Política de Servicio de Sellado de Tiempo Cualificado

02/02/2024*: v1.1*

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	víntegris SEGURIDAD DE LA INFORMACIÓN
Versión:	1.1
Fecha edición:	02/02/2024
Fichero:	Víntegris_Política_del_Servicio_de_Sellado_de_Tiempo_v1.1.docx
Formato:	Office 365
Autores:	Víntegris

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: VH Fecha: 02/02/2024	Nombre: RR Fecha: 02/02/2024	Nombre: VH Fecha: 02/02/2024

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento.		22/01/2023
1.1	Todo	Revisión general y de estilo	VH/RR	02/02/2024
	1.2.1, 1.5.1, 6	Eliminación de la TSA nebulaSUITE		

Índice

1 Introducción

1.1 Resumen

Este documento declara la política de sellado de tiempo cualificado de VinCAsign, la Entidad de Certificación de Víntegris.

Víntegris es un Prestador de Servicios de Confianza Cualificado conforme al Reglamento (UE) del Parlamento 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 (Reglamento eIDAS) y se encuentra cualificado para la prestación del servicio de sellado de tiempo, cumpliendo con los requisitos establecidos en el artículo 42 del mencionado Reglamento eIDAS.

- Esta política de la autoridad de sellado de tiempo (TSA) de Víntegris es conforme a los estándares técnicos definidos en ETSI, concretamente los siguientes: ETSI EN 319 401 V2.3.1 (2021-05) *"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*"; ETSI EN 319 421 v1.1.1 (2016-06) *"Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps "*; ETSI EN 319 422 v1.1.1 (2016-03) *"Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".* Así como, por la recomendación definida en el RFC-3628 *"Policy Requirements for time-stamping authorities".*
- Esta Política matiza y complementa a la Declaración de Prácticas de Certificación (DPC) de Víntegris.

1.2 Nombre e identificación del documento

Este documento es la "Política de Sellado de Tiempo Cualificado de VinCAsign".

Nombre del documento	POLITICA DE SELLADO DE TIEMPO CUALIFICADO
Versión	1.1
Fecha de emisión de la versión actual	02/02/2024

Localización	BARCELONA
OID	1.3.6.1.4.1.**47155.0.3.0**

1.2.1 Identificadores de certificados (OIDs)

La política de sellos cualificados de tiempo electrónico admitida es la correspondiente a la definida en la norma ETSI 319 421: "*Best Practices Pólice for Time-Stamp (BTSP)*", cuyo OID es: **0.4.0.2023.1.1**

Los sellos de tiempo electrónico declarados como cualificados siguen las indicaciones del Reglamento UE 910/2014 y el certificado de la TSA es expedido bajo la política declarada en ETSI EN 319 411-2.

VinCAsign ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

OID	Tipo de certificado
1.3.6.1.4.1.47155.2.9.1	Certificados corporativos de Sello de tiempo electrónico – CA TrustServices

En caso de contradicción entre este Documento de Política del Servicio de Confianza y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Política.

1.3 Definiciones

Para los propósitos del presente documento, se aplican los siguientes términos y definiciones:

Autoridad de Sellado de Tiempo (TSA): Sistema de emisión y gestión de sellos de tiempo llevado a cabo por un Prestador de Servicios de Confianza autorizado.

Declaración de divulgación de la TSA: Conjunto e declaraciones sobre las políticas y prácticas de una TSA que requieren especialmente énfasis o divulgación a los suscriptores y a las partes usuarias, por ejemplo, para cumplir los requisitos reglamentarios.

Declaración de Prácticas de los servicios electrónicos de confianza (DPC): políticas y prácticas de un Prestador de Servicios Electronicos de Confianza, especialmente orientado a suscriptores y terceras partes.

Política de sello de tiempo: Conjunto de reglas que indica la aplicabilidad de un sello de tiempo a una comunidad y/o clase de aplicación con requisitos de seguridad comunes.

Subscriptor: Persona física o jurídica que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo de Víntegris y que está vinculada por las obligaciones del suscriptor.

Sellos de tiempo: Datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

Tiempo Universal Coordinado (UTC): Tiempo solar en el meridiano principal (0º). La escala de tiempo está basada en el segundo, según se define en ETSI TS 102.023 y en UIT-RTF.460-6 [1].

Unidad de Sellado de Tiempo (TSU): Conjunto de hardware y software que se gestiona como una unidad y tiene una única clave de sellado de tiempo y una clave de firma activa en un momento dado.

UTC(k): Escala de tiempo realizada por un laboratorio "k" de acuerdo con UTC, con el objetivo de conseguir una desviación máxima de +-100ns.

1.4 Abreviaturas

CEN: Comité Europeo de Normalización

CRL: Certificate Revocation List

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standards Institut

IETF: Internet Engineering Task Force

FIPS: Federal Information Processing Standards

GPS: Global Positioning System

HSM: Hardware Security Module

RFC: Request for comment

TSA: Autoridad de Sellado de Tiempo

TSQ: Solicitud de sello de tiempo

TSS: Servicio de sellado de tiempo

TST: Token de sello de tiempo

UTC: Universal Time Coordinated

1.5 Participantes en los servicios de sello de tiempo

1.5.1 Prestador del servicio de sellado de tiempo (TSA)

Víntegris es un prestador de servicios de confianza conforme al Reglamento UE eIDAS, y el estándar técnico ETSI EN 319 401, que emite sellos de tiempo.

La TSA de Víntegris ha sido desplegada en sus propias infraestructuras y en caso de tercerizar el servicio o alguna de sus operaciones críticas, la TSA de Víntegris asume la responsabilidad sobre su provisión conforme se indica en esta Política y en la DPC

Los servicios de sellado cualificado de tiempo electrónico son emitidos por las siguientes jerarquías de certificación de VÍNTEGRIS:

- CA Víntegris ROOT TrustServices (1.3.6.1.4.1.47155.2.9.1)

Siendo los certificados de TSU emitidos, los señalados a continuación:

- CA Víntegris TSA1 TrustServices

CN	CA Víntegris TSA1 TrustServices
Huella digital	B0 15 74 43 78 43 A8 0A C0 0C D5 35 A8 31 0D E6 56 1E 37 03
Válido desde	2022-03-08 12:27:58 CET
Válido hasta	2027-03-07 12:27:58 CET
Longitud de clave RSA	4096 bits

- CA Víntegris TSA2 TrustServices

CN	CA Víntegris TSA2 TrustServices
Huella digital	4D 27 C6 70 69 05 8B 6D 68 DA 4C 82 D8 A7 1F A2 F8 A2 84 8C
Válido desde	2022-03-03 16:12:33 CET
Válido hasta	2027-03-02 16:12:33 CET
Longitud de clave RSA	4096 bits

Para más información acerca de las jerarquías de certificación y las Entidades de Certificación de VÍNTEGRIS, se remite al lector a la Declaración de Prácticas de Certificación y, a la Política de Divulgación de los servicios de sellado de tiempo, ambos documentos disponibles en:

https://www.VinCAsign.net

Las características del sello de tiempo son las siguientes:

- Las unidades de sellado de tiempo (TSU) que dan soporte a las autoridades de sellado de tiempo de VinCAsign disponen de claves generadas según lo especificado en la DPC y se encuentran almacenadas en dispositivos en HSM de Primekey “SignServer” cumpliendo con los requisitos del perfil de protección EN 419 221-5 o FIPS 140-2 L3.
- Los sellos de tiempo emitidos por el Servicio de Sellado de Tiempo de VinCAsign son conforme a la norma ETSI EN 319 422 (Apartado 5.2).
- Algoritmos de hash aceptados: SHA256, SHA512
- OID de Política: ver apartado Tipo y finalidad del servicio de sellado cualificado de tiempo electrónico.
- qcStatements: esi4-qtstStatement-1 (sello de tiempo cualificado)
- La TSU emite sellos de tiempo, en referencia a UTC (tiempo universal coordinado) con una precisión mínima de 1 segundo.

- Las unidades de sello de tiempo (TSU) de Víntegris se utilizan para generar sellos de tiempo seguros, a solicitud de los usuarios del servicio (suscriptores o terceras partes), para garantizar la existencia de un documento, en un tiempo concreto; también para proteger una firma electrónica de larga duración, código ejecutable y transacciones realizadas en servicios electrónicos ofrecidos telemáticamente.

1.5.2 Disponibilidad del servicio

El servicio de sellado de tiempo se ofrece en modalidad 24x7 de manera autenticada, sobre el servicio de nebulaSUITE.

El servicio acepta peticiones basadas en el protocolo de sellado de tiempo especificado por el estándar RFC 3161[1].

1.5.3 Usuarios del servicio

Los usuarios del servicio de sello de tiempo son suscriptores y terceras partes que requieran el servicio.

1.5.4 Suscriptores del servicio de sello de tiempo

El Suscriptor es la persona física o jurídica que ha contratado los servicios de sellado de tiempo electrónico de VinCAsign.

1.5.5 Obligaciones de los suscriptores

El suscriptor se obliga a:

- Realizar las solicitudes de sellos cualificados de tiempo electrónico de acuerdo con el procedimiento establecido en esta Política y, si es necesario, los componentes técnicos suministrados por VinCAsign, de conformidad con lo que se establece en esta Política, en la Declaración de Prácticas de Confianza (DPC) y en la documentación de VinCAsign.
- Verificar las firmas electrónicas de los sellos de tiempos electrónicos, incluyendo la validez del certificado usado.

[1] Accesible en https://www.ietf.org/rfc/rfc3161.txt

- Usar los sellos de tiempo electrónicos dentro de los límites y el ámbito descritos en esta Política y en la Declaración de Prácticas.

1.5.6 Terceros que confían en los sellos de tiempo emitidos

Los terceros que confían en los sellos de tiempo de Víntegris deberían ser capaces de comprobar los sellos de tiempo y los certificados que los acompañan. Las TSA solo emiten sellos de tiempo mientras el certificado está vigente y si fuera preciso revocarlo, se deja de usar la clave privada asociada. Aunque no se prevé que pueda quedar expuesta la clave privada, la consulta de la revocación de certificado permite descartar cualquier riesgo en ese sentido.

Los terceros que confían se comprometen a cumplir los requisitos técnicos, operativos y de seguridad descritos en esta Política y en la DPC de VinCAsign.

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC y esta Política.

Si el verificador confía en una firma electrónica correspondiente a un sello cualificado de tiempo electrónico no verificada, asumirá todos los riesgos derivados de esta actuación.

1.6 Uso de los sellos

Esta sección lista las aplicaciones para las que puede emplearse los sellos de tiempo y establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones.

1.6.1 Usos permitidos para los sellos de tiempo

Los sellos de tiempo se podrán solicitar para cualquier tipo de documento, firmado o no electrónicamente, y para cualquier tipo de objeto digital, incluso código ejecutable, garantizándose la existencia de dichos contenidos a la fecha indicada dentro del sello.

1.6.2 Límites y usos prohibidos de los sellos de tiempo

Los sellos de tiempo electrónico limitan su uso en las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

No se utilizarán los sellos de tiempo electrónico para fines distintos de los especificados anteriormente.

El empleo de los sellos de tiempo en operaciones que contravienen esta Política, la Declaración de Prácticas (DPC) y la política de Divulgación para el servicio de sellado de tiempo (PDS), o los contratos de servicio suscritos, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a VinCAsign, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los sellos de tiempo que realice el suscriptor o cualquier tercero.

VinCAsign no tiene acceso a los datos sobre los que se puede aplicar el uso de un sello de tiempo. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de VinCAsign emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un sello de tiempo.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta política, la DPC, la PDS, o los contratos o convenios suscritos, 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.

El suscriptor y los terceros que confían se obligan a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de VinCAsign, sin previo consentimiento escrito.

Adicionalmente, se obligan a no comprometer intencionadamente la seguridad de los servicios públicos de sellado de tiempo de VinCAsign.

Los servicios de sellado cualificado de tiempo electrónico prestados por VinCAsign no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

1.7 Obligaciones de VINCASIGN

En relación con la prestación del servicio de sellado cualificado de tiempo electrónico VinCAsign se obliga a:

a) Emitir, entregar y administrar los sellos cualificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de VinCAsign.

b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.

c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.

1.8 Organización que administra el documento

VÍNTEGRIS SLU (VinCAsign)

Carrer Pallars, 99

Planta 3, Oficina 33

08018 Barcelona

Tel.: (+34) 934 329 098

Fax. +34 934 329 344

1.7.1 Datos de contacto de la organización

VÍNTEGRIS SLU (VinCAsign)

Carrer Pallars, 99

Planta 3, Oficina 33

08018 Barcelona

Tel.: (+34) 934 329 098

Fax. +34 934 329 344

Quejas y sugerencias y compromiso de clave o uso indebido del certificado:

- Teléfono +34 93 432 90 98,
- email: info@VinCAsign.net
- Formulario en https://www.VinCAsign.net/ (apartado de “Ayuda”)

1.7.2 Persona que determina la idoneidad de la política de Sello de Tiempo

Esta Política será revisada y actualizada anualmente por VinCAsign. para su revisión se tendrá en cuenta lo establecido en la Declaración de Prácticas de Certificación y otros documentos internos relacionados.

VinCAsign dispone de uno o varios depósitos de sellos, en el que se publican las informaciones relativas a los servicios de sellado electrónico de tiempo.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de VinCAsign, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 4.7.2 de la Declaración de Prácticas de Confianza.

2 Publicación de información y repositorios

2.1 Depósito de sellos

VinCAsign dispone, por medio del conjunto de las soluciones tecnológicas que implementa o que desarrolla, de un depósito de información sobre los sellos de tiempo y la documentación asociada a su operación y emisión.

2.2 Publicación de información de sellos de tiempo

VinCAsign publica las siguientes informaciones, en su Depósito:

- Los sellos emitidos a solicitud del suscriptor.
- Los certificados de Entidades de Sellado de Tiempo
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados, correspondientes a las Entidades de Sellado de Tiempo propias.
- La política de sellado de tiempo
- La Declaración de Prácticas de Servicios de Confianza a los servicios de sellado
- Los textos de divulgación (PKI Disclosure Statements - PDS), como mínimo en lengua inglesa.
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en sellos de tiempo
- Las modificaciones de los documentos anteriormente indicados

2.3 Frecuencia de publicación

La información del prestador de servicios de sellado de tiempo, incluyendo los textos de divulgación (PDS), la Declaración de Prácticas de Confianza y la actualización de esta política, se publican en cuanto se encuentran disponibles.

Los cambios en los documentos de referencia se regirán por lo establecido en esta Política y en la Declaración de Prácticas de Certificación.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de la Declaración de Prácticas de Confianza.

2.4 Control de acceso a los repositorios

Conforme se estipula en la Declaración de Prácticas de Confianza de VinCAsign.

3 Procedimiento de solicitud de sello de tiempo

El suscriptor del servicio solicita a VinCAsign el servicio de sellado de tiempo de su interés.

Las partes suscribirán un contrato de términos condiciones del servicio. VinCAsign se compromete a ofrecer la información de términos y condiciones en soporte duradero, en papel o electrónicamente y con un lenguaje comprensible.

Una vez suscrito por ambas partes el acuerdo de referencia, VinCAsign habilitará los medios técnicos para recibir solicitudes de sello. VinCAsign soportará protocolos de transporte (RFC 3161, sección 3) de las solicitudes de sellado de tiempo que sean síncronos o asíncronos, y entre ellos, al menos dispondrá de la posibilidad de solicitar el servicio empleando HTTP.

Tras la verificación de la solicitud se procederá a la emisión del sello de tiempo, de forma segura. VinCAsign deberá:

- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.
- Emplear fuentes de tiempo fiables, de acuerdo con los requisitos establecidos en la sección correspondiente de esta política.
- Generar sellos de tiempo conteniendo las informaciones incluidas en esta política.
- Emplear una clave específica para la firma de los sellos generados, de acuerdo con los requisitos de gestión de claves especificados en esta política.

VinCAsign deberá entregar el sello al suscriptor, mediante el protocolo de transporte empleado para la solicitud. La respuesta protocolaria deberá contener el resultado de la solicitud y, en su caso, el sello emitido (RFC 3161, sección 2.4.2).

4 Controles de seguridad física, de gestión y de operaciones

Conforme se estipula en la Declaración de Prácticas de Confianza de VinCAsign.

4.1 Controles de seguridad física

Conforme se estipula en la DPC de VinCAsign.

4.2 Controles de procedimientos

Conforme se estipula en la DPC de VinCAsign.

4.3 Controles de personal

Conforme se estipula en la DPC de VinCAsign.

4.4 Procedimientos de auditoría de seguridad

Conforme se estipula en la DPC de VinCAsign.

4.5 Archivos de registros

Conforme se estipula en la DPC de VinCAsign.

4.6 Cambio de claves

Conforme se estipula en la DPC de VinCAsign.

4.7 Compromiso de claves y recuperación de desastre

Conforme se estipula en la DPC de VinCAsign.

4.7.1 Procedimiento ante el compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de VinCAsign, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación y desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Sellado de Tiempo (TSA).

En caso de compromiso de la clave privada de la TSA, VinCAsign:

1. Desactivar el uso de la clave privada de la entidad de sellado de tiempo.
2. Informará del compromiso de clave a sus suscriptores, usuarios y otras TSA´s con los cuales tenga acuerdos u otro tipo de relación. Dicha información podrá hacerse mediante la publicación de un aviso en su página web https://www.VinCAsign.net/.
3. Deberá indicar que los sellos de tiempo generados usando la clave de la entidad de sellado de tiempo comprometida, ya no son válidos.
4. Deberá notificar al Órgano de Supervisión Nacional en un plazo de 24 horas tras tener conocimiento del compromiso.

VinCAsign ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario en un centro de datos alternativo.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratará los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la TSA para implementar dichos procesos.

4.7.2 Continuidad del negocio después de un desastre

Conforme se estipula en la DPC de VinCAsign.

4.8 Terminación del servicio

Conforme se estipula en la DPC de VinCAsign.

5 Controles de seguridad técnica

VinCAsign emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de sellado de tiempo a los que sirven de soporte. Asimismo, se comprometa al empleo de fuentes de tiempo fiables que garanticen la precisión del sello.

5.1 Fiabilidad de la fuente de tiempo.

VinCAsign dispone de su propia fuente de tiempo, es un NTP Stratum 1 en las instalaciones del CPD de ATLASEdge Barcelona. (Modelo Meinberg LANTIME M200/GPS) con el que sincroniza todos sus servicios.

Además, VinCAsign tiene un procedimiento de sincronización de tiempo coordinado con el ROA Real Instituto y Observatorio de la Armada en San Fernando (Cádiz), a través de la Sección de Hora, que resulta accesible mediante el servicio NTP, conforme al RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification.

Este organismo tiene entre sus misiones la del mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala de “Tiempo Universal Coordinado”, considerada a todos los efectos como la base de la hora legal en todo el territorio nacional, según el Real Decreto 1308/1992, de 23 de octubre.

Todos los sistemas que constituyen la infraestructura de la TSA de VinCAsign están sincronizados en fecha y hora.

Se prevé el uso de certificados cualificados. La validez de los certificados cualificados orientados al sellado de tiempo se establece en los propios certificados.

- La calibración de los relojes debe ser mantenida de forma que no resulte previsible un desplazamiento en el tiempo de los mismos.
- Los relojes serán protegidos contra amenazas que pudieran resultar en un cambio no detectado que descalibre el reloj.
- Se asegurará que se detectarán los desplazamientos y saltos del reloj, que impidan su sincronización con Tiempo Universal Coordinado.
- Se asegurará que se mantiene la sincronización del reloj cuando se notifica un segundo de salto, notificado por el órgano competente.

5.1.1 Generación del par de claves

La generación de las claves de firma de la TSA de VinCAsign se lleva a cabo en un entorno físicamente seguro, por personal designado con roles de confianza, bajo al menos, control dual. El personal de referencia se limita a aquellos requeridos para hacerlo.

La generación de las claves de firma de la TSA se lleva a cabo empleando hardware criptográfico que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 parte 2, según proceda, o de acuerdo con un objetivo de seguridad o perfil de protección equivalente; o FIPS 140-2 Nivel 3 (o superior).

La longitud de las claves de las Entidades de Sellado de Tiempo será de 4096 bits.

5.1.2 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1 de la Declaración de Prácticas.

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

Conforme se estipula en la DPC de VinCAsign.

5.2.1 Estándares y normas de los módulos criptográficos

En relación a los módulos que gestionan las claves de VinCAsign y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

5.2.2 Control multipersonal (n de m) de la clave privada

Conforme se estipula en la DPC de VinCAsign.

5.2.3 Depósito de la clave privada

Conforme se estipula en la DPC de VinCAsign.

5.2.4 Copia de respaldo de la clave privada

Conforme se estipula en la DPC de VinCAsign.

5.2.5 Archivo de la clave privada

Conforme se estipula en la DPC de VinCAsign.

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

Las claves privadas de los componentes internos de VinCAsign se generan directamente en los módulos criptográficos de producción de VinCAsign.

5.2.7 Método de desactivación de la clave privada

Conforme se estipula en la DPC de VinCAsign.

5.3 Otros aspectos de gestión del par de claves

5.3.1 Archivo de la clave pública

Conforme se estipula en la DPC de VinCAsign.

5.4 Controles de seguridad informática

Conforme se estipula en la DPC de VinCAsign.

5.5 Controles técnicos del ciclo de vida

Conforme se estipula en la DPC de VinCAsign.

5.5.1 Controles de seguridad del ciclo de vida

Según lo previsto en el apartado 6.6 de la declaración de prácticas de certificación.

5.6 Controles de seguridad de red

Conforme se estipula en la DPC de VinCAsign.

6 Perfiles de Certificados de Sellos de Tiempo

Los sellos de tiempo electrónico declarados como cualificados siguen las indicaciones del Reglamento UE 910/2014 y el certificado de la TSA es expedido bajo la política declarada en ETSI EN 319 411-2.

Los certificados de sello electrónico de TSA/TSU son cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Estos certificados funcionan con el OID 1.3.6.1.4.1.47155.2.9.1 (Jerarquía CA Víntegris ROOT TrustServices).

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo cualificado (QSCD). La información de usos en el perfil de certificado indica lo siguiente:

a. El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

   a. Content Commitment

b. El campo “extend key usage” tiene activada la función:

b. TimeStamping

c. En el campo “Qualified Certificate Statements” aparece la siguiente declaración:

c. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

d. El campo “User Notice” describe el uso de este certificado.

Los sellos tendrán el contenido y campos ajustados a las siguientes normas:

- ETSI EN 319 422 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- IETF RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).

- XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0. OASIS Standard. 11 April 2007.

Más detalles en los documentos de perfiles que son accesibles desde la página web de VinCAsign (https://www.VinCAsign.net).

7 Requisitos comerciales y legales

7.1 Tarifas y Política de reintegro

Conforme se estipula en la DPC de VinCAsign.

7.2 Capacidad financiera

Conforme se estipula en la DPC de VinCAsign.

7.3 Confidencialidad

Conforme se estipula en la DPC de VinCAsign.

7.4 Protección de datos personales

Conforme se estipula en la DPC de VinCAsign.

7.5 Derechos de propiedad intelectual

Conforme se estipula en la DPC de VinCAsign.

7.6 Declaraciones y garantías

7.6.1 Declaraciones y garantías de VinCAsign

VinCAsign garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

VinCAsign presta los servicios de sellado de tiempo conforme a lo establecido en esta Política, en la Declaración de Prácticas de Confianza y en el texto de divulgación del servicio de sellado de tiempo (PDS).

Con anterioridad de la prestación del servicio de sellado de tiempo al suscriptor, VinCAsign informa al suscriptor de los términos y condiciones, de su precio y de sus limitaciones, mediante un contrato de suscriptor.

Este requisito de información también se cumple mediante un documento PDS[2], también denominado texto de divulgación, que incorpora sigue la estructura definida en el Anexo B de la norma ETSI EN 319 421-1 V1.1.1 (2016-03), documento que puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

VinCAsign comunica de forma permanente los cambios[3] que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web a suscriptores, poseedores de claves y terceros que confían en sus servicios de sellado de tiempo mediante dicho PDS, en lenguaje escrito y comprensible,

7.7 Renuncias a las garantías

Conforme se estipula en esta Política y en la DPC de VinCAsign.

7.8 Limitaciones de responsabilidad

VinCAsign limita su responsabilidad a la generación de sellos de tiempo electrónicos a partir de su Autoridad de Sellado de Tiempo conforme ha expresado en esta Política y en la DPC, y puede rechazar todas las garantías que no estén vinculadas a obligaciones derivadas de la normativa vigente (actualmente la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento eIDAS)

7.9 Indemnizaciones

Conforme se estipula en la DPC de VinCAsign.

[2] Anexo B ETSI EN 319 421 V1.1.1 (2016-03).

7.10 Duración y terminación

7.10.1 Duración

Esta Política entrará en vigor en el momento de su publicación.

7.10.2 Terminación

La presente Política de Sello de Tiempo será derogada en el momento que una nueva versión del documento sea publicada.

La nueva versión sustituirá íntegramente el documento anterior.

7.10.3 Efecto de la terminación y supervivencia

Conforme se estipula en la DPC de VinCAsign.

7.11 Avisos y comunicaciones individuales con los participantes

Conforme se estipula en la DPC de VinCAsign.

7.12 Modificaciones

7.12.1 Procedimiento de modificación

Conforme se estipula en la DPC de VinCAsign.

7.12.2 Mecanismo y plazo de notificación

En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos o modificaciones mutuamente.

7.12.3 Circunstancias en las que debe modificarse la OID

Sin estipulación.

7.13 Disposiciones para la resolución de litigios

Conforme se estipula en la DPC de VinCAsign.

7.14 Legislación aplicable

La TSA establece, en el contrato de suscriptor y en el PDS, que la legislación aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

VinCAsign asume la aplicación de la normativa siguiente:

- Reglamento (UE) No 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 999/93/CE (Reglamento eIDAS)
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- 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
- 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
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD GDD).

7.15 Miscelanea

7.15.1 Acuerdo completo

VinCAsign establece, en el contrato de suscriptor, y en el PDS la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

7.15.2 Cesión

Sin estipulación.

7.15.3 Divisibilidad

VinCAsign establece, en el contrato de suscriptor, y en el PDS la cláusula de divisibilidad, en virtud de la cual la invalidez de una cláusula no afectará al resto del contrato.

7.15.4 Ejecución (honorarios de abogados y renuncia de derechos)

Sin estipulación.

7.15.5 Fuerza mayor

VinCAsign establece, en el contrato de suscriptor, y en el PDS cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

7.16 Otras disposiciones

Sin estipulación.