TEXTO DE DIVULGACIÓN (PDS) CORRESPONDIENTE A LOS CERTIFICADOS DE AUTENTICACIÓN DE SITIO WEB (SSL)

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 11:14:38 +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. 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 SSL NO CUALIFICADOS 5
2.2 CERTIFICADOS SSL CUALIFICADOS (EV) 6
2.3 VALIDACIÓN DE CERTIFICADOS 7
3 LÍMITES DE USO DEL CERTIFICADO 7
4 OBLIGACIONES DE LA CA 7
5 OBLIGACIONES DE LA ENTIDAD DE REGISTRO 9
6 OBLIGACIONES DE LOS SUSCRIPTORES 9
7 OBLIGACIONES DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS DE LAS PARTES QUE CONFÍAN. 11
8 LIMITACIONES DE RESPONSABILIDAD 11
9 ACUERDOS APLICABLES Y DECLARACIÓN DE PRÁCTICAS DE CONFIANZA 11
10 POLÍTICA DE PRIVACIDAD 12
11 POLÍTICA DE DEVOLUCIÓN 12
12 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS 12
13 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA 12

El presente documento constituye la *PKI Disclousure Statement* (en adelante, PDS) correspondiente a los certificados no cualificados y cualificados *de autenticación de sito web* 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 de la revocación tramitará ante Izenpe la solicitud de revocación.
3. En el caso de que la revocación fuera solicitada por persona distinta del solicitante o del suscriptor de forma previa o simultánea a la revocación, Izenpe comunicará al al suscriptor del certificado la revocación de su certificado y la causa por la que se ha llevado a cabo.
4. El solicitante podrá revocar el certificado a través de los siguientes canales:
   - Presencialmente;
     - Ante Izenpe solicitando cita previa a través de www.izenpe.eus;
     - O ante la organización suscriptora con la que Izenpe haya suscrito el instrumento legal pertinente.
   - Remitiendo a la dirección de correo electrónico izenpe@izenpe.eus la solicitud de revocación firmada con el DNI electrónico o con un certificado cualificado incluido en la lista de confianza

- Acceso aplicación de revocación on line disponible en: https://servicios.izenpe.com/gestionCertificados/

2 TIPO Y FINALIDAD DEL CERTIFICADO.

2.1 CERTIFICADOS SSL NO CUALIFICADOS.

5. Los certificados de autenticación de sitio web (en adelante SSL) no cualificados permiten autenticar un sitio web y lo vinculan con la persona jurídica a quien se ha expedido.
6. Izenpe emite los siguientes certificados SSL no cualificados:
   - Certificado SSL OV: este certificado, con la consideración de no cualificado, será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía razonable al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado.
   - Certificado SSL DV: este certificado, con la consideración de no cualificado, será utilizado para la identificación de la titularidad del dominio que alberga el sitio web, proporcionando una garantía razonable al usuario de un navegador de Internet.

   Estos certificados electrónicos son expedidos en conformidad con los requisitos del Reglamento eIDAS[1].
7. La validez de estos certificados es de 395 días.

Jerarquía CA raíz 2007 (CN=Izenpe.com).

SERVIDOR SEGURO (SSL/TLS)			
Breve descripción	Soporte	Identificador de política	OID Política
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.1.2.1
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.1.2.4

[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,

Jerarquía CA raíz 2020 no cualificados (CN= ROOT CA NQC IZENPE).

SERVIDOR SEGURO (SSL/TLS) INTERNO			
Breve descripción	Soporte	Identificador de política	OID Política
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.14.1.2

.

Jerarquía CA raíz 2024 (CN=ROOT CA SSL IZENPE 2024).

SERVIDOR SEGURO 2024			
Breve descripción	Soporte	Identificador de política	OID Política
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.50.2.2

2.2 CERTIFICADOS SSL CUALIFICADOS (EV).

8. Este certificado tiene la consideración de cualificado según el Reglamento eIDAS. Será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía robusta al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado.
9. La validez de estos está marcada por las reglas de CABforum.
10. Jerarquía CA raíz 2007 (CN=Izenpe.com).

SERVIDOR SEGURO (SSL/TLS)			
Breve descripción	Soporte	Identificador de política	OID Política
SSL cualificado	Software	QEVCP-w	1.3.6.1.4.1.14777.50.3.2
SSL cualificado	Software	QEVCP-w	1.3.6.1.4.1.14777.6.1.3

11. Jerarquía CA raíz 2024 (CN=ROOT CA SSL IZENPE 2024).

SERVIDOR SEGURO 2024			
Breve descripción	Soporte	Identificador de política	OID Política
SSL Cualificado	Software	QEVCP-w	1.3.6.1.4.1.14777.50.3.2

2.3 VALIDACIÓN DE CERTIFICADOS.

12. La verificación del estado de los certificados es obligatoria, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.
13. Izenpe suministra información a los verificadores acerca de cómo y dónde encontrar la CRL y/o OCSP correspondiente.

3 LÍMITES DE USO DEL CERTIFICADO.

14. Los certificados de autenticación de sitio web permiten autenticar un sitio web y lo vinculan con la persona física o jurídica a quien se ha expedido.
15. Todos los certificados de autenticación de sitios web cualificados expedidos bajo este PDS son certificados cualificados conforme al Reglamento eIDAS y a los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-4 "Certificate profile for web site certificates".
16. Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.
17. Asimismo, los certificados deben emplearse únicamente de acuerdo con la legislación aplicable.
18. Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.
19. Si una entidad usuaria o un tercero confía en estos certificados sin acceder al servicio de información y consulta sobre el estado de validez de los certificados incluidos en esta PDS, no se obtendrá cobertura de la DPCG y de la DPC particular correspondiente, y carecerá de legitimidad alguna para reclamar o emprender acciones legales contra Izenpe por daños, perjuicios o conflictos provenientes del uso o confianza en un Certificado.
20. Izenpe prohíbe el uso de los certificados emitidos bajo la presente política para la intercepción ilegal o descifrado de comunicaciones cifradas (MITM), inspección profunda de paquetes (DPI), etc.

4 OBLIGACIONES DE LA CA.

21. Las obligaciones y responsabilidades de Izenpe, como prestador de servicios de confianza, con el suscriptor del certificado y, en su caso, con las partes usuarias y terceros que confían, quedarán determinadas, principalmente, en el documento relativo a las condiciones de utilización o el contrato de expedición del certificado, y, subsidiariamente, por la presente PDS.

22. Izenpe cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411 para la expedición de certificados y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.
23. Izenpe emite los certificados de autenticación de sitios web de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser Forum que pueden consultarse en la dirección https://cabforum.org/
24. Asimismo, adaptará sus prácticas de expedición de certificados a la versión vigente de los citados requisitos. En caso de cualquier incoherencia con esta PDS, dichos requisitos prevalecerán sobre este documento.
25. Adicionalmente, Izenpe se compromete a cumplir, en relación con la expedición de certificados cualificados, los requisitos establecidos por la entidad CA/Browser Fórum para este tipo de Certificados (EV SSL Certificate Guidelines), que pueden consultarse en la dirección https://cabforum.org/extended-validation/. En caso de cualquier incoherencia con esta PDS dichos requisitos prevalecerán sobre este documento.
26. Sin perjuicio de lo dispuesto en la normativa de aplicación a este tipo de certificados, así como las obligaciones descritas en el apartado correspondiente de la DPCG, Izenpe, con carácter previo a la expedición del certificado, se obliga a:
    - Comprobar la identidad y circunstancias personales del solicitante del certificado y del suscriptor y/o su representante y recoger la manifestación de que el solicitante está autorizado por el suscriptor para realizar la solicitud.
    - En el proceso de registro, comprobar los datos relativos a la personalidad jurídica del suscriptor y a la capacidad del representante. Todas estas comprobaciones se realizarán según lo dispuesto en este documento y los protocolos y procedimientos de registro de Izenpe.
    - En los procesos de comprobaciones anteriores, Izenpe podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de Registros competentes.
    - Verificar que toda la información contenida en la solicitud del certificado se corresponde con la aportada por la persona solicitante.
    - Comprobar que la persona solicitante está en posesión de la clave privada asociada a la clave pública que se incorpora al certificado a emitir.
    - Garantizar que los procedimientos seguidos aseguran que las claves privadas correspondientes a los certificados de autenticación de sitios web son generadas sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de Izenpe.
    - Realizar la comunicación de información al suscriptor, representante y solicitante de tal forma que se garantice su confidencialidad.
    - Poner a disposición del solicitante, suscriptor, representante y demás interesados (DPCG de Izenpe y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los certificados objeto de esta PDS de conformidad con la normativa aplicable.

5 OBLIGACIONES DE LA ENTIDAD DE REGISTRO.

27. Las actividades relativas a la entidad de registro (en adelante, RA) serán realizadas exclusivamente por Izenpe para todos los certificados de autenticación de sitios web.

28. La RA tiene las siguientes obligaciones:

    - Con carácter general, seguir los procedimientos establecidos por Izenpe en la DPCG de aplicación en el desempeño de sus funciones de gestión, expedición y revocación de certificados y no alterar dicho marco de actuación.
    - En particular, comprobar la identidad, y cualesquiera circunstancias personales relevantes para la finalidad determinada, de los solicitantes de los certificados, suscriptores y sus representantes, mediante cualquier medios admitido en Derecho y conforme a lo previsto con carácter general en la DPCG y con carácter particular en la presente PDS.

29. Comprobar que la titularidad del nombre de dominio se corresponde con la identidad del Suscriptor o, en su caso, obtener la autorización de éste, que se asociará al Certificado de autenticación de sitios web, por los medios a su alcance que, razonablemente, permitan acreditar tal titularidad, de conformidad con el estado de la técnica.

    - Recoger expresamente el poder de decisión del suscriptor respecto a la titularidad del dominio del certificado de autenticación de sitios web.
    - Conservar toda la información y documentación relativa a los certificados, cuya solicitud, renovación o revocación gestiona durante 15 años.
    - Realizar la recepción y gestión de las solicitudes a través de la aplicación de gestión de solicitudes publica en www.izenpe.eus
    - Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los certificados.

6 OBLIGACIONES DE LOS SUSCRIPTORES.

30. Los suscriptores deben tener el control del nombre de dominio de sitio web incluido en dichos certificados y mantener bajo su uso exclusivo las Claves privadas asociadas.

31. El solicitante y el Suscriptor tienen la obligación de:

    - No usar el certificado fuera de los límites especificados en la presente PDS y en la DPCG.
    - No usar el certificado en caso de que el prestador de servicios de confianza haya cesado su actividad como entidad emisora de certificados, especialmente en los casos en los que los datos de creación del certificado del prestador puedan estar comprometidos, y así se haya comunicado.
    - Aportar información veraz en la solicitud de los certificados y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
    - No solicitar para el Sujeto del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.

- Actuar con diligencia respecto de la custodia y conservación de los datos de creación de firma o cualquier otra información sensible como claves, códigos de activación del certificado, palabras de acceso, números de identificación personal, etc., así como de los soportes de los certificados, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los certificados previstas en las condiciones de uso y en la DPCG y en particular, las limitaciones de uso de los Certificados.
- Conocer y cumplir las modificaciones que se produzcan en la DPCG.
- Solicitar la revocación del correspondiente certificado, según el procedimiento descrito en el presente documento, notificando diligentemente a Izenpe las circunstancias para la revocación o sospecha de pérdida de la Confidencialidad, la divulgación, modificación o uso no autorizado de las claves privadas asociadas,
- Revisar la información contenida en el certificado, y notificar a Izenpe cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los certificados, la firma electrónica o el sello electrónico avanzados del prestador de servicios de confianza emisor del certificado.
- Notificar diligentemente a Izenpe cualquier modificación de los datos aportados en la solicitud del certificado, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.

32. Será en todo caso responsabilidad del suscriptor utilizar de manera adecuada y custodiar diligentemente el certificado, según el propósito y función para el que ha sido expedido, así como informar a Izenpe acerca de cualquier variación de estado o información respecto de lo reflejado en el certificado, para su revocación y nueva expedición.
33. Asimismo, será el suscriptor quien deba responder, en todo caso, ante Izenpe, las entidades usuarias y, en su caso, ante terceros, del uso indebido del certificado, o de la falsedad o errores de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a Izenpe o a terceros.
34. Será responsabilidad y, por tanto, obligación del suscriptor no usar el certificado en caso de que Izenpe haya cesado en la actividad como entidad emisora de certificados que realizó la expedición del certificado en cuestión y no se hubiera producido la subrogación prevista en la ley. En todo caso, el suscriptor no usará el certificado en los casos en los que los datos de creación de firma del prestador puedan estar amenazados y/o comprometidos, y así se haya comunicado por el prestador o, en su caso, hubiera tenido noticia de estas circunstancias.
35. Las relaciones de Izenpe y el suscriptor quedarán determinadas principalmente, a los efectos del régimen de uso de los certificados, a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del certificado y atendiendo a los acuerdos, convenios o documento de relación entre Izenpe y la Entidad correspondiente.

7 OBLIGACIONES DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS DE LAS PARTES QUE CONFÍAN.

36. Las terceras partes que confían y aceptan el uso de los certificados emitidos por Izenpe deberán verificar:

    - Que el certificado continúa vigente y no está revocado.
    - El estado de los certificados incluidos en la cadena de certificación.

8 LIMITACIONES DE RESPONSABILIDAD.

37. 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:

    - 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 declaración de prácticas de certificación.
    - Izenpe no será responsable 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.
    - Izenpe no será responsable 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.
    - Izenpe no será responsable 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.

38. 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.

39. 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.

9 ACUERDOS APLICABLES Y DECLARACIÓN DE PRÁCTICAS DE CONFIANZA.

40. El documento DPCG, 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 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 este tipo de certificados.

41. El documento PDS correspondiente a los certificados de autenticación de sitio weB , publicado en la dirección https://www.izenpe.eus/documentacion-juridica/webize01-cndocjuridica/es/, recoge la información pública de las condiciones y características de los servicios de expedición de certificados electrónicos SSL no cualificados y cualificados, recogiendo las obligaciones y procedimientos que se compromete a cumplir en relación con la expedición de estos certificados.

10 POLÍTICA DE PRIVACIDAD.

42. 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.

11 POLÍTICA DE DEVOLUCIÓN.

43. Izenpe no dispone de una política de reintegro.

12 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS.

44. 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.

13 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA.

45. 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”.

46. 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.