajo el control exclusivo del firmante. **IvSign** dispone de una Declaración de Prácticas de Gestión de Servicio de Confianza (en adelante PS de IvSign) que describe los procedimientos, prácticas y controles del sistema confiable IvSign para garantizar este objetivo.

Por estos motivos, cuando aplique, esta CPS hará, en todo momento, referencia a las siguientes Declaraciones de Prácticas de servicios:

- CPS IvSign Root CA con OID 1.3.6.1.4.1.47304.3.1, localization: https://policy.ivnosys.com/
- Declaración de Prácticas de Gestión del Servicio de Centralización de Claves y Firma Electrónica a Distancia IvSign de Ivnosys Soluciones S.L.”, con OID 1.3.6.1.4.1.47304.1.1, localización: https://policy.ivnosys.com

Signaturit Solutions, S.L.U. tiene registrado el siguiente OID raíz (o “arc”) para identificar todas sus políticas:

OID	1.3.6.1.4.1.50646.
Descripción	Signaturit Solutions, S.L.U.

Signaturit Global CA es una CA intermedia multi-politica que puede emitir certificados para personas físicas y jurídicas (actualmente, sólo para personas físicas bajo la versión inicial de esta CPS) conforme al Reglamento eIDAS y Ley 6/2020. Todas las políticas de certificados que se emiten por la CA **Signaturit Global CA** de acuerdo con esta CPS están identificadas mediante un OID con el prefijo 1.3.6.1.4.1.50646.5.1.

Con carácter general, todos los certificados emitidos bajo esta CPS disponen, al menos, de dos políticas de certificación:

- La política estándar para certificados cualificados de la Unión Europea emitidos a personas físicas o jurídicas definida por la serie de estándares europeo ETSI EN 319 411 y ETSI EN 319 412:
    - ETSI EN 319 412-2, para la expedición de certificados electrónicos cualificados a personas físicas:
        - **QCP-n**, para firmas electrónicas avanzadas basadas en un certificado cualificado.
        - **QCP-n-qscd**, para firmas electrónicas cualificadas.
    - ETSI EN 319 412-3, para la expedición de certificados electrónicos cualificados a personas jurídicas:
        - **QCP-l**, para sellos electrónicos avanzados basados en un certificado cualificado
        - **QCP-l-qscd**, para sellos electrónicos cualificados.
- Y una política propia de la CA que regula el ámbito de uso de los certificados. Bajo esta CPS se identifican las siguientes políticas de este tipo:

- **Ciudadano**: Identifica a una persona física sin establecer ningún tipo de vinculación.

- En aquellos certificados que lo permitan, se incluye una tercera política que hace referencia a los **perfiles de certificados basados en la Ley española 40/2015**. Consultar el Anexo de políticas, donde se especifica los perfiles compatibles con esta política, en caso de haber sido creado. (no disponible en la versión 1 de esta CPS)

En la siguiente tabla se relacionan todos los OIDs que identifican las políticas de certificación cualificadas de **Signaturit Global CA** y vigentes en cada versión de la CPS aprobada:

Tipo certificado cualificado (PERSONALES)	OID POLÍTICAS		SOPORTE
	S	SIGNATURIT SOLUTIONS	
	E	ETSI EN 319 411 2	
Ciudadano	S	1.3.6.1.4.1.50646.5.16.1.1.2	Software
	E	0.4.0.194112.1.0	

1.2 IDENTIFICACIÓN DE DOCUMENTO

Esta CPS tiene los siguientes datos de identificación:

Nombre	DECLARACION DE PRACTICAS DE Y POLITICAS DE CERTIFICACION DE SIGNATURIT GLOBAL CA
Versión	1
OID	1.3.6.1.4.1.50646.5.1
Localización	https://policy.signaturit.com

1.3 COMUNIDAD Y ÁMBITO DE APLICACIÓN

1.3.1 Autoridades de certificación

Una CA es el ente responsable de la emisión y gestión del ciclo de vida de los certificados digitales. Actúa como tercera parte de confianza, entre el Titular y la Parte Usuaria o Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona. La CA tiene la responsabilidad final en la provisión de los servicios de certificación. La CA está identificada en el campo Asunto (Issuer) del certificado digital.

Una CA pertenece a un prestador de servicios de confianza (TSP) que ofrece el servicio de emisión certificados digitales. El TSP es una entidad jurídica indicada en el atributo organización (O) del campo emisor (Issuer) del certificado digital asociado.

Una Autoridad de certificación (CA) utiliza Autoridades de registro (RA) para realizar las labores de comprobación y almacenamiento de la documentación de los contenidos incorporados en el certificado digital. En cualquier momento la CA puede cubrir las labores de una RA.

Signaturit Global CA es Autoridad de Certificación subordinada a la Autoridad de Certificación de la siguiente Jerarquía de la Root de Ivnosys Soluciones:

Distinguised Name (DN)	CN = IvSign Root CA O = IVNOSYS SOLUCIONES S.L.U. 2.5.4.97 = VATES-B98333362 OU = TRUST SERVICES S = VALENCIA C = ES
Huella digital (SHA-256)	C94BFDADED2CFAF77469C871531956B1 455B24EC21148E66AE1C85E368323A8C
URL publicación	http://ca.ivsign.com/certs/ivsignrootca.crt

Por lo que bajo esta CPS, Ivnosys Soluciones, gestiona la jerarquía de IvSign Root CA.

En cuanto a la Autoridad de Certificación intermedia **Signaturit Global CA**, propiedad de Signaturit Solutions, S.L.U., tiene la siguiente identificación:

Distinguised Name (DN)	CN = Signaturit Global CA O = SIGNATURIT SOLUTIONS S.L.U. 2.5.4.97 = VATES-B66024167 S = BARCELONA C = ES
Huella digital (SHA-256)	3BE056DA32623D5E006C90006A846615EFC4A7573FF339607FA0144BF920FAF4
URL publicación	https://policy.signaturit.com

1.3.2 Autoridades de Registro (RA)

Una RA puede ser una persona física o jurídica que actúa conforme esta CPS y, en su caso, mediante un acuerdo suscrito con Signaturit, ejerciendo las funciones de gestión de las solicitudes, identificación, validación de documentación, registro de los solicitantes del certificado y validación de las emisiones. Las RA son autoridades delegadas de la CA, aunque ésta es la responsable del servicio en última instancia.

Bajo las presentes prácticas se reconocen, además del propio PSC, los siguientes tipos de RA:

- **RA Externa**: Aquella gestionada por una organización pública o una entidad privada para la distribución de certificados, con carácter general, a personas físicas o a entidades con las que tenga establecido algún tipo de relación (laboral, mercantil, colegial, etc.).
- **RA Remota**: RA Externa integrada que se comunica con la CA mediante la capa de integración de la plataforma de gestión de la PKI de Signaturit.
- **PVP**: Punto de Verificación Presencial dependiente de una RA. Su principal misión es la de cubrir la identificación del solicitante y de la entrega de documentación a la RA, la cual la validará según la Política aplicable para tramitar la solicitud de emisión del certificado.

A los efectos de la presente CPS podrán actuar como RA:

- La propia Autoridad de Certificación.
- Las Autoridades de Registro Externas, como entidades delegadas de una CA, a la que se vinculan contractualmente, para llevar a cabo los registros completos de Sujetos/Firmantes dentro del ámbito de actuación acordado.

A su vez, cualquier RA puede delegar en los Puntos de Verificación Presencial (PVP) la función de identificación del titular del solicitante, de recogida de documentación y, si así queda establecido, de cotejo de documentación y verificación de su idoneidad. Se vinculan contractualmente con una RA mediante un contrato tipo proporcionado por el PSC. En base a la documentación suministrada por el PVP, el operador de la RA comprueba la documentación, y en su caso, da curso a la emisión del certificado por la CA sin necesidad de realizar nueva verificación de la identidad. En la presente CPS, para simplificar, nos referiremos a funciones de registro u obligaciones de la RA sin distinción de si lo ejecuta la RA o el PVP, lo cual viene regulado contractualmente.

1.3.3 Solicitante

El Solicitante es aquella persona física que realiza los trámites necesarios para la obtención de un certificado digital.

En los certificados personales, es la persona que solicita el certificado para sí misma o en representación de un tercero.

En los certificados de sello electrónico (no disponibles en la versión 1 de esta CPS), es la persona con facultades de representación suficientes para solicitar el certificado en nombre de una Entidad.

1.3.4 Sujeto/Titular, Firmante o Creador del sello

El Titular del certificado es la persona física o persona jurídica que ostentará la titularidad del certificado y cuyos datos identificativos aparecen en el certificado.

Entendemos por Firmante el Titular persona física que crea la firma electrónica. En la CA de Signaturit el Firmante puede ser (según los perfiles creados):

- Una persona física que actúa en su propio nombre y derecho
- Una persona física en representación de una Entidad con o sin personalidad jurídica. (no disponible en la versión 1 de esta CPS)

- Una persona física autorizada para ser identificada como vinculada a una Entidad con o sin personalidad jurídica (no disponibles en la versión 1 de esta CPS)

Entendemos por Creador del sello, el Titular persona jurídica que es el creador del sello en los certificados de sello electrónico (no disponibles en la versión 1 de esta CPS)

El Titular del certificado viene descrito en el atributo CN (Common Name) del campo DN (Distinguished Name) del certificado.

1.3.5 Suscriptores

Los suscriptores de los certificados emitidos por la CA son personas físicas o entidades con o sin personalidad jurídica que han contratado el servicio de certificación con Signaturit. Por tanto, serán los propietarios de los certificados.

En concreto:

- En los certificados personales, el Suscriptor es la persona física Titular del certificado.
- En los certificados personales con atributo de vinculación o representación con una Entidad, el Suscriptor es la Entidad que contrata el servicio para las personas con las que mantiene una determinada relación (no disponibles en la versión 1 de esta CPS).
- En los certificados de sello electrónico, el Suscriptor es la Entidad o su matriz (no disponibles en la versión 1 de esta CPS).

1.3.6 Parte Usuaria o Tercero que confía en el certificado

La Parte usuaria o Tercero que confía en el certificado (en ingles, *relaying p*arty), es la persona que recibe una transacción electrónica realizada con un certificado emitido por una CA incluida en esta CPS y que voluntariamente confía en el Certificado emitido por ésta y por ende, en el servicio de confianza que le respalda.

1.3.7 Otros participantes

1.3.7.1 Entidad

En los certificados personales, la Entidad es la organización con o sin personalidad jurídica, de carácter público o privado, individual o colectivo, reconocido en derecho, que tiene una determinada vinculación con el Titular persona física. (no disponibles en la versión 1 de esta CPS)

En los certificados de sello electrónico (no disponible bajo la versión 1 de esta CPS) la Entidad es la persona jurídica Titular del certificado.

1.3.7.2 Responsable del certificado

El Responsable del certificado es la persona física responsable del uso de la clave privada asociada a la clave pública del certificado.

En los certificados personales, el Responsable del certificado es el Titular.

En los certificados de sello electrónico, sin perjuicio de las obligaciones del Titular, el Responsable del certificado es el Solicitante o una persona autorizada por el Solicitante (no disponible bajo la versión 1 de esta CPS).

1.3.7.3 Entidad de Acreditación u Organismo de Supervisión

La entidad de supervisión será el órgano gestor correspondiente que admite, acredita y supervisa a los TSP dentro de un ámbito geográfico concreto. Esta tarea dentro del Estado Español recae en el Ministerio de Asuntos Económicos y Transformación Digital, siendo la autoridad competente dependiendo del Estado Español miembro de la Unión Europea.

1.4 USO DE LOS CERTIFICADOS

1.4.1 Ámbito de Aplicación y Usos

Los certificados emitidos por las CA’s recogidas en esta CPS podrán usarse en los términos establecidos por las Políticas de Certificación correspondientes.

En términos generales, se admiten los certificados para los siguientes usos:

- Autenticación basada en certificados X.509v3.
- Firma electrónica avanzada basada en certificados X.509v3.
- Firma electrónica avanzada basada en certificados cualificados X.509v3.
- Firma electrónica cualificada basada en certificados X.509v3 emitidos en QSCD remoto.
- Cifrado asimétrico o mixto, basado en certificados X.509v3.

1.4.2 Usos Prohibidos y no Autorizados

Los certificados no podrán ser empleados fuera de los límites y usos para los que hayan sido emitidos en cada caso y que vienen descritos en las políticas de certificación correspondientes.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

Signaturit incorpora en el certificado información sobre la limitación de uso, bien en campos estandarizados en los atributos “uso de la clave” (key usage), “restricciones básicas” (basic constraints) marcados como críticos en el certificado y por lo tanto de cumplimiento obligatorio por parte de las aplicaciones que lo utilicen, o bien limitaciones en atributos como “uso extendido de clave” (extended key usage), “restricciones de nombre” (name constraints) y/o mediante textos incorporados el campo “declaración del emisor” (user notice) marcados como “no crítico” pero de obligado cumplimiento por parte del titular y del usuario del certificado.

A pesar de que es posible el cifrado de datos con los certificados, Signaturit no se responsabiliza de los daños causados por la pérdida de control del titular de la clave privada necesaria para descifrar la información.

1.5 ADMINISTRACIÓN DE LA CPS

1.5.1 Organización

La redacción, publicación, revisión y modificación de esta CPS es responsabilidad de:

Organización	SIGNATURIT SOLUTIONS S.L.U.
E-Mail	info@signaturit.com
Página Web	https://www.signaturit.com

1.5.2 Persona de contacto

Para cualquier consulta acerca de esta CPS contactar con:

Organización	SIGNATURIT SOLUTIONS S.L.U.
Responsable	Director de Compliance
E-mail / Teléfono	legal@signaturit.com / 960 031 203

1.5.3 Responsable para determinar la idoneidad de esta CPS con las políticas

Departamento Calidad & Compliance de Signaturit.

1.5.4 Procedimiento de aprobación de la política

Las políticas y esta CPS se aprueban en el comité TSP de Signaturit (antes llamado “Coordination Committee”), según el procedimiento interno establecido al efecto. Cada nueva versión de CPS de publica en la pagina web de Signaturit: https://www.signaturit.com/es/legalidad/autoridad-certificacion/.

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 Definiciones

Prestador de Servicios de Confianza (TSP por sus siglas en inglés): Un prestador de servicios de confianza es una persona física o jurídica que presta uno o más servicios de confianza, bien como servicios cualificados o como servicios no cualificados de confianza.

Prestador Cualificado de Servicios de Confianza (QTSP por sus siglas en inglés): Un prestador de servicios de confianza cualificado presta uno o varios servicios de confianza a los que el organismo de supervisión ha concedido la cualificación.

Servicio de confianza: Dentro de los servicios de confianza definidos en eIDAS se encuentran:

- La creación, verificación y validación de firmas electrónicas. Se incluyen los certificados relativos a estos servicios.

- La creación, verificación y validación de sellos electrónicos. Se incluyen los certificados relativos a estos servicios.
- La creación, verificación y validación de sellos de tiempo electrónicos. Se incluyen los certificados relativos a estos servicios.
- La entrega electrónica certificada. Se incluyen los certificados relativos a estos servicios.
- La creación, verificación y validación de certificados para la autenticación de sitios web.
- La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

Servicio de confianza cualificado: un servicio de confianza que cumple los requisitos aplicables establecidos en el Reglamento eIDAS.

1.6.2 Acrónimos

CA: Autoridad de Certificación (Certification Authority)

CPS: Declaración de Prácticas de Certificación (Certification Practice Statement)

CRL: Certificate Revocation List

eIDAS: Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

HSM: Hardware Security Module

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PC: Certificate Policy

PDS: PKI Disclosure Statement

PKI: Public Key Infrastructure

PS: Declaración de Prácticas (Practice Statement)

QSCD: Qualified Secure Creation Device

RA: Registration Authority

SubCA: Autoridad de Certificación Subordinada o Intermedia (Subordinate Certification Authority)

TSA: Time Stamp Authority

2 RESPONSABILIDADES DE LA PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

Signaturit publica los siguientes datos e informaciones de la CA:

- La Declaración de Prácticas de Certificación y las políticas específicas, que estarán disponibles de forma publica en la dirección https://policy.signaturit.com/
- Las PDS (PKI Disclosure Statement) correspondientes en las siguientes URL:
    - Inglés: https://pds.signaturit.com/en
    - Castellano: https://pds.signaturit.com/es
- Los Términos y Condiciones de los servicios prestados https://policy.signaturit.com/
- Enlaces a la información del certificado de la CA
    - http://ca.ivsign.com/certs/ivsignrootca.crt
- Enlaces a CRL y OCSP de la CA:
    - CRLs:
        - http://crl1.ivsign.com/ivsignroot.crl
        - http://crl2.ivsign.com/ivsignroot.crl
    - OCSP:
        - http://ocsp.ivsign.com
        - http://ocsp2.ivsign.com

Todo cambio en las especificaciones o condiciones del servicio estará disponible para los usuarios a través de las URL especificadas para cada repositorio, también accesibles desde la web https://www.signaturit.com/es/legalidad/autoridad-certificacion/

2.2 PUBLICACIÓN DE INFORMACIÓN DE LOS CERTIFICADOS

Signaturit publica la siguiente información de los certificados en la página: https://policy.signaturit.com/

- Las claves públicas de los certificados: http://ca.signaturit.com/certs/sitglobalca.crt
- Las listas de revocación de certificados en las direcciones:
    - http://crl1.signaturit.com/sitglobal.crl
    - http://crl2.signaturit.com/sitglobal.crl
- Un repositorio on-line de consulta del estado de los certificados, mediante protocolo OCSP.
    - http://ocsp.signaturit.com
    - http://ocsp2.signaturit.com

2.3 FRECUENCIA DE ACTUALIZACIÓN

Los certificados de CA son publicados por Signaturit en el repositorio correspondiente en la fecha de su vigencia o de publicación en las listas de confianza por primera vez.

Los certificados de entidad final son publicados automática e inmediatamente después de haber sido emitidos tras la aprobación del Sujeto/Firmante, pudiendo consultarse su estado a través de los medios disponibles identificados en el punto 2.2. Publicación de información de los certificados.

Signaturit publica de forma inmediata, una vez aprobadas y vigentes, en los repositorios correspondientes cualquier modificación en las Políticas, CPS o PDS, manteniendo el histórico de versiones.

2.4 CONTROL DE ACCESO

Todos los repositorios especificados en este punto son de acceso público, no requiriendo por parte del suscriptor o usuario de un certificado ningún tipo de control de acceso.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 POLÍTICAS DE NOMBRES

3.1.1 Nombre identificativo del certificado

El nombre identificativo del certificado se introduce en el campo Sujeto (Subject) mediante un nombre distintivo (Distinguised Name o DN) de acuerdo con el tipo de nombre estándar X.501.

La estructura, contenido y significado de los datos que forman el DN del certificado están definidos en los documentos perfil de certificado para cada uno de los tipos de certificados emitidos por la CA.

3.1.2 Significado de los nombres

Todos los nombres utilizados en el DN serán significativos.

3.1.3 Pseudónimos

En la actualidad no se emiten certificados de pseudónimos.

3.1.4 Reglas utilizadas para interpretar varios formatos de nombres

Signaturit atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

3.1.5 Unicidad de los nombres

Dentro de una misma CA el nombre asignado en el campo sujeto del certificado será único, e identificará a un mismo titular de certificado identificado. No se podrá asignar un nombre de Sujeto/Titular ya asignado a un Solicitante diferente, lo cual se controlará incorporando el

identificador fiscal único o equivalente a la cadena del nombre que distingue al Titular del certificado.

Se puede expedir varios certificados a un mismo Sujeto siempre que el tipo de certificado (Campo descripción del certificado) sea diferente.

3.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos

Signaturit no asume compromisos en la emisión de certificados respecto al uso de marcas y otros signos distintivos. Signaturit no permite deliberadamente el uso de un signo distintivo sobre el que el Titular o el Suscriptor no ostente derechos de uso. Sin embargo, ni Signaturit ni las RA están obligadas a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados.

3.2 REGISTRO INICIAL

3.2.1 Métodos de prueba de la posesión de la clave privada

La generación de las claves privadas será realizada por la CA en el momento de la emisión de los certificados. El control de la clave privada será entregado directamente al Titular (o al Responsable del certificado para los certificados de sello electrónico), a través de los medios de contacto indicados en la solicitud (dirección de correo electrónico y/o número de teléfono móvil):

- **En formato Software:** Se entregan al Titular mediante generación online del fichero protegido según el estándar PKCS#12. (no disponible bajo versión 1 de esta CPS)
- **En entorno centralizado:** Se generarán directamente en el sistema de centralización de certificados IvSign, asociados a la cuenta del Titular. (no disponible en la versión 1 de esta CPS)
- **En formato Hardware:** Las claves pueden ser entregadas por la CA al Titular, directamente o a través de una RA en un dispositivo cualificado de creación de firma (QSCD) del tipo tarjeta/token que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS. (no disponible en la versión 1 de esta CPS)

No obstante, se permitirá la generación de las claves privadas por parte del Titular, el cual deberá probar la posesión de la clave privada remitiendo a la RA una petición PKCS#10 asociada a la solicitud del certificado.

3.2.2 Autenticación de entidades

(no disponibles en la versión 1 de esta CPS)

3.2.3 Autenticación de la identidad de un individuo

Para la emisión de certificados cualificados, la autenticación de la identidad de un individuo se comprobará mediante la presentación a la RA de alguno de los siguientes documentos:

- Documento Nacional de Identidad Español
- Tarjeta de Residencia en España o Tarjeta de Identidad de Extranjero

- Pasaporte español
- Documento de identidad de cualquier país miembro de la UE o EEE acompañado del Certificado del Número de Identidad de Extranjero (NIE)
- Para los extranjeros no titulares de NIE, se admitirán los Pasaportes y los Documentos de identidad oficiales del país de origen siempre y cuando el operador de la CA, RA o PVP entienda el idioma del documento y pueda verificar su autenticidad a través de una fuente fiable como la base de datos PRADO Public Register of Authentic identity and travel Documents Online (https://www.consilium.europa.eu/prado/en/prado-start-page.html). En caso de no conocer el idioma del documento o de no tener acceso a una base de datos para corroborar su autenticidad, el documento deberá presentarse con la Apostilla de la Haya y, si se considera necesario, con una traducción oficial.

No se pueden emitir certificados a menores de edad no emancipados, incapacitados judicialmente total o parcial, o cuando existen sospechas fundamentadas de que el solicitante no está en posesión de sus plenas capacidades mentales.

La comprobación de la identidad podrá realizarse:

- Mediante personación física ante un operador de CA, RA o PVP. El Solicitante puede optar alternativamente por personarse ante un Notario y aportar la solicitud de expedición del certificado con su firma legitimada en presencia notarial.
- A distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 (del Reglamento eIDAS) con respecto a los niveles de seguridad «sustancial» o «alto». Se aceptarán los sistemas de identificación electrónica notificados por un estado miembro en virtud del artículo 9.1 del Reglamento eIDAS con un nivel de seguridad sustancial o alto (por ejemplo, el DNI electrónico en España)
- Mediante otro certificado cualificado vigente expedido por una CA de Ivnosys Soluciones o de otro Prestador, para cuya expedición se hubiese identificado a la persona física presencialmente o utilizando medios de identificación electrónica conformes a lo indicado en el punto anterior, siempre y cuando los datos de identidad de la persona física (y en su caso los atributos en el certificado solicitado) estén contenidos en el certificado utilizado. Si fuera necesario, se solicitará al otro Prestador que confirme cuándo se produjo la última personación.
- Signaturit podrá incorporar otros métodos de identificación reconocidos a escala nacional, cuya seguridad sea equivalente a la personación física, de acuerdo con la norma aplicable, en particular las condiciones y requisitos técnicos establecidos en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.).

En virtud del artículo 7.6 de la Ley 6/2020 no será necesaria una nueva personación cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la CA o a la RA en virtud de una relación preexistente de dichos solicitantes con la CA o con la RA, en la que, para la identificación del interesado, se hubiese empleado el medio señalado en el apartado 1 (personación física) y el período de tiempo transcurrido desde la identificación fuese menor de cinco años. Por tanto, si se dieran tales circunstancias lo indicado en este punto podrá no ser exigible.

Para certificados no cualificados se atenderá a lo establecido en las políticas correspondientes, siendo la organización responsable de la RA la que establece las normas de identificación de los titulares.

La RA registrará los datos y documentos relativos a la identificación y autenticación de la persona física y/o de la Entidad. Conforme al artículo 24.2.h) del Reglamento eIDAS, estas actividades de registro podrán realizarse por medios electrónicos tanto si los documentos aportados son documentos electrónicos validos en derecho como si son documentos papel. En este último caso, el Operador de la RA deberá guardar una copia escaneada y firmarla digitalmente con su Certificado personal, para su conservación en ficheros informáticos custodiados por la propia RA durante la vigencia de la relación contractual con la CA y cuando ésta termine por la CA durante el plazo legal requerido.

3.2.4 Información no verificada de un suscriptor

Toda la información incluida en el campo Subject del certificado está verificada.

3.2.5 Validación de autoridad para la solicitud

La autoridad para poder solicitar un certificado se validará en el momento de la comprobación de la identidad del titular y su concordancia con los documentos de identidad presentados.

La autoridad sobre la vinculación, representación o emisión de un certificado a una entidad se validará mediante la documentación especificada en los puntos 3.2.2. Autenticación de entidades y 3.2.3. Autenticación de la identidad de un individuo

3.2.6 Criterios para la interoperabilidad

Signaturit podría interoperar con otras CA (p.e. certificación cruzada), en particular las CA Intermedias de Ivsign Root CA en los términos y criterios que se establecerán contractualmente.

3.3 RENOVACIÓN DE LA CLAVE

3.3.1 Identificación y autenticación para la renovación de claves

Antes de renovar, la CA o la RA deberá comprobar que la información utilizada para verificar la identidad y demás datos del Firmante y del poseedor de la clave sigue siendo válida.

Dichas comprobaciones se realizarán mediante autenticación del titular en base al certificado que pretende renovar, que deberá encontrarse vigente y haber sido emitido por Signaturit.

Si cualquier información del Firmante o del poseedor de la clave ha cambiado, se debe realizar un nuevo registro y emisión, de acuerdo con lo establecido en las secciones correspondientes en este documento

Este proceso no se podrá realizar de forma automatizada si han pasado más de 5 años desde el último proceso de identificación y autenticación del Suscriptor y/o Titular. En este caso se deberá iniciar un nuevo proceso de emisión de certificado.

3.3.2 Identificación y autenticación para la renovación de claves tras una revocación

Al quedar el certificado invalidado no se podrá realizar la renovación de forma automática utilizando el método indicado en el punto anterior 3.3.1. Se deberá iniciar un nuevo proceso de emisión de certificado.

Si la revocación se produce en certificados de entidad final como consecuencia de un proceso de sustitución o por un error en su emisión o una pérdida, se considera que la renovación después de una revocación puede realizarse, siempre que la información empleada en su día para la emisión del certificado revocado sigue siendo válida. Se reutilizará la documentación soporte entregada para la emisión del certificado sustituido y se eliminaría la necesidad de una nueva autenticación del titular siempre y cuando ésta se haya producido hace menos de 5 años.

En ningún caso se podrá sustituir un certificado tras la revocación si:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado

3.4 REVOCACIÓN DE LA CLAVE

La autenticación del Solicitante para revocar o suspender un certificado se realiza de la siguiente forma:

- Si es el propio Titular o el Responsable del certificado:
    - Mediante una solicitud firmada dirigida desde el mismo correo electrónico del Titular o el Responsable del certificado que consta al TSP.
    - A través de la aplicación de gestión de certificados puesta a disposición de los solicitantes de certificados.
    - Por personación física en la RA, previa presentación de alguno de los documentos de identificación indicados en el punto *3.2.3. Autenticación de la identidad de un individuo*.
- Por el Suscriptor diferente del Sujeto o un representante de la Entidad a la que está vinculado un certificado:
    - Mediante una comunicación escrita firmada y sellada por un representante de la Entidad acompañada del documento justificativo de sus facultades de representación.
- Por un tercero:

- Podrá comunicar cualquier circunstancia que pudiera suponer la revocación como sospecha de fraudes, usos indebidos, datos erróneos, etc. Tales circunstancias deberán ser comprobadas por el PSC o la RA que tomarán la decisión de revocación de acuerdo al punto siguiente.

- El PSC, directamente por iniciativa propia o a través de una RA, puede solicitar la revocación de un certificado si conoce o sospecha que la clave privada del suscriptor se ha visto comprometida, o si conoce o sospecha de cualquier otro evento que aconseje tomar dicha medida. Adicionalmente, los operadores autorizados de la AC podrán tramitar la solicitud de revocación masiva de certificados por cese de actividad de la AC o de una AR conforme los procedimientos del Plan de cese del PSC.

En cualquier caso, en el momento de la revocación del certificado, se enviará una notificación por correo electrónico al Sujeto/Titular o Responsable especificando la fecha y hora y el motivo de la revocación.

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

Signaturit emplea para la gestión del ciclo de vida de los certificados la plataforma de RA de Ivnosys Soluciones. Esta plataforma permite la solicitud, registro, publicación y revocación de todos los certificados emitidos.

Signaturit garantiza que los servicios de confianza ofrecidos según esta CPS se realizan bajo políticas de no discriminación, de forma que:

- No existen procedimientos distintos a los especificados en esta CPS para la gestión de los servicios.
- Sin perjuicio de lo anterior, se podrán habilitar procedimientos especiales de solicitud y del resto de procesos del ciclo de vida de los certificados, para aquellos suscriptores con necesidades especiales por cualquier tipo de discapacidad que les impida solicitar los servicios de acuerdo con los procedimientos especificados en esta CPS.
- Los servicios son accesibles para cualquier persona física que cumpla con los criterios necesarios para la emisión de un certificado digital según las políticas marcadas en esta CPS, no exigiéndose ningún tipo de condición especial.

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Quién puede iniciar una solicitud de certificado

La solicitud de un certificado la puede realizar la persona física o el representante autorizado cuya identidad coincida con el Sujeto del certificado a emitir.

4.1.2 Proceso de solicitud

4.1.2.1 Solicitud individual mediante formulario web

Las solicitudes de los certificados se realizan, de forma general, con el siguiente procedimiento:

(1) El Solicitante deberá cumplimentar un formulario para iniciar el proceso. Para ello la CA o la RA proporcionará las aplicaciones y cuentas de acceso necesarias a los usuarios.
(2) Durante el proceso de alta se verificará la cuenta de correo electrónico del solicitante (y/o su número de teléfono móvil) mediante el envío de un correo (o sms), en el cual se pedirá al Solicitante confirmar a través de la aplicación de CA o de RA la corrección de sus datos (y en su caso los de la Entidad) y la aceptación de los Términos y Condiciones de uso del servicio y Política de privacidad.
La confirmación de los datos y la aceptación de los Términos y Condiciones de uso del certificado podrá alternativamente formalizarse por el Solicitante y en su caso el Suscriptor dentro de un proceso operativo, interno o externo, aprobado por la RA.
(3) Con la presentación de la solicitud el Solicitante deberá presentar electrónicamente la documentación necesaria a través de la aplicación proporcionada y cumplir con el requisito de identificación presencial, si ésta es pertinente, para identificación y validación de la documentación.

4.1.2.2 Solicitud múltiple mediante lotes

En este caso, se enviará por el Suscriptor a la RA un fichero estructurado con los datos de los Solicitantes. La RA procederá a la carga de dichas peticiones en el aplicativo de gestión, continuando la gestión para cada una de las solicitudes desde el paso (2) del punto anterior.

4.2 GESTIÓN DE LAS SOLICITUDES

Las solicitudes son procesadas por un gestor asociado a la RA.

4.2.1 Identificación y autenticación

Una vez realizada una solicitud de certificado el gestor comprobará:

(1) Que se ha procedido a la identificación del titular según lo especificado en el punto 3.2. Registro inicial.
(2) Que el solicitante ha presentado toda la documentación requerida para el tipo de certificado solicitado.

4.2.2 Aprobación o rechazo de la solicitud

Validada la solicitud por un gestor ésta será tramitada por un Operador de RA:

(1) El Operador de RA verifica que la información proporcionada en la solicitud es conforme para poder emitir el certificado.
(2) Si la identificación realizada o la información proporcionada no fueran correctas, de acuerdo con lo establecido en el punto *3.2. Registro inicial* de esta CPS, el Operador de RA solicitará las correcciones necesarias, o rechazará la solicitud comunicando al Solicitante los motivos para que pueda subsanar y rehacer la solicitud de nuevo si lo desea.

(3) En caso de que los datos se verifiquen según los procedimientos establecidos el operador de RA aprobará la solicitud para proceder a la emisión del certificado.

Las solicitudes vía servicios web se ejecutan directamente al recibirse estas autenticadas con un certificado previamente reconocido como RA por Signaturit.

4.2.3 Tiempo de proceso de las solicitudes

No está estipulado un tiempo de proceso para las solicitudes.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 Acciones de la CA para la emisión de los certificados

Tras la aprobación de la solicitud el operador de RA gestionará la emisión del certificado con sus credenciales de autenticación.

Para los certificados en software el titular recibe un correo electrónico con la notificación de la aprobación de la solicitud y el procedimiento para la generación y descarga del certificado en formato software.

Para su instalación necesitará un código de instalación que se habrá entregado en el mail de confirmación de la solicitud.

Para los certificados centralizados se realizará de acuerdo con la PS de IvSign. La emisión se realiza en el momento que lo ejecuta el Operador de RA y firma la operación con su certificado de Operador de RA.

4.3.2 Notificación al suscriptor de la emisión del certificado

Una vez emitido el certificado, el suscriptor recibirá en el correo electrónico o teléfono móvil (a través de un SMS) suministrados en la solicitud el PIN de activación de la clave privada.

En los certificados centralizados, el suscriptor recibirá otro mensaje por alguno de los canales especificados con el medio de autenticación (por usuario y contraseña) de acceso al sistema de gestión de certificados de **IvSign**. Este mensaje sólo lo recibirá en el momento de la emisión del primer certificado en su cuenta de IvSign.

4.4 ACEPTACIÓN DE CERTIFICADOS

4.4.1 Conducta que constituye la aceptación del certificado

Una vez notificada la emisión del certificado al suscriptor, éste dispone de un periodo de 7 días naturales para comprobar su correcta emisión. Transcurrido este tiempo se considerará que el suscriptor ha aceptado el certificado emitido.

Si el certificado no ha sido emitido correctamente por causas técnicas, el certificado se revocará y se emitirá uno nuevo, una vez detectada la incidencia o comunicada a la RA por parte del suscriptor.

4.4.2 Publicación del certificado por la CA

Una vez emitido, el certificado es publicado inmediatamente en el repositorio de certificados estando disponible para la consulta de su estado a través de los servicios habilitados al efecto (Ver punto 2.2. Publicación de información de los certificados).

4.4.3 Notificación de la emisión del certificado a otras entidades

No hay procesos para la notificación de la emisión de un certificado a otras entidades.

4.5 USO DE LOS CERTIFICADOS

4.5.1 Uso de la clave privada y del certificado por el suscriptor

El Titular de un certificado, bien directamente o a través de un tercero autorizado (el Solicitante o el Responsable del certificado para los sellos), estará obligado a cumplir con lo dispuesto por la normativa, por esta CPS en su condición de firmante/creador del sello y a lo establecido en los Términos y Condiciones impuestas por la CA, los cuales se habrán aceptado como paso previo a la confirmación de la solicitud del certificado.

En todo caso deberá usar su certificado en base a los usos permitidos, de acuerdo con lo indicado en el punto 1.4. Uso de los certificados.

4.5.2 Uso de la clave pública y del certificado por la parte usuaria

Será obligación de la Parte Usuaria cumplir con lo dispuesto en la normativa vigente y, además:

- Verificar la validez de los certificados antes de aceptar cualquier operación realizada por su titular. Signaturit dispone de diversos mecanismos para realizar dicha comprobación como el acceso a listas de revocados (CRL) o a servicios de consulta en línea como OCSP. El acceso a estos mecanismos está descrito en esta CPS.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas (accesible desde el campo “Directivas del certificado”).

4.6 RENOVACIÓN DE CERTIFICADOS

4.6.1 Circunstancias para la renovación de certificados

Se podrán renovar aquellos certificados donde esté prevista la renovación de acuerdo con su política de certificación.

La renovación debe realizarse antes de su caducidad.

Sólo se pueden renovar los certificados en los que no cambie ninguno de sus datos, permitiendo sólo la modificación del correo electrónico. Si existen otros datos incorporados en el certificado que han cambiado, el certificado debe revocarse y realizar una emisión nueva.

4.6.2 Quién puede solicitar la renovación

La renovación deberá solicitarla el Titular del certificado o la persona física que lo representa en el caso de certificados emitidos a entidades (Solicitante o Responsable del certificado).

4.6.3 Proceso de renovación

La renovación de certificados bajo esta CPS se realiza siempre emitiendo nuevas claves, por lo tanto, el proceso técnico de emisión es igual al que se sigue cuando se realiza una nueva petición.

En el caso de renovación de los certificados cualificados de persona física, se permite la emisión de certificado sin repetir el proceso de comprobación de identidad descrito en el punto 3.2.3. Autenticación de la identidad de un individuo hasta en un periodo de 5 años desde el último registro presencial. Una vez superado este plazo el titular deberá realizar un proceso de emisión presencial igual al realizado para la primera emisión.

Antes de la caducidad la CA realiza cuatro avisos de renovación al titular (30 días, 15 días, 7 días, 1 día) vía email notificando que el certificado va a caducar.

El proceso de renovación se inicia desde la aplicación proporcionada por el PSC e indicada en los correos de renovación. Este proceso requiere disponer de acceso a la clave privada del certificado válido (no revocado) que se va a renovar.

- El usuario deberá identificarse con su cuenta de usuario
- Una vez identificados, el aplicativo presenta al Firmante los datos del certificado antiguo y le pide la confirmación de dichos datos.
- El aplicativo permite al Firmante modificar únicamente el email asignado al certificado.
- La petición se incorpora al aplicativo de RA donde el operador, una vez revisados los datos, procede a pedir la emisión del certificado a la CA.
- Como norma general emite un nuevo certificado tomando como inicio de validez la finalización del certificado a renovar. En algún caso se permite en los procesos de emisión a través de los servicios web, la renovación del certificado con fecha en el mismo momento de renovación, procediendo posteriormente a revocar el certificado a renovar.

4.6.4 Notificación del nuevo certificado emitido al suscriptor

Al tratarse de una nueva emisión de claves el proceso de notificación es el mismo que el descrito en el punto *4.3.2. Notificación al suscriptor de la emisión del certificado*.

4.6.5 Conducta que constituye la aceptación del certificado renovado

Al tratarse de una nueva emisión de claves el proceso de aceptación es el mismo que el descrito en el punto *4.4.1. Conducta que constituye la aceptación del certificado*.

4.6.6 Publicación del certificado renovado por la CA

Al tratarse de una nueva emisión de claves el proceso de publicación es el mismo que el descrito en el punto 4.4.2. Publicación del certificado por la CA.

4.6.7 Notificación de la emisión del certificado renovado a otras entidades

No hay procesos para la notificación de la renovación de un certificado a otras entidades.

4.7 REEMISIÓN DE CERTIFICADOS

La renovación y emisión de nuevos certificados tras una revocación, suspensión o modificación siempre se realiza generando nuevas claves, por tanto, no existe bajo esta CPS un procedimiento específico para la reemisión de un certificado con nuevas claves.

4.8 MODIFICACIÓN DE CERTIFICADOS

Cualquier necesidad de modificación de certificados implicará una nueva solicitud. Se realizará una revocación del certificado y una nueva emisión con los datos corregidos. Por tanto, no existe ningún procedimiento de modificación de certificado.

En el caso de tratarse de un proceso de sustitución de certificados, se considerará una renovación y así computa a la hora del cálculo de los años de renovación sin presencia física tal como marca la ley.

Se podrá proceder a la sustitución de certificados como renovación cuando los atributos del Firmante o del poseedor de claves que formen parte del control de unicidad previsto para esta política no hayan variado.

4.9 SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS

4.9.1 Circunstancias para la revocación de certificados

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de este en función de alguna circunstancia distinta a la de su caducidad.

Los posibles motivos de revocación son:

- Solicitud formulada por el Titular, una persona representando al Titular o un tercero autorizado
- Fallecimiento del Titular o capacidad modificada judicialmente sobrevenida, total o parcial
- Extinción de la personalidad jurídica o disolución del Creador del sello
- Datos del certificado incorrectos,
- Cambio desde el momento de la emisión de los datos o circunstancias del titular, de su facultad de representación o relativos a la entidad que representa o a la que está vinculado el firmante.
- Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.
- Violación o compromiso de la clave (robo, pérdida, …)
- Violación, puesta en peligro o pérdida de control de los datos de activación de la clave (PIN)
- Reemplazo del certificado
- Fin del periodo estipulado de suspensión

- Cuando los algoritmos criptográficos utilizados se vieran comprometidos, no permitiendo asegurar la relación entre la clave pública y privada
- Compromiso de las claves de la CA
- En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.
- Que el certificado deje de cumplir con las PC
- Resolución judicial o administrativa que lo ordene
- Cese de operaciones de la CA o porque el certificado ya no sirve para el propósito por el que fue emitido según las condiciones contractuales acordadas con el Sujeto y/o el Suscriptor.

4.9.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por:

- El Sujeto/Titular
- El Solicitante autorizado.
- La entidad/organización (a través de un representante de la misma)
- El Suscriptor diferente del Sujeto
- La RA o la CA.
- También se contempla la posibilidad de que por parte de terceros o partes interesadas se pueda comunicar cualquier circunstancia que pudiera suponer la revocación. Tales circunstancias deberán ser comprobadas por el PSC o la RA que tomarán la decisión de revocación.

4.9.3 Proceso de revocación

Las solicitudes de revocación y suspensión deberán realizarse de acuerdo con los medios de identificación indicados en el punto ‘3.4. Revocación de la clave’. Además, la AC o la AR pueden poner a disposición métodos adicionales para presentar la solicitud de revocación, siempre que dichos métodos permitan una correcta identificación del Sujeto.

En caso de revocación por falta de pago del precio del certificado emitido, la RA o la CA requerirá previamente y en dos ocasiones sucesivas al Firmante a la dirección de correo electrónico de contacto, para que regularice esta situación en plazos de 8 días, a falta de lo cual, se procederá a la revocación con carácter inmediato.

Una vez validada la solicitud de revocación por un gestor ésta será remitida a un operador de RA que procederá a la revocación a través de la aplicación de gestión de certificados de la CA.

Por procedimiento se ha establecido que el operador de RA que revoque un certificado debe ser distinto al que validó la emisión de ese certificado. Se exceptúa de lo anterior la situación de RA externa con un solo operador en cuyo caso se le permitirá realizar validaciones y revocaciones bajo el control de la RA del PSC que deberá aplicar medidas específicas para evitar malas prácticas (control de plazos entre emisión y revocación, control de los motivos alegados, auditorias inopinadas, etc.).

Una vez revocado el certificado, se envía un comunicado mediante email al Titular comunicando la hora de suspensión y la causa de esta. En caso de existir un Suscriptor diferente del o los Sujetos titulares de los certificados revocados, la revocación será notificada por la AC al Suscriptor con el que la AC haya suscrito un acuerdo específico.

4.9.4 Periodo de gracia para la solicitud de revocación

No se ha estipulado.

4.9.5 Periodo de proceso de una solicitud de revocación

El periodo de revocación desde que Signaturit o una RA tiene conocimiento autenticado de la solicitud de revocación de un certificado será cómo máximo de 24 horas desde la confirmación de los datos, incorporándose en la próxima CRL a emitir y en la base de datos de la plataforma de gestión donde se alimenta el respondedor OCSP.

Si la solicitud de revocación no puede confirmarse en este plazo por falta de información o documentación acreditativa, no se tramitará y el Operador de RA lo comunicará al solicitante de la revocación o al gestor para que subsane los defectos.

4.9.6 Requisitos de comprobación de CRLs

Los Terceros que confían deben comprobar previamente a su uso, el estado de los certificados, debiendo comprobar en todo caso la última CRL emitida, que podrá descargarse en la URL que aparece en la extensión Punto de Distribución de CRL (CRL Distribution Point) de cada certificado.

Signaturit publica siempre las CRLs firmadas por la CA que ha emitido el certificado.

La CRL contiene un campo (NextUpdate) con la fecha de su próxima actualización.

4.9.7 Frecuencia de emisión de CRLs

La frecuencia de emisión de las CRL de **Signaturit Global CA** es como máximo de 1 día, pudiéndose emitir en un intervalo menor si se produce una revocación.

Signaturit emitirá la última CRL de una CA en el momento que todos los certificados emitidos bajo esa CA estén expirados o revocados, por cualquiera de las posibles circunstancias (expiración o revocación de la CA).

4.9.8 Latencia máxima para las CRL

Las CRL estarán disponibles de forma inmediata en el repositorio una vez se genere una nueva CRL.

4.9.9 Disponibilidad de comprobación on-line de la revocación

Signaturit ofrece un servicio de consultas OCSP en la dirección especificada en cada certificado y en esta CPS. (ver apartado 2.1 REPOSITORIO)

Las direcciones de acceso a estos servicios vienen referenciadas en el certificado digital. Para las CRL en la extensión puntos de distribución de CRL (CRL Distribution Point) y la dirección de OCSP en la extensión Acceso a la Información de la Autoridad (Authority Information Access).

En los certificados puede aparecer más de una dirección de acceso a las CRL para garantizar su disponibilidad.

Signaturit no mantiene los certificados revocados en las CRL después de su expiración. Para la consulta de certificados expirados se deberá utilizar el servicio de consulta OCSP.

Las CRL se mantendrán publicadas durante un periodo mínimo de 5 años desde la expiración o revocación de la CA. El servicio OCSP podrá ser interrumpido indefinidamente en caso de expiración o revocación de la CA.

Debido a las diferentes naturalezas de los servicios de OCSP y CRL, en caso de obtener respuestas distintas para un certificado, se mantendrán como respuesta válida la ofrecida por el OCSP.

4.9.10 Requisitos de la comprobación on-line de la revocación

Se deberá comprobar que las CRL van firmadas por la CA que emitió el certificado revocado.

Las respuestas OCSP van firmadas por certificados “OCSP Responder” firmados por la CA que emite el certificado a consultar, por lo que es necesario dicho certificado para validar la respuesta. .

4.9.11 Otras formas de divulgación de información de revocación disponibles

No existen otras formas de consulta.

4.9.12 Requisitos especiales de revocación por compromiso de las claves

No existen requisites especiales.

4.9.13 Circunstancias para la suspensión

La suspensión supone una revocación con causa de suspensión (es decir un caso particular de revocación “Certificate Hold”). Consiste en revocar un certificado de forma cautelar hasta que se decida sobre la oportunidad o no de realizar una revocación con causa definitiva o su re-activación.

Los posibles motivos para la suspensión son:

- Solicitud formulada por el Titular, una persona representando al Titular o un tercero autorizado
- Resolución judicial o administrativa que lo ordene
- En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.
- Duda sobre posible violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o utilización indebida de dichos datos por un tercero
- Duda sobre posible la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.

Un certificado en estado de suspensión será claramente visible en las consultas de comprobación de la revocación indicadas en el punto *4.9.9. Disponibilidad de comprobación*

on-line de la revocación y en las mismas condiciones que las consultas de revocación (al tratarse de un tipo de revocación).

4.9.14 Quién puede solicitar la suspensión de un certificado

Por los mismos usuarios que la revocación.

4.9.15 Procedimiento de solicitud de suspensión de un certificado

Mismo proceso que la revocación, indicando que se solicita la suspensión del certificado.

4.9.16 Límites del periodo de suspensión

Cuando se produce una suspensión, Signaturit tendrá una semana para decidir el estado definitivo del certificado: (revocado o activo). En caso de no tener en este plazo toda la información necesaria para la verificación de su estado definitivo, Signaturit revocará el certificado con causa desconocida.

4.10 SERVICIOS DE CONSULTA DE CERTIFICADOS

El PSC publica un repositorio actualizado con la información de los certificados los cuales se podrán consultar a partir del DN. (ver apartado 2.1 REPOSITORIO)

4.11 CADUCIDAD DEL CERTIFICADO

La caducidad de los certificados se establece de acuerdo con lo especificado en los perfiles de los certificados.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

Signaturit no custodia directamente claves en formato software (PKCS#12).

La custodia de las claves en formato centralizadas se realizará de acuerdo con la PS de **IvSign** en dispositivos HSM sin consideración de QSCD o en HSM con la certificación como QSCD. Estas claves no son exportables y están bajo el control exclusivo de su titular.

5 CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

Signaturit Global CA es una CA Subordinada de Ivnosys Soluciones, que utiliza para operar la misma infraestructura técnica que la CA raíz de Ivnosys Soluciones. Por tanto, a nivel general le aplican los controles definidos en la CPS de **IvSign Root CA**.

A continuación, se detallan los aspectos específicos que afectan a Signaturit Global CA como operador de la CA.

En cuando a la Plataforma de gestión centralizada de claves (IvSign) los controles aplicados se pueden consultar en su propia Declaración de Practicas de Gestion.

5.1 CONTROLES DE SEGURIDAD FÍSICA

Al tener contratado la infraestructura desde la cual Signaturit Global CA presta sus servicios a Ivnosys Soluciones, S.L.U. no existen estipulaciones adicionales a las específicas de la infraestructura la cual está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001 para los sistemas que sustentan los servicios de confianza, la cual a su vez, regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

5.1.1 Situación y características del CPD

La infraestructura utilizada para la operación y para el servicio de contingencia de la CA se encuentra ubicada en dos centros de datos (CPD) de Ivnosys Soluciones que garantizan la disponibilidad 24x7 de los sistemas de comunicación y disponibilidad de los sistemas.

Los CPD están ubicados dentro del territorio de la Unión Europea.

5.1.2 Control de acceso físico

El centro cuenta con las siguientes medidas de seguridad física:

- Videovigilancia y videograbación perimetral en accesos, parking y áreas de instalaciones.
- Personal 24x7 en el centro
- Control de accesos al edificio:
    - El centro cuenta con un sistema de control de accesos que garantiza el acceso seguro 24x7x365 al personal autorizado del cliente al área de servicio contratada.
    - Los accesos se registran individualmente con datos personales del personal autorizado del cliente.
    - El acceso multinivel está restringido a todas las áreas sensibles del centro, con tarjeta sin contacto, huella dactilar y/o llave.
- El acceso a las zonas de seguridad está protegido con control dual y monitorizado constantemente mediante CCTV y sensores de apertura de la zona.

5.1.3 Alimentación eléctrica y climatización

El centro cuenta con servicios de energía de alta disponibilidad con las siguientes infraestructuras:

- 2 salas de UPSs de alterna con SAIs de 120kvAs en configuración 2N.
- Grupos electrógenos de respaldo en configuración N+1
- Depósitos de fuel para una autonomía de más de 48horas de funcionamiento del centro.
- Cuadros eléctricos de sala alimentados desde los grupos de UPS independientes.

El control del clima en el CPD cumple la norma ETSI EN 300 019 clase 3.1, “Centros de Comunicaciones”.

Las Salas Técnicas están climatizadas con equipos partidos de condensación por aire, con impulsión de aire por falso suelo y humidificador del ambiente, de expansión directa redundantes e independientes en cada sala, en configuración N + 1 rotativo. La aportación de aire exterior para ventilación de las salas del CPD se toma de la red de conductos proveniente del ventilador de impulsión de aire exterior, que pasa a través de una unidad de filtrado que mantiene las condiciones biológicas y de sustancias químicas activas.

5.1.4 Exposición al agua

El CPD se ubica en una zona donde el riesgo de inundación es nulo, estando situado a 1500 metros de un área de riesgo de tipo 5, frecuencia baja (menos de 500 años).

5.1.5 Protección y prevención de incendios

El sistema de extinción de incendios del centro cubre salas técnicas e instalaciones críticas:

- Sistemas de detección constituidos por detectores iónicos de humos y gases de combustión.
- Zonas de detección controladas por central analógica microprocesada modular con plena autonomía de señalización, centralización de fuego y avería.
- Agente extintor FE-13.

5.1.6 Media storage

Cada Medio de Almacenamiento desmontable (cintas, cartuchos, CD, discos, etc.) permanece solamente al alcance de personal autorizado por las medidas de acceso físico al CPD y al armario RACK correspondiente.

5.1.7 Off-site backup

Se mantendrá una copia de seguridad en CPD distinto desde el que se realiza la prestación del servicio con una frecuencia menor a 7 días.

5.2 CONTROLES DE PROCEDIMIENTO

5.2.1 Roles de confianza

Los roles de confianza para la operación **Signaturit Global CA** son compartidos con los roles de confianza de Ivnosys Soluciones, en concreto:

ROL	DESCRIPCIÓN
Auditor Interno	Responsable del cumplimiento de los procedimientos operativos. Autorizados a ver los archivos y registros de auditoría de los servicios de confianza del PSC. Estas funciones estarán subordinadas a la Dirección de Compliance Estratégico.

Administrador de Sistemas	Responsable del funcionamiento correcto de las comunicaciones y los sistemas que sustentan la CA.
Operador de RA	Persona responsable de aprobar las peticiones de certificación realizadas por el Firmante. Los operadores de RA actuarán también como Operadores de revocación.
Responsable de Seguridad	Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de Ivnosys Soluciones. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
Operador criptográfico	Personas encargadas de la activación de los módulos criptográficos para la gestión de claves Root y subordinadas

5.2.2 Número de personas requeridas por tarea

En la siguiente tabla se establece el número de personas requeridas para la ejecución de las tareas de cada rol de confianza en la regla n de m personas.

ROL	NÚMERO DE PERSONAS
Auditor Interno	1 de 1 personas.
Administrador de Sistemas	1 de 1 personas.
Operador de RA	1 de múltiples personas.
Responsable de Seguridad	1 de 1 personas.
Operador criptográfico	3 de 5 para los dispositivos de la Root 2 de 5 para los dispositivos de las claves intermedias

5.2.3 Identificación y autentificación para cada rol

Cada rol tiene asignada una o varias personas, todas ellas nombradas por la dirección. Los operadores criptográficos custodiarán los tokens criptográficos de gestión de los dispositivos. El resto de roles se autenticarán mediante los usuarios y certificados del Active Directory o de los sistemas específicos de IvSign (usuario y contraseña) o de la CA (certificado digital), según las funciones a realizar.

5.2.4 Roles que requieren separación de funciones

A continuación, se detallan las incompatibilidades entre roles de confianza.

ROL	NÚMERO DE PERSONAS
Auditor Interno	Incompatible con cualquier otro rol.
Administrador de Sistemas	Incompatible con Auditor Interno y Responsable de Seguridad.
Operador de RA	Incompatible con Auditor Interno. Un operador de RA que haya emitido un certificado no podrá realizar la revocación del mismo certificado, salvo excepción indicada en el punto 4.9.3.
Responsable de Seguridad	Incompatible con Auditor Interno y Administrador de Sistemas.
Operador criptográfico	Incompatible con Auditor Interno.

5.3 CONTROLES DE SEGURIDAD DE PERSONAL

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

Signaturit se asegura de que el personal designado como operador de RA es confiable y, en su caso, que es nombrado por el organismo delegado para realizar las tareas de registro.

Para el personal propio Signaturit realizará una selección basada en entrevistas personales con los candidatos para valorar su calificación y experiencia, y les requiere realizar formaciones internas especificas a sus roles.

5.3.2 Procedimientos de comprobación de antecedentes

Signaturit podrá solicitar certificados que acrediten la no existencia de antecedentes penales para sus empleados de acuerdo con lo establecido en el procedimiento interno **PG002 - Procedimiento de Formación y Seguridad**.

5.3.3 Requerimientos y frecuencia de la actualización de la formación

Signaturit elabora un Plan de Formación anual donde se detectan las necesidades de formación del personal y se planifican de la forma adecuada.

Específicamente, el Operador de RA habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones impartido por Signaturit o Ivnosys Soluciones.

5.3.4 Requerimientos de formación

Para las nuevas incorporaciones los responsables de área y de producto, además de la formación técnica específica de su puesto, deben asegurarse de que se conoce la política, procedimientos y requisitos del SGSI de Signaturit y/o Ivnosys Soluciones, conociendo las consecuencias de una desviación de dichos procedimientos especificados. Para facilitar esta labor se dispone de una Manual de Bienvenida.

5.3.5 Frecuencia y secuencia de rotación de tareas.

No hay tareas especiales que requieran rotación de personal.

5.3.6 Sanciones por acciones no autorizadas

El proceso disciplinario está especificado en el procedimiento interno **PG002 - Procedimiento de Formación y Seguridad** y está basado en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

5.3.7 Requerimientos de contratación independientes

Los operadores de una RA delegada será personal bajo control y responsabilidad de la organización delegada de la RA, debiendo ser autorizados por Signaturit para realizar las labores de registro y, tras recibir la formación requerida para un Operador de RA.

5.3.8 Documentación proporcionada al personal

El estipulado a nivel general dentro del Manual de Bienvenida de Signaturit y el específico del puesto de trabajo a desempeñar (manuales de operación, procedimientos técnicos o de programación, procedimientos de soporte, …)

Los operadores de RA reciben el manual Guía de operación de RA (solicitudes y certificados) y la matriz de documentación para la emisión de certificados cualificados.

5.4 PROCEDIMIENTOS DE AUDITORÍA DE REGISTROS

Signaturit Global CA de Signaturit es una CA Subordinada de IvSign Root CA de Ivnosys Soluciones que utiliza para operar la misma infraestructura técnica que la CA raíz de Ivnosys Soluciones. Por tanto, le aplican los procedimientos definidos en la CPS de IvSign Root CA.

Del mismo modo, el Servicio IvSign dispone de sus propios procedimientos de acuerdo su PS.

5.5 ARCHIVO DE REGISTROS

Signaturit Global CA de Signaturit es una CA Subordinada de IvSign Root CA de Ivnosys Soluciones que utiliza para operar la misma infraestructura técnica que la CA raíz de Ivnosys Soluciones. Por tanto, le aplican las reglas de archivo de registros definidos en la CPS de IvSign Root CA, pero en instancias separadas y de acceso exclusivo al personal autorizado por Signaturit de cara a mantener la confidencialidad de los datos

Respecto del Servicio IvSign, no soporta archivos de información más allá de la información de auditoria indicada en el punto anterior.

No obstante, a continuación se recogen los procedimientos de archivo de registros en relación con la documentación de la RA que aplican a Signaturit Global CA.

5.5.1 Tipo de archivos registrados

Signaturit o sus RA almacenarán directamente:

- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y RA. Los datos relativos a su identificación y su ubicación.
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Autoridad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Políticas y Prácticas de Certificación

Signaturit es responsable del correcto archivo de todo este material.

5.5.2 Periodo de retención para el archivo

Los certificados, los contratos con los Sujetos/Firmantes y cualquier información relativa a la identificación y autenticación del Sujeto/Firmante serán conservados durante al menos 15 años desde la expiración de la validez de cada certificado o desde su revocación.

5.5.3 Protección del archivo

El archivo de la RA de Signaturit es electrónico y se aplican las medidas de protección establecidas en la norma UNE-ISO/IEC 27001 del SGSI del Grupo Signaturit.

5.5.4 Procedimientos de copia de respaldo del archivo

Signaturit tiene asegurado la protección del archivo mediante una política de copias de seguridad diaria.

5.5.5 Requerimientos para el sellado de tiempo de los registros

No hay especificaciones especiales para el sellado de tiempo del archivo.

5.5.6 Sistema de recogida de información de auditoria

A través de los sistemas del proveedor Ivnosys Soluciones.

5.5.7 Procedimientos para obtener y verificar información archivada

La gestión del archivo es la especificada para las copias de seguridad a través de su proveedor Ivnosys Soluciones. El acceso a la información archivada debe ser solicitada al responsable de sistemas de Ivnosys Soluciones por la propia persona interesada o persona con facultades suficientes de representación de la organización.

5.6 CAMBIO DE CLAVES

El cambio de claves de entidad final es realizado mediante la realización de un nuevo proceso de emisión.

El cambio de clave de la CA subordinada se realizará antes de que el certificado de la CA caduque de acuerdo con los procedimientos establecidos por Ivnosys Soluciones. El certificado a actualizar de la CA y su clave privada solo se usará para la firma de CRLs mientras existan certificados activos emitidos por dicha CA. Se generará un nuevo certificado de CA con una clave privada nueva y un CN (common name) distinto al del certificado de la CA a sustituir.

También se realizará cambio de certificado de una CA cuando el estado del arte criptográfico (algoritmos, tamaño de claves…) lo requiera.

5.7 RECUPERACIÓN ANTE DESASTRES

5.7.1 Procedimientos de tratamiento de incidentes

El tratamiento de incidentes en el SGSI de Signaturit está recogido en procedimientos específicos de la certificación de la norma UNE-ISO/IEC 27001.

Los incidentes de la CA serán comunicados de forma inmediata a Ivnosys Soluciones para su gestión y tratamiento.

5.7.2 Recursos informáticos, software o datos corruptos

Se atenderá a los establecido en la CPS de IvSign Root CA y al PS de IvSign. En caso de detectar desde Signaturit problemas de datos se tratará como incidente de acuerdo con lo establecido en el punto anterior.

5.7.3 Procedimientos ante el compromiso de una clave privada de entidad

El conocimiento del compromiso de una calve de entidad final por parte de Signaturit o de una RA desencadenará el proceso de revocación de la clave privada y su notificación a los titulares.

Signaturit mantendrá en todo caso la publicación de una última CRL una vez todos los certificados de la CA hayan sido revocados, siguiendo el Plan de Recuperación ante Desastres de Signaturit/Ivnosys.

5.7.4 Capacidad para la continuidad de negocio ante desastres

Signaturit dispone para su Sistema SGSI de un plan de continuidad de negocio en la certificación de la norma UNE-ISO/IEC 27001

Adicionalmente, la capacidad de continuidad de la CA Signaturit Global CA ante un desastre está supeditada a la de Ivnosys Soluciones como CA, lo cual está recogido en la gestión de riesgos, la cual dispone de un Sistema de Gestión Continuidad de Negocio (SGCN) implantado y auditado de acuerdo con la norma ISO 22301. El alcance del SGCN incluye todos los servicios de confianza del PSC, incluida IvSign Root CA.

El SGCN dispone de dos procesos principales de gestión:

- **Gestión de la Continuidad**, que se desencadena ante cualquier incidente de continuidad de un servicio.
- **Gestión de Crisis**

El **Plan de Continuidad del Negocio** proporciona la planificación, los responsables y la orientación para que Ivnosys Soluciones sea capaz de brindar la continuidad de los servicios críticos ante condiciones y amenazas existentes en un momento determinado. Si bien la gravedad de una emergencia no se puede predecir, por medio de este plan se busca minimizar el impacto de sus consecuencias en la operativa crítica y en el equipo humano de la empresa.

El **Plan Operativo de Continuidad del Negocio** contiene las estrategias e instrucciones de continuidad y recuperación predeterminados que Ivnosys Soluciones debe seguir durante una crisis para minimizar cualquier impacto de negocio. El objetivo del es recuperar procesos críticos dentro de un marco de tiempo aceptable.

5.8 CESE DE CA

Signaturit dispone de un Plan de Cese, cuyo procedimiento está definido en un documento específico. Dicho Plan está basado en permitir la continuidad del servicio como primera opción y define el plan de comunicación a todas las partes afectadas (CAs, usuarios finales y órgano regulador) tanto en el caso que se transfiera el servicio a otro proveedor como si finalmente se suspende el servicio.

El plan de cese garantiza que las CRL se mantengan disponibles en la medida de lo posible en su URL original y, en todo caso, se remitirán al organismo supervisor para su custodia y publicación de acuerdo con lo estipulado en la Ley de firma electrónica.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 Generación del par de claves

La generación de las claves intermedias de Signaturit Global CA es realizada según los procesos de Ivnosys Soluciones de ceremonias de generación y gestión de claves raíz y subordinadas en equipos HSM certificados Common Criteria EAL4+ dentro de un entorno seguro.

La generación de las claves de entidad final en formato software PKCS#12 se realiza en los momentos previos a la descarga por parte del titular, utilizando las herramientas de RA que le proporciona Ivnosys Soluciones y siguiendo los controles establecidos por Ivnosys Soluciones y reflejados en su propia CPS.

La generación del par de claves de entidad final en la plataforma de gestión centralizada de claves atiende a los especificado en la PS de **IvSign**, mediante un proceso de integración directa desde los sistemas de gestión de claves de Ivnosys Soluciones.

6.1.2 Entrega de la clave privada al suscriptor

La entrega de la clave privada en formato software al suscriptor se realiza en el momento de su generación mediante un proceso on-line desencadenado por el propio suscriptor. Este proceso se puede realizar tras la aceptación de un operador de RA. Tras la validación llegará un mail al suscriptor con las claves que le permitirán descargar su certificado en formato PKCS#12.

La entrega del control de la clave privada centralizada a su suscriptor se realiza según lo establecido en la PS de **IvSign**, a través de la cuenta generada al efecto. El PIN de activación de la clave privada será entregada al correo electrónico especificado del titular.

6.1.3 Entrega de la clave pública al suscriptor del certificado

Bajo esta política la clave pública se entrega siempre junto a la privada, en el momento de la generación y descarga por parte del titular, dentro del formato PKCS#12.

En las claves emitidas en formato centralizado la clave pública se puede descargar desde el panel de control del Servicio **IvSign**.

Para certificados certificados emitidos en Hardware la clave pública será descargada por el solicitante en el momento de generar el certificado, una vez aportado el CSR. (no disponible en la versión 1 de esta CPS)

6.1.4 Entrega de la clave pública de la CA a los usuarios

La clave pública de Signaturit Global CA estará disponible para descarga on-line en el repositorio público correspondiente (Ver punto 2.2. Publicación de información de los certificados).

6.1.5 Longitud de las claves

La longitud de la clave para la CA es de 4.096 bits utilizando un algoritmo de firma sha256WithRSAEncryption.

Las claves privadas del Sujeto/Firmante están basadas en el algoritmo **RSA** con una longitud mínima de **2048** bits.

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

El certificado de la CA Signaturit Global CA y de los Firmantes siguen los estándares RFC 5280 y ETSI EN 319 412.

6.1.7 Usos de la clave

La limitación de uso de la clave viene definida en el contenido del certificado en las extensiones: keyUsage, extendedKeyUsage y basicConstraints, de acuerdo a las reglas establecidas en las normas indicadas en el punto anterior.

6.2 PROTECCIÓN DE LA CLAVE PRIVADA

Al estar la CA Signaturit Global CA generada en los sistemas de Ivnosys Soluciones como CA Subordinada, los procedimientos y controles de protección de las claves privadas vienen definidas en la CPS de IvSign Root CA y PS IvSign, tal como se recoge a continuación.

6.2.1 Módulos criptográficos

Los módulos criptográficos utilizados para la gestión de claves privadas de las CA intermedias de IvSign Root CA disponen de certificación Common Criteria EAL4+.

Las claves privadas de los firmantes en formato centralizado se generan en los HSM de los sistemas de IvSign (de acuerdo con la PS IvSign).

Las claves privadas de los firmantes de certificados para firma cualificada se generan en dispositivos HSM considerados QSCD.

6.2.2 Control de la clave privada

La clave privada de la entidad raíz IvSign Root CA se almacena y custodia completamente off-line, de forma que sólo se podrá utilizar mediante ceremonia de claves en entorno seguro. Cualquier operación con los dispositivos criptográficos de la clave raíz requieren de un control multi-persona, es decir, de la intervención de n personas de un total de m (3 de 5 en el caso de los dispositivos criptográficos de la entidad raíz).

La clave privada de la CA intermedia Signaturit Global CA es utilizada desde el aplicativo de gestión de la CA mediante una licencia cliente configurada en la aplicación.

La operación de generación de claves privadas en los dispositivos criptográficos de la CA intermedia Signaturit Global CA requieren de un control multi-persona, es decir, de la intervención de n personas de un total de m (2 de 5 en el caso de los dispositivos criptográficos de la CA intermedia).

Las claves privadas de entidad final en formato software (PKCS#12) son generadas en el momento de la descarga por el titular protegidas por una contraseña. Esta deberá ser custodiada por el titular desde el momento que les es entregada.

Las claves privadas de entidad final en formato centralizado son generadas en los dispositivos HSM de IvSign y custodiadas con un doble cifrado: la clave maestra del dispositivo criptográfico y el PIN del usuario. Sólo proporcionando el PIN se podrá activar la clave privada, con lo que el titular deberá mantener el control de este PIN.

6.2.3 Custodia de clave privadas

Las claves de la entidad raíz IvSin Root CA son custodiados en caja fuerte dentro ubicada en el entorno de alta seguridad de la CA.

Ivnosys Soluciones almacena los certificados de la CA intermedia Signaturit Global CA en dispositivos criptográficos ubicados en entornos de alta seguridad.

Las claves de los firmantes sólo se custodian por el PSC en el caso de certificados centralizados de acuerdo con la PS de IvSign.

6.2.4 Copias de seguridad de claves privadas

Las claves de la CA disponen de copias de seguridad en varios dispositivos en alta disponibilidad y en un centro de contingencia. Además, se almacenan en zonas de alta seguridad copias cifradas externas a los dispositivos en sistema de almacenamiento que cumplen con el estándar FIPS 140-2 y mediante control de 3 de 5 personas para su descifrado y restauración.

Las claves de las firmantes custodiadas por IvSign se rigen según su declaración de prácticas.

6.2.5 Archivo de claves privadas

Las claves de CA son archivadas durante un periodo de 10 años desde la última emisión de un certificado por dichas claves.

El firmante será el responsable de la destrucción de sus claves en formato software.

El archivado de las claves centralizadas se regirá por la declaración de prácticas de IvSign.

6.2.6 Generación de claves privadas en módulos criptográficos

Las claves de CA siempre se generan en el interior de los módulos criptográficos destinados al efecto.

Las claves centralizadas se generan del mismo modo en los módulos criptográficos del sistema IvSign.

6.2.7 Almacenamiento de claves privadas en módulos criptográficos

Las claves de CA se almacenan y usas en los módulos criptográficos destinados a tal efecto, no pudiendo ser exportadas tras la realización de las copias de seguridad iniciales.

6.2.8 Método de activación de la clave privada

Las claves de los firmantes en formato software se activan introduciendo el PIN de la clave. Cada aplicativo de firma puede gestionar de forma diferente el número de veces que solicita el PIN dentro de una misma sesión o proceso de trabajo.

Las claves centralizadas se activan de acuerdo a lo especificado en la PS de IvSign, siendo necesario un inicio de sesión y la introducción del PIN de activación para realizar la firma. Los aplicativos de firma que integren con IvSign podrían gestionar de forma diferente el número de veces que solicita el PIN dentro de una misma sesión o proceso de trabajo.

Las claves de CA intermedias se activan exclusivamente desde los aplicativos de gestión de CA a través de conectividad directa con los dispositivos criptográficos.

Las claves Root sólo se pueden activar mediante la intervención de 3 personas de un total de 5.

6.2.9 Método de desactivación de la clave privada

Las claves de los firmantes en formato software se desactivan por el usuario eliminándolas del aplicativo donde hayan sido configuradas.

Las claves centralizadas se desactivan de acuerdo con lo especificado en la PS de IvSign, siendo necesario un inicio de sesión para la desactivación.

Las claves de CA intermedias se desactivan mediante procesos controlados por los operadores criptográficos.

6.2.10 Método de destrucción de la clave privada

Las claves de los firmantes en formato software se destruyen por el usuario eliminando todas las copias del archivo software que contiene la clave privada, previa desactivación de acuerdo con lo indicado en el punto anterior.

Las claves centralizadas se destruyen de acuerdo con lo especificado en la PS de IvSign, siendo necesario un inicio de sesión para la destrucción.

Las claves de CA intermedias se destruyen mediante procesos controlados por los operadores criptográficos.

6.2.11 Calificación del módulo criptográfico

Los dispositivos criptográficos utilizados por la CA cumplen con los estándares de seguridad Common Criteria EAL4+.

Los dispositivos utilizados para firma cualificada centralizada son dispositivos cualificados (QSCD).

6.3 OTROS ASPECTOS DE LA GESTIÓN DE LAS CLAVES

6.3.1 Archivo de la clave pública

El archivo de las claves públicas será realizado por el PSC en la infraestructura de Ivnosys Soluciones, por un periodo mínimo de 15 años desde la caducidad de las claves, siempre y cuando la tecnología de cada momento lo permita.

6.3.2 Periodo de uso para las claves públicas y privadas

El periodo de validez del certificado se determina en función del estado de la tecnología y tecnología criptográfica y en función del uso destinado al certificado.

La clave privada no debe ser usada después del periodo de validez del certificado de clave pública asociada. Los certificados expedidos a personas físicas o jurídicas tienen una validez máxima de 60 meses.

La clave pública o su certificado de clave publica puede ser usada como mecanismo de verificación de datos cifrados con la clave pública fuera del ámbito temporal para labores de validación.

Una clave privada podrá usarse fuera del periodo marcado por el certificado digital correspondiente, únicamente para la recuperación de datos cifrados.

6.4 DATOS DE ACTIVACIÓN DE LAS CLAVES PRIVADAS

En este punto se describen los procesos relacionados con los datos de activación de las claves privadas de entidad final, generadas en formato PKCS#12.

Para las claves centralizadas almacenadas en la Plataforma **IvSign CA** se atenderá a lo establecido en su MPS.

6.4.1 Instalación y generación de los datos de activación

El certificado se entrega en un fichero estandarizado PKCS#12 protegido por una contraseña generada por el aplicativo de gestión y entregada al sujeto mediante enlace para la generación a través del correo indicado en la solicitud.

6.4.2 Protección de los datos de activación

Los datos de activación son comunicados al sujeto por el correo electrónico indicado en la solicitud.

6.4.3 Otros aspectos de los datos de activación

No hay otras consideraciones relativas a los datos de activación.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

A nivel general los controles de seguridad informática de los sistemas son los utilizados por Ivnosys Soluciones para operar la CA y la RA de Signaturit Global CA. Signaturit y Ivnosys Soluciones utilizan sistemas fiables para la prestación de los servicios de certificación y ambos han realizado controles y auditorias informáticas para gestionar sus activos con el nivel de seguridad requerido para la gestion de dichos sistemas. En relación con la seguridad de la información, ambas entidades aplican su SGSI certificado por la norma UNE-ISO/IEC 27001.

6.5.1 Requerimientos técnicos de seguridad informática específicos

Se aplican los establecidos en el SGSI de Signaturit y Ivnosys Soluciones, para los sistemas de operación de la CA y RA de Signaturit Global CA, así como a los establecidos en la PS de IvSign.

6.5.2 Valoración de la seguridad informática

La seguridad de los sistemas viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.1 Controles de los sistemas de desarrollo

Los sistemas de desarrollo del sistema que soporta la CA Signaturit Global CA son responsabilidad de Ivnosys Soluciones que utiliza un software comercial de gestión de CA, por lo que no realiza desarrollos propios para la emisión, renovación y revocación de certificados.

En lo referente al sistema de claves centralizadas **IvSign**, propiedad de Ivnosys Soluciones, consultar su PS.

6.6.2 Controles de gestión de la seguridad

Los controles de gestión de la seguridad del SGSI de Signaturit y de Ivnosys Soluciones están definidos en la Declaración de Aplicabilidad (SOA, Statement of Applicability) de la certificación de la norma UNE-ISO/IEC 27001.

Signaturit organiza formaciones anuales y actividades de sensibilización a los empleados en el ámbito de la seguridad.

Signaturit regula contractualmente las medidas de seguridad equivalentes para los proveedores que colaboran de la prestación del servicio.

6.6.3 Controles de seguridad del ciclo de vida

Los controles de seguridad del ciclo de vida de los certificados son los que aplica Ivnosys Soluciones la cual cuenta con instrucciones específicas dentro de los procedimientos de Seguridad física y del ambiente para la reutilización o retirada segura de equipos, donde se especifican los pasos previos a la retirada y los procesos de eliminación o destrucción segura,

entre otros, de los dispositivos HSM QSCD que almacenan las claves de los certificados centralizados.

6.7 CONTROLES DE SEGURIDAD DE RED

Los controles de seguridad de red aplicables forman parte del SGSI de Ivnosys Soluciones y están definidos en la Declaración de Aplicabilidad (SOA, Statement of Applicability) de la certificación de la norma UNE-ISO/IEC 27001.

6.8 FUENTES DE TIEMPO

Signaturit utiliza los servicios de Sello de Tiempo de Ivnosys Soluciones. Todos los servidores de Ivnosys Soluciones están sincronizados en tiempo con fuentes fiables externas.

7 PERFILES DE CERTIFICADOS Y CRL

7.1 PERFILES DE CERTIFICADOS

Los perfiles de certificados siguen la norma RFC 5280.

Todos los certificados cualificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3 y los diferentes perfiles descritos en la normativa EN 319 412.

7.1.1 Número de versión

X.509 Versión 3.

7.1.2 Extensiones del certificado

Según el tipo de certificado vienen identificadas en los perfiles de certificación concretos.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es 1.2.840.113549.1.1.11 - sha256WithRSAEncryption.

El campo Subject Public Key Info (1.2.840.113549.1.1.1) incorpora el valor rsaEncryption.

7.1.4 Formato de nombres

El formato de nombre sigue las pautas descritas en esta CPS. La semántica exacta está descrita en los perfiles de certificación concretos.

7.1.5 Restricciones de los nombres

Las restricciones de los nombres siguen las pautas descritas en esta CPS. Restricciones específicas para cada tipo de certificado vendrán especificadas en cada una de los perfiles de certificación.

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

Los OIDs de las políticas de certificación están detallados en esta CPS en el punto 1.1. Vista general.

7.1.7 Uso de la extensión “*Policy Constraints*”

No está estipulado en esta CPS.

7.1.8 Sintaxis y semántica de los calificadores de política

No está estipulado en esta CPS.

7.1.9 Tratamiento semántico para la extensión crítica “Certificate Policy”

La extensión “Certificate Policy” identifica la política que define las prácticas que Signaturit asocia explícitamente con el certificado. Se pueden encontrar las políticas aplicadas a cada tipo de certificado en el punto 1.1. Vista general, los cuales se deberán interpretar de acuerdo con la siguiente tabla:

PSC	Servicio	Cualificación	Tipo certificado	Vinculación	Tipo vinculación	Formato	Uso
1.3.6.1.4.1.50646: Signaturit Soluciones	5: Signaturit Global CA	16: Certificados cualificados	1: Firma electrónica	1: Ciudadano		1: Centralizado 2: Software 3: QSCD centralizado 4: HSM 5: HW	1: Firma 2: Autenti-cación 3. Cifrado
				2: Corporativo			
				12: Corporativo UE			
				3: Representa-ción	1: Poderes generales		
					2: Trámites AA.PP.		
					3: Apodera-miento especial		
				4: Empleado público	1: Nivel medio		
					2: Nivel alto		
				5: Empleado público con seudónimo			
			6: Sello electrónico	2: Empresarial			
				4: AA.PP.	1: Nivel medio		

					2: Nivel alto		
				8: Timestamp			

7.2 PERFIL DE CRL

Las CRLs son firmadas por la CA que ha emitido los certificados.

7.2.1 Número de versión

Las CRL emitidas por la CA son de la versión 2.

7.2.2 CRL y extensiones

Las CRL’s incluirán el campo “Número de CRL”.

Las CRL’s no incluirán la extensión “ExpiredCertsOnCRL”

7.3 PERFIL OCSP

La CA dispone de un certificado respondedor OCSP. Este certificado se utiliza para firmar y verificar las respuestas del servicio OCSP sobre el estado de los certificados emitidos por esta CA.

7.3.1 Frecuencia de emisión certificado respondedor OCSP

Los certificados OCSP responder se renovará anualmente junto con las claves el mismo, las claves anteriores se eliminarán de acuerdo con los procedimientos establecidos por Signaturit Global CA por personal de confianza del TSP.

Se revisarán periódicamente los algoritmos a aplicar en la generación del certificado y su par de claves y se actualizarán en caso necesario acorde a las recomendaciones indicadas en el estándar ETSI TS 119 312 o norma equivalente.

Actualmente el tamaño de claves utilizado es de 2048 bits y el algoritmo de firma sha256WithRSAEncryption.

7.3.2 Número de versión

Los certificados de respondedor OCSP son versión 3. Estos certificados son emitidos por cada CA gestionada por Signaturit según el estándar RFC 6960.

7.3.3 OCSP extensions

Los certificados de OCSP Responder incluyen las siguientes extensiones:

- Comprobación de no revocación habilitado (idpkix-ocsp-nocheck).
- Política de certificación.
- Punto de distribución CRL.

Este certificado dispone de la siguiente identificación:

Distinguised Name	CN = OCSP Responder Signaturit Global CA O = SIGNATURIT SOLUTIONS S.L.U. 2.5.4.97 = VATES-B66024167 S = BARCELONA C = ES
OID	1.3.6.1.4.1.50646.5.16.9.7.

8 AUDITORIA DE CONFORMIDAD Y OTRAS EVALUACIONES

Los servicios de confianza cualificados son sometidos a una auditoria con una frecuencia mínima bienal (cada dos años) por un Organismo de Evaluación de la Conformidad debidamente acreditado, en aplicación del Reglamento UE nº 910/2014 (eIDAS).

El Organismo de Evaluación de la Conformidad de Signaturit es **Trust Conformity Assessment Body S.L.**

Adicionalmente todos los servicios de confianza ofrecidos por Signaturit se encuentran dentro del alcance de las siguientes auditorias de calidad y seguridad:

- Sistema de Gestión de Seguridad de la Información.
    - Renovación cada 3 años con auditorías de seguimiento anuales
    - Auditor: **AENOR Internacional S.A.U**
    - Norma ISO/IEC 27001
- Sistema de Gestión de la Calidad.
    - Renovación cada 3 años con auditorías de seguimiento anuales.
    - Auditor: **AENOR Internacional S.A.U**
    - Norma UNE-EN ISO 9001:2015

8.1.1 Frecuencia y circunstancias de la auditoria

Signaturit está sujeta a las siguientes auditorías externas que cubren la operación de la CA:

- Acreditación del cumplimiento de un Sistema de gestión de Servicios Electrónicos de Confianza, en aplicación del Reglamento UE nº 910/2014 (eIDAS).
    - La frecuencia de la auditoría es bienal (al menos cada dos años), con auditorías de seguimiento anuales.
- Certificado del Sistema de Gestión de Seguridad de la Información.
    - Renovación cada 3 años con auditorías de seguimiento anuales.
- Certificado del Sistema de Gestión de la Calidad.
    - Renovación cada 3 años con auditorías de seguimiento anuales.

Adicionalmente su proveedor de infraestructura Ivnosys Soluciones, en su condición de Prestador Cualificado de Servicios de confianza dispone asimismo de acreditaciones de cumplimiento de servicios eIDAS así como de certificaciones de sus Sistema de Gestion de Seguridad de la Información (UNE-ISO/IEC 27001), Sistema de Gestion de la Calidad (UNE-

EN-ISO 9001), Sistema de Gestion de Continuidad de Negocio (UNE-EN ISO 22301) y Esquema Nacional de Seguridad Nivel Medio.

Las referidas certificaciones de Signaturit y de Ivnosys Soluciones se pueden consultar en:

https://www.signaturit.com/es/legalidad/

https://www.signaturit.com/es/legalidad-ivnosys/

Con estas auditorias Signaturit garantiza que se hace una revisión como mínimo cada 12 meses de todo el sistema de gestión y de seguridad de la Autoridad de Certificación.

8.1.2 Identificación del auditor

Las auditorías de certificación son realizadas por:

- Sistema de gestión de Servicios Electrónicos de Confianza del Cliente, en aplicación del Reglamento UE nº 910/2014 (eIDAS): **Trust Conformity Assessment Body S.L.**
- Sistema de Gestión de Seguridad de la Información: **AENOR Internacional S.A.U**
- Sistema de Gestión de la Calidad: **AENOR Internacional S.A.U**

8.1.3 Relación del auditor con la entidad auditada

No existe vinculación ni dependencia financiera ni orgánica entre las empresas auditoras e Ivnosys Soluciones.

8.1.4 Temas cubiertos por la auditoria

Las auditorías realizadas cubren los siguientes aspectos:

- Sistema de gestión de Servicios Electrónicos de Confianza del Cliente, en aplicación del Reglamento UE nº 910/2014 (eIDAS):
  - Servicio de emisión de certificados digitales de firma electrónica
  - Normas de aplicación: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-5
- Sistema de Gestión de Seguridad de la Información:
  - Alcance: entre otros, los sistemas de información que soportan los procesos de instalación y operación del siguiente servicio de confianza en modalidad cloud: Gestión del ciclo de vida de los certificados digitales (emisión, validación, mantenimiento y revocación).
  - Norma de aplicación: UNE-ISO/IEC 27001:2014
- Sistema de Gestión de la Calidad:
  - Alcance: Actividades de Diseño, desarrollo e implementación de software; Soporte al usuario y mantenimiento correctivo, perfectivo y evolutivo de software
  - Norma de aplicación: UNE-EN-ISO9001:2008

8.1.5 Acciones tomadas como resultado de una deficiencia

Todas las auditorías disponen de un informe final de auditoría donde, en su caso, se han tomados todas las acciones correctoras de las No conformidades menores que han llevado a la concesión de la certificación.

8.1.6 Comunicación de resultados

Los resultados de la auditoria como PSC se comunicarán al organismo regulador de acuerdo con lo marcado por el Reglamento eIDAS.

9 OTROS REQUISITOS LEGALES Y DE NEGOCIO

9.1 TARIFAS

9.1.1 Tarifas de emisión de certificados y renovación

Todas las tarifas de emisión y renovación de certificados están sujetos a una negociación comercial previa. Para obtener una propuesta comercial se puede contactar con el Departamento comercial de Signaturit a través de los datos de contacto indicados en la dirección https://www.signaturit.com/es/contacto/.

9.1.2 Tarifa de acceso a los certificados

El acceso a la información pública de los certificados es gratuita.

9.1.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

Signaturit provee, de forma gratuita, la información relativa al estado de revocación de los certificados a través de listas de certificados revocados (CRL) y del servicio OCSP.

9.1.4 Otros servicios

Los servicios de centralización de claves se ofrecen comercialmente de forma independiente a los de emisión de certificados, de acuerdo con la oferta comercial recibida por el cliente.

9.1.5 Política de reembolso

Signaturit no tiene una política de reintegros específica, y se acoge a la normativa general vigente.

9.2 RESPONSABILIDAD FINANCIERA

Signaturit, en cuanto Prestador de Servicios de Confianza, está supeditado a las normas nacionales sobre responsabilidad establecidas en el Reglamento eIDAS, siendo responsable “de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica debido al incumplimiento de las obligaciones establecidas”.

Signaturit será responsable de los servicios prestados a las CA, respondiendo ante los usuarios del servicio y demás terceros o usuarios afectados por el servicio de acuerdo con esta CPS.

9.2.1 Cobertura del seguro

En cumplimiento de la legislación vigente Signaturit dispone de un seguro de responsabilidad civil que cubre la prestación de los servicios identificados en esta PS, por valor de 3.000.000 €.

9.2.2 Otros activos

No estipulado

9.2.3 Aseguramiento y garantía para entidades finales

Incluido en el Seguro de Responsabilidad Civil.

9.3 CONFIDENCIALIDAD

9.3.1 Ámbito de la información confidencial

Los datos de creación de firma electrónica son considerados datos confidenciales que no podrán ser revelados por ninguna de las partes en la medida que tengan acceso a ellos.

De forma general, Signaturit considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

9.3.2 Información fuera del ámbito de la confidencialidad

La información contenida en los certificados y el estado de los mismos, así como las políticas de certificación y la declaración de prácticas de certificación no se considera información confidencial.

9.3.3 Responsabilidad para proteger la información confidencial

El firmante es responsable de mantener de forma confidencial los datos de creación de firma.

Signaturit aplica todas las medidas de seguridad necesarias, descritas en esta CPS, para mantener la confidencialidad de la información.

La información de identificación de las solicitudes es recopilada y almacenada en el sistema de gestión de certificados de Signaturit (subcontratado a Ivnosys Soluciones) asociadas en la base datos a cada una de las solicitudes de certificados.

9.4 POLÍTICA DE PRIVACIDAD

9.4.1 Plan de privacidad

Signaturit ha elaborado en su análisis de riesgos una evaluación de impacto relativa a los datos y ha establecido los controles de seguridad necesarias de acuerdo con este análisis en el ámbito de su Sistema Gestión de Seguridad de la Información (SGSI).

Asimismo ha desarrollado una Política de privacidad de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD - Reglamento General de Protección de Datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Respecto de los datos personales de los Solicitantes, Sujetos/Titulares así como los relaciones con las entidades, Signaturit actúa como Responsable del tratamiento de conformidad con el RGPD y la LOPDGDD. Dispone de un Registro de Actividades del Tratamiento de datos de carácter personal donde está recogido el tratamiento “Gestión de Certificados” cuya finalidad es la gestión de las solicitudes y de los certificados emitidos y la prestación de los servicios de certificación asociados.

9.4.2 Información tratada como privada

Toda la información no pública es tratada como privada en el ámbito de la CA.

9.4.3 Información no considerada privada

Por el propio funcionamiento del sistema de certificación los datos personales incluidos en el Directorio de Certificados para comprobar la validez de un certificado determinado y su consulta por todos los usuarios, entendiendo por tales a las personas que voluntariamente confían y hacen uso de los certificados de Signaturit y siempre de acuerdo con lo establecido en la Política de Certificación.

9.4.4 Responsabilidad para la protección de la información privada

Signaturit trata toda la información personal y privada de acuerdo con los documentos de seguridad de la información establecidos en la norma UNE-ISO/IEC 27001.

9.4.5 Advertencia y consentimiento del uso de información privada

Se informa que, para el cumplimiento de la prestación del servicio de certificación y firma electrónica, la Autoridad de Registro (RA) competente tendrá acceso a los datos recogidos en la solicitud de servicios de certificación, para el cumplimiento de sus funciones de RA.

Esta información será advertida y aceptada por el solicitante en el momento de la introducción de los datos del certificado en la solicitud. Del mismo modo, en los Términos y Condiciones de Utilización del Certificado que firma el suscriptor, éste acepta las condiciones respecto al uso de los datos personales incluidos en el certificado.

Además, por requerimientos de la legislación de firma electrónica es necesaria la conservación de sus datos de identificación y de los datos asociados al certificado emitido

durante un periodo de 15 años desde la caducidad del certificado. Por tanto, por imperativo legal, no podrá ejercer en su totalidad los derechos en materia de protección de datos.

9.4.6 Divulgación de conformidad con un proceso judicial o administrativo

Signaturit velará por la seguridad de la documentación y datos puestos bajo su custodia, impidiendo que terceras personas no autorizadas puedan acceder a dicha información, excepto cuando así lo exigiera un mandato judicial u otra autoridad competente.

9.4.7 Otras circunstancias de divulgación de información

No estipulado.

9.5 PROPIEDAD INTELECTUAL

Signaturit es titular de los derechos de propiedad intelectual sobre esta CPS y sobre los certificados electrónicos que emite, salvo acuerdo en otro sentido.

9.5.1 CA

SIGNATURIT SOLUTIONS, S.L.U. actúa como Autoridad de Certificación, relacionando una determinada clave pública con una persona concreta a través de la emisión de un Certificado Digital.

9.5.2 RA

La AUTORIDAD DE REGISTRO está encargada, entre otras funciones, de hacer entrega del Certificado emitido a nombre del SOLICITANTE y verificar la identidad de éste. Todas o parte de las funciones de RA podrán ser delegadas a una tercera entidad que se constituirá, según los casos, como Autoridad de Registro Externa (RA Externa), y que actuará en cualquier caso a efectos de esta CPS como Autoridad de Registro.

9.5.3 Suscriptor

El SOLICITANTE es una persona física vinculada a una ENTIDAD (con o sin personalidad jurídica) por una relación de representación, de pertenencia corporativa o por algún tipo de relación mercantil, poseedor de un dispositivo de creación de firma, y que asume la condición de TITULAR y FIRMANTE en el sentido del marco legal aplicable a la prestación del servicio.

9.5.4 Parte usuaria

Persona que recibe una transacción electrónica realizada con un certificado emitido por Signaturit Global CA y que voluntariamente confía en el Certificado emitido por ésta.

9.5.5 Otros participantes

No estipulado

9.6 DECLARACIONES Y GARANTÍAS

9.6.1 De la AC

De acuerdo con la legislación vigente en materia de prestación de servicios de certificación, Signaturit debe garantizar el cumplimiento de las obligaciones y procedimientos descritos en esta DPC y PC y en este sentido es el único responsable de ello incluso si delega parte de las operaciones a un tercero subcontratado.

Signaturit es responsable de los daños y perjuicios causados a los usuarios de sus servicios, ya sea el Sujeto o la Parte que Confía, y a otros terceros de acuerdo con los términos y condiciones establecidos en la legislación vigente.

En este sentido, Signaturit es la única responsable de la emisión de los certificados y de su gestión durante su ciclo de vida así como, si es necesario, en caso de revocación de los certificados. En particular, Signaturit es responsable de:

- La exactitud de toda la información contenida en el certificado
- De que la clave pública y privada funcionan conjunta y complementariamente, utilizando dispositivos y mecanismos criptográficos certificados.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Publicar los certificados emitidos en un directorio
- Revocar los certificados conforme se indica en la presente CPS y publicar dichas revocaciones en las CRLs
- Publicar esta DPC y PC e informar de los cambios a los intervinientes en el sistema de certificación.
- Proteger los datos de creación de firma si procede
- Conservar los datos relativos a los certificados durante el plazo legal exigible.

Con anterioridad de la emisión y entrega del certificado al suscriptor, el PSC informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor (Términos y Condiciones de uso) y mediante el documento PDS o texto divulgativo, ambos publicados en su página web, para que los intervinientes conozcan los contenidos mínimos de las obligaciones de la AC y del resto de actores, y sus cambios.

9.6.2 De la RA

El Artículo 10 de la Ley 6/2020 de Servicios de Confianza establece que: “*Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado*”

En este sentido, las RA también se obligan en los términos definidos en la presente CPS para la emisión de certificados y previamente al inicio de sus funciones deben formalizar un Acuerdo privado donde asumen una serie de obligaciones y responsabilidades hacia la AC y hacia los Suscriptores y Terceros que confían.

La AR será plenamente responsable del procedimiento de identificación y autentificación de los Suscriptores, Solicitantes, Sujetos o Responsables, del completo registro de las solicitudes

y validación de los certificados, y de la conservación de la información y documentación acreditativa de los datos incluidos en el certificado y legalmente exigible. Lo hará de acuerdo con lo establecido en la presente DPC o de acuerdo a otro procedimiento aprobado por el PSC.

Por lo tanto, las AR son responsables de las posibles consecuencias debidas al incumplimiento de los deberes de registro, y se comprometen a respetar esta CPS, que las AR deben tener perfectamente controlada y que deben utilizar como guía.

En caso de reclamación por parte de un Sujeto, Suscriptor o Tercero que Confía, si existen pruebas de que la causa de la reclamación se debe a una incorrecta validación o comprobación de los datos por parte de la RA, la AC puede responsabilizar a la AR de las consecuencias, de acuerdo con el acuerdo firmado con ella.

9.6.3 Del Solicitante, Sujeto/Titular y Responsable

El Solicitante como tal y en su condición de futuro Sujeto/Titular del certificado, así como el Responsable del certificado de sello electrónico, se obliga a cumplir con lo establecido en la normativa vigente, y en particular a:

- Suministrar toda la información y documentación exigida por la CA o RA para realizar una correcta identificación,
- Garantizar la exactitud y veracidad de la información proporcionada.
- Hacer un uso del certificado de forma responsable, custodiar las claves secretas, passwords o pines de activación de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso, no autorizados, de forma a mantener el control exclusivo sobre el uso del certificado.
- Responsabilizarse ante la Entidad que representan o a la que están vinculado ante usos no autorizados o incorrectos del certificado.
- Solicitar la suspensión/revocación del Certificado cuando se cumpla alguno de los supuestos de suspensión y revocación de certificados previstos en esta CPS.
- Notificar inmediatamente a la CA o RA en caso de que detecte que se ha incluido cualquier información incorrecta o inexacta o en caso de que, de forma sobrevenida, la información del Certificado no se corresponda con la realidad o haya cambiado posteriormente a su emisión.
- Informar inmediatamente a la CA o RA acerca de cualquier situación que pueda afectar a la validez del Certificado, o a la seguridad de las claves, y cesar en su uso.
- No utilizar la clave privada ni el certificado desde el momento en que se solicite o se le avise por la AC o la AR de la revocación del mismo, o una vez haya expirado el plazo de validez del certificado.
- Autorizar a la AC y a la AR para que procedan al tratamiento de los datos personales contenidos en los certificados, en el marco de las finalidades de la relación telemática y, en todo caso, para el cumplimiento de las obligaciones legales de verificación de los certificados.
- Cualquier otra que se derive del contenido de las PC específicas para cada tipo de Certificado.

9.6.4 Del Suscriptor

Además de lo establecido en la normativa vigente, el Suscriptor de un certificado estará obligado a:

- Aceptar los Términos y Condiciones del Prestador
- Informar a la AR o a la AC de cualquier cambio en los datos aportados para la emisión del certificado durante su periodo de validez.
- Informar a la AR o a la AC lo antes posible de la existencia de cualquier causa de revocación.

9.6.5 Del Tercero que confía

El Tercero que confía en el certificado está obligada a:

- Validar el certificado a través del anclaje de confianza de la TSL y verificar que se trata de un certificado cualificado emitido por una CA cualificada de Signaturit
- Verificar el estado del certificado consultando el servicio OCSP o las CRL. Para la consulta de certificados expirados deberá utilizar el servicio de consulta OCSP.
- Conocer y someterse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía. En particular, en el caso de certificados con atributo de representación de una Entidad basada en un poder especial o documento privado con facultades limitadas, el Tercero que confía deberá comprobar los límites de dichas facultades.

9.6.6 De la Entidad

En el caso de certificados de atributo de representación o que impliquen una vinculación entre una persona física y una Entidad, la Entidad estará obligada a solicitar a la AC o a la AR la revocación del certificado cuando la persona física deje de estar vinculada a la Entidad.

9.7 LIMITACIONES DE RESPONSABILIDAD

Según la legislación vigente, la responsabilidad de Signaturit y de la RA, no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Sujeto, y a la Parte Usuaria por:

- No haber proporcionado información adecuada, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación
- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad
- No haber solicitado la suspensión o revocación de los datos del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables a la Parte Usuaria si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado

- De los daños ocasionados al Sujeto o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible.
- Un uso inadecuado o fraudulento del certificado en caso de que el Sujeto/Titular y/o el Responsable lo haya cedido o autorizado su uso a favor de un tercero siendo responsabilidad exclusiva del Sujeto/Titular y del Responsable el control de las claves asociadas al certificado.

Signaturit y las RAs tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en la presente CPS y las Políticas de Certificación
- Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la CA
- Por el uso de la información contenida en el Certificado o en la CRL o respuesta OCSP.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Sujeto.

En relación con las acciones o inacciones de la Parte que Confía en el certificado, Signaturit o la RA no será responsable si ésta:

- No verifica las restricciones contenidas en el certificado o en esta DPC y en las PCs respecto a sus posibles usos.
- No comprueba la fecha de caducidad del certificado indicada en la extensión de la validez del certificado o no verificar la firma digital.

Mas generalmente, ni Signaturit ni la RA serán responsable por el empleo de los certificados digitales en operaciones que contravienen las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS o los Contratos de la CA con las RA o con el Sujeto/Titular y/o el Firmante tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la CA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

En ningún caso Signaturit emitirá valoración alguna sobre el contenido firmado, asumiendo por tanto el signatario cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado. Asimismo, le será imputable al signatario cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los contratos de la CA con el firmante (sujeto), así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

Respecto a la publicación de los datos personales en los certificados para las consultas necesarias a las partes usuarias de los mismos y, ante la imposibilidad de que se pueda controlar el uso posterior que los usuarios del sistema puedan hacer de sus datos, la CA queda exonerada de cualquier responsabilidad derivada de un uso indebido de los mismos.

9.8 INDEMNIZACIONES

El seguro cubrirá todas las cantidades que Signaturit deba pagar legalmente, hasta el límite de cobertura contratado, como consecuencia de cualquier procedimiento judicial en el que se declare su responsabilidad.

Cuando la revocación de un certificado a instancias de la CA sea injustificada, la CA podrá indemnizar a aquellos SOLICITANTES que lo soliciten por escrito dentro de los tres meses siguientes a la fecha de revocación. Esta indemnización no podrá ser superior a lo pagado por el propio SOLICITANTE por la obtención del referido Certificado.

9.9 DURACIÓN Y RESOLUCIÓN

9.9.1 Duración

La CPS entrará en vigor en el momento de su publicación.

En el momento en que una nueva versión del documento sea publicada, la presente CPS será derogada en todos los puntos que haya sufrido alguna modificación respecto a la versión anterior.

Con carácter general esta CPS entrará en vigor para el suscriptor de un certificado en la fecha de emisión del certificado y terminará coincidiendo con las fechas de caducidad, ambas indicadas en el Certificado y pudiendo ser renovado con arreglo a los términos establecidos en esta CPS y en las PC correspondientes.

9.9.2 Resolución

El incumplimiento de las estipulaciones contenidas en esta CPS y/o en las PC por cualquiera de las partes será causa de resolución del contrato de prestación de servicios de certificación. En tal caso, la parte no incumplidora tendrá derecho a resolver el acuerdo con efecto inmediato. El incumplimiento por parte del SOLICITANTE dará derecho a la CA a revocar el Certificado, con independencia de los daños y perjuicios que pudiera reclamar.

La CA tendrá derecho a revocar y no renovar el Certificado con anterioridad al plazo previsto de vigencia en los casos previstos en la PC correspondiente.

El SOLICITANTE podrá resolver libremente el acuerdo en cualquier momento mediante la notificación por escrito con una antelación de 30 días. En ningún caso, dicha resolución dará derecho a la devolución de las cantidades abonadas por la obtención del Certificado.

Si el ejercicio de los derechos de oposición, o cancelación de los datos expuestos en el presente documento dificultase la prestación de servicios objeto de este contrato, Signaturit quedará facultada para resolver el presente acuerdo.

9.9.3 Efectos de la resolución y mantenimiento de clausulas

En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la CA vela porque, al menos los requisitos contenidos en las secciones 9.6 (Declaraciones y Garantías), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad) de este documento, continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.

9.9.4 Notificaciones y comunicaciones entre los participantes

Tanto el solicitante como la parte usuaria podrá ponerse en contacto con la CA o la RA a través de los medios indicados en esta CPS o en la página web de Signaturit.

La CA podrá comunicarse o notificar a los suscriptores a través de cualquiera de los medios indicados en su solicitud de certificado.

9.10 MODIFICACIONES

9.10.1 Procedimiento de modificación

Esta CPS se modificará cuando se produzcan cambios relevantes en la gestión de cualquier tipo de certificados sujetos a ella. Se producirán al menos revisiones anuales en caso de que no se produzcan cambios en este tiempo. Estas revisiones quedaran reflejadas en el cuadro de versiones al inicio del documento.

9.10.2 Mecanismo de notificación y plazos

Las modificaciones se comunicarán al SOLICITANTE, cuando el cambio incida directamente en sus derechos y obligaciones, de acuerdo con lo estipulado en el acuerdo de prestación de servicios aceptado por el solicitante en el momento de confirmación de la solicitud de un certificado.

9.10.3 Circunstancias para el cambio de OID

No están previstas.

9.11 PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS

En caso de cualquier controversia o conflicto derivado de las presentes DPC y Términos y Condiciones, las partes, con renuncia a cualquier otra jurisdicción que pudiera corresponderles, se someten a la Corte Española de Arbitraje, salvo que el reclamante sea un consumidor, por lo que será competente el Juez o Tribunal que corresponda al domicilio del consumidor.

9.12 LEGISLACIÓN APLICABLE

Esta CPS se regirá por la legislación española y de la Unión Europea en materia de certificación y firma electrónica aplicable en cada momento y, con arreglo a la cual deberá ser interpretado su contenido.

9.13 CLAUSULAS DIVERSAS

9.13.1 Marco legal

Las Políticas de Certificación de Signaturit (en adelante PC) y esta Declaración de Prácticas de Certificación (en adelante CPS), junto a los términos y condiciones aceptadas en el momento de la solicitud constituyen el acuerdo completo que regulará la relación entre las partes, internamente y frente a terceros, sin perjuicio de lo dispuesto en la legislación vigente.

9.13.2 Asignación

No estipulado.

9.13.3 Separabilidad

No estipulado.

9.13.4 Cumplimiento

No estipulado.

9.13.5 Fuerza mayor

Ni la CA, ni la RA, asumirán responsabilidad por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de las PC si tal falta de ejecución o retraso resultara o fuera consecuencia de desastres naturales, la guerra, el estado de sitio, de alarma o de emergencia sanitaria o cualquier otro supuesto de fuerza mayor.

9.14 OTRAS CLAUSULAS

No estipulado.

ANEXO

POLÍTICAS DE USO DE LOS CERTIFICADOS DE SIGNATURIT GLOBAL CA

1 INTRODUCCIÓN

En el siguiente ANEXO se recogen los usos específicos de los diferentes tipos de certificados emitidos por Signaturit Global CA.

Cada tipo de certificado referencia las políticas de certificación que le aplican:

- Política de la CA. Identifica el perfil dentro de la propia CA
- Política eIDAS. Identifica la política definida por la norma ETSI EN 319 411 2 “Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates”
- Política Ley 40/2015, según se definen en el documento “PERFILES DE CERTIFICADOS ELECTRÓNICOS” - NIPO: 630-16-298-6 (no disponible en la versión 1 de esta CPS)

2 CERTIFICADO DE CIUDADANO

2.1 OIDS DE POLÍTICA

- Software
  - 1.3.6.1.4.1.50646.5.16.1.1.2 (Signaturit Global CA)
  - 0.4.0.194112.1.0 (ETSI EN 319 411 2)

2.2 USOS

Certificado emitido a una persona física que garantiza la identidad del titular del certificado.

El uso de este certificado está restringido únicamente a su titular, bajo su propia responsabilidad.

Los certificados podrán utilizarse para firma electrónica y para autenticación del titular.

Los certificados centralizados y en software generarán firmas avanzadas con certificado cualificado.

Los certificados centralizados en QSCD generarán firmas cualificadas.

2.3 SOLICITANTE / TITULAR

Es la persona física identificada en el certificado por su nombre, apellidos y Documento de identidad.

2.4 DOCUMENTACIÓN

La documentación que deberá presentarse ante la Autoridad de Registro o un Punto de Verificación Presencial en copia electrónica es un documento de identificación de acuerdo con lo estipulado en la Declaración de Prácticas correspondiente. Durante la identificación se deberá cotejar con el original.