POLITICA DE CERTIFICADO DEL TIPO PROFESIONAL

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2022.10.26 07:22:48 +02'00'

CONTROL DE CAMBIOS

VERSION	CAMBIO
1.1	➢ 1.1. Definición: emisión de certificados *Profesional-Personal de Entidad Pública* con seudónimo. ➢ 1.2. Soporte y nivel de seguridad. Emisión de certificados Profesionales en soporte tarjeta/token USB y software. ➢ 1.3. Ámbito de uso: se corrige el ámbito de uso de los certificados profesionales. ➢ 1.4. Identificación certificada: se asigna un nuevo OID para los certificados del tipo *Profesional* emitidos en soporte tarjeta/token USB y software. ➢ 2.1. Verificación de la identidad: actualización de los documentos de identificación requeridos a ciudadano extracomunitario: NIE y pasaporte. ➢ 3. Importe: previsión de diferentes modalidades de pago en base a proyectos específicos.
	Eliminación: ➢ Apartado 1.1. La versión 1.0 definía diferentes tipos de certificados en función de la consideración de la entidad suscriptora como perteneciente al sector público o sector privado. La versión 1.1 elimina esta diferenciación. ➢ Apartado 1.2. Soportes: se elimina la previsión de emisión de certificados en soporte HSM y navegador. ➢ Apartado 1.5: Disposiciones Generales: se consideran aspectos regulados en la DPC.
1.2	➢ Apartado 1.2., se elimina la previsión de emisión en soporte HSM
1.3	– La versión 1.3 de la Política de Representante regula la expedición de este certificado en soporte HSM. – Epígrafe 2, se actualiza la descripción del ciclo de vida del certificado.
1.4	– Se han añadido los perfiles de las nuevas raíces 2020

VERSIÓN	FECHA	CAMBIO
1.5	21/03/2022	– Epígrafe 1.2_Jerarquia CA raíz 2007: actualización del identificador de política. – Epígrafe 2: actualización de la redacción del ciclo de vida y actualización de la documentación requerida. – Epígrafe 2.6: se actualiza el procedimiento de revocación.

		– Se incluyen los epígrafes 5: privacidad y protección de datos, 6: mecanismo de resolución de conflictos y 7: actualización del proceso de gestión del cambio.
1.6	01/09/22	Epígrafe, – 1.1. Actualización de la normativa aplicable. – 1.2. Jerarquía CA raíz 2007: actualización del identificador de política. OID de tipo de firma de seudónimo a Avanzada – 2.2.2. Verificación de la identidad de la persona solicitante, – Actualización de la documentación requerida para su identificación. – Actualización del procedimiento de verificación realizado por medio de un certificado cualificado vigente. – 2.6. Revocación del certificado, – Se incluye como posible solicitante de revocación a un tercero con interés legítimo. – Se actualiza el procedimiento de revocación de un certificado realizado a través de la remisión a la dirección izenpe@izenpe.eus. – Se incluye la revocación a través de la aplicación de revocación on line. – 4. Inclusión de referencias a la seguridad de la información. – 5 y 6. Modificación del orden de los epígrafes. – Se actualiza el documento desde la perspectiva del lenguaje inclusivo en cuanto al género.
1.7	21/10/2022	Epígrafe, – 1.2: Jerarquía CA raíz 2007 (CN=Izenpe.com): se actualiza el valor de identificador de política a QCP-n en los OIDs en vigor en chip criptográfico.

ÍNDICE

El presente documento recoge la *Política* correspondiente a los certificados del tipo *Profesional* emitidos por *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.* (en adelante, Izenpe).

Su finalidad es detallar y completar lo definido de forma genérica en la *Declaración de Prácticas de Certificación de* Izenpe www.izenpe.eus/dpc

1 DESCRIPCIÓN DEL CERTIFICADO

1.1 Definición

Según el ámbito de emisión, Izenpe emite certificados del tipo,

- *Profesional-Personal de Entidad Pública*,

  Emitido en el ámbito de la *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

  Se configura como un certificado cualificado de persona física según el *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* (en adelante, eIDAS) y la *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.*

  Este certificado 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.

  La Administración suscriptora podrá realizar funciones de identificación de los poseedores de claves pertenecientes a la misma.

  En este ámbito Izenpe emite certificados con seudónimo según lo determinado en el documento de *Perfiles de Certificados electrónicos* del Ministerio de Hacienda y Administraciones Públicas.

- *Profesional-Corporativo*,

  Emitido en el ámbito de una organización perteneciente tanto sector público como al ámbito privado.

  Tipos,

  - *Profesional-Corporativo cualificado*,

    Configurado como un certificado de firma electrónica con la consideración de cualificado según *eIDAS.*

    Identifica a la entidad actuante como suscriptora del certificado y a la persona que desempeña un cargo o puesto en la misma, como poseedora de claves que responde de la custodia de las claves.

  - *Profesional-Corporativo no cualificado*,

    Identifica, con un grado medio de aseguramiento, la entidad actuante como suscriptora del certificado, así como a la persona que desempeña un cargo o puesto en la misma, como poseedor de claves.

    No tiene la consideración de cualificado según eIDAS.

Tendrá la consideración de,

- Suscriptor: Administración Pública o entidad identificada en el certificado.
- Persona poseedora de claves: persona física identificada en el certificado que posee o responde de la custodia de las claves de firma digital.
- Persona solicitante: persona que solicita el certificado en nombre de una organización (Administración Pública y/o entidad).

Todos los certificados incluidos en la presente Política tienen una duración de 4 años.

1.2 Soporte y nivel de seguridad

El certificado del tipo *Profesional* se expide en diferentes soportes y según los niveles de aseguramiento determinados en,

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

PROFESIONAL					
Breve descripción	**Soporte**	**Identificador de política**	**OID política**	**Nivel identificación eIDAS**	**Tipo firma eIDAS**
Personal de Entidad Pública	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.4.14.1	Alto	Avanzada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.4.14.2	Sustancial	Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Alto (con tarjeta virtual) / Sustancial (con Giltza)	Avanzada
Personal de Entidad Pública con seudónimo	Chip criptográfico	QCP-n	Firma 1.3.6.1.4.1.14777.4.13.1.1	Alto	Avanzada
		NCP+	Autenticación 1.3.6.1.4.1.14777.4.13.1.2	Alto	n/a
		n/a	Cifrado 1.3.6.1.4.1.14777.4.13.1.3	Alto	n/a
Corporativo cualificado	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.19.1	Alto	Avanzada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.19.2	Sustancial	Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Alto (con tarjeta virtual) / Sustancial (con Giltza)	Avanzada
Corporativo no cualificado	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a (no cualificado)	Avanzada

Personal de las Entidades públicas (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	n/a	Reconocida
Personal del Gobierno Vasco (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.7.1	n/a	Reconocida
Corporativo público reconocido (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	n/a	Reconocida
Corporativo público no reconocido (pre-eIDAS)	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a	Avanzada
Corporativo privado reconocido (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	n/a	Reconocida
Corporativo privado no reconocido (pre-eIDAS)	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.5.2.2	n/a	Avanzada

1.2.2 Jerarquía CA raíz 2020 cualificados (CN=ROOT CA QC IZENPE)

PROFESIONAL						
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS		Tipo firma eIDAS
Personal de Entidad Pública	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.9.1.1	Alto		Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.9.1.2	Sustancial		Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.9.1.3	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada
Personal de Entidad Pública con seudónimo	Chip criptográfico	QCP-n-qscd	Firma 1.3.6.1.4.1.14777.9.2.1	Alto		Cualificada
		NCP+	Autenticación 1.3.6.1.4.1.14777.9.2.2	Alto		n/a
		n/a	Cifrado 1.3.6.1.4.1.14777.9.2.3	Alto		n/a

Corporativo cualificado	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.8.2.1	Alto		Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.8.2.2	Sustancial		Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.8.2.3	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada

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

PROFESIONAL					
Breve descripción	**Soporte**	**Identificador de política**	**OID política**	**Nivel identificación eIDAS**	**Tipo firma eIDAS**
Profesional no cualificado	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.11.4.2	n/a (no cualificado)	Avanzada

1.3 Ámbito de uso

El certificado será utilizado por la persona poseedora de claves en aquellos servicios ofrecidos por terceros que admitan su uso, con las condiciones y limitaciones definidas en el documento de Términos y Condiciones, www.izenpe.eus/condicionesuso, y en la *Declaración de Prácticas de Certificación, www.izenpe.eus/dpc,* de Izenpe.

2 CICLO DE VIDA DEL CERTIFICADO

2.1 Solicitud

Mediante el acceso a www.izenpe.eus, la persona solicitante y la poseedora de claves completarán el formulario de solicitud del certificado.

A través de la firma de la solicitud, la persona poseedora de claves aceptará los Términos y Condiciones del certificado.

2.2 Verificación de la identidad del poseedor de claves.

2.2.1 Certificado no cualificado.

En los casos de certificado no cualificado no será necesario verificar de forma presencial o equivalente la identidad de la persona poseedora, aunque sí se requerirá una solicitud firmada.

2.2.2 Certificado cualificado.

Izenpe verificará la identidad de la persona poseedora de claves,

– De manera presencial

La persona solicitante mediante acceso a www.izenpe.eus, solicitará cita para personarse ante la Entidad de Registro con la siguiente documentación en vigor,

- Ciudadano/a de nacionalidad española: DNI, pasaporte o permiso de conducción.
- Ciudadano/a de la Unión Europea: pasaporte o documento de identidad de su país de origen junto con Tarjeta de Identificación de Extranjero o certificado emitido por el Registro de Ciudadanos miembros de la Unión o documento oficial de concesión del NIE.
- Ciudadano/a extracomunitario/a: pasaporte junto con Tarjeta de Identificación de Extranjero o documento oficial de concesión del NIE.

La identificación del poseedor de claves podrá realizarse ante la organización solicitante con la que Izenpe haya suscrito el instrumento legal pertinente.

– Legitimación de la firma de la Solicitud de Emisión por notario.

El solicitante,

- Completará y firmará la *Solicitud de emisión* y aceptará los *Términos y Condiciones de uso*. El notario legitimará la firma de la solicitud.
- Enviará la documentación requerida a la dirección IZENPE, S.A.- C/ BEATO TOMAS DE ZUMARRAGA, 71 -1ª PLANTA – 01008 VITORIA-GASTEIZ.

– O por medio de un certificado cualificado vigente.

Para ello, la persona solicitante accederá a www.izenpe.eus y firmará la *Solicitud de Emisión* mediante la utilización de un certificado cualificado expedido por una CA incluida en la EU TSL (Trusted Service List).

2.3 Acreditación de la organización y facultades del solicitante

Izenpe comprobará la constitución y vigencia de la entidad y las facultades de la persona solicitante mediante los documentos que acrediten estos extremos o mediante comprobaciones registrales pertinentes.

2.4 Procedimiento de emisión y entrega

Izenpe procederá a la emisión y entrega del certificado,

➢ CONTENEDOR DE IZENPE

1. Izenpe envía por correo electrónico a la dirección indicada en la solicitud un contenedor vacío a la persona poseedora de claves.
2. La persona poseedora de claves inicializa el contenedor y genera un par de claves y la petición técnica (csr).
3. La persona poseedora de claves envía el fichero de petición técnica (csr) a Izenpe.
4. Izenpe emite el certificado utilizando la petición técnica proporcionada por la persona poseedora de claves.
5. Izenpe envía el certificado a la dirección de email indicada en el formulario de solicitud.

➢ TARJETA / TOKEN USB

– Entrega presencial.
Izenpe entregará a la persona solicitante o a tercera persona (deberá aportar documento de autorización firmado y legitimado por notario) el certificado, el PIN y el código de desbloqueo (PUK).

– Entrega no presencial.
Izenpe enviará el certificado a la dirección postal indicada en la *Solicitud de Emisión* junto con las claves en 2 envíos diferenciados, haciéndose cargo de los gastos de envío la entidad solicitante.

Izenpe verifica que el envío se entrega únicamente al poseedor de claves.

➢ HSM

Izenpe,

– Generará el certificado en su HSM y un usuario y una contraseña (garantizando que únicamente se entregan al poseedor de claves).

– Y enviará un correo electrónico a la dirección indicada en la *Solicitud de Emisión* junto con las instrucciones de utilización.

2.5 Verificación del certificado

La persona firmante dispondrá de 15 días hábiles desde la emisión del certificado para verificar su correcto funcionamiento y, en caso de que fuera necesario, comunicar a Izenpe los defectos de funcionamiento.

Únicamente si los defectos de funcionamiento se debieran a causas técnicas (entre otras: mal funcionamiento del soporte del certificado, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado aplicables a Izenpe, Izenpe revocará el certificado y procederá a emitir uno nuevo asumiendo los costes derivados.

2.6 Revocación del certificado

➢ Causas de revocación

Pueden consultarse en la Declaración de Prácticas de Certificación www.izenpe.eus

➢ Solicitud de revocación

Podrán solicitar la revocación del certificado,

– La persona suscriptora, a nombre del cual fue emitido el certificado.

– Izenpe, en las causas identificadas en la DPC.

– Tercera persona con interés legítimo.

- Procedimiento de revocación

  La persona solicitante de la revocación tramitará ante Izenpe la Solicitud de Revocación.

  Podrá revocar el certificado 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 de Izenpe, S.A.- c/ Beato Tomás de Zumárraga, 71 -1ª planta – 01008 Vitoria-Gasteiz
  - Remitiendo a la dirección 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 https://servicios.izenpe.com/gestionCertificados/

  Izenpe revocará el certificado en las 24 horas siguientes a la recepción de la solicitud de un día laborable e informará por correo electrónico al solicitante y al suscriptor del cambio de estado del certificado.

2.7 Renovación de certificados

En el plazo de 60 días previos a la caducidad del certificado se podrá proceder a su renovación.

Izenpe tramitará la renovación según el procedimiento de emisión y entrega previsto.

3 IMPORTE

Anualmente Izenpe publica en su web www.izenpe.eus las tarifas aplicables.

Opciones de pago ofrecidas,

- En el caso de solicitud de emisión firmada electrónicamente,
  - Pago on line a través de pasarela de pago
  - Carta de pago para presentar ante la entidad bancaria.
- O pago presencial ante la Entidad de Registro de Izenpe a través de tarjeta bancaria.

4 PERFILES DE CERTIFICADOS

Izenpe publica en www.izenpe.eus los perfiles de los certificados.

5 SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Izenpe publica en www.izenpe.eus/datos la información relativa a la seguridad y privacidad de la información.

6 GESTIÓN DEL CAMBIO

Los cambios de esta Política serán aprobados por del Comité de Seguridad de Izenpe.

Las versiones actualizadas de la documentación específica podrán ser consultadas en la dirección www.izenpe.eus.

7 MECANISMOS DE RESOLUCIÓN DE CONFLICTOS

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.