TEXTO DE DIVULGACIÓN (PDS) CORRESPONDIENTE A LOS CERTIFICADOS DE SELLO DE PERSONA JURÍDICA EMITIDOS POR IZENPE

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 11:12:59 +02'00'

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	Aprobaciçon del documento.

ÍNDICE

1. INFORMACIÓN DE CONTACTO 4
1.1 ORGANIZACIÓN RESPONSABLE 4
1.2 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 4
1.3 PERSONA DE CONTACTO 4
1.4 CONTACTO PARA PROCESOS DE REVOCACIÓN 4
1.5 4
2 TIPO Y FINALIDAD DEL CERTIFICADO 5
2.1 CERTIFICADOS CUALIFICADOS DE PERSONA JURÍDICA 5
2.1.1 SELLO DE ENTIDAD 5
2.1.1.1 CONTENEDOR SOFTWARE 5
2.1.1.2 HSM 6
2.1.2 SELLO EXPEDIDO EN EL ÁMBITO DE LA ADMINISTRACIÓN 6
2.1.2.1 CONTENEDOR SOFTWARE DE IZENPE 6
2.1.2.2 HSM 7
2.2 VALIDACIÓN DE LOS CERTIFICADOS 8
3 LÍMITES DE USO DEL CERTIFICADO DIRIGIDOS A LOS FIRMANTES 8
4 OBLIGACIONES DE LOS SUSCRIPTORES 8
5 OBLIGACIONES DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS DE LAS PARTES QUE CONFÍAN 9
6 LIMITACIONES DE RESPONSABILIDAD 9
7 ACUERDOS APLICABLES Y DECLARACIÓN DE PRÁCTICAS DE CONFIANZA GLOBAL 10
8 POLÍTICA DE PRIVACIDAD 10
9 POLÍTICA DE DEVOLUCIÓN 11
10 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS 11
11 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA 11

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

1. INFORMACIÓN DE CONTACTO.

1.1 Organización responsable.

1. 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

1.2 Organización que administra el documento.

- 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

1.3 Persona de contacto.

- 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

1.4 Contacto para procesos de revocación

2. La persona solicitante podrá tramitar la solicitud de revocación ante Izenpe en cualquier momento a través de los siguientes canales:
   - Presencialmente: ante Izenpe solicitando cita previa a través de www.izenpe.eus.
   - Vía postal: remitiendo la solicitud de revocación del certificado firmada y legitimada en presencia notarial a la dirección postal de Izenpe, S.A.- C/ Beato Tomás de Zumárraga, 71 -1ª planta – 01008 Vitoria-Gasteiz
   - Remitiendo a la dirección de correo electrónico izenpe@izenpe.eus la solicitud de revocación firmada con un certificado cualificado expedido por una CA incluida en la EU TSL (Trusted Service List).
   - Acceso aplicación de revocación on line disponible en: https://servicios.izenpe.com/gestionCertificados/

2 Tipo y finalidad del certificado

2.1 Certificados cualificados de sello de persona jurídica

3. Los medios de identificación regulados en el presente PDS se expiden de acuerdo con lo establecido en el Reglamento eIDAS[1], y con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
4. Estos certificados son cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento eIDAS y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2 y por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
5. Izenpe emite los siguientes certificados cualificados de persona jurídica:
   - Sello de entidad emitido en contenedor software de Izenpe;
   - Sello de entidad emitido en HSM; y,
   - Sello expedido en el ámbito de la Administración emitido en contenedor software de Izenpe; y,
   - Sello expedido en el ámbito de la Administración emitido en HSM.
6. Estos certificados se expiden conforme a los niveles de seguridad determinados en el 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.

2.1.1 Sello de entidad

2.1.1.1 Contenedor software

7. Este certificado permite la identificación de la entidad, así como, en su caso, de la persona solicitante. Así mismo permite probar que un documento electrónico ha sido expedido por ésta, aportando certeza sobre el origen y la integridad del documento.
8. Izenpe expide el certificado de *Sello de entidad* tanto a entidades con personalidad jurídica como a entidades sin personalidad jurídica.
9. Este certificado tiene una duración de hasta 3 años.

[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.

10. Los certificados de sello de entidad en contenedor software de Izenpe permiten la generación de sellos electrónicos avanzados.
11. Jerarquía CA raíz 2007 (CN=Izenpe.com).

SELLO DE ENTIDAD				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Sello de entidad	Contenedor software de Izenpe	QCP-l	1.3.6.1.4.1.14777.2.11	Avanzada

2.1.1.2 HSM

12. Este certificado permite la identificación de la entidad, así como, en su caso, de la persona solicitante. Así mismo permite probar que un documento electrónico ha sido expedido por ésta, aportando certeza sobre el origen y la integridad del documento.
13. El certificado de sello de entidad tiene una duración de hasta 3 años.
14. Los certificados de sello de entidad en HSM son gestionados de forma centralizada y permiten la generación de sellos electrónicos avanzados.
15. Jerarquía CA raíz 2007 (CN=Izenpe.com)

SELLO DE ENTIDAD				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Sello de entidad	HSM	QCP-l	1.3.6.1.4.1.14777.2.20	Avanzada

2.1.2 Sello expedido en el ámbito de la Administración.

2.1.2.1 Contenedor software de Izenpe.

16. Izenpe emite este certificado en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
17. Este certificado permite la identificación de la administración, órgano, organismo público o entidad de derecho público, así como, en su caso, la identidad de la persona titular del órgano.
18. Los certificados de sello expedido en el ámbito de la Administración en contenedor software de Izenpe permiten la generación de sellos electrónicos avanzados.

19. Según los niveles de aseguramiento definidos en el Esquema de Identificación y Firma electrónica, Izenpe emite el certificado de Sello electrónico de nivel medio.
20. La vigencia de este certificado puede ser hasta 3 años.
21. Jerarquía CA raíz 2007 (CN=Izenpe.com)

SELLO DE ADMINISTRACIÓN				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Sello de administración	Contenedor software de Izenpe	QCP-l	1.3.6.1.4.1.14777.4.11.2	Avanzada

2.1.2.2 HSM

22. Izenpe emite este certificado en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
23. Este certificado permite la identificación de la administración, órgano, organismo público o entidad de derecho público, así como, en su caso, la identidad de la persona titular del órgano.
24. Los certificados de sello expedido en el ámbito de la Administración en HSM son gestionados de forma centralizada y permiten la generación de sellos electrónicos avanzados.
25. Según los niveles de aseguramiento definidos en el Esquema de Identificación y Firma electrónica, Izenpe emite el certificado de Sello electrónico de nivel medio.
26. La vigencia de este certificado puede ser de hasta 3 años.

    Jerarquía CA raíz 2007 (CN=Izenpe.com)

SELLO DE ADMINISTRACIÓN				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Sello de administración	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3	Avanzada

2.2 Validación de los certificados.

1. La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

27. Izenpe suministra información a los verificadores acerca de cómo y dónde encontrar la CRL y/o OCSP correspondiente. Disponible en: https://servicios.izenpe.com/gestionCertificados/mostrarValidacionCertificado.do

3 Límites de uso del certificado dirigidos a los firmantes.

28. Los certificados indicados en esta PDS solo pueden ser utilizados para generar sellos electrónicos.

29. El creador de sellos tiene que utilizar el servicio de certificación prestado por IZENPE exclusivamente para los usos autorizados en la relación contractual entre IZENPE y la persona jurídica suscriptora. Asimismo, el creador de sellos se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por IZENPE.

30. El creador de sellos tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

31. El creador de sellos no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de IZENPE, sin previo permiso expreso.

32. Izenpe conserva durante 15 años (a partir de la fecha de extinción del mismo toda la información y documentación relativa a los certificados cualificados.

4 Obligaciones de los suscriptores.

33. El suscriptor está obligado a:

- Facilitar a Izenpe información completa y adecuada, conforme a los requerimientos de la Declaración de Prácticas de Certificación en especial en lo relativo al procedimiento de registro.
- Garantizar la veracidad, totalidad y actualidad de la información que haya de constar en los certificados.
- Conocer y aceptar las condiciones de utilización de los certificados, así como las modificaciones que se realicen sobre las mismas.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Garantizar el buen uso y la conservación de los soportes de los certificados.
- Emplear adecuadamente el certificado y, en concreto, cumplir con las limitaciones de uso de los certificados.
- Emplear la clave privada para funciones criptográficas dentro de un dispositivo criptográfico seguro, cuando proceda.
- Emplear la clave privada bajo su control.

- Se recomienda emplear el par de claves únicamente para realizar sellos electrónicos.
- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la Declaración de Prácticas de Certificación.
- Notificar a Izenpe y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  - La pérdida, el robo o el compromiso potencial de su clave privada.
  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo criptográfica) o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, instando la revocación del certificado cuando dicha modificación constituya causa de revocación del mismo.
- Dejar de emplear la clave privada transcurrido el periodo de validez del certificado.
- Transferir a los poseedores de claves las obligaciones específicas de los mismos.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de la Entidad de Certificación.
- No comprometer intencionadamente la seguridad de los servicios de certificación.
- No emplear las claves privadas correspondientes a las claves públicas contenidas en los certificados, con el propósito de firmar ningún certificado, como si se tratase de una Entidad de Certificación.

5 Obligaciones de verificación del estado de los certificados de las partes que confían.

34. El usuario verificador de certificados queda obligado a:
    - Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
    - Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados. Disponible en: https://servicios.izenpe.com/gestionCertificados/mostrarValidacionCertificado.do
    - Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de verificador.

6 Limitaciones de responsabilidad.

35. Izenpe responderá:
    - Por negligencia o falta de la debida diligencia en los servicios de certificación descritos en la presente PDS, así como cuando incumpla las obligaciones

impuestas en la legislación sobre firma electrónica, excepto en los siguientes supuestos:

- Por los daños causados por las informaciones contenidas en los certificados, siempre que el contenido de los mismos cumpla sustancialmente con la DPCG.
- Por los daños causados por la extinción de la eficacia de los certificados, siempre que cumpla sustancialmente con las obligaciones de publicación previstas en la DPCG.
- De ningún daño directo e indirecto, especial, incidental, emergente, de cualquier lucro cesante, pérdida de datos, daños punitivos, fuesen o no previsibles, surgidos en relación con el uso, entrega, licencia, funcionamiento o no funcionamiento de los certificados, las firmas digitales, o cualquier otra transacción o servicio ofrecido o contemplado en la DPCG en caso de uso indebido.
- Por los daños y perjuicios ocasionados al suscriptor o terceros de buena fe, por la inexactitud de los datos que consten en el certificado, si éstos le han sido acreditados mediante documento público notarial, judicial o administrativo, salvo en el caso del documento aportado por la Entidad de Registro.
- Por los daños y perjuicios ocasionados al suscriptor o a terceros de buena fe, por el incumplimiento de los deberes inherentes a la condición de suscriptor o terceros que confían en los certificados.

36. Izenpe responderá por los daños y perjuicios que cause a cualquier persona por la falta o retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados o de la extinción de la vigencia de los certificados.
37. Asimismo, asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que delegue para el ejercicio de las funciones necesarias para la prestación de servicios de certificación. En este sentido, se ha constituido un seguro de responsabilidad civil para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados.

7 Acuerdos aplicables y Declaración de Prácticas de Confianza Global.

38. El documento *Declaración de Prácticas de Confianza Global*, publicado en la dirección https://www.izenpe.eus/declaracion-de-practicas-de-certificacion/webize01-cndocjuridica/es/, recoge la información pública de las condiciones y características de los servicios de certificación y servicios de expedición de certificados electrónicos por parte de IZENPE como Prestador de Servicios de Confianza, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición de estos tipos de certificados.

8 Política de privacidad.

39. 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 (Reglamento general de protección de datos, en adelante RGPD), así como con los requisitos que sean de aplicación por normativa nacional específica en esta materia.

9 Política de devolución.

40. Izenpe no dispone de una política de reintegro.

10 Ley aplicable, quejas y resolución de disputas.

41. 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.

11 Licencias y repositorio, marcas confiables y auditoría.

42. 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.
    - Certificados de Sellos de Entidad: Expedición y administración de certificados electrónicos cualificados de conformidad con los estándares europeos:
        - ETSI EN 319 411-1 “Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements”;
        - ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”; y,
        - ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons”.
43. Los Sellos de Entidad y los sellos expedidos en el ámbito de la Administración se expiden como cualificados conforme al Reglamento 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.
44. 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.