DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PKI ADMINISTRACIÓN PÚBLICA ANDORRANA

Govern d'Andorra

Versión 2.1.0

Idioma: **Castellano**

Índice de Contenido

Contenido

1. INTRODUCCIÓN

1.1. Visión General

La Infraestructura de Clave Pública (PKI) de la Administración Pública Andorrana ha sido creada para permitir la autenticación fiable y segura de la identidad, además de facilitar la confidencialidad e integridad de transacciones electrónicas. Este documento identifica las prácticas y procedimientos que emplea la Oficina de Serveis de Confiança Electrònica del Principat d'Andorra, OSCEPA en adelante, en la emisión de certificados digitales dentro de dicha infraestructura.

Estas prácticas están alineadas con los requisitos marcados en *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* elaborado por el CA/B Forum http://www.cabforum.org en su versión 1.6.6.

En el caso de que exista alguna inconsistencia entre este documento y los *Baseline Requirements*, los *Baseline Requirements* tendrán prioridad sobre este documento.

1.2. Identificación y nombre del documento

Este documento es la Declaración de Prácticas de Certificación de la OSCEPA.

Todos los certificados que emita la OSCEPA contendrán un identificador de política correspondiente al tipo de certificado aplicable.

La OSCEPA emite los siguientes tipos de certificados que pueden identificarse mediante el identificador de objetos de política de certificados contenida en la extensión *certificatePolicy* de un certificado. A continuación se identifican los tipos de certificado emitidos por la OSCEPA.

- Certificados corporativos públicos, adquiridos por parte del sector público para cubrir sus necesidades de seguridad.
- Certificados de la ciudadanía, emitidos por la Entidad de Certificación de la Administración Pública Andorrana, o por otros prestadores de servicios de certificación, cuando hayan sido objeto de admisión por parte de la Administración Pública.

Complementariamente, se define la siguiente tipología de certificados:

- Certificados individuales de persona física.
- Certificados individuales de persona física con profesión regulada.
- Certificados corporativos de persona física al servicio de una administración pública.
- Certificados corporativos de persona física al servicio de una organización privada.
- Certificado de representante de persona jurídica privada, pública o entidad sin personalidad jurídica.
- Sello de órgano, Administración pública o entidad de derecho público.
- Sello de empresa.

1.3. Participantes en la PKI

1.3.1 Autoridades de Certificación

Es el componente de una PKI responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Firmante (Suscriptor) y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona.

Una Autoridad de certificación (AC) utiliza Autoridades de registro (AR) para realizar las labores de comprobación y almacenamiento de la documentación de los contenidos incorporados en el certificado digital.

Una AC pertenece a una entidad jurídica indicada en el campo organización (O) del certificado digital asociado.

La información relativa a la AC gestionada por la Administración Pública Andorrana puede encontrarse en este documento o la dirección Web
https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

1.3.2 Autoridades de Registro

Una AR puede ser una persona física o jurídica que actúa conforme esta CPS y, en su caso, mediante un acuerdo suscrito con una AC concreta, ejerciendo las funciones de gestión de las solicitudes, identificación y registro de los solicitantes del certificado y aquellas que se dispongan en las Políticas de Certificación concretas. Las AR son autoridades delegadas de la AC, aunque ésta es la última responsable del servicio en última instancia.

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

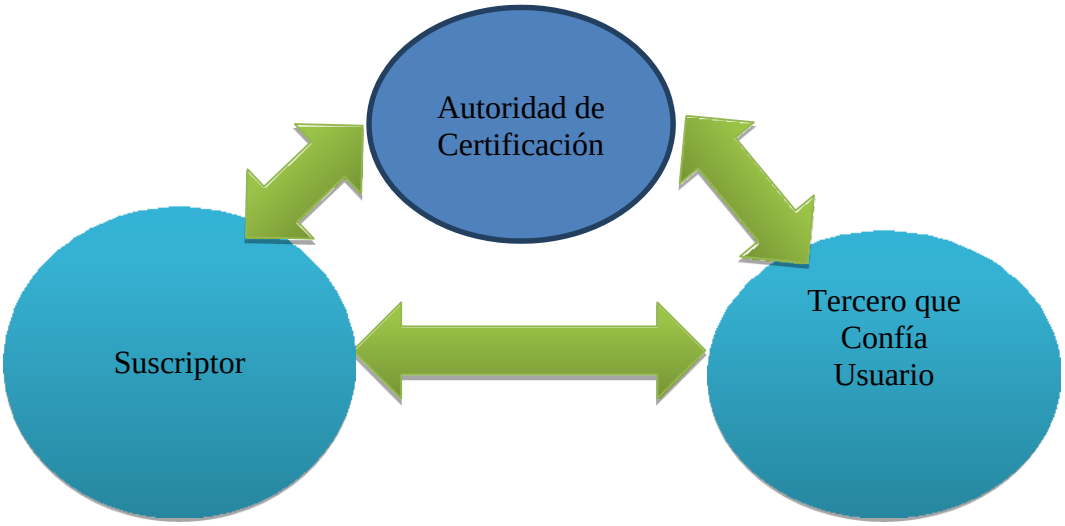
- La propia Autoridad de Certificación.
- Cualquier agente nacional o internacional que mantenga una relación contractual con la AC y supere los procesos de alta y las auditorias que demuestren que se siguen los requisitos de los exigidos en este documento.

1.3.3 Firmante/Suscriptor

Entendemos por Firmante/Suscriptor al titular del certificado cuando éste sea una persona física o jurídica y viene descrita en el campo CN del certificado. Cuando se emita a nombre de un dispositivo hardware o aplicativo informático, se considerará firmante/Suscriptor, la persona física o jurídica solicitante del certificado emitido.

1.3.4 Parte que confía

En esta CPS se entiende por Tercero que confía o usuario, la persona que recibe una transacción electrónica realizada con un certificado emitido por la AC gestionada por la OSCEPA y que voluntariamente confía en el Certificado emitido por ésta.



1.3.5 Otros participantes

No aplica.

1.4. Ámbito de aplicación y usos

1.4.1 Usos apropiados de los certificados

Los certificados de la OSCEPA podrán usarse en los términos establecidos en este documento.

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

- Autenticación basada en certificados X.509v3.
- Firma electrónica, avanzada o reconocida, basada en certificados X.509v3.
- Cifrado asimétrico o mixto, basado en certificados X.509v3.

1.4.2 Usos prohibidos de los certificados

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso y que vienen descritos en este documento.

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.

El empleo de los certificados digitales en operaciones que contravienen la CPS o los Contratos

de la AC con las AR o con sus Firmantes/Suscriptores tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

La OSCEPA no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la OSCEPA emitir valoración alguna sobre dicho contenido, 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 la CPS y los contratos de la AC con sus Firmantes, 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.

La OSCEPA 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 constrains*) y/o "restricciones de nombre" (*name constrains*) 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*) y/o mediante textos incorporados el campo "declaración del emisor" (*user notice*) marcados cono "no crítico" pero de obligado cumplimiento por parte del titular y del usuario del certificado.

1.5. Autoridad de Políticas

Esta CPS define la forma en que la Autoridad de Certificación da respuesta a todos los requerimientos y niveles de seguridad impuestos por las Políticas de Certificación correspondientes.

La actividad de la Autoridad de Certificación podrá ser sometida a la inspección de la Autoridad de las Políticas (PA) o por personal delegado por la misma.

Para las jerarquías descritas en este documento la autoridad de las Políticas corresponde a la dirección técnica de la OSCEPA.

1.5.1 Organización que administra el documento

La redacción y control de esta CPS está gestionada por la dirección técnica de la OSCEPA.

1.5.2 Datos de contacto de la organización

Dirección:	Carrer Prat de la Creu, 62-64
Teléfono:	+376 875700
Email:	oficina.certificacio@govern.ad

Para reportar incidentes de seguridad relacionados con los certificados pueden ponerse en contacto con la Administración Pública Andorrana mediante a través de una comunicación dirigida a la cuenta de email oficina.certificacio@govern.ad

1.5.3 Persona que determina la idoneidad de CPS para la política

La dirección técnica de la OSCEPA se constituye por lo tanto en la Autoridad de las Políticas (PA) de las Jerarquías y Autoridades de Certificación descritas anteriormente siendo responsable de la administración de la CPS.

1.5.4 Procedimientos de gestión del documento

La publicación de las revisiones de esta CPS deberá estar aprobada por la dirección técnica de la OSCEPA.

La Administración Pública Andorrana publica en su página web cada nueva versión. La CPS está publicada en formato PDF firmado electrónicamente con un certificado digital.

1.6. Acrónimos y Definiciones.

1.6.1 Acrónimos

AC	Autoridad de Certificación
RA	Autoridad de Registro
CPS	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL	*Certificate Revocation List.* Lista de certificados revocados
CSR	*Certificate Signing Request.* Petición de firma de certificado
DES	*Data Encryption Standard*. Estándar de cifrado de datos
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm.* Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
DSADCF	Dispositivo seguro de almacén de datos de creación de firma
FIPS	*Federal Information Processing Standard Publication*
IETF	*Internet Engineering Task Force*

ISO	*International Organization for Standardization.* Organismo Internacional de Estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso a directorios
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PA	*Policy Authority.* Autoridad de Políticas
PC	Política de Certificación
PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de cifrado
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

1.6.2 Definiciones

Autoridad de Certificación	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza entre el Sujeto/Firmante y la Parte Usuaria, vinculando una determinada clave pública con una persona.
Autoridad de políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y CPS.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.

Certificación cruzada	El establecimiento de una relación de confianza entre dos AC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.
Clave privada	Valor matemático conocido únicamente por el Sujeto/Firmante y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma. La clave privada de la AC será usada para firma de certificados y firma de CRL
CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
Datos de Activación	Datos privados, como PIN o contraseñas empleados para la activación de la clave privada
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del Sujeto/Firmante de forma que solo él tenga el control sobre la misma.
DSCF	*Dispositivo Seguro de creación de firma*. Elemento software o hardware empleado por el Sujeto/Firmante para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Sujeto/Firmante.
Entidad	Dentro del contexto de estas políticas de certificación, aquella empresa u organización de cualquier tipo con la que el solicitante tiene algún tipo de vinculación.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera:

	a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes
Solicitante	Dentro del contexto de esta política de certificación, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de la entidad.
Sujeto/Firmante	Dentro del contexto de esta declaración de prácticas de certificación, la persona física cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Parte Usuaria	Dentro del contexto de esta política de certificación, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado

2. RESPONSABILIDAD DE PUBLICACIÓN Y REPOSITORIOS

2.1. Repositorios

La OSCEPA hace público su certificado de AC, estado de validez de los certificados digitales emitidos y CPS.

El repositorio se encuentra en https://www.signaturaelectronica.ad/ajuda

Los servicios de consulta están diseñados para garantizar una disponibilidad de 24 horas por día 7 días a la semana.

La OSCEPA solicita previamente la autorización del titular antes de proceder a la publicación del certificado.

2.2. Publicación de información de certificados

La OSCEPA publica las CRL y el acceso el servicio OCSP en:

http://crl.govern.ad/GovernAndorra.crl
http://crl1.govern.ad/GovernAndorra.crl
http://ocsp.govern.ad
http://ocsp1.govern.ad

2.3. Frecuencia de publicación.

La OSCEPA emite y publica listas de revocados de forma periódica siguiendo la tabla marcada en el apartado de estas prácticas *"Frecuencia de emisión de CRLs"*.

La OSCEPA publica de forma inmediata en su página Web https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio. Cualquier modificación en las Políticas y la CPS, manteniendo un histórico de versiones.

Esta información se publicará cuando se encuentre disponible y en especial, de forma inmediata cuando se emitan las menciones relativas a la vigencia de los certificados.

Los cambios en la CPS se regirán por lo establecido en la sección correspondiente de la CPS.

La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en la sección correspondiente de esta CPS.

Al cabo de 15 (quince) días desde la publicación de la nueva versión, se podrá retirar la referencia al cambio de la página principal y se inserta en el depósito. Las versiones antiguas de la documentación serán conservadas, por un periodo de 15 (quince) años por la Entidad de Certificación, pudiendo ser consultadas, por causa razonada por los interesados.

2.4. Controles de acceso a los repositorios.

El acceso al repositorio de la OSCEPA es libre.

Se mantienen controles físicos y lógicos para impedir modificaciones o borrado de información no autorizado en dicho repositorio.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Denominación

3.1.1 Tipos de nombres

El Firmantes/Suscriptor se describe en los certificados mediante un nombre distintivo (DN, distinguished name, Subject) conforme al estándar X.501. Las descripciones del campo DN están reflejadas en cada una de las fichas de perfil de los certificados. Asimismo incluye un componente " Common Name "(CN =).

Las fichas de perfil se pueden solicitar a través del soporte al cliente en oficina.certificacio@govern.ad y en https://www.signaturaelectronica.ad/ajuda.

En certificados correspondientes a personas físicas la identificación del signatario estará formada por su nombre y apellidos, más su NIA.

En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su NRT.

3.1.2 Significado de los nombres

Todos los Nombres Distinguidos deben ser significativos, y la identificación de los atributos asociados al suscriptor debe ser en una forma legible por humanos. Ver 7.1.4

3.1.3 Anonimato o pseudónimos de suscriptores

No aplicable.

3.1.4 Reglas utilizadas para interpretar varios formatos de nombres

La OSCEPA 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 la misma AC no se puede volver a asignar un nombre de suscriptor que ya haya sido ocupado, a un suscriptor diferente, esto se consigue incorporando el identificador fiscal único a la cadena del nombre que distingue al titular del certificado.

3.1.5.1 Emisión de varios certificados de persona física para un mismo titular

Bajo esta CPS suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Administrativa (NIA) de la persona física
- Número de Registro Tributario (NRT) de la empresa
- Tipo de Certificado (Campo descripción del certificado).

Como excepción esta CPS permite la validación de una solicitud de un certificado cuando coincida NIA, NRT, Tipo, con un certificado válido, siempre que exista algún elemento diferenciador entre ambos, en los campos TITLE y/o DEPARTAMENT

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

La OSCEPA no asume compromisos en la emisión de certificados respecto al uso de marcas y otros signos distintivos. La OSCEPA no permite deliberadamente el uso de un signo distintivo sobre el Sujeto/Firmante que no ostente derechos de uso. Sin embargo, la Administración Pública Andorrana no está obligada a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados, por lo que puede negarse a generar o solicitar la revocación de cualquier certificado involucrado en una disputa.

3.1.7 Procedimiento de resolución de disputas de nombres

La OSCEPA no tiene responsabilidad en el caso de resolución de disputas de nombres. En todo caso, la asignación de nombres se realizará basándose en su orden de entrada.

La Administración Pública Andorrana no arbitra este tipo de disputas que deberán ser resueltas directamente por las partes.

3.2. Validación inicial de la identidad

3.2.1 Métodos de prueba de la posesión de la clave privada.

La OSCEPA emplea diversos circuitos para la emisión de certificados donde la clave privada se gestiona de diferente forma. La clave privada puede ser generada tanto por el usuario como por la OSCEPA

a) Generación de claves por parte de la OSCEPA.

   En Software: Se entregan al Sujeto/Firmante en mano o mediante correo a través de ficheros protegidos utilizando el Standard PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso al fichero PKCS#12 que posibilita la instalación de éste en las aplicaciones, es entregada por un medio distinto al utilizado en la recepción del fichero.

   En Hardware: Las claves pueden ser entregadas por la OSCEPA al Sujeto/Firmante, directamente o a través de una autoridad de registro en un dispositivo seguro de creación de firma.

b) Generación de las claves por el suscriptor.

El Firmante dispone de un mecanismo de generación de claves ya sea software o hardware, La prueba de posesión de la clave privada en estos casos es la petición recibida por la OSCEPA en formato PKCS#10 o criptográficamente equivalente.

3.2.2 Identificación de la entidad

3.2.2.1 Identidad

Con carácter previo a la emisión y entrega de un certificado emitido a una persona jurídica o a una persona física con atributo de vinculación a una entidad, es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad.

Para estos certificados, se exige en todos los casos, la identificación de la entidad, para lo que la RA requerirá la documentación pertinente en función del tipo de entidad.

Además, se comprueba:

- Que los datos o documentos aportados no tengan una antigüedad superior a 1 año.
- Que la antigüedad de existencia l egal de la organización es de 1 año mínimo.

En Administraciones públicas: No se exige la documentación acreditativa de la existencia de la administración pública, organismo o entidad de derecho público, dado que dicha identidad forma parte del ámbito corporativo de las AAPP del Estado.

3.2.2.2 Marcas registradas

Ver punto 3.1.6

3.2.2.3 Verificación del país

Ver punto 3.2.2.1

3.2.2.4 Validación de la autorización o control de dominio

Ver punto 3.2.5.1

3.2.2.5 Autenticación de una dirección IP

No aplicable.

3.2.2.6 Validación del dominio Wildcard

No aplicable.

3.2.2.7 Exactitud de las fuentes de datos

Ver punto 3.2.2.1

3.2.2.8 Registros CAA

No aplicable.

3.2.3 Identificación de la identidad de un individuo.

Con carácter previo a la emisión y entrega de un certificado, se exige la personación física del Sujeto/Titular o Firmante cuando éste sea una persona física o del Solicitante cuando el Sujeto/Titular es una entidad jurídica, presentando un documento oficial que acredite de forma fehaciente su identidad (documento oficial de identidad, tarjeta de residencia, pasaporte o cualquier otro documento admitido en derecho) de acuerdo con lo dispuesto en el artículo 26 de la Ley 35/2014, de 27 de noviembre, de servicios de confianza electrónica, siempre que contenga, al menos , la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado.

En el caso de documentos de identidad extranjeros, se podrá pedir traducción jurada en castellano con apostilla de la Haya si se considera necesario.

3.2.4 Información de suscriptor no verificada

No está permitido bajo estas prácticas de certificación incluir información no verificada en el "subject" de un certificado.

3.2.5 Validación de la autoridad

3.2.5.1 Identificación de la vinculación.

Tipo de certificado	Documentación
Certificados individuales de persona física Certificados individuales de persona física con profesión regulada Certificados corporativos de persona física al servicio de una administración pública Certificados corporativos de persona física al servicio de una organización privada Certificado de representante de persona jurídica privada, pública o entidad sin personalidad jurídica	El artículo 26.2 de la Ley Andorrana 35/2014, de 27 de noviembre, de servicios de confianza electrónica, establece que: "el prestador de servicios de confianza electrónico cualificado deberá verificar fehacientemente la identidad y, en su caso, cualquier otra atribución específica de la persona natural a quien le expide el certificado electrónico cualificado, mediante la exhibición de los documentos públicos o privados que acredite suficientemente. Esta información debe ser verificada por el proveedor de servicios cualificado o por un tercero que actúe bajo la responsabilidad del proveedor de servicios cualificado: i. A través de la presencia física de esta persona, o ii. A distancia, utilizando otros certificados electrónicos reconocidos emitidos por un proveedor de servicios cualificado". Por otra parte, el artículo 26.3 de la Ley Andorrana 35/2014, de 27 de noviembre, de servicios de confianza electrónico, establece que en el caso de: "certificados electrónicos expedidos a personas físicas pero vinculadas a una organización, entidad, institución, empresa u otra persona jurídica, el prestador del servicio de confianza deberá acreditar, además de la identidad del solicitante y de la persona identificada en el certificado electrónico, los datos relativos a la constitución y personalidad jurídica de la entidad, o a la extensión y validez de las facultades o poderes de representación del solicitante, mediante los documentos públicos que acredite de forma específica o mediante la consulta del registro público correspondiente, que es el resultado de los datos que deban figurar en el mismo".
Sello de òrgano, Administración pública o entidad de derecho público Sello de empresa (Persona Jurídica)	El artículo 26.2 de la Ley Andorrana 35/2014, de 27 de noviembre, de servicios de confianza electrónica, establece que: "el prestador de servicios de confianza electrónico cualificado verificará la identidad y, en su caso, cualquier otra atribución específica de la persona jurídica a la que se expida el certificado electrónico cualificado, mediante la exhibición de documentos públicos o privados que acredite suficientemente. Esta información debe ser verificada por el proveedor de servicios cualificado o por un tercero que actúe bajo la responsabilidad del proveedor de servicios cualificado: i. Mediante la presencia física de un representante autorizado de dicha persona jurídica, o ii. A distancia, utilizando otros certificados electrónicos reconocidos emitidos por un proveedor de servicios cualificado".

3.2.6 Criterios para la interoperación

La OSCEPA puede proporcionar servicios que permitan que otra CA opere dentro de, o interopere con, su PKI. Dicha interoperación puede incluir certificación cruzada, certificación unilateral u otras formas de operación. La OSCEPA se reserva el derecho de proporcionar servicios de interoperación e interoperar con otras CA; los términos y criterios de los cuales deben establecerse contractualmente.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados

La identificación de una solicitud de renovación se realiza a través del certificado a renovar. No se renovará si el certificado para renovar ha pasado los 5 años desde la última verificación física o proceso equivalente.

3.3.2 Identificación y autenticación de la solicitud de renovación tras una revocación

La política de identificación y autenticación para la renovación del certificado después de una revocación será la misma que para el registro inicial.

3.4. Identificación y autenticación de la solicitud de revocación

La forma de realizar las solicitudes de revocación se establece en el apartado 4.9.3 de este documento.

La OSCEPA puede, por propia iniciativa, 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.

4. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

La OSCEPA emplea para la gestión del ciclo de vida de los certificados una plataforma que permite la solicitud, registro, publicación y revocación de todos los certificados emitidos.

4.1. Solicitud de certificados

4.1.1 Quién puede realizar la solicitud de un certificado

Una solicitud de certificado puede ser presentada por el sujeto del certificado o por un representante autorizado del mismo, en el caso de sello de empresa.

4.1.2 Procedimiento de alta y responsabilidades

4.1.2.1 Formularios Web.

Las solicitudes de los certificados se realizan de forma general mediante el acceso a los formularios de solicitud en la dirección, o mediante el envío al solicitante de un enlace a un formulario concreto o presencialmente en cualquier Entidad de Registro.

https://www.signaturaelectronica.ad

En la página Web se encuentran los formularios necesarios para realizar la solicitud de cada tipo de certificado distribuido por la OSCEPA en diferentes formatos y los dispositivos de generación de firma, si estos fueran necesarios.

El formulario permitirá la incorporación de un CSR (PKCS#11) en caso de que el usuario haya creado las claves.

El usuario recibe, posteriormente a la confirmación de los datos de solicitud, un correo electrónico en la cuenta asociada a la solicitud del certificado un enlace para confirmar la solicitud y aceptar las condiciones de uso.

Una vez confirmada la solicitud el suscriptor es informado de la documentación que debe presentar en una oficina de registro habilitada y cumplir con el requisito de identificación presencial si esta es pertinente.

4.1.2.2 Solicitudes vía capa de Web Services (WS).

Con objeto de incorporar la integración de aplicaciones de terceros con la plataforma de gestión de certificados STATUS ® propiedad de AC Camerfirma, se ha desarrollado una capa de Servicios Web (WS) que ofrecen procesos de emisión y revocación de certificados. Las llamadas a estos WS están firmadas con un certificado reconocido por la plataforma.

La emisión “ciega” de este tipo de certificados hace que el proceso sea revisado en detalle. Antes de iniciar la emisión mediante este sistema se debe contar con un informe técnico

favorable de la AC Camerfirma, un contrato donde la autoridad de registro se compromete a mantener el sistema en condiciones de seguridad óptimas y a notificar a la OSCEPA cualquier modificación o incidencia. Adicionalmente el sistema deberá ser sometido a auditorias anuales donde se comprueba:

1. Expedientes documentales de los certificados emitidos
2. Que los certificados están siendo emitidos bajo las directrices marcadas por las políticas de certificación bajo la que se rigen.

4.1.2.3 Lotes.

La plataforma STATUS permite igualmente circuitos de solicitud mediante lotes. En este caso, se enviará por el solicitante a la AR un fichero estructurado según un diseño prefijado por OSCEPA con los datos de los solicitantes. La AR procederá a la carga de dichas peticiones en el aplicativo de gestión.

4.2. Procesamiento de las solicitudes de certificados

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez haya tenido lugar una petición de certificado, el operador de la RA mediante el acceso a la plataforma de gestión PKI (STATUS o SIAVAL SafeCert) verifica la información proporcionada es conforme.

El operador de la plataforma posee un certificado de gestión interna emitido para realizar estas operaciones y que se obtiene después de un proceso de formación y evaluación.

El certificado utilizado por el operador de registro es considerado un acceso multi-factor usado no solo para el acceso a la plataforma de gestión PKI (STATUS o SIAVAL SafeCert) sino para aprobar cada petición de emisión de un certificado realizando una firma electrónica.

4.2.2 Aprobación o rechazo de la solicitud

Para los certificados de entidad final:

El operador de registro visualiza las peticiones pendientes de tramitar y que le han sido asignadas.

El operador de la RA queda a la espera de que el sujeto/Firmante entregue la documentación correspondiente.

Si la información no es correcta, el RA deniega la petición. En caso de que los datos se verifiquen correctamente la Entidad de Registro aprobará la emisión del certificado mediante la firma electrónica con su certificado de operador.

4.2.3 Plazo para resolver la solicitud

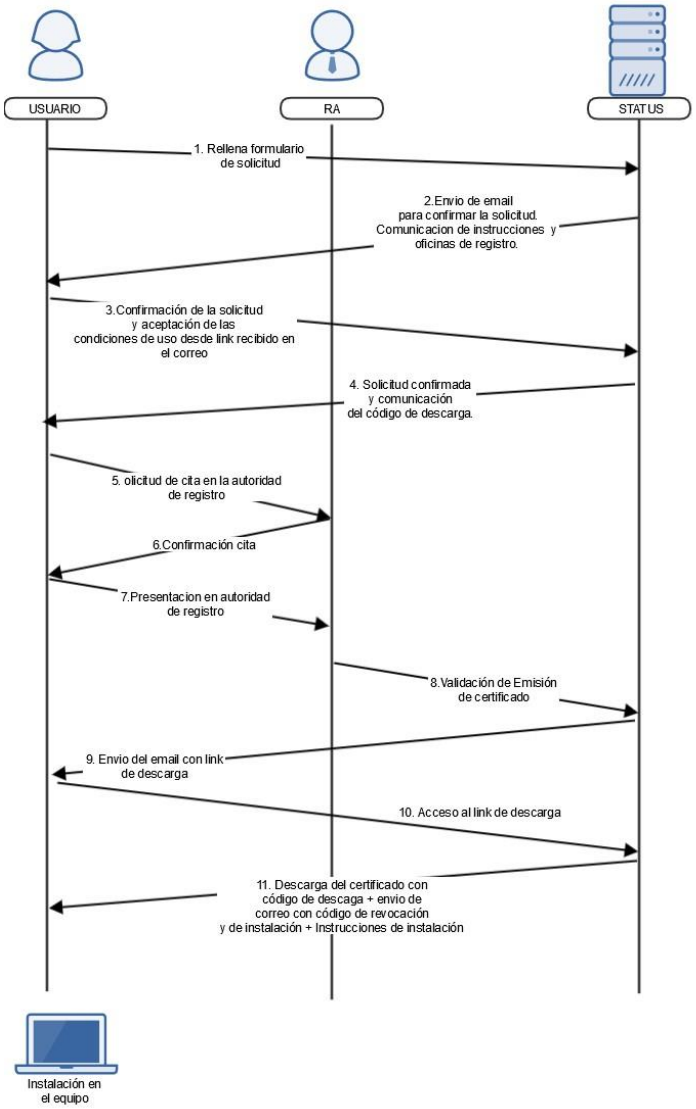
Las solicitudes presentadas por la plataforma PKI STATUS se validan una vez comprobada la documentación acreditativa asociado al perfil del certificado. La OSCEPA procederá siempre que sea viable a eliminar las solicitudes mayores de 1 año.

4.3. Emisión de certificados

4.3.1 Acciones de la CA durante el proceso de emisión

4.3.1.1 Certificados en Software

Una vez aprobada la solicitud el suscriptor recibe un correo electrónico con la notificación de este hecho y con él proceder a la generación y descarga del certificado. Para su instalación necesitara del código de producto que le ha sido entregado con el contrato y un código de instalación que se habrá entregado en un email independiente conjuntamente con un código de revocación.



4.3.1.2 Certificados en HW (Dispositivo Seguro de Creación de Firma):

La clave privada la genera el titular mediante el proceso de emisión provisto por el prestador, una vez ha sido personado y validado por la AR.

Los pares de claves se generan en un dispositivo cualificado de creación de firma electrónica o QSCD SIAVAL SafeCert Server Signing System. Las claves son protegidas bajo el control exclusivo del firmante y, por lo tanto, no existe ninguna entrega de la clave privada al titular, la protección se realizad con su PIN o contraseña y un segundo factor de autenticación basado en mensaje SMS enviado al teléfono móvil del usuario.

El sistema informará al titular de que se le va a emitir su certificado de firma centralizada y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

La clave pública es generada junto a la clave privada sobre el dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System y es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

4.3.2 Notificación de la emisión al suscriptor

La OSCEPA notifica mediante un correo electrónico al solicitante la aprobación o denegación de la solicitud.

4.4. Aceptación de certificados

4.4.1 Conducta que constituye aceptación del certificado

Una vez emitido el usuario dispone de un periodo de 7 días para comprobar su correcta emisión.

Si el certificado no ha sido emitido correctamente por causas técnicas, el certificado se revocará y se emitirá uno nuevo.

4.4.2 Publicación del certificado por la AC

OSCEPA ofrece un sistema de consulta del estado de los certificados emitidos, en su página web https://secure.camerfirma.com/solicitudes_status/estado_certificado.php. El acceso a esta página es libre y gratuito.

4.4.3 Notificación de emisión de certificado por la AC a otras entidades

OSCEPA ofrece un sistema de consulta del estado de los certificados emitidos, en su página web https://secure.camerfirma.com/solicitudes_status/estado_certificado.php. El acceso a esta página es libre y gratuito.

4.5. Uso del par de claves y los certificados

4.5.1 Uso del certificado y la clave privada del suscriptor

La limitación de uso de la clave viene definida en el contenido del certificado en las extensiones: *keyUsage*, *extendedKeyUsage* y *basicConstraints*

CA	Key Usage	Extended Key Usage	Basic Constraints
Entitat de Certificació de l'Administració Pública Andorrana	critical, cRLSign, keyCertSign	-	critical,CA:true
PERSONA FÍSICA en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA AMB PROFESSIÓ REGULADA en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA AMB PROFESSIÓ REGULADA en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA AMB PROFESSIÓ REGULADA en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'ÒRGAN, ADMINISTRACIÓ PÚBLICA O ENTITAT DE DRET PÚBLIC en HSM - signatura	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'ÒRGAN, ADMINISTRACIÓ PÚBLICA O ENTITAT DE DRET PÚBLIC en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
SEGELL D'ÒRGAN, ADMINISTRACIÓ PÚBLICA O ENTITAT DE DRET PÚBLIC en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false

A pesar de que es posible técnicamente el cifrado de datos con los certificados, la OSCEPA no se responsabiliza de los daños causados por la pérdida de control del titular de la clave privada necesaria para descifrar la información, excepto en el certificado emitido exclusivamente para este uso.

4.5.2 Uso de la clave pública y del certificado por la parte que confía

Las partes que confían deben acceder y usar la clave pública y el certificado según lo estipulado en esta CPS y según lo indicado en las "Condiciones de uso" bien en un documento físico o mediante su aceptación en el proceso de emisión.

4.6. Renovación del certificado

4.6.1 Circunstancia para la renovación del certificado

Un certificado debe renovarse antes de la fecha de caducidad del certificado a renovar. Una vez renovado la OSCEPA emite el certificado renovado con fecha de inicio igual a la fecha de caducidad del certificado a renovar.

Los certificados de OCSP se emiten periódicamente y no se establecen procesos de renovación.

4.6.2 Quién puede solicitar renovación

En aquellos certificados donde se permite la renovación, la autenticación del poseedor se realiza sobre la base de su certificado a renovar.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Antes de renovar un certificado, la OSCEPA comprueba que la información utilizada para verificar la identidad y demás datos del Firmante y del poseedor de la clave sigue siendo válida.

En el caso de renovación de los certificados de entidad final de persona física, se permite la emisión de certificado sin presencia física hasta un periodo de 5 años desde el último registro presencial. Una vez superado el plazo marcado el Firmante deberá realizar un proceso de emisión presencial igual al realizado la primera emisión. Bajo estas prácticas, si en el momento de la renovación del certificado no han trascurrido más de 5 años, la presencia física del titular no será requerida.

Bajo estas prácticas, 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.

La OSCEPA realiza las renovaciones de certificados emitiendo siempre nuevas claves, por lo tanto, el proceso técnico de emisión es igual al que se sigue cuando se realiza una nueva petición.

La OSCEPA realiza cuatro avisos (30 días, 15 días, 7 días, 1 día) vía email al Firmante notificando que el certificado va a caducar.

El proceso de renovación se inicia a partir del correo de aviso de caducidad o directamente a través de la página Web de la OSCEPA https://www.signaturaelectronica.ad
Este proceso requiere disponer del certificado válido a renovar.

- Una vez identificado con el certificado a renovar, el aplicativo presenta al Firmante los datos del certificado antiguo y le pide la confirmación de dichos datos. El aplicativo permite al Firmante modificar el email asignado al certificado. Si existen otros datos incorporados en el certificado que han cambiado, el certificado debe revocarse y proceder a realizar una emisión nueva.
- 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 AC.
- La OSCEPA 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 de nueva emisión de certificado al suscriptor

La notificación de la emisión de un certificado renovado se producirá tal como se describe en la sección 4.3.2 de este documento.

4.6.5 Conducta que constituye la aceptación de un certificado de renovación

Según el apartado 4.4.1 de este documento.

4.6.6 Publicación del certificado de renovación por la CA

Según el apartado 4.4.2 de este documento.

4.6.7 Notificación de emisión de certificado por la CA a otras entidades

En algunos casos se envían certificados de entidad final a los supervisores nacionales que regulan las actividades de las autoridades de certificación.

Los certificados de OCSP se comunican a diferentes organismos gubernamentales que disponen de plataforma de validación de certificados.

Los certificados de Autoridad de Certificación Raíz y de Autoridad de Certificación intermedia se notifican al supervisor nacional para su incorporación en su TSL. Adicionalmente a un repositorio de información gestionado por Mozilla, que incorpora información sobre autoridades de certificación – CCADB. Esta base de datos es utilizada por diversos programas comerciales para gestionar sus almacenes de confianza

4.7. Renovación de claves

Este es el procedimiento habitual de la renovación de los certificados de la OSCEPA, por lo que todos los procesos descritos en la sección 4.6 se refieren a este método de renovación.

La OSCEPA no permite la renovación de certificados sin renovación de claves.

4.7.1 Circunstancia para la renovación de claves (re-key) certificado

La renovación de certificados normalmente tendrá lugar como parte de la renovación de un Certificado.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

Según lo estipulado en 4.6.2

4.7.3 Procesamiento de solicitudes de cambio de claves del certificado

Según lo estipulado en 4.6.3

4.7.4 Notificación de nueva emisión de certificado al suscriptor

Según lo estipulado en 4.6.4

4.7.5 Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed)

Según lo estipulado en 4.6.5

4.7.6 Publicación del certificado con renovación de claves (re-keyed) por la AC

Según lo estipulado en 4.6.6

4.7.7 Notificación de emisión de certificado por la AC a otras entidades

Según lo estipulado en 4.6.7

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.

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 modificación de certificados como renovación cuando los atributos del suscriptor o del poseedor de claves que formen parte del control de unicidad previsto para esta política no hayan variado.

Si la solicitud de modificación se hace dentro del período ordinario previsto para la renovación del certificado, se procederá a realizar dicha renovación.

4.8.1 Circunstancia para la modificación del certificado

No aplicable.

4.8.2 Quién puede solicitar la modificación del certificado

No aplicable.

4.8.3 Procesamiento de solicitudes de modificación de certificados

No aplicable.

4.8.4 Notificación de la emisión de un nuevo certificado al suscriptor

No aplicable.

4.8.5 Conducta que constituye la aceptación del certificado modificado

No aplicable.

4.8.6 Publicación del certificado modificado por la CA

No aplicable.

4.8.7 Notificación de emisión de certificado por la CA a otras entidades

No aplicable.

4.9. Revocación y suspensión 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.

La suspensión por su parte supone una revocación con causa de suspensión (es decir un caso particular de revocación), esto es, se revoca un certificado temporalmente hasta que se decida sobre la oportunidad o no de realizar una revocación definitiva o su activación.

El periodo máximo de suspensión de un certificado es de 7 días naturales. En caso de llegar al periodo máximo de suspensión y el certificado no ha sido activado, el sistema automáticamente revoca definitivamente el certificado con causa "sin especificar".

La extinción de la vigencia de un certificado electrónico por causa de revocación o suspensión producirá efectos frente a terceros desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación (publicación de la lista de certificados revocados o consulta al servicio OCSP).

La OSCEPA mantiene los certificados en la lista de revocación hasta el fin de su validez. Cuando esta situación se produce, se eliminan de la lista de certificados revocados. La OSCEPA solo eliminará de la Lista de revocación un certificado cuando se produzca alguna de las dos siguientes situaciones.

- Caducidad del certificado
- Certificado revocado por causa de suspensión que una vez revisado se ha concluido que no se encuentran causas para su revocación definitiva.

No obstante, la OSCEPA mantendrá la información sobre el estado de un certificado caducado en sus bases de datos y accesible a través del servicio de OCSP.

No está permitido en ningún caso bajo estas prácticas la utilización de un certificado revocado.

La respuesta de OCSP para un certificado revocado cuando caduca mantiene el estado de revocado y su causa.

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

Para la OSCEPA el servicio de consulta del estado de un certificado primario es el ofrecido por OCSP.

4.9.1 Causas de revocación

Como norma general se procederá a la revocación de un certificado por:

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto o incompleto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
- Falta de pago del certificado.

Por circunstancias que afectan la seguridad de la clave o del certificado

- Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
- Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta CPS.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del Firmante o del responsable de certificado.
- Acceso o utilización no autorizada, por un tercero, de la clave privada del Firmante o del responsable de certificado.
- El uso irregular del certificado por el Firmante o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.

Por circunstancias que afectan la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del Firmante o del responsable de certificado

Por circunstancias que afectan el Firmante o responsable del certificado.

- Finalización de la relación entre Entidad de Certificación y Firmante o responsable del certificado.
- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al Firmante o responsable del certificado.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
- Infracción por el Firmante o responsable del certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en esta Declaración de Prácticas de Certificación.
- La incapacidad sobrevenida o la muerte del Firmante o responsable del certificado.
- La extinción de la persona jurídica Firmante del certificado, así como la finalidad de la autorización del Firmante al responsable del certificado o la finalización de la relación entre Firmante y responsable del certificado.
- Solicitud del Firmante de revocación del certificado, de acuerdo con lo establecido en esta CPS.
- Resolución firme de la autoridad administrativa o judicial competente

Otras circunstancias

- La suspensión del certificado digital por un periodo superior al establecido en esta CPS.
- Por la emisión de un certificado que no cumpla los requisitos establecidos en esta declaración de prácticas de certificación
- La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección correspondiente en esta CPS.

Para justificar la necesidad de revocación que se alega se deberán presentar ante la RA o la AC los documentos correspondientes, en función de la causa que motiva la solicitud.

- Si solicita la revocación el titular del certificado o la persona física solicitante de un certificado de persona jurídica, deberá presentar una declaración firmada por él donde indique el certificado a revocar y la causa de esta solicitud e identificarse ante la RA

- Si la revocación la solicita un tercero deberá presentar una autorización bien del titular persona física bien del representante legal de la persona jurídica titular donde se indiquen además las causas por las que se solicita la revocación del certificado e identificarse ante la RA.

- Si solicita la revocación la Entidad vinculada al titular por causa de la terminación de la relación con éste, deberá acreditar dicha circunstancia (revocación de poderes, terminación contrato…) e identificarse ante la RA como facultado para representar a la Entidad.

Los Firmantes disponen de los códigos de revocación que pueden usar en los servicios de revocación vía Web o mediante llamada telefónica a los servicios de soporte.

4.9.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El Sujeto/Firmante
- El Solicitante responsable
- La Entidad (a través de un representante de la misma)
- La AR o la AC.
- También se contempla la posibilidad de que por parte de terceros o partes interesadas se pueda comunicar fraudes, malos usos, conductas inapropiadas, o datos erróneos, en cuyo caso, la AR o la AC podrá revocar el certificado tras comprobar la veracidad de dichas causas de revocación.

4.9.3 Procedimiento de solicitud de revocación.

Todas las solicitudes deberán realizarse:

- A través del Servicio de Revocación ONLINE, mediante el acceso al servicio de revocación localizado en la página de la Web de la OSCEPA e introduciendo el PIN de Revocación.

  https://www.signaturaelectronica.ad

- A través de la personación física en la AR en horario de atención al público mostrando el documento identificativo válido del Firmante/Suscriptor o Solicitante.
- Enviando a la OSCEPA un documento firmado por un representante con capacidad de representación suficiente de la Entidad solicitando la revocación del certificado.

  La OSCEPA mantiene en su página web toda la información relativa a los procesos de revocación de los certificados.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de la OSCEPA. Estos servicios estarán disponibles las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la OSCEPA, la OSCEPA realizará los mayores esfuerzos para asegurar que estos servicios no se encuentren inaccesibles durante un periodo máximo de 24 horas.

4.9.4 Periodo de gracia de la solicitud de revocación

El periodo de revocación desde que la OSCEPA o una AR tiene conocimiento autenticado de la revocación de un certificado esta se produce de manera inmediata, incorporándose en la próxima CRL a emitir y en la base de datos de la plataforma de gestión donde se alimenta el respondedor OCSP.

4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación

La OSCEPA procesará una solicitud de revocación de forma inmediata a partir del procedimiento descrito en el punto 4.9.3

En las revocaciones producidas por una mala emisión del certificado se notificará previamente al titular para acordar los plazos de su sustitución.

La OSCEPA en todo caso y bajo estas prácticas de certificación, puede realizar la revocación de un certificado de forma unilateral e inmediata por motivos de seguridad, sin que el titular pueda reclamar ningún tipo de indemnización por este hecho.

4.9.6 Requisitos de comprobación de la revocación por las partes que confían

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.

La OSCEPA emite siempre CRLs firmadas por la AC 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 CRL's

CA	Frecuencia de emisión	Duración
Entitat de Certificació de l'Administració Pública Andorrana	24 horas	48 horas

4.9.8 Máxima latencia de CRL

Las CRL se publican cada 24 horas con una validez de 48 horas.

4.9.9 Disponibilidad de comprobación on-line de la revocación

AC proporciona un servicio on-line de comprobación de revocaciones vía HTTPS en https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

También mediante consultas OCSP en:

https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp

Las direcciones de acceso a estos servicios vienen referenciadas en el certificado digital. Para las CRL y ARL 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.

El servicio de OCSP se alimenta de las CRL emitidas por las diferentes autoridades de certificación (CA) o por accesos a la BBDD de la plataforma (EE). Los datos técnicos de acceso así como los certificados de validación de las respuestas OCSP se encuentran publicadas en la Web de la OSCEPA https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp

Estos servicios estarán disponibles las 24 horas del día los 7 días de la semana 365 días al año.

La OSCEPA realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre inaccesible de forma continua más de 24 horas, siendo este un servicio crítico en las actividades de la OSCEPA y por lo tanto tratado de forma adecuada en el Plan de contingencias y de continuidad de negocio.
La latencia de publicación en el servicio de OCSP de una revocación es de 1 hora

4.9.10 Requisitos de la comprobación on-line de la revocación

Para realizar la comprobación de una revocación el Tercero que confía deberá conocer el e-mail asociado al certificado que se desea consultar si se realiza mediante acceso Web o el número de serie si se comprueba mediante el servicio OCSP.

Las respuestas OCSP van firmadas por las AC que emite el certificado a consultar, por lo que es necesario dicho certificado para validar la respuesta. Los certificados actualizados se pueden encontrar en el link https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp

4.9.11 Otras formas de divulgación de información de revocación disponibles

Los mecanismos que la OSCEPA pone a disposición de los usuarios del sistema, estarán publicados en su página Web: https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

4.9.12 Requisitos especiales de revocación por compromiso de las claves

No estipulado

4.9.13 Circunstancias para la suspensión

Cuando se produce una suspensión, la OSCEPA 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, la OSCEPA revocará el certificado.

En el caso de producirse una suspensión del certificado, se envía un comunicado mediante email al Firmante/Suscriptor comunicando la hora de suspensión y la causa de la misma.

Si finalmente la suspensión no da lugar a la revocación definitiva y el certificado tiene que ser de nuevo activado, el Firmante/Suscriptor recibirá un correo indicando el nuevo estado del certificado.

El proceso de suspensión no se aplica a certificados
- De Operador de AR.
- De OCSP

4.9.14 Quién puede solicitar la suspensión

Ver sección 4.9.2

4.9.15 Procedimiento de solicitud de suspensión

La solicitud de suspensión se realizará según mediante el acceso a la página correspondiente de la web de la OSCEPA o mediante comunicación oral o escrita previamente autenticada. El suscriptor debe poseer el código de revocación para proceder a la suspensión del certificado.

4.9.16 Límites del periodo de suspensión

Un certificado no permanecerá suspendido más de 7 días.

La OSCEPA supervisará mediante un sistema de alertas de la plataforma de gestión de certificados que el periodo de suspensión marcado por esta CPS no se sobrepasa.

4.10. Servicios de comprobación del estado de los certificados

4.10.1 Características operacionales

La OSCEPA dispone de un servicio de consulta de certificados emitidos y listas de revocación. Estos servicios están disponibles públicamente en su página Web: https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

4.10.2 Disponibilidad del servicio

Los servicios de consulta están diseñados para garantizar una disponibilidad de 24 horas por día 7 días a la semana.

4.10.3 Características opcionales

No estipulado

4.11. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio. Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

4.12. Custodia y Recuperación de Claves

4.12.1 Política y prácticas de custodia y recuperación de claves

Las claves de los usuarios se generan y custodian en dispositivo cualificado de creación de firma electrónica, de forma que el prestador de servicios de certificación no podrá en ningún momento recuperar la clave de los usuarios ni podrá hacer una recuperación de la misma. En caso de pérdida, se deberá revocar el certificado y emitir uno nuevo generando un nuevo par de claves.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

No estipulado.

5. CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES

5.1. Controles de seguridad física

La OSCEPA está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001:2007 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

La OSCEPA tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación certificados ofrece protección frente:

- Accesos físico no autorizados
- Desastres naturales
- Incendios
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura
- Inundaciones
- Robo
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso

5.1.1 Ubicación y construcción

Las instalaciones en las que se encuentra la OSCEPA están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una caja de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas antihumedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

5.1.2 Acceso físico

El acceso físico a las dependencias de las instalaciones en las que se encuentra la OSCEPA donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Cualquier persona externa debe estar acompañada por un responsable de la organización cuando esta se encuentre por cualquier motivo dentro de áreas restringidas.

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

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

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

El acceso a los sistemas de certificación está protegido con 4 niveles de acceso. Edificio, Oficinas, CPD y Sala criptográfica.

5.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones en las que se encuentra la OSCEPA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 Exposición al agua

Las instalaciones en las que se encuentra la OSCEPA están ubicadas en una zona de bajo riesgo de inundación y en una primera planta. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

Los dispositivos criptográficos, y soportes que almacenen claves de las Entidades de Certificación, cuentan con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

5.1.6 Sistema de almacenamiento.

Cada Medio de Almacenamiento desmontable (cintas, cartuchos, CD, discos, etc.) permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento se guarda en armarios ignífugos o bajo llave permanentemente en requiriéndose autorización expresa para su retirada.

5.1.7 Eliminación de residuos

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga.

Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

5.1.8 Backup externo

La OSCEPA utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro operacional.

Se requiere al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2. Controles procedimentales

5.2.1 Roles de confianza

Los roles de confianza garantizan una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación, y con una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tienen en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

Auditor Interno:
Responsable del cumplimiento de los procedimientos operativos. Es una persona externa al departamento de Sistemas de Información.

Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

Administrador de Sistemas:
Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación.

Las tareas de administrador de sistemas son incompatibles con las tareas de certificación y no pueden llevar a cabo tareas de auditores de operaciones.

Administrador de AC.
Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.

Las tareas del administrador de AC son incompatibles con las tareas de certificación y sistemas.

Operador de AC.
Responsable necesario conjuntamente con el Administrador de AC de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.

Las tareas de operador de AC son incompatibles con las de administrador de AC y no puede realizar tareas de auditor ni auditor interno.

Operador de RA:
Persona responsable de aprobar las peticiones de certificación realizadas por el Firmante.

Las operaciones de operador de RA son incompatibles con las de administrador de RA ni puede realizar tareas de auditoría interna ni externa.

Operador de revocación:
Las tareas del operador de revocación son incompatibles con las tareas de Auditoria

Responsable de Seguridad:
Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de la OSCEPA. Debe encargarse aspecto relacionado con la seguridad de la información: lógica, física, redes, organizativa, etc.

5.2.2 Número de personas requeridas por tarea

OSCEPA garantiza al menos **dos personas para realizar las tareas clasificadas como sensibles**. Principalmente en la manipulación del dispositivo de custodia de las claves de la autoridad de certificación.

5.2.3 Identificación y autentificación para cada rol

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación

5.2.4 Roles que requieren separación de tareas

Tabla de segregación de roles.

	Responsable de Seguridad	Administracion de Sistemas	Oeración de sistemas	Auditor Plataforma CA	Especialidsta Validacion SSL	Operador RA
Responsable de Seguridad		SI	NO	SI	SI	SI
Administracion de Sistemas	NO		NO	NO	NO	NO
Operación de Sistemas	NO	NO		NO	NO	NO
Auditor Plataformas CA	NO	NO	NO		SI	SI
Especialidsta Validacion SSL	NO	NO	NO	SI		SI
Operador RA	NO	NO	NO	NO	SI	

5.2.5 Arranque y parada del sistema de gestión PKI.

El sistema de PKI se compone de los siguientes módulos:

Módulo de Gestión de AR, para lo cual se activarán o desactivarán los servicios del gestor de páginas especifico.

Módulo de gestión de solicitudes, para lo cual se activará o desactivará los servicios del gestor de páginas específico.

Módulo de gestión de claves, ubicado en el equipo HSM. Se activa o desactiva mediante encendido físico.

Módulo de BBDD, Gestión centralizada de los certificados y CRL gestionados, OCSP y TSA. Arranque y parada del servicio específico del Gestor de BBDD.

Módulo OCSP. Servidor de respuestas de estado de los certificados en línea. Arranque y parada del servicio de sistema encargado de esta tarea.

El proceso de apagado de módulos seguiría la secuencia:

- Módulo de solicitud
- Módulo de AR
- Módulo OCSP
- Módulo BBDD
- Módulo gestión de claves.

Se realizará el encendido en proceso inverso.

5.3. Controles del personal

5.3.1 Calificaciones, experiencia y requisitos de autorización

Todo el personal que realiza tareas calificadas como confiables lleva al menos **un año** trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza se encuentra libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

La OSCEPA se asegura de que el personal de registro o Administradores de AR es confiable y pertenece a un organismo delegado para realizar las tareas de registro.

El Administrador de AR habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, la OSCEPA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

La OSCEPA no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación, hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad

5.3.2 Procedimientos de comprobación de antecedentes

OSCEPA dentro de sus procedimientos de RRHH realiza las investigaciones pertinentes antes de la contratación de cualquier persona y dentro del Govern d'Andorra se siguen los procedimientos según la ley 1/2019 del 17 de enero de la función pública.

OSCEPA nunca asigna tareas confiables a personal con menos de una antigüedad de un año.

OSCEPA en la solicitud para el puesto de trabajo en determinados roles se informa sobre la necesidad de someterse a una investigación previa y se advierte que la negativa a someterse a la investigación implicará el rechazo de la solicitud. Asimismo consentimiento inequívoco del afectado para la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la legislación de protección de datos de carácter personal.

5.3.3 Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado en los términos que establecen las Políticas de Certificación. Existe un plan de formación que forma parte de los controles UNE-ISO/IEC 27001:2007.

La formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación.
- Versiones de hardware y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal

5.3.4 Requerimientos y frecuencia de la actualización de la formación

OSCEPA realiza los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas.

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado

5.3.6 Sanciones por acciones no autorizadas

La OSCEPA dispone de un régimen sancionador interno, descrito en su política de RRHH, para su aplicación cuando un empleado realice acciones no autorizadas pudiéndose llegar a su cese.

5.3.7 Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por la OSCEPA. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la CPS, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución.

5.3.8 Documentación proporcionada al personal

La OSCEPA pone a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, en particular la normativa de seguridad y la CPS.

Esta documentación se encuentra en un repositorio interno accesible por cualquier empleado de la OSCEPA, en el repositorio existe una lista de documentos de obligado conocimiento y cumplimiento.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

5.4. Procedimientos de registro de eventos

OSCEPA está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001:2007que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

5.4.1 Tipos de eventos registrados

OSCEPA registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la AC.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.

La OSCEPA también conserva, ya sea manualmente o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física y vulnerabilidades en las infraestructuras que dan soporte a la emisión y gestión de certificados

la OSCEPA mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de registros de auditoría.
- Que los ficheros de registros de auditoría no se reescriben.

- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de registros de auditoría se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.2 Frecuencia de tratamiento de registros de auditoria

OSCEPA revisa sus registros de auditoría cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

5.4.3 Periodos de retención para los LOGs de auditoria

La OSCEPA almacena la información de los registros de auditoría al menos durante cinco años.

5.4.4 Protección de los registros de auditoría

Los registros de auditoría de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de registros de auditoría está reservado solo a las personas autorizadas.

Los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de registros de auditoría.

5.4.5 Procedimientos de copia de respaldo de los registros de auditoría

OSCEPA dispone de un procedimiento adecuado de copia de respaldo de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de copia de respaldo de los registros de auditoría.

OSCEPA tiene implementado un procedimiento de back up seguro de los logs de auditoría, realizando semanalmente una copia de todos los registros de auditoría en un medio externo.

Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6 Sistema de recogida de información de auditoria

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, la red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado, todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación al sujeto causa del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de la OSCEPA. Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación UNE-ISO/IEC 27001.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

Mensualmente la OSCEPA ejecuta un análisis de los sistemas con objetivo de detectar actividades sospechosas. Este informe es ejecutado por una empresa externa incorpora:

- Detección de intrusión - IDS (HIDS)
- Sistema de control de integridad OSSEC
- SPLUNK. Inteligencia operacional.
- Informe correlación de eventos.

OSCEPA corrige cualquier problema reportado y es registrado por el departamento de sistemas.

5.5. Archivo de registros

5.5.1 Tipo de archivos registrados.

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la AC o por las RAs:

- Todos los datos de auditoría de sistema. PKI y OCSP incorporando los eventos de firma realizados.
- 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 Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación

OSCEPA es el 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 quince años.

Las versiones antiguas de la documentación también son conservadas, por un periodo de quince años por la OSCEPA, pudiendo ser consultadas, por causa razonada por los interesados.

5.5.3 Protección del archivo

OSCEPA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

5.5.4 Procedimientos de copia de respaldo del archivo

OSCEPA dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

La OSCEPA como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realiza copias de respaldo completas semanalmente para casos de recuperación de datos.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable vía NTP, GPS y sistemas de sincronización vía Radio.

La OSCEPA dispone de un documento de seguridad informática donde describe la configuración de los parámetros de fecha y hora de los equipos utilizados en la emisión de certificados.

5.5.6 Sistema de recogida de información de auditoria

OSCEPA dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos para obtener y verificar información archivada

OSCEPA dispone de un documento de seguridad informática donde se describe el proceso para verificar que la información archivada es correcta y accesible.

5.6. Cambio de clave

El cambio de claves de entidad final es realizado mediante la realización de un nuevo proceso de emisión (ver apartado correspondiente de esta CPS).

Antes de que el certificado de la AC caduque se realizará un cambio de claves. El certificado a actualizar de la AC y su clave privada solo se usará para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará un nuevo certificado de AC con una clave privada nueva y un CN (*common name*) distinto al del certificado de la AC a sustituir.

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

5.7. Recuperación en caso de compromiso de la clave o desastre

El caso de compromiso de la clave raíz se toma como un caso particular en el documento de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos del sector privado y público. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos de reconocimiento. El documento de contingencia y continuidad de negocio incorpora estos términos puramente técnicos y operativos para que las nuevas claves estén disponibles, pero no así su reconocimiento por terceros.

El compromiso de los algoritmos o los parámetros asociados utilizados en la generación de certificados digitales o servicios asociados se incorporan también en el plan de contingencias y continuidad de negocio.

5.7.1 Procedimientos de gestión de incidencias y compromisos

OSCEPA ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario un centro de datos alternativo como parte de la certificación UNE-ISO/IEC 27001:2007

5.7.2 Corrupción de recursos, aplicaciones o datos

Si algún equipo se daña o deja de funcionar pero las claves privadas no se destruyen, la operación debe restablecerse lo más rápido posible, dando prioridad a la capacidad de generar

información del estado del certificado según el plan de recuperación de desastres de la OSCEPA.

5.7.3 Compromiso de clave privada de la entidad

El Plan de contingencias enmarcado en la certificación UNE-ISO/IEC 27001:2007 de la OSCEPA trata el compromiso de la clave privada de la AC como una situación de desastre.

En caso de compromiso de una clave raíz:

- Informará a todos los Firmantes/Suscriptores, Tercero que confía y otras ACs con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

5.7.4 Continuidad del negocio después de un desastre

La OSCEPA restablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con el plan de contingencias y continuidad de negocio enmarcado en la certificación UNE-ISO/IEC 27001:2007 indicando un restablecimiento en las 24 horas siguientes.

OSCEPA dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descrito en el plan de continuidad de negocio.

5.8. Cese de la AC o AR

Antes del cese de su actividad la OSCEPA realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras ACs con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de seis meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Las claves privadas de la AC serán destruidas o deshabilitadas para su uso.
- La OSCEPA mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

6.1.1 Generación del par de claves

Los equipos usados por la OSCEPA son nCipher. Estos dispositivos albergaran claves raíces y están certificados FIPS 140-2, en su nivel 3.

Las claves raíz se generan y gestionan en un equipo fuera de línea en una sala criptográfica.

La creación de claves de autoridad de certificación intermedia se generan en equipos HSM donde se albergarán para su correspondiente uso. El certificado emitido por la calve raíz se realiza en una sala criptográfica segura.

6.1.1.1 Generación del par de claves del suscriptor

Las claves del Sujeto/Firmante pueden ser creadas en por el mismo mediante dispositivos hardware (SSCD) o software autorizados por la OSCEPA o pueden ser creadas por la OSCEPA en formato software PKCS#12.

La plataforma de gestión STATUS genera con sus propios recursos una contraseña aleatoria robusta y una clave privada protegida con dicha contraseña usando el algoritmo 3DES. A partir de esa clave privada genera una petición de firma de certificado en formato PKCS#10. Con esa petición la AC realiza la firma del certificado del Firmante. El certificado es entregado al usuario en un fichero PKCS#12 en el que se incluye el propio certificado y la clave privada asociada a él. La contraseña de la clave privada y del fichero PKCS#12 nunca está en claro en el sistema.

Las claves son generadas usando el algoritmo de clave pública RSA.

Las claves también pueden ser creadas en un sistema remoto usando la capa de servicios WEB para generar una solicitud PKCS#10 y la recogida del PKCS#7 correspondiente.

Las claves tienen una longitud mínima de 2048 bits.

6.1.1.2 Hardware/software de generación de claves

Las claves de los Firmantes/Suscriptores pueden ser generadas por ellos mismos en un dispositivo autorizado por la OSCEPA. Ver 6.1.1.1

Para las claves de autoridad de certificación intermedia se utiliza un dispositivo criptográfico que cumple las especificaciones FIPS 140-2 level 2 y level 3.

6.1.2 Entrega de la clave privada al firmante

Ver 3.2.1

6.1.3 Entrega de la clave pública al emisor del certificado

El envío de la clave pública a la OSCEPA para la generación del certificado cuando el circuito así lo requiera, se realiza mediante un formato estándar preferiblemente en formato PKCS#10.

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

El certificado de la AC y su *fingerprint* (huella digital) estarán a disposición de los usuarios en la página Web de https://www.signaturaelectronica.ad/descarrega-claus-publiques

6.1.5 Tamaño de las claves

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

El periodo de uso de la clave pública y privada varía en función del tipo de certificado. Ver apartado 6.1.1.

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

La clave pública de la autoridad de certificación intermedia y de los certificados de los suscriptores está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA

- Tamaño de claves = mínimo 2048 bits
- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-256

6.1.7 Propósitos de uso de claves

Todos los certificados emitidos contienen los atributos "KEY USAGE" y "EXTENDED KEY USAGE", tal como se define en el estándar X.509v3. Más información disponible en la sección 7.1.2.

6.2. Protección de la clave privada y estándares para los módulos criptográficos

6.2.1 Controles y estándares de módulos criptográficos

6.2.1.1 Clave privada de la AC

La clave privada de firma de la autoridad de certificación intermedia es mantenida en un dispositivo criptográfico que cumple las especificaciones FIPS 140-2 nivel 3.

Cuando la clave privada de la AC está fuera del dispositivo esta se mantiene cifrada.

Existe un back up de la clave privada de firma de la AC, que es almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro.

Las copias de back up de la clave privada de firma de la AC están almacenadas de forma segura. Este procedimiento se describe en detalle en las políticas de seguridad de la OSCEPA.

6.2.1.2 Clave privada del suscriptor

La clave privada del suscriptor se puede almacenar en un dispositivo software o hardware.

Cuando se almacene en formato software la OSCEPA ofrecerá las instrucciones de configuración adecuada para un uso seguro.

Respecto a los dispositivos criptográficos distribuidos por la OSCEPA para albergar certificados cualificados, cumplen todos con los requisitos de dispositivos cualificados de creación de firma cualificados y por lo tanto son aptos para la generación de firma cualificada.

La información respecto al proceso de creación y custodia de claves que utiliza la OSCEPA se incorpora en el propio certificado digital, mediante el OID correspondiente permitiendo a la Parte Usuaria actuar en consecuencia.

6.2.2 Control multipersonal (n de entre m) de la clave privada

Se requiere un control multipersonal para la activación de la clave privada de la AC. En el caso de esta CPS, en concreto existe una política de 2 de 4 personas para la activación de las claves.

6.2.3 Depósito de clave privada

La OSCEPA no almacena ni copia las claves privadas de los titulares.

Excepciones:

- En caso de certificados para cifrado de información la OSCEPA puede guardar una copia de dicha clave.

6.2.4 Copia de seguridad de la clave privada

La OSCEPA realiza una copia de back up de las claves privadas de la ACs que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de esta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del Firmante en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación tal como se indica en el manual de instalación de claves en software.

Las claves del Firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

La OSCEPA guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.5 Archivo de la clave privada

Las claves privadas de las ACS son archivadas por un periodo de 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

El Firmante podrá almacenar las claves entregadas en software durante el periodo de duración del certificado, posteriormente deberá destruirlas asegurándose antes de que no tiene ninguna información cifrada con la clave pública.

Solo en caso de certificados de cifrado el Firmante podrá almacenar la clave privada el tiempo que crea oportuno. En este caso la OSCEPA también guardará copia de la clave privada asociada al certificado de cifrado.

La OSCEPA pone a disposición de los titulares de certificados cuya clave privada sea generada por el prestador desde el momento de la entrega de dicho certificado la descarga del fichero PKCS#12, que contiene dicha clave privada y su certificado asociado, durante tres días hábiles.

OSCEPA guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.6 Introducción de la clave privada en el módulo criptográfico.

Las claves de la autoridad de certificación intermedia se almacenan en equipos HSM de red en línea, de forma que se puedan acceder desde los aplicativos de PKI para la generación de certificados.

6.2.7 Almacenamiento de clave privada en el módulo criptográfico

Las claves de la autoridad de certificación intermedia se almacenan en equipos HSM de red en línea, de forma que se puedan acceder desde los aplicativos de PKI para la generación de certificados.

6.2.8 Método de activación de la clave privada.

El acceso a la clave privada del suscriptor se realiza por medio de una clave de activación que conocerá solamente el suscriptor y que evitará tenerlo por escrito.

La activación de la clave privada de la autoridad de certificación intermedia es gestionada por el aplicativo de gestión del HSM.

La OSCEPA guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.9 Método de desactivación de la clave privada

Cuando la clave esté en soporte software, podrá ser desactivada mediante el borrado de dichas claves de la aplicación correspondiente en la que estén instaladas.

Para la desactivación de la clave privada de la AC se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Para claves de AC se realizará una ceremonia criptográfica de la que se elaborará el acta correspondiente.

6.2.10 Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves se emitirá una revocación del certificado de la clave pública asociada a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la AC. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del Firmante en software se podrán destruir mediante el borrado de estas siguiendo las instrucciones de la aplicación que las alberga.

Las claves del Firmante en hardware podrán ser destruidas mediante un software especial en los puntos de Registro o en la AC.

La OSCEPA guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.11Calificación del módulo criptográfico

Los módulos criptográficos están certificados FIPS-140-2 nivel 3 son manejados por al menos dos operadores en un modelo n de m. Los equipos están albergados en entornos seguros. El módulo criptográfico que almacenas las claves de Root se gestiona dentro de una sala criptográfica aislada y desconectada. Los módulos criptográficos que almacenan las claves de la autoridad de certificación intermedia se almacenan en entornos seguros dentro de un CPD siguiendo normativa ISO27001.

6.3. Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

OSCEPA, en cumplimiento de lo establecido por el artículo 26 de la ley 35/2014, del 27 de noviembre, de servicios de confianza electrónica, mantendrá sus archivos por un periodo

mínimo de quince (15) años siempre y cuando la tecnología de cada momento lo permita. Dentro de la documentación a custodiar se encuentran los certificados de clave pública emitidos a sus suscriptores y los certificados de clave pública propios.

6.3.2 Periodo de uso para las claves públicas y privadas

La clave privada no debería ser usada después del periodo de validez del certificado de clave pública asociada.

La clave pública o su certificado de cave 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

6.4.1 Generación y activación de los datos de activación

Los datos de activación de la clave privada de usuario se generan de diferente forma según el tipo de certificado

En software. El certificado se genera por el prestador y se entrega en un fichero estandarizado PKCS#12 protegido por una contraseña generada por el aplicativo de gestión y entregada al sujeto mediante el correo asociado al certificado digital.

En Dispositivo hardware. Las tarjetas utilizadas por la OSCEPA se generan en el puesto de registro protegidas con un PIN y PUK calculado de fábrica. Esta información es enviada por la plataforma de gestión al sujeto mediante el correo asociado al certificado digital. El sujeto dispone de un software para cambiar el PIN y PUK de su tarjeta.

En Dispositivo hardware (HSM) de tercero. La OSCEPA homologa dispositivos de terceros, aunque estas disponen de una gestión independiente. Las claves se generan en una ceremonia independiente y se entrega a la OSCEPA una solicitud de emisión de certificado conjuntamente con el acta de la ceremonia.

6.4.2 Protección de los datos de activación

Los datos de activación son comunicados al sujeto por un canal independiente a la plataforma de gestión PKI. La OSCEPA no almacena dicha información custodiada en su base de datos cuando hablamos de certificados en formato software o hardware. En la plataforma centralizada no los almacenamos siendo conocidos y custodiados por el titular. Los datos pueden ser enviados de nuevo al sujeto bajo solicitud previa al correo asociado al certificado, y serán eficaces siempre que el usuario no haya realizado un cambio en ellos previamente.

6.4.3 Otros aspectos de los datos de activación

No estipulados.

6.5. Controles de seguridad informática

La OSCEPA emplea sistemas fiables para ofrecer sus servicios de certificación. La OSCEPA ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se sigue el esquema de certificación sobre sistemas de gestión de la información ISO 270001

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de la OSCEPA, en los siguientes aspectos:

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento correcto del sistema.
4. Configuración de Usuarios y permisos.
5. Configuración de eventos de Log.
6. Plan de backup y recuperación.
7. Configuración antivirus
8. Requerimientos de trafico de red

6.5.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de la OSCEPA incluye las siguientes funcionalidades:

- control de acceso a los servicios de AC y gestión de privilegios
- imposición de separación de tareas para la gestión de privilegios
- identificación y autenticación de roles asociados a identidades
- archivo del historial del suscriptor y la AC y datos de auditoria
- auditoria de eventos relativos a la seguridad
- auto-diagnóstico de seguridad relacionado con los servicios de la AC
- Mecanismos de recuperación de claves y del sistema de AC

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2 Valoración de la seguridad informática

La seguridad de los equipos 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

Cuando las claves criptográficas asociadas a un certificado se almacenan en un dispositivo hardware, este es siempre un dispositivo cualificado de creación de firma cumpliendo el anexo II de eIDAS. El dispositivo hardware puede ser una tarjeta criptográfica, token USB o HSM.

Respecto a los dispositivos hardware

a) Los dispositivos hardware son preparados y estampadas por un proveedor externo.
b) La gestión de distribución del soporte la realiza el proveedor externo que lo distribuye a las autoridades de registro para su entrega al Firmante.
c) El Firmante o la RA utiliza el dispositivo para generar el par de claves y enviar la clave pública a la AC.
d) La AC envía un certificado de clave pública al Firmante o la RA que es introducido en el dispositivo.
e) El dispositivo es reutilizable y puede mantener de forma segura varios pares de claves.
f) El dispositivo queda en propiedad del sujeto/Firmante.

Respecto a los dispositivos utilizados en la plataforma de gestión centralizada de claves: El dispositivo que almacena dichas claves está certificado FIPS-104-2 nivel 3 o EAL4+ y autorizado por el supervisor europeo para los servicios catalogados como QSCDManagedOnBehalf.

6.6.1 Controles de desarrollo del sistema

OSCEPA posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

Como respuesta a los análisis de intrusión y vulnerabilidades se realizan las adaptaciones de los sistemas y aplicaciones que pueden tener problemas de seguridad y a las alertas de seguridad recibidas desde los servicios de seguridad gestionadas contratados con terceros, se ejecutan los RFC (*Request for Changes*) correspondientes para la incorporación de los parches de seguridad o la actualización de las versiones con problemas.

En el RFC se incorporan y se documentan las medidas tomadas para la aceptación, ejecución o la denegación de dicho cambio.

En los casos que la ejecución de la actualización o corrección de un problema incorpore una situación de vulnerabilidad o un riesgo importante se incorpora en el análisis de riesgos y se ejecutan controles alternativos hasta que el nivel de riesgo sea asumible.

6.6.2 Controles de gestión de la seguridad

6.6.2.1 Gestión de seguridad

El Departamento de la Función Pública desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad.

Para realizar esta función dispone de un plan de formación anual.

OSCEPA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.2 Clasificación y gestión de información y bienes

El Departamento de Sistemas de Información (DSI) mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de Govern detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.6.2.3 Operaciones de gestión

El Departamento de Sistemas de Información (DSI) dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En el documento de seguridad de la OSCEPA se desarrolla en detalle el proceso de gestión de incidencias.

La OSCEPA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de los soportes y seguridad
Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema
El departamento de Sistemas de Govern mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

El Departamento de Sistemas de Información (DSI) dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

La OSCEPA define actividades, asignadas a personas con un rol de confianza, distintas a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4 Gestión del sistema de acceso

La OSCEPA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.
En particular:

AC General

a) Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.

b) Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.

c) La OSCEPA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

d) La OSCEPA dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.

e) Cada persona tiene asociado un rol para realizar las operaciones de certificación.

f) El personal de la OSCEPA es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado
La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la AC.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de AC.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5 Gestión del ciclo de vida del hardware criptográfico

OSCEPA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

OSCEPA registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

OSCEPA realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de la AC así como sus modificaciones y actualizaciones son documentadas y controladas.

OSCEPA posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.6.3 Evaluación de la seguridad del ciclo de vida

No estipulado

6.7. Controles de seguridad de la red

OSCEPA protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

La política empleada para la configuración de los sistemas y elementos de seguridad es partir de un estado inicial de bloqueo total e ir abriendo servicios y puertos necesarios para la ejecución de los servicios. Como parte de las tareas a realizar en el departamento de sistemas se incorpora la revisión de los accesos.

Los sistemas de administración y los sistemas de producción están en entornos separados.

6.8. Fuentes de Tiempo

OSCEPA tiene un procedimiento de sincronización de tiempo coordinado con el ROA Real Instituto y Observatorio de la Armada Española en San Fernando vía NTP También obtiene una fuente segura vía GPS y sincronización vía Radio.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. Perfil de Certificado

Los perfiles de certificados cumplen el RFC 5280.

Todos los certificados cualificados o reconocidos emitidos bajo esta política están en conformidad con el estándar X.509 versión 3 y al RFC 3739 y ETSI 101 867 "Qualified Certificate Profile".

Los perfiles de dichos certificados se pueden solicitar al correo gestion_soporte@camerfirma.com o al teléfono +34 902 361 207

7.1.1 Número de versión

OSCEPA emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Los documentos de las extensiones de los certificados se encuentran detallados en las fichas de perfiles. Los perfiles de dichos certificados se pueden solicitar al correo gestion_soporte@camerfirma.com o al teléfono +34 902 361 207

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es
- 1.2.840.113549.1.1.5 - sha1withRSAEncryption
- 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.

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica.

En general, los certificados de uso en el sector público deberán contener la identidad de la persona que los recibe, preferiblemente en los campos Subject Name o Subject Alternative Name, incluyendo los siguientes datos:

- Nombre y apellidos de la persona Firmante, poseedora o representada, en campos separados, o con indicación del algoritmo que permite la separación de forma automática.
- Denominación social de la persona jurídica, cuando corresponda.
- Números de documentos de identificación correspondientes, de acuerdo con la legislación aplicable a la persona Firmante, poseedora o representada, sea física o jurídica.

La semántica exacta de los nombres se describe en las fichas de los perfiles. Los perfiles de dichos certificados se pueden encontrar https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

7.1.5 Restricciones de los nombres

OSCEPA puede utilizar restricciones de nombre (utilizando la extensión del certificado "name constrains") en aquellos certificados de AC subordinada emitidos a terceras partes de forma que solo se pueda emitir por la AC subordinada el conjunto de certificados permitido en dicha extensión.

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

Todos los certificados Camerfirma tienen un identificador de política que comienza desde la base 1.3.6.1.4.1.17326.

Govern d'Andorra (OSCEPA) = 2.16.20.2.1.3.1

7.1.7 Uso de la extensión "Policy Constraints"

OSCEPA puede utilizar restricciones de política (utilizando la extensión del certificado "*policy constrains*") en aquellos certificados de AC subordinada emitidos a terceras partes de forma que solo se pueda emitir por la AC subordinada el conjunto de certificados permitido en dicha extensión.

7.1.8 Sintaxis y semántica de los calificadores de política

No estipulado

7.1.9 Tratamiento semántico para la extensión critica "*Certificate Policy*"

La extensión "*Certificate Policy*" identifica la política que define las prácticas que OSCEPA asocia explícitamente con el certificado. La extensión puede contener un calificador de la política. Ver 7.1.6.

7.2. Perfil de CRL

El perfil de las CRLs se corresponde con el propuesto en las Políticas de certificación correspondientes. Las CRLs son firmadas por la AC que ha emitido los certificados.

El perfil detallado de la CRL se puede solicitar en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207.

7.2.1 Número de versión

Las CRL emitidas por OSCEPA son de la versión 2.

7.2.2 CRL y extensiones

Las impuestas por las políticas de certificación correspondientes. El perfil detallado de la CRL y sus extensiones se puede solicitar en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207.

7.3. Perfil de OCSP

7.3.1 Número de versión

Los certificados de respondedor OCSP son versión 3. Estos certificados son emitidos por la AC gestionada por OSCEPA según el estándar RFC 6960.

7.3.2 Extensiones OCSP

Se puede obtener el perfil de los certificados respondedores de OCSP en el siguiente correo gestion_soporte@camerfirma.com o al teléfono 902 361 207.

Se puede obtener una lista actualizada de los certificados de OCSP en https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp.

8. ADITORÍAS DE CONFORMIDAD

La OSCEPA es una organización comprometida con la seguridad y la calidad de sus servicios.

Los objetivos de la OSCEPA respecto a la seguridad y la calidad han sido fundamentalmente la obtención de la certificación ISO/IEC 27001, ISO/IEC 20000 y la realización de Auditorías internas bienales al Sistema de certificación de la OSCEPA, y fundamentalmente a las Autoridades de registro, para garantizar el cumplimiento de los procedimientos internos.

La OSCEPA está sujeta a unas auditorias periódicas con el sello WEBTRUST for CA que asegura que los documentos de políticas y CPS tienen un formato y alcance adecuado a la vez que están completamente alineadas con su políticas y prácticas de certificación.

La OSCEPA está también sujeta a los controles que realiza el organismo regulador nacional respecto a su actividad, siendo este la Comissió Nacional d'Acreditació (CNAC).

Las Autoridades de Registros pertenecientes a ambas jerarquías están sujetas a un proceso de auditoría interna. Estas auditorías se realizan periódicamente de forma discrecional en base a una valoración de riesgo por el número de certificados emitidos y número de operadores de registro, lo que determinará también que se realice la auditoria de forma presencial o remota. Las auditorias se describen en un "Plan Anual de Auditorias".

La OSCEPA está sujeta a una auditoria bienal sobre protección de datos.

La OSCEPA realiza una auditoría interna. En esta auditoria la OSCEPA comprueba de forma aleatoria un número de certificados emitidos por dicha autoridad de registro, asegurándose de que las evidencias recogidas sean correctas y suficientes para la emisión del certificado.

8.1. Frecuencia o circunstancias de las auditorias

Como se ha indicado en el apartado 2.7, la OSCEPA lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza de forma discrecional

- Auditoria ISO 27001, ISO20000, ISO 9001, ciclo de 3 años con revisiones anuales.
- WEBTRUST for CA de forma anual.
- Evaluación de conformidad eIDAS, bienal con revisión anual
- Un análisis de vulnerabilidades trimestral
- Un análisis de intrusión anual.
- Auditorías de RA de forma discrecional.

8.1.1 Auditoria en las Autoridades de Registro

Todas las AR son auditadas. Estas auditorías se realizan al menos cada dos años de forma discrecional y en base a un análisis de riesgos. Las auditorias comprueban el cumplimiento de los requerimientos exigidos por estas CPS para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado.

Dentro de la auditoría interna realizada se toman muestreos sobre certificados emitidos, verificando su correcto procesamiento.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por las compañías independientes externas siguientes de amplio reconocimiento en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación:

- Para la auditoria WEBTRUST - AUREN http://www.auren.com.
- Para las auditorías ISO27001/20000 ISO 9001 -AENOR. http://www.aenor.es
- Para las auditorías internas / RA – AUREN http://www.auren.com/

8.3. Relación entre el auditor y la AC

Las empresas de auditoría son independientes y de reconocido prestigio contando con departamentos especializados en la realización de auditorías informáticas en la gestión de certificados digitales y servicios de confianza, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la AC.

No existe vinculación ni dependencia financiera ni orgánica entre las empresas auditoras y AC la OSCEPA.

8.4. Tópicos cubiertos por la auditoria

En líneas generales, las auditorías verifican:

a) Que la OSCEPA tiene un sistema que garantiza la calidad del servicio prestado.
b) Que la CPS, se ajusta a lo establecido en las Políticas, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.
c) Que la OSCEPA gestiona de forma adecuada la seguridad de sus sistemas de información.
d) En los certificados la auditoría comprueba la alienación con las políticas marcadas por CA/B Forum en sus "*Baseline Requirements*".

En líneas generales, los elementos objeto de auditoría serán los siguientes:

- Procesos de la OSCEPA, ARs y elementos relacionados en la emisión de certificados y servicios de validación en línea OCSP.
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación requerida para cada tipo de certificado.
- Verificación de que los operadores de RA conocen la CPS de la OSCEPA

8.5. Acciones tomadas como resultado de las deficiencias

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, la OSCEPA discutirá, con la entidad que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo con objeto de solucionar las deficiencias.

Si la Entidad auditada es incapaz de desarrollar y / o ejecutar dicho plan en el plazo de tiempo solicitado, o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicar inmediatamente la autoridad de políticas, que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar el certificado correspondiente, y regenerar la infraestructura.
- Terminar el servicio a la Entidad.
- Otras acciones complementarias que resulten necesarias.

8.6. Comunicación de resultados

La comunicación de resultados ser realiza al responsable de seguridad y cumplimiento normativo por parte de los auditores que han realizado la evaluación. Se realiza en un acto con presencia de la dirección corporativa. El certificado de auditoria se publica en la Web la OSCEPA.

9. ASPECTOS LEGALES Y OTROS ASUNTOS

9.1. Tarifas

9.1.1 Tarifas de emisión de certificados y renovación.

Los precios de los servicios de certificación o cualquier otro servicio relacionado están disponibles y actualizados en la página Web Butlletí Oficial del Principat d'Andorra https://www.bopa.ad.

Cada tipo de certificado tiene publicado su precio concreto, excepto aquellos que están sujetos a una negociación comercial previa.

9.1.2 Tarifas de acceso a los certificados.

El acceso a los certificados emitidos es gratuito. La OSCEPA implementa controles para evitar los casos de descarga masiva de certificados. Cualquier otra circunstancia que a juicio de la OSCEPA deba ser considerada a este respecto se publicara en la página Web de la OSCEPA https://www.signaturaelectronica.ad.

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

La OSCEPA provee un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito a través de listas de certificados revocados o mediante acceso vía Web en la dirección Internet de la OSCEPA https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp.
OSCEPA ofrece el servicio de OCSP de forma gratuita. https://ocsp.govern.ad.

9.1.4 Tarifas por el acceso al contenido de estas Prácticas de certificación.

El acceso al contenido de la presente CPS es gratuito, en la dirección Web de la OSCEPA https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

9.1.5 Política de reintegros.

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

9.2. Responsabilidad financiera

9.2.1 Cobertura del Seguro

OSCEPA, en su actividad como PSC, dispone de un seguro de responsabilidad civil que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios: el Sujeto/Firmante y la Parte Usuaria y a terceros, por un importe conjunto de 600.000 de euros.

9.2.2 Otros activos

No estipulado.

9.2.3 Seguro de cobertura o garantía para entidades finales

Ver apartado 9.2.1

9.3. Confidencialidad de la información del negocio

9.3.1 Tipo de información a mantener confidencial

La OSCEPA 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.

La OSCEPA dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

9.3.2 Tipo de información considerada no confidencial

La OSCEPA considera como información no confidencial:

a) La contenida en la presente CPS y en las Políticas de Certificación
b) La información contenida en los certificados.
c) Cualquier información cuya accesibilidad no sea prohibida por la normativa vigente.

9.3.3 Responsabilidad de proteger la información confidencial

La OSCEPA es responsable de la protección de la información confidencial generada o comunicada durante todas las operaciones. Las partes delegadas, como las entidades que administran las CA emisoras subordinadas o las autoridades de registro, son responsables de proteger la información confidencial que se ha generado o almacenado por sus propios medios. Para las entidades finales, los suscriptores del certificado son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesaria para acceder o usar la clave privada.

9.3.3.1 Divulgación de información de revocación / suspensión de certificados

La OSCEPA difunde la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRLs.

La OSCEPA dispone de un servicio de consulta de CRL y Certificados en el sitio de Internet: https://crl.govern.ad

La OSCEPA dispone de un servicio de consulta online de estado de los certificados basado en el estándar OCSP en la dirección http://ocsp.govern.ad. El servicio OCSP ofrece respuestas estandarizadas bajo el RFC 2560 sobre el estado de un certificado digital, es decir, si el certificado consultado está activo, revocado o si ha sido emitido o no por la autoridad de certificación.

9.3.3.2 Envío a la Autoridad Competente

La OSCEPA proporcionará la información solicitada por la autoridad competente o al organismo regulador correspondiente, en los casos y forma establecidos en la legislación vigente.

9.4. Privacidad de la información personal

9.4.1 Plan de privacidad

La OSCEPA cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos, en particular, ha adaptado sus procedimientos al REGLAMENTO (UE) 2016/679 General de Protección de Datos (RGPD).

9.4.2 Información tratada como privada

La información personal sobre un individuo que no está públicamente disponible en los contenidos de un certificado o CRL se considera privada.

9.4.3 Información no considerada privada

La información personal sobre un individuo disponible en los contenidos de un certificado o CRL, se considera como no privada al ser necesaria a la prestación del servicio contratado, sin perjuicio de los derechos correspondientes al titular de los datos personales en virtud de la legislación RGPD.

9.4.4 Responsabilidad de proteger la información privada

Es responsabilidad del responsable del tratamiento proteger adecuadamente la información privada.

9.4.5 Aviso y consentimiento para usar información privada

Antes de entablar una relación contractual, la OSCEPA ofrecerá a los interesados la información previa acerca del tratamiento de sus datos personales y ejercicio de derechos, y en su caso, recabará el consentimiento preceptivo para el tratamiento diferenciado del tratamiento principal para la prestación de los servicios contratados.

9.4.6 Divulgación de conformidad con un proceso judicial o administrativo

Los datos personales que sean considerado privados o no, solo podrán divulgarse en caso cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

9.4.7 Otras circunstancias de divulgación de información

No se cederán datos personales a terceros salvo obligación legal.

9.5. Derechos de propiedad intelectual

OSCEPA es titular de los derechos de propiedad intelectual sobre esta CPS.

9.6. Obligaciones y Responsabilidad Civil

9.6.1 Obligación y responsabilidad de la CA

9.6.1.1 AC

OSCEPA se obliga según lo dispuesto en esta CPS, así como lo dispuesto en normativa vigente sobre prestación de servicios de Certificación a:

- Respetar lo dispuesto en el alcance de esta CPS.
- Proteger sus claves privadas de forma segura.
- Emitir certificados conforme a esta CPS, a las Políticas de Certificación y a los estándares técnicos de aplicación.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados o reconocidos.
- Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
- Informar a los Sujetos/Firmantes de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
- Publicar esta CPS y las Políticas de Certificación correspondientes en su página Web.
- Informar sobre las modificaciones de esta CPS y de las Políticas de Certificación a los Sujetos/Firmantes y a las RAs que estén vinculadas a ella.
- No almacenar ni copiar los datos de creación de firma del Sujeto/Firmante excepto para los certificados de cifrado y para los casos en los que legalmente se prevea o permita dicho almacenaje o copia.
- Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

La OSCEPA será responsable de los daños y perjuicios ocasionados a los usuarios por sus servicios, ya sea al Firmante/Suscriptor o al Tercero que confía, y a otros terceros en los términos establecidos en la legislación vigente y en las Políticas de Certificación.

En este sentido la OSCEPA es la única responsable (i) de la emisión de los certificados, (ii) de su gestión durante todo el ciclo de vida de éstos y (iii) en particular, si es preciso, en caso de suspensión y revocación de los certificados. En concreto, OSCEPA fundamentalmente será responsable de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión, mediante la confirmación de los datos del solicitante y las prácticas de AR.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Firmante/Suscriptor, la clave privada correspondiente a la clave pública dada o identificada en el certificado cuando el proceso así lo requiera, mediante la utilización de peticiones estandarizadas en formato PKCS#10.
- La garantía 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.
- Cualquier responsabilidad que se establezca por la legislación vigente.

En cumplimiento de la legislación vigente OSCEPA dispone de un seguro de responsabilidad civil que cubre los requerimientos marcados por las políticas de certificación afectadas por estas prácticas de certificación.

9.6.2 Obligación y responsabilidad de la RA

Las AR son las entidades delegadas por la AC para realizar las tareas de registro y aprobación de las solicitudes de certificados, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

- Respetar lo dispuesto en esta CPS.
- Proteger sus claves privadas que les servirán para el ejercicio de sus funciones.
- Comprobar la identidad de los Sujetos/Firmantes y Solicitantes de los certificados cuando resulte necesario, acreditando definitivamente la identidad del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización, de acuerdo con lo establecido en las secciones correspondientes de este documento.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- Proporcionar al Firmante, en caso de certificados individuales, o al futuro poseedor de claves, en caso de certificados de organización, acceso al certificado.
- Entregar, en su caso, el dispositivo criptográfico correspondiente.
- Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o Firmante.
- Respetar lo dispuesto en los contratos firmados con la OSCEPA y con el Sujeto/Firmante.
- Informar a la OSCEPA de las causas de revocación, siempre y cuando tomen conocimiento.
- Ofrecer información básica sobre la política y uso del certificado, incluyendo especialmente información sobre la OSCEPA y la Declaración de Prácticas de Certificación aplicable, así como de sus obligaciones, facultades y responsabilidades.
- Ofrecer Información sobre el certificado y el dispositivo criptográfico.
- Recopilar información y evidencias del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de dichos elementos.
- Informar del método de imputación exclusiva al poseedor de la clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones correspondientes de este documento.

La información sobre el uso y responsabilidades de suscriptor se suministra mediante la aceptación de las cláusulas de uso previamente a la confirmación de la solicitud del certificado y mediante correo electrónico.

La responsabilidad de las RA

Las RA suscriben un contrato de prestación de servicio con la OSCEPA mediante el cual la OSCEPA delega las funciones de registro en las RA, consistente fundamentalmente en:

1.- Obligaciones previas a la expedición de un certificado.

a) Informar adecuadamente a los solicitantes de la firma de sus obligaciones y responsabilidades.
b) La adecuada identificación de los solicitantes, que deben ser personas capacitadas o autorizadas para solicitar un certificado digital.
c) La correcta comprobación de la validez y vigencia de esos datos de los solicitantes y de la Entidad, en el caso de que exista una relación de vinculación ó representación.
d) Acceder a la aplicación de Autoridad de Registro para gestionar las solicitudes y los certificados emitidos.

2.- Obligaciones una vez expedido el certificado.

a) Suscribir los contratos de Prestación de Servicios de Certificación Digital con los solicitantes. En la mayoría de los procesos de emisiones este contrato es formalizado mediante la aceptación de condiciones en las páginas web que forman parte del proceso de emisión del certificado, no pudiéndose realizar la emisión sin antes no haber aceptado las condiciones de uso.
b) El mantenimiento de los certificados durante su vigencia (extinción, suspensión, revocación).
c) Archivar las copias de la documentación presentada y los contratos debidamente firmados por los solicitantes en conformidad con Políticas de Certificación publicadas por OSCEPA y la legislación vigente.

Así pues, las RA se responsabilizan de las consecuencias en caso de incumplimiento de sus labores de registro, y a través del cual se comprometen a respetar además las normas reguladoras internas de la OSCEPA (CPS) las cuales deberán ser perfectamente controladas por parte de las RA y que deberán servirles de manual de referencia.

En caso de reclamación por un Sujeto, una Entidad, o un usuario, la AC deberá aportar la prueba de la actuación diligente y si se constata que el origen de la reclamación radica en un error en la validación o comprobación de los datos, la AC podrá en virtud de los acuerdos firmados con las RA, hacer soportar a la RA responsable la asunción de las consecuencias. Porque, aunque legalmente sea la AC la persona jurídica responsable frente al Sujeto, una Entidad, o Parte Usuaria, y que para ello dispone de un seguro de responsabilidad civil, según el acuerdo vigente y las Políticas vinculantes, la RA tiene como obligación contractual "identificar y autenticar correctamente al Solicitante y, en su caso, a la Entidad que corresponda", y en su virtud deberá responder frente a la OSCEPA de sus incumplimientos.

Por supuesto, no es intención de la OSCEPA descargar todo el peso de la asunción de responsabilidad a las RA en cuanto a los posibles daños cuyo origen vendría de un incumplimiento de las tareas delegadas a las RA. Por esta razón, al igual que lo previsto para la AC, la RA se ve sometida a un régimen de control que será ejercido por la OSCEPA, no

solamente a través de los controles de archivos y procedimientos de conservación de los archivos asumidos por la RA mediante la realización de auditorías para evaluar entre otros, los recursos empleados y el conocimiento y control de los procedimientos operativos para ofrecer los servicios de RA.

Las mismas responsabilidades deberá asumir las RA en virtud de incumplimientos de las entidades delegadas como por ejemplo los puntos de verificación presencial (PVP), sin perjuicio de su derecho a repercutir contra ellas.

9.6.3 Obligación y responsabilidad del suscriptor

9.6.3.1 Firmante/Suscriptor

El Firmante/Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Usar el certificado según lo establecido en la presente CPS y en las Políticas de Certificación aplicables.
- Respetar lo dispuesto en los documentos firmados con la OSCEPA y la AR.
- Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión /revocación.
- Notificar cualquier inexactitud o cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la OSCEPA o la AR de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.
- Hacer uso del certificado digital con el carácter de personal e intransferible y, por tanto, asumir la responsabilidad por cualquier actuación que se lleve a cabo en contravención de esta obligación, así como cumplir las obligaciones que sean específicas de la normativa aplicable a las dichas certificaciones digitales.
- Autorizar a la OSCEPA proceder al tratamiento de los datos personales contenidos en los certificados, en conexión con las finalidades de la relación electrónica y, en todo caso, para cumplir las obligaciones legales de verificación de certificados.
- Responsabilizarse de que toda la información incluida, por cualquier medio, la solicitud del certificado y en el mismo certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.
- Informar inmediatamente al prestador de servicios de certificación correspondiente, de cualquier inexactitud en el certificado detectada una vez se haya emitido, así como de los cambios que se produzcan en la información aportada por la emisión del certificado.
- Si se trata de certificados en un dispositivo material, en caso de que pierda su posesión, ponerlo en conocimiento fehaciente de la entidad que lo haya emitido en el plazo más breve posible y, en todo caso, dentro de las 24 horas siguientes a la producción de la mencionada circunstancia, con independencia del hecho concreto que la haya originado o de las acciones que eventualmente pueda ejercer.
- No utilizar la clave privada, el certificado electrónico o cualquier otro soporte técnico entregado por el prestador de servicios de certificación correspondiente para realizar ninguna transacción prohibida por la ley aplicable.

En el caso de certificados calificados, el suscriptor o el poseedor de certificados debe utilizar el par de claves exclusivamente para la creación de firmas o sellos electrónicos y de acuerdo con cualesquiera otras limitaciones que le sean notificadas.

Asimismo, debe ser especialmente diligente en la custodia de su clave privada y de su dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados. Será el único responsable frente a terceros o frente a la entidad que representa si no está autorizado para ello, de las consecuencias que un uso indebido o no correctamente controlado pueda generar.

Si el suscriptor genera sus propias claves, se obliga a:

- Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica, en su caso cualificado, o el sello electrónico, en su caso cualificado.
- Crear las claves dentro del dispositivo de creación de firma o de sello, utilizando un dispositivo seguro cuando proceda.
- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica, en su caso cualificado, o el sello electrónico, en su caso calificado.

9.6.3.2 Solicitante del certificado

El Solicitante (bien directamente o a través de un tercero autorizado) de un certificado estará obligado a cumplir con lo dispuesto por la normativa y además a:

- Suministrar a la AR la información necesaria para realizar una correcta identificación.
- Garantizar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Custodiar su clave privada de manera diligente.

9.6.3.3 Entidad

En el caso de aquellos certificados que impliquen vinculación a una Entidad, la Entidad vendrá obligada a solicitar a la RA la suspensión/revocación del certificado cuando el Sujeto/Firmante cese dicha vinculación respecto a la organización.

9.6.4 Obligación y responsabilidad de terceras partes

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

- Verificar la validez de los certificados antes de realizar cualquier operación basada en los mismos. La OSCEPA dispone de diversos mecanismos para realizar dicha comprobación como el acceso a listas de revocados o a servicios de consulta en línea como OCSP, todos estos mecanismos están descritos en la página Web de la OSCEPA. En particular, para asegurarse de que está ante un certificado cualificado deberá realizar la validación contra la TSL vigente en cada momento.
- 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. En los certificados de Representante de Persona Jurídica que implican una relación de representación basada en un poder especial notarial o documento privado con facultades limitadas, las terceras partes deberán comprobar los límites de dichas facultades.
- Comprobar la validez de la cualificación de una firma asociada a un certificado emitido por OSCEPA comprobando que la autoridad de certificación que ha emitido el certificado se encuentra publicada en la lista de confianza del supervisor nacional correspondiente.

9.6.5 Obligación y responsabilidad de otras participantes

No estipulado

9.7. Exoneración de responsabilidad

Según la legislación vigente, la responsabilidad de la OSCEPA 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 lo haya cedido o haya autorizado su uso a favor de una tercera persona en virtud de un negocio jurídico como el mandato o apoderamiento, siendo exclusiva responsabilidad del Sujeto /Titular el control de las claves asociadas a su certificado.

OSCEPA 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 las Políticas de Certificación
- Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la AC
- Por el uso de la información contenida en el Certificado o en la CRL.
- 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.

9.8. Limitación de responsabilidad en caso de pérdidas por transacciones

El límite máximo que la OSCEPA permite en las transacciones económicas realizadas es de 0 (cero) euros.

9.9. Indemnizaciones

Ver apartado 0

9.10. Plazo y Finalización

9.10.1 Plazo

Ver apartado 5.8

9.10.2 Terminación

Ver apartado 5.8

9.10.3 Efecto de la terminación y la supervivencia

Ver apartado 5.8

9.11. Notificaciones individuales y comunicación con los participantes

Cualquier notificación referente a la presente CPS se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto 1.5.2.

9.12. Modificaciones

9.12.1 Procedimiento de modificación.

La CA se reserva el derecho de modificar este documento por razones técnicas o para reflejar cualquier cambio en los procedimientos que se hayan producido debido a requisitos legales, reglamentarios (eIDAS, CA/B Forum, Organismos de Supervisión Nacional, etc.) o como resultado de la optimización del ciclo de trabajo. Cada nueva versión de esta CPS reemplaza a todas las versiones anteriores, que siguen siendo, sin embargo, aplicables a los certificados emitidos mientras esas versiones estaban vigentes y hasta la primera fecha de vencimiento de esos certificados. Se publicará al menos una actualización anual. Estas actualizaciones quedaran reflejadas en el cuadro de versiones.

Los cambios que pueden realizarse a esta CPS no requieren notificación excepto que afecte de forma directa a los derechos de los Sujetos/Firmantes de los certificados, en cuyo caso podrán presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

9.12.2 Mecanismo de notificación y plazos

9.12.2.1 Lista de elementos

Cualquier elemento de esta CPS puede ser cambiado sin preaviso.

9.12.2.2 Mecanismo de notificación

Todos los cambios propuestos de esta política serán inmediatamente publicados en la Web de la OSCEPA

https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

En este mismo documento existe un apartado de cambios y versiones donde se puede conocer los cambios producidos desde su creación y la fecha de dichas modificaciones.

9.12.2.3 Periodo de comentarios

Los Firmantes/Suscritores y Terceros que confían, afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los **15 días** siguientes a la recepción de la notificación. Las Políticas dicen que 15 días

9.12.2.4 Mecanismo de tratamiento de los comentarios

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA

9.12.3 Circunstancias en las que se debe cambiar el OID

No estipulado

9.13. Procedimiento de resolución de conflictos

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

9.14. Legislación aplicable

La ejecución, interpretación, modificación o validez de la presente CPS se regirá por lo dispuesto en la legislación andorrana y de la Unión Europea vigente en cada momento.

9.15. Conformidad con la Ley Aplicable

Ver punto 9.14

9.16. Otras disposiciones

9.16.1 Acuerdo completo

Los Titulares y terceros que confían en los Certificados asumen en su totalidad el contenido de la presente Declaración de Prácticas y Políticas de Certificación.

9.16.2 Asignación

Las partes de esta CPS no pueden ceder ninguno de sus derechos u obligaciones bajo esta CPS o acuerdos aplicables sin el consentimiento por escrito de la OSCEPA.

9.16.3 Separabilidad

Si las disposiciones individuales de esta CPS resultan ineficaces o incompletas, esto se hará sin perjuicio de la efectividad de todas las demás disposiciones.

La disposición ineficaz será reemplazada por una disposición efectiva que se considera que refleja más de cerca el sentido y el propósito de la disposición ineficaz. En el caso de disposiciones incompletas, se acordará una modificación que se considere que corresponde a lo que razonablemente se habría acordado de acuerdo con el sentido y los propósitos de esta CPS, si el asunto se hubiera considerado de antemano.

9.16.4 Cumplimiento (honorarios de abogados y exención de derechos)

OSCEPA puede solicitar una indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de dicha parte. El hecho de que OSCEPA no haga cumplir una disposición de esta CPS no elimina el derecho de la OSCEPA de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de esta CPS. Para ser efectiva, cualquier renuncia debe estar por escrito y firmada por la OSCEPA.

9.16.5 Fuerza mayor

Las cláusulas de fuerza mayor, si existen, están incluidas en el "Acuerdo del suscriptor".

9.17. Otras provisiones

9.17.1 Publicación y copia de la política

Una copia de esta CPS estará disponible en formato electrónico en la dirección de Internet:

https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

9.17.2 Procedimientos de aprobación de la CPS

La publicación de las revisiones de esta CPS deberá estar aprobada por la autoridad de políticas de la OSCEPA.

La OSCEPA publica en su página web cada nueva versión. La CPS se publica en formato PDF firmado electrónicamente por la OSCEPA.

ANEXO I: historia del documento

Oct 2013	**V1.0**	**Versión Inicial**
Nov 2017	V1.0	**Revisión**
Oct 2019	V2.0	**Cambio de orden, denominación y desarrollo en diversos puntos para alinear con RFC3647**
02 2020	**V2.1**	**Cambio de sintaxis**