TEXTO DE DIVULGACIÓN (PDS) CORRESPONDIENTE A LOS CERTIFICADOS DE SELLO DE UNIDADES DE SELLADO DE TIEMPO EMITIDOS POR ZIURTAPEN ETA ZERBITZU ENPREA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE, S.A.

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2025.06.23 11:16:27 +02'00'

ã Izenpe 2025

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.

ÍNDICE

1 ACUERDO INTEGRO....4
2 INFORMACIÓN DE CONTACTO DE LA TSA....4
3 TIPO DE SELLO DE TIEMPO Y USO....4
4 LÍMITES DE USO DEL CERTIFICADO....5
5 OBLIGACIONES DE LOS SUSCRIPTORES....5
6 OBLIGACIONES DE VERIFICACIÓN DE LAS PARTES QUE CONFÍAN DEL ESTADO DE LOS CERTIFICADOS TSU....5
7 LIMITACIONES DE RESPONSABILIDAD....6
8 ACUERDOS APLICABLES Y DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN....6
9 POLÍTICA DE PRIVACIDAD....6
10 POLÍTICA DE DEVOLUCIÓN....7
11 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS....7
12 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA....7

El presente documento constituye la PKI Disclousure Statement (en adelante, PDS) correspondiente a los certificados de sello de TSU expedidos por Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, Izenpe).

1 ACUERDO INTEGRO

1. La presente declaración informativa de la Autoridad de Sellado de Tiempo de Izenpe no pretende definir las condiciones completas bajo las que se presta el Servicio cualificado de Sellado de tiempo por dicha entidad, sino tan solo un resumen de las mismas.

2 INFORMACIÓN DE CONTACTO DE LA TSA

2. La Autoridad de Certificación de Izenpe es una iniciativa de:
   - Ziurtapen eta Zerbitzu Enpresa – Empresa de Certificación y Servicios, Izenpe S.A.
   - C/ Beato Tomás de Zumárraga, 71 – 01008 Vitoria-Gasteiz
   - Teléfono: 900 840 123

3 TIPO DE SELLO DE TIEMPO Y USO

3. El servicio cualificado de sellado de tiempo es ofrecido por la autoridad de sellado de tiempo de Izenpe como prestador de servicios de confianza y de conformidad con el Reglamento eIDAS[5].
4. Esta PDS tiene las siguientes características:
   - 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 (Timestamping protocol and time-stamp token profiles).
   - Los requisitos de la política de TSA están basados en criptografía de clave pública, certificados de clave pública (X.509) y fuentes de tiempo fiables.
   - 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 Time-stamp empleado para firmar el token.
   - 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.
   - El algoritmo hash del token es SHA-256.

[5] 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,

5. El tiempo de vigencia del certificado de TSU que Izenpe utiliza para ofrecer el servicio cualificado de sellado de tiempo es de hasta 5 años.
6. 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).
7. Los certificados indicados en esta PDS solo pueden ser utilizados para generar sellos de tiempo electrónico.
8. La verificación del estado de los certificados es obligatoria para cada uso de los certificados, mediante la consulta de la lista de revocaciones (CRL). La información acerca de cómo y dónde encontrar la CRL se encuentra en el propio certificado.
9. Sin haber hecho las comprobaciones pertinentes en cuanto a la validación del sello electrónico y la verificación del estado de vigencia del certificado que Izenpe emplea en la creación de los sellos de tiempo electrónicos, no se debe confiar en los mismos. En este caso, se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra Izenpe por daños, perjuicios o conflictos provenientes del uso o confianza en este servicio.

4 LÍMITES DE USO DEL CERTIFICADO

10. La TSA de Izenpe asegura la precisión de tiempo compatible con los estándares mínimos de tiempo UTC de +/- 1 segundo. La TSA de Izenpe no emitirá tokens de sello de tiempo si no se puede asegurar dicha precisión.
11. Izenpe obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada (ROA) siguiendo el protocolo NTP a través de la conexión establecida con el Gobierno Vasco. La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905.
12. Izenpe conserva durante 15 años desde la extinción del certificado o la finalización del servicio prestado toda la información y documentación relativa a este servicio de confianza.

5 OBLIGACIONES DE LOS SUSCRIPTORES

13. En la Declaración de Prácticas del servicio de Sellado de Tiempo de Izenpe quedan definidas las obligaciones de todas las partes que actúan en relación con el uso de este servicio. Disponible en www.izenpe.eus.

6 OBLIGACIONES DE VERIFICACIÓN DE LAS PARTES QUE CONFÍAN DEL ESTADO DE LOS CERTIFICADOS TSU

14. 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.
15. Mientras el certificado utilizado para generar sellos de tiempo no esté caducado, es posible comprobar su validez en la CRL correspondiente, disponible en la ubicación especificada en el mismo certificado.

16. 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.

7 LIMITACIONES DE RESPONSABILIDAD

17. Izenpe opera su TSA de acuerdo con la Declaración de Prácticas del servicio de Sellado de Tiempo, su DPCG, y los términos de cualquier otro acuerdo vinculante entre Izenpe y usuarios del servicio de sellado de tiempo.
18. Izenpe realiza esfuerzos para proporcionar alta disponibilidad en sus servicios, pero no ofrece una garantía total en cuanto a disponibilidad. 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.
19. Izenpe no será responsable de daños consecuencia de infracciones cometidas por el suscriptor o terceras partes en los términos y condiciones aplicables. Así, Izenpe no responderá ante personas cuyo comportamiento en la utilización de los sellos de tiempo electrónicos haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la Declaración de Prácticas de Confianza particular del servicio de Sellado de Tiempo y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.
20. Izenpe no será, bajo ningún concepto, 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. 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.

8 ACUERDOS APLICABLES Y DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN

21. El documento declaración de prácticas de confianza particular del servicio de sellado de Tiempo publicado en la dirección www.izenpe.eus , recoge la información pública de las condiciones y características de este servicio de confianza ofrecido por parte de Izenpe como prestador de servicios de confianza, recogiendo las obligaciones de las partes implicadas y las reglas y los procesos que la TSA aplica en relación con la expedición de un token de sello de tiempo. Disponible en: https://www.izenpe.eus/politica-tsa/webize01-cndocjuridica/es/

9 POLÍTICA DE PRIVACIDAD

22. El tratamiento de datos de carácter personal que realiza Izenpe se alinea con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, así como con los requisitos que sean de aplicación por normativa nacional específica en esta materia.

23. Izenpe informa a los interesados de la inclusión del número de serie del certificado en la lista de certificados revocados (CRL) para que sea visualizado por cualquier usuario, aunque no disponga de un certificado electrónico, tanto en el ámbito público como privado.

10 POLÍTICA DE DEVOLUCIÓN

24. Izenpe no dispone de una política de reintegro.

11 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS

25. La provisión de servicios de confianza de Izenpe se regirá por lo dispuesto en la legislación española.
26. Con carácter general, los usuarios de los servicios de confianza de Izenpe aceptan que todo litigio, discrepancia, cuestión o reclamación resultante de la ejecución o interpretación de DPCG y/o declaraciones de prácticas particulares y PDS's relacionadas, directa o indirectamente, se resolverá de conformidad con lo establecido en los correspondientes contratos, condiciones generales y/o encomiendas o convenios.
27. Las partes acuerdan resolver cualquier cuestión que surja entre ellas mediante un proceso de Derecho Colaborativo, pudiendo acudir a los Juzgados y Tribunales de la ciudad de Vitoria-Gasteiz, en caso de no llegar a un acuerdo.

12 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA

28. Izenpe, como prestador de servicios de confianza, mantiene varias acreditaciones y certificaciones de su infraestructura de clave pública, de las cuales aplican especialmente a estos tipos de certificados las siguientes:
    - Certificación ISO/IEC 27001, estándar para la seguridad de la información.
    - Certificación ISO/IEC 27701, extensión para la gestión de la privacidad de ISO/IEC 27001 cuyo objetivo es proporcionar orientación sobre la protección de la privacidad, incluida la forma en que las organizaciones deben gestionar la información personal, además de ayudar a demostrar el cumplimiento de la normativa en privacidad, como el Reglamento General de Protección de Datos.
    - Servicio de sellado electrónico de tiempo: Expedición y administración de sellos electrónicos de tiempo de conformidad con los estándares europeos:
        - ETSI EN 319 421-"Policy and Security Requirements for Trust Service Providers issuing Time-Stamps)
        - ETSI EN 319 422 "Timestamping protocol and time-stamp token profiles".
29. La TSA de Izenpe es un servicio cualificado de sellado de tiempo según eIDAS. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/esES/datosabiertos/catalogo/lista-prestadores-tsl.
30. Las auditorías a las que se somete IZENPE se llevan a cabo con la periodicidad requerida, y por un Organismo de Evaluación de la Conformidad acreditado para tal fin.