TEXTO DE DIVULGACIÓN (PDS) CORRESPONDIENTE A LOS CERTIFICADOS 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 11:06:09 +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 CUALIFICADOS DE PERSONA FÍSICA 5
2.1.1 CIUDADANÍA. 5
2.1.1.1 BAKQ. 5
2.1.1.2 CERTIFICADO DEL TIPO CIUDADANO. 6
2.1.2 REPRESENTANTE. 6
2.1.2.1 REPRESENTANTE DE ENTIDAD. 6
2.1.2.1.1 TARJETA/CHIP CRIPTOGRÁFICO. 6
2.1.2.1.2 CONTENEDOR SOFTWARE. 7
2.1.2.2 REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA 7
2.1.2.2.1 TARJETA/CHIP CRIPTOGRÁFICO. 7
2.1.2.2.2 CONTENEDOR SOFTWARE 8
2.1.3 PROFESIONAL 8
2.1.3.1 PERSONAL DE EMPLEADO PÚBLICO. 8
2.1.3.1.1 HSM ..... ¡ERROR! MARCADOR NO DEFINIDO.
2.1.3.1.2 TARJETA/CHIP CRIPTOGRÁFICO 9
2.1.3.1.3 CONTENEDOR SOFTWARE 9
2.1.3.2 PERSONAL DE ENTIDAD PÚBLICA CON SEUDÓNIMO 9
2.1.3.2.1 TARJETA/CHIP CRIPTOGRÁFICO. 10
2.1.3.2.2 CONTENEDOR SOFTWARE 10
2.1.3.3 PROFESIONAL CORPORATIVO 10
2.1.3.3.1 HSM 10
2.1.3.3.2 TARJETA/CHIP CRIPTOGRÁFICO 11
2.1.3.3.3 CONTENEDOR SOFTWARE 11
2.2 VALIDACIÓN DE LOS CERTIFICADOS 11
3 LÍMITES DE USO DEL CERTIFICADO DIRIGIDOS A LOS FIRMANTES 12
4 OBLIGACIONES DE LOS SUSCRIPTORES 12
5 OBLIGACIONES DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS DE LAS PARTES QUE CONFÍAN. 13
6 LIMITACIONES DE RESPONSABILIDAD 13
7 ACUERDOS APLICABLES Y DECLARACIÓN DE PRÁCTICAS DE CONFIANZA 14
8 POLÍTICA DE PRIVACIDAD 14
9 POLÍTICA DE DEVOLUCIÓN 15
10 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS 15
11 LICENCIAS Y REPOSITORIO, MARCAS CONFIABLES Y AUDITORÍA 15

1. El presente documento constituye la *PKI Disclousure Statement* (en adelante, PDS) correspondiente a los certificados cualificados del tipo Ciudadano, Representante de entidad (con y sin personalidad jurídica), Personal de entidad pública (con y sin seudónimo) y profesional corporativo 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.

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

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.

3. La persona solicitante podrá tramitar la solicitud de revocación 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 persona física.

4. Los medios de identificación regulados en la presente PDS se expiden de acuerdo con lo establecido en el Reglamento eIDAS[1] y en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, LSEC)
5. Estos certificados son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento eIDAS. En caso de emplear un dispositivo cualificado de creación de firma, los certificados cualificados son conformes con el Anexo II del mencionado Reglamento.
6. Los certificados 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.
7. Izenpe emite los siguientes certificados cualificados de persona física:

2.1.1 Ciudadanía.

2.1.1.1 BaKQ.

8. BaKQ es un medio que permite la identificación y firma de personas físicas formado por:
   - Un número de referencia coincidente con el DNI/NIE del usuario.
   - Una contraseña.
   - Un código de un solo uso que se enviará bien por SMS al teléfono móvil de la persona usuaria o bien a través de la aplicación NIK Patrika siempre que la persona usuaria haya autorizado la recepción de avisos de Izenpe.
   - Un certificado cualificado emitido en un repositorio centralizado de Izenpe que servirá para los actos de firma y atenticación si se hace uso de la tarjeta virtual.
9. La emisión de BakQ implica la emisión de una Bak[2], por lo que, si la persona solicitante es ya titular de una Bak en el momento de solicitar BakQ, se procederá a la revocación de la Bak inicial.
10. Los certificados cualificados BakQ son gestionados de forma centralizada, y permiten la generación de firma electrónica avanzada basada en certificado electrónico cualificado:
11. Jerarquía CA raíz 2007 (CN=Izenpe.com)

[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.

[2] Consultar la PDS de certificados no cualificados de persona física. Disponible en: www.izenpe.eus

CIUDADANO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
BakQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Avanzada

12. El certificado cualificado de persona física BakQ tiene una duración de hasta 4 años.

2.1.1.2 Certificado del tipo Ciudadano.

13. Este certificado se expide en tarjeta y permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado
14. Jerarquía CA raíz 2007 (CN=Izenpe.com)

CIUDADANO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Certificado Ciudadano	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.18.1	Avanzada

15. El certificado cualificado de persona física del tipo Ciudadano tiene una duración de hasta 4 años.

2.1.2 Representante.

2.1.2.1 Representante de entidad.

16. Este certificado se expide con la consideración de cualificado de persona física de acuerdo con lo establecido en el Reglamento eIDAS y en la LSEC.
17. Está vinculado a la entidad y acredita la condición de representante legal de la persona física identificada.
18. Tiene una duración de hasta 4 años.
19. Se expide en: los siguientes soportes:

2.1.2.1.1 Tarjeta/chip criptográfico.

20. Permitiendo la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
21. Jerarquía CA raíz 2007 (CN=Izenpe.com).

REPRESENTANTE DE ENTIDAD				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Representante entidad	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.16	Avanzada

2.1.2.1.2 Contenedor software.

22. Este certificado no se gestiona de forma centralizada, y permiten la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
23. Jerarquía CA raíz 2007 (CN=Izenpe.com).

REPRESENTANTE DE ENTIDAD				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Representante entidad	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.12	Avanzada

2.1.2.2 Representante de entidad sin personalidad jurídica.

24. Se expide con la consideración de cualificado de persona física de acuerdo con lo establecido en el Reglamento eIDAS y en la LSEC.
25. Se expide en los siguientes soportes:

2.1.2.2.1 Tarjeta/chip criptográfico.

26. Permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
27. Jerarquía CA raíz 2007 (CN=Izenpe.com)

REPRESENTANTE DE ENTIDAD SPJ				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Representante Entidad SPJ	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.13	Avanzada

2.1.2.2.2 Contenedor software.

28. Permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
29. Jerarquía CA raíz 2007 (CN=Izenpe.com).

REPRESENTANTE DE ENTIDAD SPJ				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Representante Entidad SPJ	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.17	Avanzada

2.1.3 Profesional.

2.1.3.1 Personal de Empleado Público.

30. Emitido en el ámbito de la "Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público".
31. Se configura como un certificado cualificado de persona física según el Reglamento Eidas.
32. Identifica a la Administración Pública actuante como suscriptora, así como a la persona que desempeña un cargo o puesto en la misma, como poseedor de claves.
33. La Administración suscriptora podrá realizar funciones de identificación de los poseedores de claves pertenecientes a la misma.
34. En este ámbito, Izenpe expide certificados con seudónimo según lo determinado en el documento de *Perfiles de Certificados electrónicos* del Ministerio de Hacienda y Administraciones Públicas.
35. Duración: hasta 4 años.
36. Medio de identificación y firma formado por:
    - Un número de referencia coincidente con el DNI/NIE de la persona usuaria.
    - Una contraseña.
    - Un código de un solo uso que se enviará bien por SMS al teléfono móvil o al correo electrónico de la persona usuaria o bien a través de la aplicación NIK Patrika siempre que la persona usuaria haya autorizado la recepción de avisos de Izenpe.
    - Un certificado cualificado emitido en un repositorio centralizado de Izenpe que servirá para actos de firma y atenticación si se hace uso de la tarjeta virtual
37. Estos certificados son gestionados de forma centralizada, y permiten la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
38. Jerarquía CA raíz 2007 (CN=Izenpe.com)
39. Se expide en los siguientes soportes:

2.1.3.1.1 HSM.

PERSONAL DE EMPLEADO PÚBLICO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Personal de Empleado Público	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Avanzada

2.1.3.1.2 Chip criptográfico.

40. Este certificado permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
41. Jerarquía CA raíz 2007 (CN=Izenpe.com)

PERSONAL DE EMPLEADO PÚBLICO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Personal de Empleado Público	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.4.14.1	Avanzada

2.1.3.1.3 Contenedor software.

42. Este certificado permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado.

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

PERSONAL DE EMPLEADO PÚBLICO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Personal de Empleado Público	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.4.14.2	Avanzada

2.1.3.2 Personal de entidad pública con seudónimo.

43. Izenpe emite certificados de empleado público con seudónimo en tarjeta/chip criptográfico según lo determinado en el documento de "*Perfiles de Certificados electrónicos* del Ministerio de Hacienda y Administraciones Públicas".
44. Este certificado se expide,

2.1.3.2.1 Chip criptográfico:

45. Estos certificados permiten la generación de firma electrónica avanzada basada en certificado electrónico cualificado.
46. Jerarquía CA raíz 2007 (CN=Izenpe.com).

PERSONAL DE EMPLEADO PÚBLICO CON PSEUDÓNIMO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Personal de Entidad Pública con seudónimo	Chip criptográfico	QCP-n	Firma 1.3.6.1.4.1.14777.4.13.1.1	Avanzada

2.1.3.2.2 Contenedor software:

47. Estos certificados permiten la generación de firma electrónica avanzada basada en certificado electrónico cualificado:
48. Jerarquía CA raíz 2007 (CN=Izenpe.com)

PERSONAL DE EMPLEADO PÚBLICO CON PSEUDÓNIMO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Personal de Entidad Pública con seudónimo	Contenedor software	QCP-n	1.3.6.1.4.1.14777.4.13.2	Avanzada

2.1.3.3 Profesional corporativo.

49. Configurado como un certificado de firma electrónica con la consideración de cualificado según el Reglamento eIDAS.

50. Identifica a la entidad actuante como suscriptora del certificado y a la persona que desempeña un cargo o puesto en la misma, como persona firmante que responde de la custodia de las claves.
51. Este certificado tiene una duración de hasta 4 años.
52. Este certifiado se expide:

2.1.3.3.1 HSM.

53. Esto certificado se gestiona de forma centralizada, y permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado:
54. Jerarquía CA raíz 2007 (CN=Izenpe.com)

PROFESIONAL CORPORATIVO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Corporativo cualificado	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Avanzada

2.1.3.3.2 Chip criptográfico.

55. En la jerarquía CA raíz 2007, este certificado permite la generación de firma electrónica avanzada basada en certificado electrónico cualificado:

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

PROFESIONAL CORPORATIVO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Corporativo cualificado	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.19.1	Avanzada

2.1.3.3.3 Contenedor software.

57. Estos certificados permiten la generación de firma electrónica avanzada basada en certificado electrónico cualificado:

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

PROFESIONAL CORPORATIVO				
Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Corporativo cualificado	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.19.2	Avanzada

2.2 VALIDACIÓN DE LOS CERTIFICADOS.

59. 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.

60. 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.

61. Los certificados indicados en esta PDS solo pueden ser utilizados para generar firmas electrónicas y para la autenticación de la identidad de los firmantes.

62. 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 suscriptora (en los certificados de ciudadano el subscriptor y el firmante son la misma persona física). En los certificados de persona vinculada, de representante o de empleado público, el subscriptor es una persona jurídica). Asimismo, el firmante se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por Izenpe.

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

64. El firmante no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de Izenpe, sin previo permiso expreso.

65. Izenpe conserva durante 15 años (desde la extinción del certificado o la finalización del servicio prestado) toda la información y documentación relativa a los certificados cualificados.

4 OBLIGACIONES DE LOS SUSCRIPTORES.

66. El suscriptor está obligado a:

- Facilitar a Izenpe información completa y adecuada, conforme a los requerimientos de la DPCG.
- 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.
- Mantener o, respectivamente, emplear la clave privada bajo su control exclusivo.
- Se recomienda emplear el par de claves únicamente para realizar firmas electrónicas.
- 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 del mismo.

– Dejar de emplear la clave privada transcurrido el periodo de validez del certificado.

– Transferir a los firmante 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.

67. 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.

68. 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 DPCG.

– 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.

69. 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.

70. 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.

71. 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.

72. Los documentos PDSs correspondiente a los medios de identificación y firma emitidos a la ciudadanía, al certificado del tipo representante y representante SPJ y certificados del tipo profesional (corporativo y empleado público), publicados en la dirección https://www.izenpe.eus/documentacion-juridica/webize01-cndocjuridica/es/, recogen la información pública, las condiciones y características de los servicios de certificación y servicios de expedición de certificados electrónicos de persona física, de representante de persona jurídica, de representante de entidad sin personalidad jurídica, de personal de entidad pública, de personal de entidad pública con seudónimo y de profesional corporativo 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.

73. 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.

9 POLÍTICA DE DEVOLUCIÓN.

74. Izenpe no dispone de una política de reintegro.

10 LEY APLICABLE, QUEJAS Y RESOLUCIÓN DE DISPUTAS.

75. 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.

76. 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 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 319 412-2 “Certificate profile for certificates issued to natural persons”.

77. Los certificados de persona física BakQ y certificado del tipo Ciudadano, de representante de entidad con y sin personalidad jurídica, de personal de entidad pública con y sin seudónimo, de profesional corporativo cualificado se expiden como cualificados conforme al Reglamento eIDAS.

78. 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.

79. 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.