TEXTO DE DIVULGACIÓN (PDS) CORRESPONDIENTE A LOS CERTIFICADOS NO CUALIFICADOS DE PERSONA FÍSICA 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 10:45:58 +02'00'

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. 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
2 TIPO Y FINALIDAD DEL CERTIFICADO. 5
2.1 CERTIFICADOS NO CUALIFICADOS DE PERSONA FÍSICA. 5
2.1.1 CIUDADANÍA 5
2.1.1.1 BAK 5
2.1.1.2 IZENPE MOBILE 6
2.1.1.3 CERTIFICADO NO CUALIFICADO DE AUTÓNOMO. 6
2.1.2 PROFESIONALES 7
2.1.2.1 CERTIFICADO DE EMPLEADO PÚBLICO CON PSEUDÓNIMO PARA AUTENTICACIÓN Y CIFRADO 7
2.2 VALIDACIÓN DE LOS CERTIFICADOS. 7
3 LÍMITES DE USO DEL CERTIFICADO DIRIGIDOS A LOS FIRMANTES 7
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. 10
10 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS. 10
11 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA. 10

El presente documento constituye la *PKI Disclousure Statement* (en adelante, PDS) correspondiente a los certificados no cualificados de *Ciudadanía* 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 no cualificados de persona física.

3. Los certificados no cualificados de persona física regulados en la presente PDS se expiden de acuerdo con el Reglamento eIDAS[5], y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.
4. Los certificados no cualificados se expiden según 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 eIDAS.
5. Izenpe expide los siguientes certificados no cualificados de persona física:

2.1.1 Ciudadanía.

2.1.1.1 BaK.

6. BaK es un medio que permite la identificación y firma de personas físicas.
7. Está formado por:
   - Un número de referencia coincidente con el DNI/NIE/pasaporte de la persona usuaria.
   - Una contraseña.
   - Un certificado no cualificado emitido en un repositorio centralizado de Izenpe que servirá para los actos de firma.
8. Estos certificados son gestionados de forma centralizada y permiten la generación de firma electrónica básica basada en certificado electrónico no cualificado.
9. Jerarquía CA raíz 2007 (CN=Izenpe.com)

CIUDADANO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
BaK	HSM	LCP	1.3.6.1.4.1.14777.5.2.5	Básica

[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.

2.1.1.2 Izenpe Mobile.

10. Izenpe Mobile es el medio que permite la identificación de personas físicas y autoriza el uso de un certificado cualificado almacenado en un repositorio centralizado seguro de Izenpe asociado a la persona.
11. Izenpe Mobile está formado por:
    - Una aplicación instalada en un dispositivo móvil, vinculada a un certificado no cualificado que facilita procesos de comunicaciones seguras.
    - Una contraseña o un factor biométrico que facilita el acceso a la aplicación.
    - Un certificado cualificado de firma electrónica emitido en un repositorio centralizado seguro de Izenpe que servirá para actos de firma.

      Para los actos de firma el certificado podrá ser: certificado cualificado BaKQ, certificado de empleado público o profesional corporativo almacenados en HSM's.
12. Jerarquía CA raíz 2007 (CN=Izenpe.com)

CIUDADANO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Izenpe Mobile	Contenedor APP	NCP	1.3.6.1.4.1.14777.5.2.5.4	n/a (para firmar se usa el de BaKQ)

2.1.1.3 Certificado no cualificado de Autónomo.

13. El certificado no cualificado de Autónomo es un certificado no cualificado expedido en soporte software que permite la identificación y firma de personas físicas que desarrollan actividades de carácter económico.
14. Permite la generación de firma electrónica avanzada basada en certificado electrónico no cualificado.
15. Jerarquía CA raíz 2007 (CN=Izenpe.com)

AUTÓNOMO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Autónomo	Software	LCP	1.3.6.1.4.1.14777.5.2.7.2	Básica

2.1.2 Profesionales.

2.1.2.1 Certificado de empleado público con pseudónimo para autenticación y cifrado.

16. Este tipo de certificado sirve a los propósitos de autenticación y cifrado.
17. Se trata de certificados no cualificados siempre que se emitan en vinculación con el certificado cualificado de empleado público con pseudónimo para firma (ver la PDS de certificados cualificados de persona física).
18. Jerarquía CA raíz 2007 (CN=Izenpe.com)

EMPLEADO PÚBLICO CON PSEUDÓNIMO PARA AUTENTICACIÓN Y CIFRADO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Empleado público con seudónimo	Tarjeta	NCP+	Autenticación 1.3.6.1.4.1.14777.4.13.1.2	n/a
		n/a	Cifrado 1.3.6.1.4.1.14777.4.13.1.3	n/a

2.2 Validación de los certificados.

19. 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.
20. Izenpe suministra información a los verificadores acerca de cómo y dónde encontrar la CRL y/o OCSP correspondiente.

3 LÍMITES DE USO DEL CERTIFICADO DIRIGIDOS A LOS FIRMANTES.

21. Los certificados indicados en esta PDS solo pueden ser utilizados para realizar procedimientos de autenticación.
22. Para la generación de firmas electrónicas, se emplean otros certificados, dependiendo del titular del certificado (p.ej. uso del certificado cualificado BaKQ en caso de personas físicas).
23. El firmante tiene que utilizar el servicio de certificación prestado por Izenpe exclusivamente para los usos autorizados en la relación contractual entre Izenpe y la persona física suscriptora. Asimismo, el firmante se obliga a utilizar el servicio de certificación de acuerdo con las instrucciones, manuales o procedimientos suministrados por Izenpe.
24. El firmante tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.
25. El firmante no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de Izenpe, sin previo permiso expreso.

26. Izenpe conserva durante 15 años (a partir de la fecha de extinción del certificado o de la finalización del servicio) toda la información y documentación relativa a los certificados no cualificados.

4 OBLIGACIONES DE LOS SUSCRIPTORES.

27. El suscriptor está obligado a:

- Facilitar a Izenpe información completa y adecuada, conforme a los requerimientos de la Declaración de Prácticas de Confianza Global 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.
- 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 Confianza Global.
- 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 de este.
- 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 Izenpe.
- 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.

28. 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.

29. 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 en los que Izenpe no será responsable:

    - 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 electrónicas, 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.
    - Izenpe tampoco será responsable 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.

30. 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.

31. 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.

32. El documento DPCG, publicado en la dirección https://www.izenpe.eus, 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.

33. Las PDS correspondientes a los medios de identificación y firma emitidos a la ciudadanía y las PDS correspondientes a certificados del tipo profesional (corporativo y empleado público), publicadas en la dirección https://www.izenpe.eus, recogen la información pública de las condiciones y características de los servicios de certificación y servicios de expedición de certificados electrónicos no cualificados de persona física de ciudadanía y de profesional corporativo no cualificado por parte de Izenpe, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición de estos tipos de certificados.

8 POLÍTICA DE PRIVACIDAD.

34. 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.

35. Izenpe no dispone de una política de reintegro.

10 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS.

36. 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.

37. 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.

- Expedición y administración de certificados electrónicos 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 319 412-2 “Certificate profile for certificates issued to natural persons”.

38. Las auditorías a las que se somete Izenpe llevan a cabo con la periodicidad requerida, y por un Organismo de Evaluación de la Conformidad acreditado para tal fin.