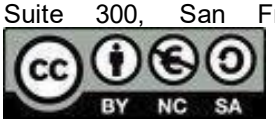
Administració Oberta de Catalunya

Declaración de prácticas del servicio de sellado cualificado de tiempo

Generalitat de Catalunya

Localret

Control documental

Estado formal	Aprobado
Elaborado por	Consorci AOC
Aprobado por	Comisión Ejecutiva del Consorci AOC del 18 de diciembre de 2024
Fecha de creación	18/12/2024
Nivel de acceso a la información	Pública
Título	Declaración de Prácticas del Servicio de Sellado Cualificado de Tiempo del Consorci AOC
Fichero	DP_TSA-1.0-ES.docx
Control de copias	Sólo las copias disponibles en la Sede electrónica del Consorci AOC garantizan la actualización de los documentos. Toda copia impresa o guardada en ubicaciones distintas se considerarán copias no controladas.
Drets d'autor	

Control de versiones

Fecha:	18/12/2024
Descripción:	Versión inicial

Administració Oberta de Catalunya

Índice

1. Introducción

1.1. Vista general

El presente documento constituye la Declaración de Prácticas (en adelante, **DP**) de los siguientes servicios de expedición de sellos electrónicos de tiempo (en adelante, servicios de sellado de tiempo) prestados por el Consorci Administració Oberta de Catalunya (en adelante, Consorci AOC):

- **SERVICIO DE EXPEDICIÓN DE SELLOS ELECTRÓNICOS CUALIFICADOS DE TIEMPO** (en adelante, servicio de sellado cualificado de tiempo)

La prestación de estos servicios se realiza de acuerdo con el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, modificado por el Reglamento (UE) 2024/1183, de 11 de abril de 2024 (en adelante, Reglamento eIDAS) y con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, Ley 6/2020).

En lo que no está especificado en este documento, los servicios de sellado de tiempo bajo esta DP se rigen por lo especificado en los documentos "Declaración de Prácticas de Certificación (DPC) Autoridad de Certificación del Consorci AOC", "Política de Certificación para Dispositivos e Infraestructuras Consorci AOC" y "Descripción de los perfiles de Certificados Consorci AOC" publicados en la página web https://epscd.aoc.cat/ca/index.html#politiques, en lo que no sea aplicable exclusivamente a los servicios de expedición de certificados del Consorci AOC, y en lo que sea aplicable a los certificados de los servicios de sellado de tiempo del Consorci AOC (ver OID políticas de certificados en punto 1.2).

Para prestar los servicios de expedición de sellos electrónicos de tiempo, el Consorci AOC subcontrata a un proveedor externo (en adelante, el proveedor tecnológico) el hosting, la gestión y la operación de los servicios de sellado de tiempo bajo esta DP.

Los servicios de sellado de tiempo bajo esta DP permiten obtener una marca de tiempo fiable y segura con todas las garantías, tanto jurídicas como técnicas, que establece la normativa vigente. Estos servicios permiten acreditar, mediante la marca de tiempo que reporta el servicio, la existencia de un elemento en formato electrónico (documento, firma, etc.) en un instante determinado del tiempo. Entre las ventajas que suponen estos servicios destacan:

- Seguridad: el sello de tiempo es una manera segura y fiable de obtener marcas temporales y a la vez vincularlas a un documento. La fecha y la hora del sello de tiempo está protegida por mecanismos robustos de seguridad (firma digital).
- Tercero de confianza: cada sello de tiempo que se emite está garantizado por un tercero de confianza, en este caso el Consorcio AOC y CATCert.
- Evidencia electrónica: cada sello de tiempo es una evidencia electrónica que acredita un instante temporal en el que se puede asegurar la existencia de un documento.
- Ahorro: el Consorcio AOC asume el coste del servicio y lo ofrece libre de coste para las aplicaciones del sector público catalán.

Los sellos de tiempo emitidos bajo esta DP son conformes a la Política BTSP (Best practices Time-Stamp Policy) definida en el estándar europeo ETSI EN 319 421, identificada mediante el OID 0.4.0.2023.1.1.

Los sellos de tiempo emitidos bajo esta DP incluyen el OID de la Política BTSP 0.4.0.2023.1.1.

La precisión de los sellos de tiempo emitidos bajo esta DP será de 1 segundo respecto a la hora UTC.

Las peticiones, las respuestas y los certificados de los servicios de sellado de tiempo bajo esta DP son conformes al estándar europeo ETSI EN 319 422.

1.2. Nombre del documento e identificación

Este documento tiene los siguientes datos de identificación:

Nombre	Declaración de Prácticas del Servicio de Sellado Cualificado de Tiempo del Consorci AOC
Versión	1.0
OID Declaración de Prácticas del Servicio de Sellado Cualificado de Tiempo	1.3.6.1.4.1.15096.3.2
OID Política del Servicio de Sellado Cualificado de Tiempo	0.4.0.2023.1.1 (ETSI EN 319 421 BTSP)
OID Políticas de Certificados del Servicio de Sellado Cualificado de Tiempo (Certificados de TSU)	1.3.6.1.4.1.15096.1.3.2.112 (Consorci AOC) 0.4.0.194112.1.1 (ETSI EN 319 411-2 QCP-l)
Localización	https://tsa.aoc.cat/regulacio

1.3. Participantes

1.3.1. Autoridad de Sellado de Tiempo (TSA)

Una Autoridad de Sellado de Tiempo (TSA, Time-Stamping Authority) es un Prestador de Servicios de Confianza que presta servicios de sellado de tiempo. El papel de una TSA es convertirse en un tercero de confianza certificando la existencia de los datos sellados en una fecha y hora concretas.

Una TSA opera una o varias Unidades de Sellado de Tiempo (TSU, Time-Stamping Units) para cada uno de los servicios de sellado de tiempo que presta.

La TSA será el responsable de la prestación de los servicios de sellado de tiempo bajo esta DP, y del cumplimiento de sus obligaciones y de las obligaciones de todas las organizaciones externas utilizadas para prestar parte de dichos servicios.

El Consorci AOC actúa como TSA bajo esta DP.

1.3.2. Suscriptor

Es una entidad del Sector Público de Cataluña que solicita el uso de un servicio de sellado de tiempo bajo esta DP, a quien se le expiden sellos de tiempo.

Comprenderá tanto a las aplicaciones del propio Suscriptor como a las personas físicas (usuarios finales) que dependan del mismo y que podrán realizar solicitudes de sellos de tiempo a la TSA

utilizando sus propios recursos y medios, las cuales asumen el cumplimiento de algunas obligaciones del Suscriptor, sin perjuicio de la responsabilidad del Suscriptor, en caso de incumplimiento de dichas obligaciones.

1.3.3. Tercero que confía

Es la persona física o entidad (con o sin personalidad jurídica) que recibe una transacción electrónica con un sello de tiempo emitido por un servicio de sellado de tiempo bajo esta DP, y que voluntariamente confía en dicho sello de tiempo (Relying party).

1.4. Obligaciones de los participantes

1.4.1. Obligaciones de la TSA

El Consorci AOC, actuando como TSA bajo esta DP, tiene las siguientes obligaciones en los servicios de sellado de tiempo que presta:

- Prestar los servicios y emitir los sellos de tiempo de acuerdo con esta DP.
- Mantener publicada la documentación especificada en el punto 1.5.5.
- Modificar este documento y notificar, en su caso, las modificaciones conforme a lo especificado en el punto 1.5.6.
- Mantener publicados los certificados asociados a las claves privadas utilizadas para la firma de los sellos de tiempo (certificados de TSU).
- Todas las que se deriven del contenido de los documentos “Declaración de Prácticas de Certificación (DPC) Autoridad de Certificación del Consorci AOC” y “Política de Certificación para Dispositivos e Infraestructuras Consorci AOC” que sea aplicable (ver punto 1.1), así como de la legislación vigente.

1.4.2. Obligaciones de las organizaciones externas que prestan parte de los servicios

El Consorci AOC, para el hosting, la gestión y la operación y la monitorización de los servicios de sellado de tiempo que presta bajo esta DP, utiliza los siguientes servicios de organizaciones externas que están sujetas a las siguientes obligaciones:

- Gestión y operación (el proveedor tecnológico)
    - Cumplir con los acuerdos de los contratos suscritos con el Consorci AOC.
    - Controlar y supervisar el funcionamiento de los servicios para garantizar que se prestan de acuerdo con esta DP.
    - Instalar, configurar, mantener, operar y consultar registros de auditoría de los elementos hardware y software de los servicios.
    - Establecer las medidas y controles de seguridad necesarios para proteger el sistema y las claves privadas de los servicios.
    - Ejecutar los servicios empleando los medios técnicos y materiales adecuados, así como el personal cualificado requerido por los estándares aplicables.

- Cumplir los niveles de calidad de los servicios requeridos por los estándares aplicables, en cuanto a aspectos técnicos, operaciones y de seguridad se refiere.
- Garantizar que los sellos de tiempo emitidos son fieles a la información en las correspondientes peticiones.
- Garantizar la fecha y hora de los sellos de tiempo emitidos con una precisión de 1 segundo respecto a la hora UTC.
- Almacenar y custodiar los registros de auditoría de los elementos hardware y software de los servicios, en el caso de las peticiones y respuestas, durante el periodo mínimo establecido en el punto 2.10.
- Cumplir con los acuerdos de nivel de servicio (SLA, Service Level Agreements) de disponibilidad, monitorización de infraestructuras y soporte a incidencias 24x7.
- Todas las que se deriven de la legislación vigente.

- Centros de Proceso de Datos (CPD)
  - Cumplir con los acuerdos de los contratos suscritos con el proveedor tecnológico.
  - Prohibir el acceso al área de los servicios a cualquier tercero ajeno al personal del centro de datos o autorizado por el proveedor tecnológico y mantener en todo momento un registro de las personas autorizadas por el proveedor tecnológico que acceden al Área de Servicio.
  - Cumplir las indicaciones dadas por el proveedor tecnológico y acordadas con el CPD respecto al manejo de sus equipos.
  - No tener ningún tipo de control sobre la información de los servicios transmitida a través de las instalaciones, ni examinar el uso que los clientes de los servicios hacen de los datos, ni conocer el tipo de información que envían, reciben o almacenan.
  - Cumplir con los SLA de disponibilidad, monitorización de infraestructuras y soporte a incidencias 24x7.
  - Todas las que se deriven de la legislación vigente.
- Computación en la nube
  - Cumplir con los acuerdos de los contratos suscritos con el proveedor tecnológico.
  - Ubicación de servidores en la Unión Europea.
  - Doble factor de autenticación para los administradores del servicio con política de contraseñas.
  - Control de acceso definido para cada aplicación y tipo de usuario.
  - Cumplir con los SLA de disponibilidad, monitorización de infraestructuras y soporte a incidencias 24x7.
  - Todas las que se deriven de la legislación vigente.

1.4.3. Obligaciones del Suscriptor

Las obligaciones del Suscriptor de un servicio de sellado de tiempo bajo esta DP son:

- Cumplir con lo que establecen las Condiciones Generales de Prestación de Servicios del Consorci AOC y las Cláusulas de Divulgación del servicio de sellado de tiempo.
- Utilizar el servicio de acuerdo con esta DP.
- Custodiar de forma diligente las claves secretas, contraseñas o pines utilizados para la identificación y autenticación del Suscriptor al servicio, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizados.
- Adecuar sus sistemas de información a los requerimientos fijados en la documentación técnica de integración para realizar las solicitudes al servicio, conforme a lo especificado en el punto 2.5, y para tratar sus respuestas, conforme a lo especificado en el punto 2.6.
- Validar los sellos de tiempo contenidos en las respuestas del servicio conforme a lo especificado en el punto 2.7, en el momento de recepción de las respuestas.
- Informar inmediatamente a la TSA acerca de cualquier de cualquier incidente o hecho que afecte al servicio prestado o que pueda afectar a la validez de los sellos de tiempo.
- Tener en cuenta las limitaciones de uso especificadas en el punto 1.7.
- Informar debidamente a los usuarios finales de las obligaciones anteriores.
- Designar a un responsable del ente, y un responsable técnico para cada una de las aplicaciones bajo la adscripción del ente que actúen como consumidoras del servicio.

1.4.4. Obligaciones del Tercero que confía

Las obligaciones del Tercero que confía en un sello de tiempo emitido por un servicio de sellado de tiempo bajo esta DP son:

- Validar el sello de tiempo conforme a lo especificado en el punto 2.7, en el momento actual o, en su caso, en el momento en el que se ha protegido la integridad del sello de tiempo (por ejemplo, mediante un sello de tiempo adicional, o almacenando el sello de tiempo de forma segura).
- Tener en cuenta las limitaciones de uso especificadas en el punto 1.7.

1.5. Administración del documento

1.5.1. Organización

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

Organización	Consorci Administració Oberta de Catalunya (Consorci AOC)
E-mail	suport@aoc.cat
Página Web	https://www.aoc.cat

1.5.2. Datos de contacto

Para cualquier consulta acerca de esta DP, se puede contactar con:

Organización	Consorci Administració Oberta de Catalunya (Consorci AOC)
Responsable	Responsable de los Servicios de Sellado de Tiempo del Consorci AOC
E-mail	scd@aoc.cat
Teléfono	+34 93 272 40 00 - 900 90 50 90

1.5.3. Responsable para determinar la idoneidad de la DP con las Políticas

El Responsable del Servicio de Certificación Digital del Consorci AOC es el responsable de determinar la idoneidad de la DP con las Políticas.

1.5.4. Procedimiento de aprobación

El sistema documental y de organización del Consorci AOC garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la DP y de las especificaciones del procedimiento de publicación de especificaciones de servicio.

La versión inicial de esta DP es aprobada por la Comisión Ejecutiva del Consorci AOC, que es el órgano colegiado de dirección ejecutiva del Consorci AOC. El Director Gerente del Consorci AOC es competente para aprobar las sucesivas modificaciones de la misma.

1.5.5. Documentación publicada

El Consorci AOC pone a disposición de todas las partes interesadas, en el repositorio público https://tsa.aoc.cat/regulacio, la siguiente documentación de los servicios de sellado de tiempo bajo esta DP:

- Esta DP.
- Las Cláusulas de Divulgación.

El Consorci AOC publica, una vez aprobada y vigente, cualquier nueva versión de esta documentación, manteniendo publicadas todas sus versiones anteriores.

1.5.6. Modificaciones

Este documento se modificará cuando se produzcan cambios relevantes en la prestación de los servicios sujetos a él o cuando se realicen revisiones del documento. Se producirá al menos una revisión bienal del documento, en caso de que no se produzcan antes cambios relevantes en la prestación de los servicios. Los cambios y las revisiones quedarán reflejados en el cuadro de control de versiones al inicio del documento.

Las modificaciones de este documento se notificarán a los Suscriptores y a los Terceros que confían, cuando los cambios en la prestación de los servicios incidan directamente en sus derechos y obligaciones, de acuerdo con lo estipulado en las Cláusulas de Divulgación de los servicios. La notificación de las modificaciones podrá ser publicada por el Consorci AOC en el repositorio público https://tsa.aoc.cat/regulacio.

1.6. Responsabilidad

El Consorci AOC será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o entidad (con o sin personalidad jurídica) debido al incumplimiento de las obligaciones establecidas en el Reglamento eIDAS y la Ley 6/2020 con respecto a los servicios de sellado de tiempo bajo esta DP.

Esta responsabilidad queda limitada por:

- Causas de fuera mayor.
- Uso indebido del servicio.
- Por el incumplimiento de las obligaciones del Suscriptor o del Tercero que confía establecidas en esta DP, así como en las Condiciones Generales de Prestación de Servicios del Consorci AOC y las Cláusulas de Divulgación del servicio.

1.7. Limitaciones de uso

- Los sellos de tiempo emitidos por los servicios de sellado de tiempo bajo esta DP están dirigidos a ser usados en el ámbito de todas las Administraciones Públicas Catalanas, para garantizar la existencia de las firmas electrónicas y los sellos electrónicos que se presentan ante las Administraciones Públicas Catalanas en un momento determinado del tiempo, así como para garantizar las transacciones y la imputabilidad en procesos entre ciudadanos, empresas y las propias administraciones.
- Los servicios de sellado de tiempo bajo esta DP no almacenan ni custodian los sellos de tiempo emitidos, pero almacenan y custodian registros de auditoría de las peticiones y respuestas de los servicios que permiten identificar los sellos de tiempo emitidos.
- El Consorci AOC no ofrece ningún software, librería o servicio para realizar las solicitudes a los servicios de sellado de tiempo bajo esta DP, conforme a lo especificado en el punto 2.5, ni para tratar sus respuestas, conforme a lo especificado en el punto 2.6, siendo responsabilidad del Suscriptor o de sus usuarios finales adaptar sus sistemas o utilizar software existente en el mercado para realizar las solicitudes y tratar las respuestas.

2. Requisitos operacionales

2.1. Funcionamiento del servicio de sellado de tiempo

El servicio de sellado de tiempo usa el protocolo definido en el estándar RFC 3161 sobre una comunicación HTTPS, conforme al estándar europeo ETSI EN 319 422.

Los pasos del protocolo son:

- El cliente envía una petición de sello de tiempo conteniendo el hash de los datos a sellar a una URL específica del servicio, según el formato establecido en el estándar RFC 3161.
- El servicio verifica la petición y, si es válida, emite el sello de tiempo, para lo cual firma el hash de los datos a sellar junto con la fecha y hora actual y otros datos con la clave privada asociada a un certificado de sellado de tiempo activo del servicio, según el formato establecido en el estándar RFC 3161.
- El sello de tiempo se remite al cliente de forma síncrona en una respuesta a la petición, según el formato establecido en el estándar RFC 3161.

El cliente tiene la obligación de validar el sello de tiempo emitido por el servicio, conforme a lo especificado en el punto 2.7.

2.2. Claves privadas y certificados de sellado de tiempo

Las claves privadas utilizadas para la firma de los sellos de tiempo (claves privadas de sellado de tiempo o claves privadas de TSU) se generan y custodian en un dispositivo criptográfico seguro (HSM) con la certificación Common Criteria EAL 4 o superior, FIPS 140-2 Level 3 o FIPS 140-3 Level 3.

Los certificados asociados a las claves privadas utilizadas para la firma de los sellos de tiempo (certificados de sellado de tiempo o certificados de TSU) son certificados cualificados de sello electrónico emitido por el Consorci AOC bajo las políticas de certificados del servicio de sellado de tiempo (ver OID en punto 1.2), conforme a los estándares europeos ETSI EN 319 411-2 y ETSI EN 319 422, y de acuerdo con los documentos "Declaración de Prácticas de Certificación (DPC) Autoridad de Certificación del Consorci AOC", "Política de Certificación para Dispositivos e Infraestructuras Consorci AOC" y "Descripción de los perfiles de Certificados Consorci AOC" publicados en la página web https://epscd.aoc.cat/ca/index.html#politiques.

Los certificados de sellado de tiempo tendrán un periodo de validez de 5 años. Las claves privadas de sellado de tiempo tendrán un periodo de validez de 2 años. Antes del fin del periodo de validez de una clave privada, se generarán nuevas claves y se emitirá un nuevo certificado que sustituirán a los anteriores en la firma de los sellos de tiempo, garantizando así una validez mínima de los sellos de tiempo de 3 años, si no se produce una revocación del certificado antes de su expiración.

Una vez finalizado el periodo de validez de una clave privada de sellado de tiempo y antes de la expiración del certificado asociado, la clave privada será destruida, incluyendo todas sus copias, de la siguiente forma que impide su recuperación:

- Se realizará un borrado seguro de la clave privada en los dispositivos criptográficos (HSM) que la tengan almacenada, siguiendo los pasos descritos en el manual de administración de los HSM.
- Se realizará un borrado seguro de todas las copias de seguridad de la clave privada.

Una clave privada y un certificado de sellado de tiempo pueden estar en uno de los tres estados siguientes:

- Activo: mientras la clave privada se está usando para firmar sellos de tiempo.
- Desactivado: cuando la clave privada se ha dejado de usar para firmar sellos de tiempo, antes del fin de su periodo de validez.
- Terminado: cuando la clave privada se ha destruido y el certificado ha expirado o ha sido revocado.

Los certificados de sellado de tiempo del Consorci AOC, tanto los actuales, en estado activo, como los anteriores, en estado desactivado o terminado, se encuentran publicados en la página web https://tsa.aoc.cat/regulacio.

2.3. Unidad de sellado de tiempo (TSU)

Una Unidad de Sellado de Tiempo (TSU, Time-Stamping Unit) es un conjunto de hardware y software que es gestionado como una unidad y tiene una única clave de firma de sellos de tiempo activa en un instante de tiempo (clave privada de sellado de tiempo o clave privada de la TSU).

Los sellos de tiempo son emitidos por las TSU de los servicios de sellado de tiempo prestados por la TSA.

Un servicio de sellado de tiempo solo tendrá una TSU activa, excepto durante el periodo transitorio de sustitución de las claves y el certificado del servicio (sustitución de TSU), durante el cual podrán estar activas la anterior TSU, con las anteriores claves y el anterior certificado, y la nueva TSU, con las nuevas claves y el nuevo certificado.

2.4. Control de acceso

El control de acceso al servicio de sellado de tiempo por parte de los Suscriptores se realiza por nombre de usuario y contraseña.

2.5. Solicitud de sello de tiempo

Para realizar una solicitud de sello de tiempo, el cliente deberá enviar una petición conteniendo el hash de los datos a sellar a una URL específica del servicio de sellado de tiempo proporcionada por el Consorci AOC.

El envío de la petición se realizará sobre una comunicación HTTPS autenticada con nombre de usuario y contraseña.

La petición deberá utilizar la sintaxis definida en el estándar RFC 3161, conforme al estándar europeo ETSI EN 319 422.

2.6. Formato de la respuesta

La respuesta del servicio de sellado de tiempo utiliza la sintaxis definida en el estándar RFC 3161, conforme al estándar europeo ETSI EN 319 422.

Si no hay ningún error, la respuesta incluye el sello de tiempo emitido, firmada con la clave privada de la correspondiente TSU activa, que contiene, entre otros datos, el mismo valor del hash de los datos a sellar en la petición y la fecha y hora actual del servidor de la TSU que procesa la petición.

El sello de tiempo emitido contiene el OID de la Política BTSP 0.4.0.2023.1.1.

En el caso del servicio de sellado cualificado del tiempo, el sello de tiempo emitido contiene la extensión qcStatements con el valor especificado en el estándar europeo ETSI EN 319 422 para los sellos cualificados de tiempo.

Ante cualquier error, la respuesta incluirá el correspondiente código de error definido en el estándar RFC 3161.

2.7. Validación del sello de tiempo

La validación de un sello de tiempo deberá ser realizada por la parte interesada por sus propios medios, utilizando los datos sellados y el certificado de la TSU con cuya clave privada se ha firmado el sello de tiempo.

Los certificados de las TSU del Consorci AOC, tanto los actuales, en estado activo, como los anteriores, en estado desactivado o terminado, se encuentran publicados en la página web https://tsa.aoc.cat/regulacio.

Para validar un sello de tiempo en un momento determinado, se deberán realizar las siguientes verificaciones:

- El hash de los datos contenido en el sello de tiempo es igual al hash de los datos sellados.
- La firma digital del sello de tiempo es correcta.
- La clave privada de la TSU usada para firmar el sello de tiempo no ha sido comprometida antes del momento de la validación del sello de tiempo. Para realizar esta verificación:
    - Durante el periodo de validez del certificado de la TSU (antes de su expiración), se puede consultar su estado de revocación a través del servicio de OCSP o CRL, conforme a los procedimientos indicados en el documento "Declaración de Prácticas de Certificación (DPC) Autoridad de Certificación del Consorci AOC" publicado en la página web https://epscd.aoc.cat/ca/index.html#politiques.
    - Después del periodo de validez del certificado de la TSU (después de su expiración), se puede consultar su estado de revocación únicamente a través del servicio de OCSP, ya que este devuelve el estado revocado de los certificados después de su expiración (la CRL no mantiene los certificados revocados después de su expiración), y la TSA puede garantizar que la clave privada de la TSU no ha sido comprometida después de la expiración del certificado de la TSU.
    - El Consorci AOC garantiza que las claves privadas de sus TSU no han sido comprometidas después de la expiración de los respectivos certificados de TSU mediante la destrucción de las claves privadas antes de la expiración de los certificados.
- Los algoritmos de hash utilizados en el sello de tiempo (en el hash de los datos sellados y en la firma del sello de tiempo), y el algoritmo y el tamaño de clave de la firma del sello de tiempo se pueden seguir considerando seguros en el momento de la validación del sello de tiempo.
- En el caso del servicio de sellado cualificado de tiempo, el certificado de la TSU ha sido emitido por una Autoridad de Certficación (CA, Certification Authority) del Consorci AOC cuyo certificado está incluido en la lista de confianza (TSL, Trust-service Status List) española, en un servicio de sellado cualificado de tiempo en estado granted en el momento de la validación del sello de tiempo o en el momento de la emisión del sello de tiempo, conforme al Reglamento eIDAS y al estándar europeo ETSI TS 119 612.

Las Administraciones Públicas Catalanas podrán llevar a cabo estas verificaciones utilizando el Servicio Validador que ofrece el propio Consorci AOC.

En caso de producirse un incidente de seguridad por compromiso o sospecha de compromiso de la clave privada de la TSU usada para firmar el sello de tiempo o por pérdida de calibración del reloj del servidor que ha emitido el sello de tiempo, se puede considerar que el sello de tiempo es válido, si la TSA confirma que el sello de tiempo no ha sido afectado por el incidente.

2.8. Sincronización de tiempos

Se realiza una sincronización del reloj de los servidores de las TSU con dos fuentes de tiempo UTC Stratum 1 mediante el protocolo NTP (RFC 5905 Network Time Protocol Version 4), monitorizando en todo momento esta sincronización:

- Sección de Hora del Real Instituto y Observatorio de la Armada en San Fernando (ROA)
- Servicio de sincronización horaria del Centro Informático Científico de Andalucía (CICA)

La precisión declarada de la hora en los sellos de tiempo con la hora UTC es de 1 segundo. Los servidores de las TSU no emitirán sellos de tiempo en caso de detectar una posible diferencia mayor entre sus relojes y las fuentes de tiempo UTC con las que se sincronizan.

2.9. Algoritmos de hash

El algoritmo de hash utilizado por el cliente en la petición para representar los datos que se van a sellar podrá ser RIPEMD-160, SHA-1, SHA-256, SHA-384 o SHA-512. De acuerdo con la norma ETSI TS 119 312 y la Guía CCN-STIC 807, se recomienda utilizar el algoritmo de hash SHA-256, SHA-384 o SHA-512.

El algoritmo de hash utilizado en la firma del sello de tiempo contenido en la respuesta del servicio es SHA-256.

2.10. Registros de auditoría

La TSA recoge registros de auditoría de los sistemas que intervienen en los servicios de sellado de tiempo, genéricos y específicos de los servicios.

Los registros de auditoría genéricos incluyen, entre otros, los eventos relativos a:

- Acceso a las zonas de seguridad
- Acceso a los sistemas de la infraestructura
- Operaciones criptográficas

Los registros de auditoría específicos de los servicios de sellado de tiempo incluyen todos los eventos relativos a:

- Peticiones y respuestas.
- Ciclo de vida de las claves y los certificados de las TSU.
- Sincronización y detección de pérdida de sincronización del reloj de los servidores de las TSU con las fuentes de tiempo UTC.

El Consorci AOC mantendrá los registros de auditoría de las peticiones y respuestas durante un periodo mínimo de 15 años, para el servicio de sellado cualificado de tiempo, desde la expiración del certificado del servicio activo en el momento de la operación o desde la finalización del servicio.

2.11. Incidentes de seguridad

El Plan de Recuperación ante Desastres del Consorci AOC contempla los casos de incidentes de seguridad por compromiso o sospecha de compromiso de la clave privada de una TSU y por pérdida de calibración del reloj de un servidor de una TSU, que puedan haber afectado a sellos de tiempo emitidos.

En caso de producirse alguno de estos incidentes de seguridad, el Consorci AOC proporcionará a los Suscriptores y Terceros que confían información que puede ser utilizada para identificar los sellos de tiempo que puedan haber sido afectados.

2.12. Cese de actividad

El Consorci AOC cuenta con un Plan de Cese donde se establecen las acciones a realizar para el cese de la actividad de los servicios de sellado de tiempo, incluyendo la revocación de todos

los certificados vigentes y la destrucción de todas las claves privadas de las TSU de los servicios, tanto los actuales, en estado activo, como los anteriores, en estado desactivado (los certificados anteriores en estado terminado no están vigentes, y las claves privadas anteriores en estado terminado ya han sido destruidas).

El cese de los servicios se comunicará previamente a los Suscriptores y todas las partes interesadas con las que el Consorci AOC tenga acuerdos u otro tipo de relaciones, en el caso del servicio de sellado cualificado de tiempo, con la antelación mínima legalmente requerida.

3. Controles de seguridad física, de procedimientos y de personal

3.1. Controles de seguridad física

Las instalaciones que albergan la infraestructura de los servicios de sellado de tiempo gestionada por el proveedor tecnológico están sujetas a las validaciones anuales de la norma UNE-ISO/IEC 27001, la cual regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

3.1.1. Situación y características del CPD

La infraestructura de los servicios de sellado de tiempo gestionada por el proveedor tecnológico se encuentra ubicada en dos centros de datos (CPD) que garantizan la disponibilidad 24x7 de los sistemas de comunicación y la disponibilidad de los sistemas de los servicios.

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

3.1.2. Control de acceso físico

Los CPD cuentan con las siguientes medidas de seguridad física:

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

3.1.3. Alimentación eléctrica y climatización

Los CPD cuentan con servicios de energía de alta disponibilidad con las siguientes infraestructuras:

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

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

3.1.4. Exposición al agua

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

3.1.5. Protección y prevención de incendios

El sistema de extinción de incendios de los CPD cubre salas técnicas e instalaciones críticas:

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

3.1.6. **Media storage**

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

3.1.7. **Eliminación de los soportes de información**

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

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para su posterior destrucción controlada.
- Medios de almacenamiento: antes de ser desechados o reutilizados, deben ser procesados para asegurar que la información contenida ha sido eliminada de forma segura.

3.1.8. **Off-site backup**

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

3.2. **Controles de procedimientos**

3.2.1. Roles de confianza

En la siguiente tabla se indican los roles de confianza de los servicios de sellado de tiempo bajo esta DP, conforme a lo especificado en el estándar ETSI EN 319 401:

ROL DE CONFIANZA	DESCRIPCIÓN
Responsables de Seguridad (*Security Officers*)	Responsables generales de administrar la aplicación de las prácticas de seguridad.
Administradores de Sistemas (*System Administrators*)	Autorizados para instalar, configurar y mantener los sistemas de confianza del PSC para la gestión de los servicios. Esto incluye la recuperación del sistema.
Operadores de Sistemas (*System Operators*)	Responsables de operar los sistemas de confianza del TSP en el día a día. Autorizados para realizar copias de seguridad del sistema.
Auditores de Sistemas (*System Auditors*)	Autorizados para ver los archivos y los registros de auditoría (*logs*) de los sistemas de confianza del TSP.

3.2.2. Número de personas requeridas por tarea

Se requieren al menos dos personas para la ejecución de las tareas de cada rol de confianza clasificadas como críticas para los servicios de sellado de tiempo bajo esta DP, como las tareas relativas a los dispositivos criptográficos (HSM) donde se generan y se usan las claves privadas de los servicios.

3.2.3. Identificación y autentificación para cada rol

Cada rol tiene asignada una o varias personas, en su caso, designadas por la dirección del Consorci AOC o del proveedor tecnológico.

Cada persona sólo 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 elementos como nombre de usuario y contraseña, certificado, doble factor de autenticación, tarjetas y/o llaves.

3.2.4. Roles que requieren separación de funciones

El rol de confianza Responsables de Seguridad no puede ser ejercido por las mismas personas que ejercen cualquier otro rol de confianza.

3.3. **Controles de Personal**

El personal afectado por lo establecido en esta sección es el asignado a los roles de confianza por el Consorci AOC y el proveedor tecnológico.

3.3.1. Requisitos de cualificación, experiencia, y autorización

La TSA se asegura de que el personal designado es confiable y tiene la cualificación y experiencia necesarias para la prestación de los servicios ofrecidos y, en particular, que tiene conocimientos mínimos en materia de seguridad y gestión. Lo anterior se requiere sin perjuicio de la posibilidad de que la TSA pueda suplir los requisitos de cualificación y experiencia mediante formación y entrenamiento apropiados.

3.3.2. Procedimientos de comprobación de antecedentes

La TSA podrá solicitar certificados que acrediten la no existencia de antecedentes penales para sus empleados siempre que la norma aplicable lo permita.

3.3.3. Requisitos de formación

Para las nuevas incorporaciones, los responsables de área o del servicio en cuestión, además de la formación técnica específica de su puesto, deben asegurarse de que conocen las practicas, las políticas, los procedimientos y los requisitos en materia de seguridad de la información y operaciones de su puesto, conociendo las consecuencias de una desviación de los procedimientos establecidos. Se facilitarán los documentos formativos e informativos en el momento de la incorporación inicial y cada vez que estos se modifiquen.

Los roles de confianza Administradores de Sistemas que realizan tareas relativas a los dispositivos criptográficos (HSM) requieren de una formación especial en la operación de los HSM.

3.3.4. Requisitos y frecuencia de la actualización de la formación

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

3.3.5. Sanciones por acciones no autorizadas

El proceso disciplinario está especificado en el procedimiento interno de la TSA basado en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, que aplicará para depurar responsabilidades derivadas de acciones no autorizadas.

3.3.6. Requerimientos de contratación independientes

La contratación de personal a través de una tercera empresa cumplirá con los requisitos establecidos en esta DP y en los procedimientos internos del proveedor tecnológico. El Consorci AOC es responsable, en todo caso, de la efectiva ejecución.

Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios por el tercero diferente del proveedor tecnológico.

3.3.7. Documentación proporcionada al personal

La TSA suministrará al personal la documentación general de los servicios y específica del puesto de trabajo a desempeñar (manuales de operación, procedimientos técnicos o de programación, procedimientos de soporte, etc.) con el fin de que pueda desarrollar de forma competente sus funciones.

4. Legislación aplicable

El Consorci AOC establece en sus instrumentos jurídicos con sus suscriptores y verificadores que la ley aplicable a la prestación del servicio, incluyendo esta DP, es la siguiente:

- Ley 29/2010, de 3 de agosto, de uso de los medios eletrónicos en el sector público de Cataluña.
- Ley 26/2010, de 3 de agosto, de régimen jurídico y procedimiento de las administracions públicas de Cataluña.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) nº 1093/2010 y se deroga la Directiva 2007/64/CE.
- Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de

creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguro.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- El Marc Normatiu de Seguretat de la Informació de l'Agència de Ciberseguretat de Catalunya en el ámbito de la Generalitat de Catalunya que determina las líneas estratégicas, políticas, estándares y guías de seguridad propias de la Generalitat de Catalunya, con carácter supletorio a falta de uno propio.
- Política de Seguridad del Consorci AOC.

5. Resto de requisitos

En lo que no está especificado en este documento, los servicios de sellado de tiempo bajo esta DP se rigen por lo especificado en los documentos "Declaración de Prácticas de Certificación (DPC) Autoridad de Certificación del Consorci AOC", "Política de Certificación para Dispositivos e Infraestructuras Consorci AOC" y "Descripción de los perfiles de Certificados Consorci AOC" publicados en la página web https://epscd.aoc.cat/ca/index.html#politiques, en lo que no sea aplicable exclusivamente a los servicios de expedición de certificados del Consorci AOC, y en lo que sea aplicable a los certificados de los servicios de sellado de tiempo del Consorci AOC (ver OID políticas de certificados en punto 1.2).