DECLARACIÓN DE PRACTICAS DE CONFIANZA PARTICULAR DEL SERVICIO DE SELLADO DE TIEMPO (TSA)

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA
Fecha: 2026.10.30 09:49:46 +01'00'

IZENPE
Beato Tomás de Zumarraga 71 - 1ª Planta
01008 Vitoria - Gasteiz
Tel.: 945 067 723
www.izenpe.com

Control de cambios

Versión	Fecha	Cambio
1.0	19/06/2025	Aprobación del documento.
1.1	06/10/2025	Se incluye la jerarquía 2025
1.2	22/10/2026	Se refuerza la recomendación de no utilizar algoritmos inferiores a SHA256, se actualiza la configuración de los HSMs utilizados que pasa de FIPS 140-2 a Common Criteria.
1.3	27/10/2026	Se actualiza el punto 4.

Índice

1 Introducción 4
1.1 Nombre del documento e identificación 4
2 Objeto 6
3 Definiciones y acrónimos. 7
3.1 Definiciones 7
3.2 Acrónimos 7
4 Partes intervinientes 8
4.1 Autoridad de Sellado de Tiempo. 8
4.2 Suscriptor 9
4.3 Partes que confían 9
5 Obligaciones y responsabilidades. 10
5.1 De la Entidad Emisora de Sellos de Tiempo 10
5.2 Obligaciones del suscriptor de sellos de tiempo 10
5.3 Obligaciones de terceras partes verificadoras de sellos de tiempo 11
5.4 Limitaciones de uso 11
6 Requerimientos operacionales. 12
6.1 Procedimiento de emisión de un sello de tiempo. 12
6.1.1 Provisión y disponibilidad del servicio de sellado de tiempo. 12
6.1.2 Petición de un sellado de tiempo 12
6.1.3 Respuesta a una petición de sellado de tiempo 13
6.1.4 Fuente de tiempo empleada para la prestación del servicio 13
6.2 Controles criptográficos 13
6.2.1 Generación de la clave de la TSA 13
6.2.2 Tamaños de claves y algoritmos 14
6.2.3 Protección de la clave privada de la TSU 14
6.2.4 Distribución de la clave pública de la TSU 14
6.2.5 Renovación con regeneración de la clave de la TSU 14
6.2.6 Fin del ciclo de vida de la clave de la TSU 14
6.2.7 Gestión del ciclo de vida del módulo criptográfico usado para firmas los sellos de tiempo 15
6.2.8 Compromiso de la clave privada del certificado de TSA 15
6.2.9 Finalización de la TSA 15
7 Perfil de certificados 16
8 Auditorías de cumplimiento 20
9 Otros asuntos legales y de actividad. 21
9.1 Tarifas 21

1 Introducción

1. Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, Izenpe) ofrece un servicio cualificado de sellado de tiempo como parte de sus servicios como prestador cualificado de servicios de confianza. Este servicio es prestado en conformidad con el Reglamento eIDAS[1].
2. Este servicio crea y registra evidencias digitales de la existencia de un dato en un instante determinado en la línea de tiempo, de una forma fiable y de confianza, mejorando significativamente la fiabilidad de los datos electrónicos.
3. Izenpe ha creado una Autoridad de Sellado de Tiempo (en adelante: TSA) para proporcionar el servicio de sellado de tiempo.
4. Los Servicios de sellado de tiempo incluyen dos componentes:
   - Provisión de sellos de tiempo: componente técnico encargado de generar los tokens de sello de tiempo
   - Administración sellos de tiempo: componente del servicio que monitoriza y controla la operación de los servicios de sellado de tiempo. La gestión de sellado de tiempo garantiza que los relojes utilizados en el sellado de tiempo están correctamente sincronizados con UTC.
5. Esta declaración de prácticas se basa en la norma ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps -, y los perfiles son de acuerdo con la norma ETSI EN 319 422 “Time-stamping protocol and time-stamp token profiles”.
6. Los procedimientos definidos y su correcta implementación son auditados por una entidad externa, según las especificaciones definidas por ETSI a través de la norma EN 319 421.

1.1 Nombre del documento e identificación

7. El presente documento se denomina “Declaración de prácticas de confianza particular para la Autoridad de Sellado de Tiempo (TSA)”, y se identifica a través de siguiente OID: 1.3.6.1.4.1.14777.10.1 y 1.3.6.1.4.1.14777.53.1.3

Nombre	Declaración de prácticas de confianza particular para la Autoridad de Sellado de Tiempo (TSA)
Identificador OID	1.3.6.1.4.1.14777.10.1

[1] 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

Identificador OID	1.3.6.1.4.1.14777.53.1.3

2 Objeto

8. Esta Declaración de Prácticas de sellado de tiempo (en adelante: DP de TSA):
    - Concreta los procesos utilizados para proporcionar los servicios de sellado de tiempo, extendiendo los procesos descritos en la DPC global de IZENPE.
    - Define las prácticas operacionales de gestión de TSA para que los suscriptores y terceros de confianza puedan evaluar la fiabilidad de los servicios de sellado de tiempo;
    - Define los aspectos de deben ser cumplidos por las partes participantes (TSA, suscriptor y partes que confían).
    - Incluyen las reglas y procesos que aplica la TSA cuando genera un token de sello de tiempo.
    - Se enfoca a procesos y políticas específicas. Detalles técnicos como la estructura organizativa, procedimientos operativos, e infraestructura de comunicaciones están especificados en la Declaración de Prácticas de Certificación (en adelante: DPC) general o en documentos internos. Los documentos internos no están disponibles al público.
    - Contiene prácticas conformes a las disposiciones del Reglamento eIDAS. Los servicios de sellado de tiempo de Izenpe pueden aplicarse a una firma electrónica o a cualquier aplicación que requiera una evidencia de la existencia de datos digitales en un punto particular en el tiempo. Estos requisitos de la política están basados en criptografía de clave pública, certificados de clave pública (X.509) y fuentes de tiempo fiables.
9. El presente documento, junto a la DPCG de Izenpe, puede ser utilizado por organismos independientes para evaluar la fiabilidad de esta TSA y sus servicios de sellado de tiempo.

3 Definiciones y acrónimos.

3.1 Definiciones

10. Esta declaración de prácticas referencia las definiciones y acrónimos usados en la Declaración de Prácticas de Certificación, además de los siguientes:

- Autoridad de Sellado de Tiempo (TSA): autoridad que emite tokens de sello de tiempo
- Terceras partes usuarias**:** usuario que confía en un sello de tiempo proporcionado por Izenpe
- Suscriptor**:** persona que utiliza los servicios proporcionados por la TSA y que acepta de forma explícita los términos y condiciones
- Declaración de prácticas de sellado de tiempo**:** reglas que aplican a la TSA cuando se genera un token de sello de tiempo
- Token de sello de tiempo**:** objeto de datos que relaciona la existencia de unos datos digitales a un momento concreto. Sirve como evidencia de que un dato existió en un instante determinado en la línea de tiempo.
- Unidad de sellado de tiempo**:** componentes hardware y software gestionados como una unidad que proporciona tokens de sello de tiempo desde una única fuente de tiempo. Los componentes pueden ser clonados o implementados en redundancia para conseguir alta disponibilidad
- Declaración de Prácticas de la TSA**:** políticas y prácticas de una TSA, especialmente orientado a suscriptores y terceras partes.
- Coordinated Universal Time**:** escala de tiempo basada en el segundo como se define en la Recommendation ITU-R TF.460-1
- UTC(k): escala de tiempo realizada por un laboratorio “k” de acuerdo con UTC, con el objetivo de conseguir una desviación máxima de +-100ns.
- eIDAS: 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital.

3.2 **Acrónimos**

- TSA: Time Stamp Authority
- TSU: Time Stamp Unit
- TST: Time Stamp Token
- UTC: Coordinated Universal Time
- DPC: Declaración de Prácticas de Certificación

4 Partes intervinientes

11. Los siguientes actores participan en la provisión y uso del servicio de sellado de tiempo:

4.1 **Autoridad de Sellado de Tiempo.**

12. IZENPE es un Prestador de Servicios de Confianza (en adelante: PSC) incluido en la Lista de Servicios de Confianza (TSL) española como prestador cualificado desde la entrada en vigor del Reglamento eIDAS.

13. IZENPE es un PSC que actúa como Autoridad de Sellado de Tiempo (en adelante: TSA) y que ofrece los servicios de confianza por sí misma y por sus propios medios, sin delegarlos en ninguna otra entidad.

14. La TSA de Izenpe emite tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo (como por ejemplo suscriptores o terceras partes).

15. La TSA de Izenpe asume toda la responsabilidad sobre la provisión de los servicios de sellado de tiempo indicados en el apartado 5.1 – De la Entidad Emisora de Sellos de Tiempo – de la presente declaración. La TSA de Izenpe puede operar varias unidades identificables de sello de tiempo (TSU's), y cada TSU puede tener una clave diferente (ver apartado 8 - Perfil del certificado – de la presente declaración").

16. IZENPE dispone de la Autoridad subordinada SUBCA QC IZENPE – TSA, para la emisión de certificados TSU.

CN	tsa.izenpe.com
VALIDEZ	06/03/2024 hasta el 06/03/2029
HASH SHA256	FD:EE:56:8A:28:BF:EF:94:BD:19:AC:3F:89:1D:B8:3E:72:6B:0B:AB:18:84:BF:90:B0:FC:91:9C:84:18:62:6C
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA

17. IZENPE dispone de la Autoridad subordinada CA QC IZENPE - TSA 2025, para la emisión de certificados TSU.

CN	IZENPE TSU - 2025
VALIDEZ	16/10/2025 hasta el 16/10/2030
HASH SHA256	3E:DC:28:C0:17:47:50:2B:35:A9:69:A2:83:D2:E6:A6:5B:8B:65:9A:E8:87:A0:19:EB:2D:9B:2D:21:4B:08:FC
TIPO CLAVE	ECC 256 (ECDSA_P256)

18. Dentro de un TSU se permite clonar claves y utilizarlo en componentes redundantes para cumplir con requerimientos de alta disponibilidad.

19. La TSA de Izenpe está identificada en el certificado digital usado por los servicios de sellado de tiempo. El perfil está disponible en el apartado "Perfil del certificado de la TSA".

4.2 Suscriptor

20. El suscriptor puede ser una organización o un particular:

    - Si el suscriptor es una organización, las obligaciones que aplican a esa organización también aplican a sus usuarios finales asociados.

      La organización debe informar adecuadamente a sus usuarios finales., siendo responsable si los usuarios finales no cumplen correctamente las obligaciones.

    - Si el suscriptor es un usuario particular, el usuario final será responsable directamente del cumplimiento de las obligaciones.

4.3 Partes que confían

21. Las partes que confían son aquellos destinatarios de sellos de tiempo que confían en dichos sellos. Las obligaciones de las partes que confían se definen en el apartado 5.3 – *Obligaciones de terceras partes verificadoras de sellos de tiempo* – de la presente declaración.

5 Obligaciones y responsabilidades.

22. Izenpe, como TSA emisora de sellos de tiempo de acuerdo con la presente Declaración de prácticas de Sellado de Tiempo, asume las siguientes obligaciones.

5.1 De la Entidad Emisora de Sellos de Tiempo

23. La Autoridad de Sellado de Tiempo de Izenpe:

- Emite tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo (se incluyen tanto suscriptores como terceras partes.
- Asume la responsabilidad de proporcionar los servicios de sellado de tiempo.
- Puede operar con diferentes unidades identificables de sellado de tiempo (TSU's), cada una de las cuales puede tener su propia clave de firma.
- Está identificada en el certificado digital utilizado para los servicios de sellado de tiempo.
- Ofrece sus servicios a todos los suscriptores y terceras partes verificadoras de sellos de tiempo que se comprometan a cumplir con sus obligaciones.

24. Izenpe opera su TSA de acuerdo con la política de TSA de Izenpe, su DPC, y los términos de cualquier otro acuerdo vinculante entre Izenpe y usuarios del servicio de sellado de tiempo.

25. Izenpe asegura la precisón del tiempo electrónico y realiza esfuerzos para proporcionar alta disponibilidad en sus servicios.

26. Izenpe no es responsable en ningún caso de pérdida de beneficios, daños indirectos o consecuentes, o pérdida de datos, en la medida en que la legislación vigente lo permita.

27. Izenpe no será responsable de daños consecuencia de infracciones cometidas por el suscriptor o terceras partes en los términos y condiciones aplicables.

28. Izenpe no será bajo ninguna circunstancia responsable de daños consecuencia de eventos de fuerza mayor como desastres naturales, caídas de electricidad o telecomunicaciones, fuego, interacciones externas no predecibles como virus o ataques de hackers, acciones gubernamentales, o huelgas.

29. En cualquier caso Izenpe realizará todas las medidas razonables para mitigar los efectos de tales eventos. Cualquier daño consecuencia de un retraso causado por un evento de fuerza mayor no será cubierto por Izenpe.

5.2 Obligaciones del suscriptor de sellos de tiempo

30. El suscriptor de sellos de tiempo puede utilizar el Servicio de Sellado de Tiempo únicamente según especificaciones de ETSI EN 319 422.

31. El suscriptor debe verificar que el token de sello de tiempo ha sido correctamente firmado por la autoridad de sellado de tiempo, y que la clave privada utilizada para firmar el token de sello de tiempo no ha sido revocado.

32. El suscriptor debe cumplir con la presente Declaración de prácticas particular de Sellado de Tiempo de IZENPE, disponible en www.izenpe.eus

5.3 Obligaciones de terceras partes verificadoras de sellos de tiempo

33. Cuando se recibe un token de sello de tiempo, la tercera parte debe verificar que el token está correctamente firmado y que la clave privada utilizada para firmar el sello de tiempo no ha sido revocada.

34. Mientras el certificado utilizado para generar sellos de tiempo no esté caducado, es posible comprobar su validez en la CRL correspondiente.

35. En el caso de que la verificación se realice después del periodo de validez del certificado, la tercera parte deberá comprobar que la función hash empleada, los algoritmos y longitud de claves criptográficas se pueden seguir considerando seguras.

5.4 Limitaciones de uso

36. Este certificado se utilizará con el fin exclusivo de fechar documentos digitales.

6 Requerimientos operacionales.

37. Ver el apartado correspondiente de la DPCG de Izenpe.

6.1 **Procedimiento de emisión de un sello de tiempo.**

38. Con objeto de la prestación del Servicio de Sellado de Tiempo, Izenpe realiza la gestión de las claves correspondientes de conformidad con lo descrito en el apartado 6.2 - *Controles criptográficos* – de la presente declaración.

39. Los Sellos de Tiempo emitidos bajo esta declaración de prácticas son firmados por certificados específicos emitidos bajo la Cadena de Certificación de la Autoridad de Certificación subordinada con CN= SUBCA QC IZENPE – TSA y CN= CA QC IZENPE-TSA 2025

40. Para obtener más información sobre la citada Cadena de Certificación de la Autoridad de Certificación raíz consultar el apartado 1.3.1 *Autoridades de Certificación* de la DPCG.

6.1.1 Provisión y disponibilidad del servicio de sellado de tiempo.

41. La emisión de Sellos de Tiempo se realizará ante la petición de la entidad usuaria. Cuando ésta desee obtener un Sello de Tiempo para un documento electrónico, calculará un valor o conjunto de valores hash a partir de este. Éste se incluirá en una estructura de petición de sello de tiempo, y será enviado a Izenpe para que proceda a la emisión del Sello de Tiempo correspondiente.

42. Este Sello de Tiempo vinculará, los datos recibidos y la fecha y hora de la recepción.

43. Izenpe no realizará comprobación o tratamiento alguno sobre la representación de los datos a sellar recibidos más allá de su inclusión en el propio Sello de Tiempo y en los sistemas de registro de eventos.

44. El Servicio de Sellado de Tiempo estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a Izenpe u operaciones de mantenimiento. Izenpe notificará esta última circunstancia con la antelación suficiente y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

45. Tanto las peticiones de Sellado de Tiempo como las respuestas se gestionan conforme a lo descrito en la recomendación IETF RFC 3161.

6.1.2 Petición de un sellado de tiempo

46. Las peticiones de Sellado de Tiempo se envían a la dirección http://tsa.izenpe.com encapsuladas como Content-Type: application/timestamp-query, codificadas en DER y descritas en ASN.1 (Ver IETF RFC 3161).

47. Los algoritmos de hash soportados son:

- md2;
- md5;
- sha256;
- sha1;
- sha384; y,
- sha512.

Siendo los SHA256 y superiores los más indicados, quedando totalmente desaconsejados los algortimos SHA1 o de complejidad inferior. En cualquier caso, Izenpe sigue las recomendaciones de la industria en cuanto a suites criptográficas.

48. La petición debe seguir las indicaciones de ETSI TS 101 861.

6.1.3 Respuesta a una petición de sellado de tiempo

49. Las respuestas a una petición de sellado de tiempo se reciben de la dirección http://tsa.izenpe.eus encapsuladas como Content-Type: application/timestamp-reply, codificadas en DER y descritas en ASN.1.

50. El contenido de la respuesta es una estructura ASN.1 en la que se incluye el resultado de la operación (*status*), es decir, si la operación se ha realizado de manera satisfactoria o no, y una estructura *CMSSignedData* (*timeStampToken*) en la que se incluye el sellado de tiempo (*TSTInfo*) firmado por la Autoridad de Sellado de Tiempo.

51. El certificado de la Autoridad de Sellado Digital es un certificado emitido por la CA con la extensión *id-kp-timestamping* que indica que este certificado se utilizará con el fin exclusivo de fechar documentos digitales.

6.1.4 Fuente de tiempo empleada para la prestación del servicio

52. La TSA de Izenpe:

- Asegura la precisión de tiempo compatible con los estándares mínimos de tiempo UTC de +/- 1 segundo.
- Obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada (ROA) siguiendo el protocolo NTP . La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905.

53. Basándose en este servicio interno, Izenpe ofrece un servicio de sellado de tiempo (TSA) que puede ser utilizado para crear sellos de tiempo sobre documentos arbitrarios, según IETF RFC 3161.

54. Existen controles para detectar cambios en la calibración y/o problemas de sincronización que puedan comprometer la precisión definida.

55. La TSA de Izenpe asegura el correcto tratamiento de los segundos intercalares durante el último minuto del día en el que está planificado el ajuste.

6.2 **Controles criptográficos**

6.2.1 Generación de la clave de la TSA

56. Izenpe genera las claves criptográficas en un entorno físicamente securizado y realizado por personal con roles de confianza. Las claves de la TSA de Izenpe son generadas siguiendo un procedimiento específico.

57. La duración máxima del certificado de la TSA será de 5 años.

58. Los sistemas y productos usados por Izenpe proporcionan los servicios adecuados de acuerdo a los niveles requeridos de aseguramiento. Izenpe lleva a cabo un análisis adecuado de los requisitos de seguridad y dispone de procedimientos de control de cambios.

6.2.2 Tamaños de claves y algoritmos

59. En concreto, para el servicio de TSA:

- Para el protocolo de sello de tiempo se siguen las normas IETF RFC 3161 y RFC 5816.
- Para el perfil de sello y políticas se siguen las normas ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Time-Stamps) y ETSI EN 319 422 (Time-stamping protocol and time-stamp token profiles).
- Todos los tokens de sellado de tiempo emitidos por Izenpe incluyen el objeto identificador de política (OID) 1.3.6.1.4.1.14777.300.1.
- Todos los tokens de sellado de tiempo emitidos por Izenpe incluyen el certificado Timestamp empleado para firmar el token.

60. El certificado que se utiliza para firmar está generado con sha256WithRSAEncryption, con longitud de clave de 4096 bits, y es de uso exclusivo para el servicio de TSA, y en la jerarquía del 2025 con ECC 384.

61. El algoritmo hash del token es SHA-256.

6.2.3 Protección de la clave privada de la TSU

62. La TSA de Izenpe asegura que se mantiene la confidencialidad e integridad de sus claves. En particular el HSM cumple con los requerimientos de Common Criteria y el nivel de aseguramiento EAL4+ del perfil correspondiente. En ese sentido las claves de la TSA se mantienen con un nivel de seguridad equivalente al descrito en la DPC para las CAs subordinadas de Izenpe.

6.2.4 Distribución de la clave pública de la TSU

63. El certificado de la TSA de Izenpe está publicado en www.izenpe.eus.

6.2.5 Renovación con regeneración de la clave de la TSU

64. Las claves de la TSA de Izenpe deben ser reemplazadas antes de la expiración del certificado si el algoritmo, longitud de clave o cualquier otra medida de seguridad deja de ser considerado fiable por la industria. En cualquier caso, se regenerarán las claves y se emitirá un nuevo certificado cada cuatro años como máximo.

6.2.6 Fin del ciclo de vida de la clave de la TSU

65. La TSA de Izenpe no permite firmar respuestas *timestamp* con un certificado caducado o revocado. En el caso de finalización de servicios de la TSA de Izenpe, todas las claves privadas de los certificados de la TSA incluyendo copias de seguridad serán destruidas de forma que dichas claves sean irrecuperables.

6.2.7 Gestión del ciclo de vida del módulo criptográfico usado para firmas los sellos de tiempo

66. Izenpe establece procedimientos para garantizar que los servicios de no repudio de los módulos de seguridad de hardware (HSM) no son manipulados durante el envío y almacenamiento.

67. La instalación y activación de las claves de firma contenidas en el hardware criptográfico es realizado únicamente por el personal con roles de confianza. Operación, procedimientos y gestión de ciclo de vida de los HSM están descritos en documentación interna de Izenpe.

6.2.8 Compromiso de la clave privada del certificado de TSA

68. En caso de compromiso de una clave privada del servicio TSA de Izenpe se aplicará el procedimiento indicado en el punto 5.7.3 *Procedimiento ante compromiso de una clave privada* de la DPC, así como, lo indicado en el punto *8.4 Servicio VA/TSA del Plan de Contingencia*, entre otros:

- No se emitirán tokens timestamp;
- En el caso de comprometerse la precisión mínima de +/- 1 segundo definida no se emitirán sellos de tiempo hasta que se corrija la calibración.

69. La TSA garantiza que en caso de que se produzca un evento de seguridad en los servicios de sellado de tiempo, incluyendo el compromiso de su clave privada o la pérdida de calibración respecto a la UTC, informará a los suscriptores y las terceras partes en la página web de Izenpe.

70. Existen procedimientos específicos de contingencia para los sistemas de TSA, que garantizan la recuperación de las operaciones y la respuesta ante compromisos de claves de TSU y pérdida de sincronismo.

71. En caso de un compromiso al menos IZENPE:

- Informará a los suscriptores y usuarios del compromiso;
- Revocará el certificado de TSA/TSU y publicará la correspondiente lista de revocación;
- Planificará la generación de un nuevo certificado de TSA para evitar la pérdida de servicio, siempre que no existan problemas de seguridad para ello.
- Investigará las causas del compromiso y tomará medidas adecuadas para evitar que se repitan.

72. En caso de una pérdida de sincronización, al menos, IZENPE:

- Parará la emisión de sellos de tiempo;
- Informará a los suscriptores y usuarios de la pérdida de sincronismo; y,
- Re-establecerá el servicio lo más rápidamente posible.

6.2.9 Finalización de la TSA

73. La terminación de la TSA de Izenpe se realizará según los procedimientos definidos en el apartado 3.8, *Cese de la TSA,* del documento PR_G_Plan_de_Cese_de_Servicios_de_Izenpe.

7 Perfil de certificados

74. Ver el apartado correspondiente de la DPC global de Izenpe.
75. Los datos de creación de firma de la TSA están vinculados al siguiente Certificado:

EXTENSION ATTRIBUTE	VALUE	COMMENT
Subject	CN = tsa.izenpe.com 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Issuer Name	CN = SUBCA QC IZENPE - TSA 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Key Usage	Firma digital (80)	
Extended Key Usage	Impresión de fecha (1.3.6.1.5.5.7.3.8)	
Subject key Identifier	<key identifier of this CA's public key>	
Authority key identifier	<key identifier of the issuing CA's public key>	
CRL Distribution Point	http://crl.izenpe.eus/cgi-bin/izenpeTSA	URLs of the CRL Distribution points
Certificate Policy	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.14777.10.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.izenpe.eus/cps [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado	

Subject Information Access	[1]Acceso a información de autoridad Método de acceso=Método de acceso desconocido (1.3.6.1.5.5.7.48.3) Nombre alternativo: Dirección URL=http://tsa.izenpe.eus/	

EXTENSION ATTRIBUTE	VALUE	COMMENT
Subject	CN = tsa.izenpe.com 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Issuer Name	CN = SUBCA QC IZENPE – TSA 2025 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Key Usage	Firma digital (80)	
Extended Key Usage	Impresión de fecha (1.3.6.1.5.5.7.3.8)	
Subject key Identifier	<key identifier of this CA's public key>	
Authority key identifier	<key identifier of the issuing CA's public key>	
CRL Distribution Point	http://crl.izenpe.eus/crls/izqcroot.crl	URLs of the CRL Distribution points
Certificate Policy	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.14777.10.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.izenpe.eus/cps [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado	
Subject Information Access	[1]Acceso a información de autoridad Método de acceso=Método de acceso desconocido (1.3.6.1.5.5.7.48.3) Nombre alternativo: Dirección URL=http://tsa.izenpe.eus/	

8 Auditorías de cumplimiento

76. Ver el apartado correspondiente de la DPC global de Izenpe.

77. El cumplimiento de esta Declaración de Prácticas de Sellado de Tiempo está sujeto a auditorías periódicas independientes, tanto internas como externas.

78. Los procedimientos definidos y su correcta implementación son auditados anualmente por una entidad externa independiente.

79. Izenpe cumple con las obligaciones y responsabilidades definidas en el apartado 5.1 - *De la Entidad Emisora de Sellos de Tiempo* – de la presente declaración y asegura la implementación de controles apropiados.

80. IZENPE verifica la conformidad de los certificados de TSU con el Reglamento eIDAS así como con los estándares europeos de aplicación:

- ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; y,
- ETSI EN 319 422 “Time stamping protocol and electronic time-tamp profiles”.

9 Otros asuntos legales y de actividad.

9.1 Tarifas

81. Ver el apartado correspondiente de la DPC global de Izenpe.

82. Existe una limitación por número de peticiones mensuales, a partir de las cuales el servicio tiene un coste asociado. Contactar con Izenpe para consultar condiciones y tarifas.