TÉRMINOS Y CONDICIONES DE USO DE MEDIOS ELECTRÓNICOS PARA IDENTIFICACIÓN Y FIRMA

Nº Versión: v 2.1
Fecha: 04 de abril de 2019

ÍNDICE

1 INTRODUCCIÓN

El presente documento tiene como finalidad describir los términos y condiciones en los que *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A."* (en adelante, Izenpe) expide medios para la identificación y firma electrónica.

Izenpe tiene la consideración de prestador cualificado de servicios de confianza en el ámbito del *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).

Como tal, expide medios para,

- Identificación,
  Además de los medios de identificación basados en certificados electrónicos, expide B@K y B@KQ, que permiten la autenticación de una persona física mediante un número de referencia coincidente con el DNI/NIE del usuario y una contraseña.
  B@KQ incorpora además un juego de coordenadas de 16 posiciones.

- Firma,
  A efectos de firma, Izenpe emite medios basados en certificados electrónicos de diferentes tipos y en distintos soportes, según las especificaciones determinadas en la *Política específica* correspondiente *y* en la *Declaración de Prácticas de Certificación*.

Este documento ha sido creado de acuerdo con los requisitos técnicos del Anexo B *de ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"*.

En ningún caso reemplaza la Declaración de Practicas de Certificación ni las políticas de certificados, disponibles en www.izenpe.eus.

2 DATOS DE CONTACTO

Nombre del prestador	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Dirección postal	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Dirección e-mail	info@izenpe.com
Teléfono	902 542 542 / 945 01 62 90

3 DEFINICIONES

- Identificación electrónica, el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.
- Medios de identificación electrónica, una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.
- Autenticación, proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
- Firma electrónica, los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- Firma electrónica avanzada, la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS.
- Firma electrónica cualificada, una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- Certificado de firma electrónica, una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.
- Certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I Reglamento eIDAS.
- Prestador de servicios de confianza, una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas.
- Prestador cualificado de servicios de confianza, un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación;
- Entidades de Registro, entidades que realiza las tareas de identificación de los solicitantes, suscriptores y poseedores de claves de los certificados, comprobación de la documentación acreditativa las circunstancias que constan en los certificados así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los certificados.
- Usuarios de los certificados.
  - Solicitante del certificado, todo certificado debe ser solicitado por una persona, en su propio nombre o en nombre de una organización.
  - Firmante, el firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
  - Suscriptor del certificado, persona física o jurídica identificada en el certificado.

- Poseedor de claves, persona física que poseen o responden de la custodia de las claves de firma digital.

- B@k, es un medio de identificación electrónica para personas físicas que permite su autenticación y firma, formado por:
  - Un número de referencia coincidente con el DNI/NIE/pasaporte del usuario y una contraseña.
  - Un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma.
  - Además, puede ser complementado por otros factores biométricos de autenticación como la huella dactilar o el reconocimiento facial.

- B@kQ, es un medio de identificación electrónica para personas físicas, que permite su autenticación y firma, formado por:
  - Un número de referencia coincidente con el DNI/NIE del usuario.
  - Una contraseña.
  - Un juego de coordenadas con 16 posiciones.
  - Un certificado cualificado de firma electrónica emitido en un repositorio centralizado seguro de Izenpe que servirá para los actos de firma.
  - Además, puede ser complementado por otros factores biométricos de autenticación como la huella dactilar o el reconocimiento facial.

4 TIPOS DE CERTIFICADO, PROCEDIMIENTO DE VALIDACIÓN Y USO

Las especificidades relativas a cada tipo de certificado emitido por Izenpe están reguladas en la *Política específica para cada certificado* que se adjunta a la *Declaración de Prácticas de Certificación.*

BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA	Nivel aseguramiento eIDAS
CIUDADANO				
B@K	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Bajo
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Sustancial
Certificado Ciudadano	Tarjeta/token USB (Chip criptográfico)	QCP-n-qscd	Perfil eIDAS 1.3.6.1.4.1.14777.2.6	Alto
			Perfil anterior a eIDAS 1.3.6.1.4.1.14777.2.18.1	Alto
REPRESENTANTE ENTIDAD				
Representante entidad	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	Sustancial
	Tarjeta/Token USB: chip criptográfico.	QCP-n-qscd	1.3.6.1.4.1.14777.2.12	Alto
	Software: Contenedor de certificados de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.16	Sustancial
REPRESENTANTE ENTIDAD SPJ				
Representante Entidad SPJ	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Sustancial
	Tarjeta/token USB: chip criptográfico.	QCP-n-qscd	1.3.6.1.4.1.14777.2.13	Alto
	Software: Contenedor de certificados de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.17	Sustancial
PROFESIONAL				

Personal de Entidad Pública	Tarjeta / token USB: chip criptográfico.	QCP-n-qscd	1.3.6.1.4.1.14777.4.14.1	Alto
	Software: contenedor de certificados de Izenpe.	QCP-n	1.3.6.1.4.1.14777.4.14.2	Sustancial
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Sustancial
Personal de Entidad Pública con seudónimo	Tarjeta / token USB: chip criptográfico	QCP-n-qscd	**Firma** 1.3.6.1.4.1.14777.4.13.1.1	Alto
		NCP+	**Autenticación** 1.3.6.1.4.1.14777.4.13.1.2	Alto
		n/a	**Cifrado** 1.3.6.1.4.1.14777.4.13.1.3	Alto
Corporativo cualificado	Tarjeta / token USB: chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.2.19.1	Alto
	Software: contenedor de certificados de Izenpe.	QCP-n	1.3.6.1.4.1.14777.2.19.2	Sustancial
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Sustancial
Corporativo no cualificado	Tarjeta / token USB	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a (no cualificado)
Personal de las Entidades públicas (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	n/a
Personal del Gobierno Vasco (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.7.1	n/a
Corporativo público reconocido (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	n/a
Corporativo público no reconocido (pre-eIDAS)	Tarjeta / token USB	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a
Corporativo privado	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	n/a

reconocido (pre-eIDAS)				
Corporativo privado no reconocido (pre-eIDAS)	Tarjeta / token USB	NCP+	1.3.6.1.4.1.14777.5.2.2	n/a

SELLO DE ENTIDAD				
Sello de entidad	Contenedor. Contenedor de certificados de Izenpe	QCP-l-qscd	1.3.6.1.4.1.14777.2.11	Sustancial
	HSM	QCP-l	1.3.6.1.4.1.14777.2.20	Sustancial

SELLO DE ADMINISTRACIÓN				
Sello de administración	Software Contenedor de certificados de Izenpe	QCP-l	1.3.6.1.4.1.14777.4.11.2	Sustancial
	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3	Sustancial
Sello de administración nivel medio (pre-eIDAS)	HSM	NCP+	1.3.6.1.4.1.14777.4.4	n/a

SERVIDOR SEGURO (SSL)				
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.1.2.4	n/a
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.1.2.1	n/a
SSL EV	Software	EVCP	1.3.6.1.4.1.14777.6.1.1	n/a
SEDE	Software	OVCP	1.3.6.1.4.1.14777.1.1.3	n/a
SEDE EV	Software	EVCP	1.3.6.1.4.1.14777.6.1.2	n/a

APLICACIÓN				
Aplicación	Software: contenedor de	NCP	1.3.6.1.4.1.14777.1.2.2	n/a

	certificados de Izenpe.			

FIRMA DE CÓDIGO				
Firma de código	Tarjeta	NCP+	1.3.6.1.4.1.14777.1.3.1	n/a

DISPOSITIVO			
Dispositivo	Software	NCP	1.3.6.1.4.1.14777.1.3.2

5 USOS DE LOS MEDIOS ELECTRÓNICOS

5.1 USOS APROPIADOS,

- PARA AUTENTICACIÓN,

  Estos medios electrónicos permiten la identificación y deberán utilizarse para la autenticación electrónica del suscriptor, o del poseedor de claves en su caso, ante aquellas Administraciones Públicas que los admitan.

  Cuando el medio sea utilizado para la identificación ante un servicio electrónico, Izenpe ofrecerá al organismo responsable del servicio el resultado de la autenticación.

- PARA FIRMA,

  - Certificados cualificados de persona física o jurídica

    Los certificados cualificados de firma y sellado pueden emplearse, si así se define en el tipo de certificado correspondiente, para firmar mensajes de autenticación, en particular desafíos de cliente SSL o TLS, correo electrónico seguro S/MIME, cifrado sin recuperación de claves u otros. Esta firma digital tiene el efecto de garantizar la identidad del suscriptor del certificado de firma.

    Adicionalmente, dichos certificados pueden dar soporte a firmas electrónicas avanzadas o cualificadas. dependiendo del soporte en que se realicen.

    Los certificados de sello electrónico deben utilizarse únicamente en el ámbito de las administraciones públicas, para el sellado electrónico de documentos.

  - Certificados no cualificados de persona física o jurídica

    Los certificados no cualificados no garantizan fehacientemente la identidad del suscriptor y, en su caso, del poseedor de la clave privada;

    En caso de emplearse para firmar, dicha firma no se podrá equiparar a la manuscrita.

    Los certificados no cualificados pueden también emplearse, si así se define en el tipo de certificado correspondiente, para firmar mensajes de autenticación, en particular desafíos de cliente SSL o TLS, correo electrónico seguro S/MIME, cifrado sin recuperación de claves, u otros.

  - Certificados de dispositivo informático

    Se emiten certificados de servidor seguro y de aplicación a entidades responsables de la operación de dispositivos informáticos.

    Los certificados de autenticación de sitio web permiten vincular un sitio web con la persona jurídica a quien se ha expedido el certificado.

    Los certificados de sede electrónica deben utilizarse únicamente en el ámbito de las administraciones públicas para la identificación de la sede electrónica.

  - Certificados de firma de código.

    Se emiten a las entidades titulares para garantizar la autenticación e integridad de un componente de dicho software.

5.2 USOS PROHIBIDOS DE LOS MEDIOS

- AUTENTICACIÓN, deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.
- FIRMA, deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades, y únicamente de acuerdo con la ley aplicable.

  Ningún certificado emitido por Izenpe se puede emplear para realizar trámites como Entidad de Registro.

  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.

6 LIMITACIONES EN LA CONFIANZA

Izenpe no aplica limitaciones específicas de confianza de sus certificados.

Se pueden consultar las limitaciones de uso (firma, sello, web) de cada tipo de certificado en el apartado anterior.

Izenpe en su actividad como prestador de servicios de confianza mantiene registros internos o asegura el archivado, de una forma segura, de los siguientes elementos:

- Evidencias de todos los eventos relacionados con el ciclo de vida de los certificados cualificados durante 15 años posteriores a la fecha de emisión.
- Evidencias de todos los eventos relacionados con el ciclo de vida de los certificados no cualificados durante 7 años posteriores a la fecha de caducidad.

7 OBLIGACIONES

7.1 DE IZENPE.

7.1.1 OBLIGACIONES GENERALES

De seguridad,

- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte, de acuerdo con su Política de Seguridad.
- Tomar medidas contra la falsificación de los medios y garantizar la confidencialidad en el proceso de generación y su entrega por un procedimiento seguro al firmante.
- Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticación e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
- Realizar de forma periódica comprobaciones regulares de la seguridad, con el fin verificar la conformidad con los estándares establecidos.
- La correcta gestión de su seguridad, gracias a la implementación de un Sistema de Gestión de la Seguridad de la Información de acuerdo a los principios establecidos por la ISO/IEC 27001 y que incluye, entre otras, las siguientes medidas:
    - Llevar a cabo una completa gestión de los sucesos de seguridad, con el fin de garantizar su detección, resolución y optimización.
    - Mantener los contactos y relaciones apropiadas con grupos de especial interés en materia de seguridad, como especialistas, foros de seguridad y asociaciones profesionales relacionadas con la seguridad de la información.
    - Planificar adecuadamente el mantenimiento y evolución de los sistemas, con el fin de garantizar en todo momento un rendimiento adecuado y un servicio que cumpla con todas las garantías las expectativas de los usuarios y clientes.
- Exigir a proveedores de albergue el cumplimiento de la normativa y estándares de seguridad (RGPD, ISO, ETSI, CABForum y Política de Seguridad de Izenpe).

Personal,

- Emplear al personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios ofrecidos y los procedimientos de seguridad y gestión adecuados en el ámbito de la firma electrónica.
- Cumplir la normativa y estándares de seguridad (RGPD, ISO, ETSI y Política de Seguridad de Izenpe).

Procedimiento,

- Antes de la emisión y entrega del medio de identificación y/o firma , Izenpe le informa de los términos y condiciones relativos a su uso, de su precio – cuando se establezca – de sus limitaciones de uso y de los instrumentos jurídicos vinculantes a los que hace referencia, en su caso, la Declaración de Prácticas de Certificación.
- Izenpe dispone de un plan de finalización del cese de su actividad en el que se especifican las condiciones en las que se realizaría.
- Izenpe informará al poseedor de claves acerca de la extinción de la vigencia de su certificado de manera previa o simultánea a su extinción, especificando los motivos y la fecha y la hora en la que el certificado quedará sin efecto.
- Toda esta información pública relativa a los certificados está recogida en el Servicio de Publicación de Izenpe definido en la Declaración de Prácticas de Certificación.

7.1.2 COMO ENTIDAD QUE EXPIDE MEDIOS ELECTRÓNICOS DE IDENTIFICACIÓN.

- Identificará al usuario de acuerdo con los niveles de aseguramiento definidos en eIDAS.
- Garantizará la complementariedad de los datos de identificación.
- Se asegurará de que el usuario está en posesión de los elementos que permiten su identificación.
- Cumplirá los requisitos técnicos y de personal exigidos por la legislación vigente.
- Antes de la emisión y entrega del medio de identificación, informará de los términos y condiciones relativos a su uso, de su precio – cuando se establezca – de sus limitaciones de uso y de los instrumentos jurídicos vinculantes.
- Izenpe ofrece mecanismos públicos de verificación de la validez de los certificados mediante los sistemas descritos en la Declaración de Prácticas de Certificación.
- Izenpe ofrecerá mecanismos de autenticación para comprobar la validez de los mecanismos de identificación

7.1.3 COMO ENTIDAD QUE EXPIDE MEDIOS ELECTRÓNICOS DE FIRMA.

- Obligaciones de prestación del servicio.

  Izenpe presta sus servicios de certificación conforme a la Declaración de Prácticas de Certificación, en la que se detallan sus funciones, procedimientos de operación y medidas de seguridad, y en concreto, responsabilizándose del cumplimiento de todas las obligaciones que le corresponden salvo las expresamente realizadas por la Entidad de Registro, siempre y cuando no actúe como tal.

  Estas obligaciones de la Entidad de Certificación son las siguientes:

- No copiar los datos de creación de firma de la persona a la que haya prestado sus servicios.
- Mantener un sistema en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida.
- Conservar registrada por cualquier medio seguro toda la información y documentación relativa a los certificados cualificados y a las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo y la relativa al resto de certificados, durante 7 años.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación. Que la identidad contenida en el certificado se corresponde de forma unívoca con la clave pública contenida en el mismo.
- La rapidez y seguridad en la prestación del servicio. En particular, se permite la utilización de un servicio rápido, seguro y gratuito de consulta de validez de los certificados y se asegura que se informa de la extinción de los certificados de forma segura e inmediata, de acuerdo con lo previsto en la Declaración de Prácticas de Certificación. El servicio está disponible 24 horas X 7 días a la semana.
- El cumplimiento de los requisitos técnicos y de personal exigidos por la legislación vigente en materia de firma electrónica:
- Demostrar la fiabilidad necesaria para prestar servicios de certificación.
- Garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado o se extinguió su vigencia.

– Obligaciones relativas a la regulación jurídica del servicio de certificación.

- Izenpe asume todas las obligaciones incorporadas directamente en el certificado o incorporadas por referencia. La incorporación por referencia se logra incluyendo en el certificado un identificador de objeto u otra forma de enlace a un documento.
- El instrumento jurídico que vincula a Izenpe y al solicitante, suscriptor o poseedor de claves y al tercero que confía en el certificado está en lenguaje escrito y comprensible.
- Prescripciones para dar cumplimiento a lo establecido en la Declaración de Prácticas de Certificación.
- Indicación de la Declaración de Prácticas de Certificación aplicable, en su caso, de que los certificados se expiden al público y de la necesidad de empleo de dispositivo seguro de creación de firma o descifrado de mensajes.
- Cláusulas relativas a la emisión, revocación, renovación y, en su caso, recuperación de claves privadas.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.

- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión de un dispositivo criptográfico y para la cesión de dicha información a terceros, en caso de terminación de operaciones de Izenpe sin revocación de certificados válidos.
- Límites de uso del certificado.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales Izenpe acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si Izenpe ha sido declarada conforme con las Políticas de Certificación de alguna o algunas de las Entidades Públicas y, en su caso, de acuerdo con qué sistema.
- Forma en la que se garantiza la responsabilidad patrimonial de Izenpe.

7.2 ENTIDAD DE REGISTRO

La Entidad de Registro asume las siguientes obligaciones:

- Comprobar la identidad y aquellas otras circunstancias personales del solicitante, suscriptor y poseedor de claves, en su caso, que consten en los medios de identificación o sean relevantes, conforme a los presentes procedimientos.
- Conservar toda la información y documentación relativa a los mismos, cuya emisión, renovación, revocación o reactivación gestiona.
- Comunicar a Izenpe, con la debida diligencia, las solicitudes de revocación de forma rápida y fiable.
- Permitir a Izenpe el acceso a los archivos y la auditoría de sus procedimientos en la realización de sus funciones y en el mantenimiento de la información necesaria para las mismas.
- Informar a Izenpe de las solicitudes de emisión, renovación, revocación y cualquier otro aspecto que afecte a los medios emitidos por la misma.
- Comprobar, con la diligencia debida, las causas de revocación que pudieran afectar a la vigencia de los medios.
- Cumplir en el desempeño de sus funciones de gestión de emisión, renovación y revocación de medios de identificación en base a los procedimientos establecidos por Izenpe y la legislación vigente en esta materia.

- En caso necesario podrá asumir la función de poner a disposición del poseedor de claves los procedimientos técnicos de creación de firma (clave privada) y de verificación de firma electrónica (clave pública).

7.3 OBLIGACIONES DEL SUSCRIPTOR DEL CERTIFICADO

- 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.
- 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 sus credenciales, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en 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 sus credenciales.
    - 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 el medio de identificación transcurrido el periodo de validez.
- 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.

El suscriptor del certificado acepta las condiciones de la DPC publicada en www.izenpe.eus/dpc, y la política de certificado correspondiente, disponible también en www.izenpe.eus.

7.4 OBLIGACIONES DEL USUARIO VERIFICADOR DE CERTIFICADOS

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.
- Conocer las condiciones de utilización de los certificados conforme a lo previsto en la Declaración de Prácticas de Certificación.

- Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- 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.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.
- 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.
- El usuario de certificados cualificados emitidos en dispositivo seguro de creación de firma queda obligado a reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con eIDAS.

8 RESPONSABILIDADES

8.3 RESPONSABILIDADES DE LA AUTORIDAD DE CERTIFICACIÓN

Izenpe responderá,

- De los daños y perjuicios que cause a cualquier persona o entidad 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.
- De los daños y perjuicios que cause a cualquier persona por la falta o retraso en la inclusión en el servicio de comprobación de la validez del mecanismo de identificación.
- 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 por importe de 3.500.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados.

Izenpe responderá por negligencia o falta de la debida diligencia en los servicios de certificación prestados así como cuando incumpla las obligaciones impuestas en la legislación sobre firma electrónica, excepto en los siguientes de daños causados por:

- Por las informaciones contenidas en los certificados, siempre que el contenido de los mismos cumpla sustancialmente con la Declaración de Prácticas de Certificación.
- Por la extinción de la eficacia de los certificados, siempre que cumpla sustancialmente con las obligaciones de publicación previstas en la Declaración de Prácticas de Certificación.
- Por el uso indebido o posterior a la revocación de los medios de identificación.
- 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 Declaración de Prácticas de Certificación 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.

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.

8.4 RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO

Cualquier organización distinta a Izenpe que actúe como Entidad de Registro será responsable frente a Izenpe por los daños causados en el ejercicio de las funciones que asuma, en los términos que se establezcan en el correspondiente instrumento legal.

8.5 RESPONSABILIDADES DEL TITULAR DE MEDIO DE IDENTIFICACIÓN

- De la falsedad o el error fáctico cometido durante el proceso de registro
- Del uso del medio de identificación en comunicaciones electrónicas con personas no autorizadas.
- Del incumplimiento del deber de custodia del secreto asociado al medio de identificación y de tomar aquellas precauciones que sean razonables para prevenir la pérdida, revelación, alteración o uso no autorizado

8.6 RESPONSABILIDADES DEL SUSCRIPTOR

El Suscriptor será responsable de todas las comunicaciones electrónicas autenticadas empleando una firma digital generada con su clave privada, cuando el certificado haya sido válidamente confirmado a través de los servicios de verificación prestados por Izenpe.

Mientras no se produzca la notificación de la pérdida o sustracción del certificado según lo establecido en la Declaración de Prácticas de Certificación, la responsabilidad que pudiera derivarse del uso no autorizado y/o indebido de los certificados, corresponderá, en todo caso, al suscriptor.

Mediante la aceptación de los certificados, el suscriptor se obliga a mantener indemne y, en su caso, a indemnizar a Izenpe, a las Entidades de Registro y a las Entidades Usuarias de cualquier acto u omisión que provoque daños, pérdidas, deudas, gastos procesales o de cualquier tipo, incluyendo los honorarios profesionales, en los que Izenpe, las Entidades de Registro y las Entidades Usuarias puedan incurrir, que sean causadas por la utilización o publicación de los certificados, y que provenga:

- Del incumplimiento de los términos previstos en el instrumento jurídico que le vincula con la Entidad de Certificación.
- Del uso de los certificados digitales en comunicaciones electrónicas con personas no autorizadas.
- De la falsedad o el error fáctico cometido por el Suscriptor.
- De toda omisión de un hecho fundamental en los certificados realizada negligentemente o con la intención de engañar a Izenpe, las Entidades Públicas Usuarias o a terceras personas que puedan confiar en el certificado del suscriptor.
- Del incumplimiento del deber de custodia de las claves privadas y de tomar aquellas precauciones que sean razonables para prevenir la pérdida, revelación, alteración o uso no autorizado de las claves privadas.

En este sentido Izenpe no será responsable de los daños y perjuicios ocasionados al suscriptor o terceros de buena fe, por el incumplimiento de los siguientes deberes inherentes a la condición de suscriptor:

- Proporcionar a Izenpe o a la Entidad de Registro información veraz, completa y exacta sobre los datos que deban constar en el certificado o que sean necesarios para la expedición o

revocación de éste, cuando su inexactitud no haya podido ser detectada por el prestador de servicios.

- Comunicar sin demora a Izenpe o a la Entidad de Registro cualquier modificación de las circunstancias reflejadas en el certificado.
- Conservar con diligencia sus datos de creación de firma con el fin de asegurar su confidencialidad y protegerlos de todo acceso o revelación.
- Solicitar la revocación del certificado en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- Abstenerse de utilizar los datos de creación de firma desde el momento en que haya expirado el período de validez del certificado o el prestador de servicios le notifique su pérdida de vigencia.
- Respetar los límites que figuren en el certificado en cuanto a sus posibles usos y utilizarlo conforme a las condiciones establecidas y comunicadas al firmante de servicios de certificación.

8.7 RESPONSABILIDADES DE LOS TERCEROS QUE CONFÍAN EN CERTIFICADOS

Un tercero que confíe en un certificado no válido o una firma digital que no haya podido ser verificada, asume todos los riesgos relacionados con la misma y no podrá exigir responsabilidad alguna a Izenpe, a las Entidades de Registro, Entidades Usuarias o suscriptores por cualquier concepto derivado de su confianza en tales certificados y firmas.

En este sentido Izenpe tampoco será responsable por los daños y perjuicios ocasionados al suscriptor o a terceros de buena fe, si el destinatario de los documentos firmados incumple alguno de los siguientes deberes de diligencia:

- Comprobar y tener en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
- Cerciorarse de la validez del certificado.

9 ACUERDOS, DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICAS DE CERTIFICADO APLICABLES

Todos los acuerdos, DPC y Políticas aplicables se encuentran en www.izenpe.eus

10 POLÍTICA DE REEMBOLSOS

Izenpe no dispone de una política de reintegro, y se acoge a la legislación vigente.

11 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El régimen aplicable a los tratamiento de los datos de carácter personal que Izenpe lleva a cabo será el previsto 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* (en adelante, RGPD) y en su normativa de desarrollo y aquella otra normativa vigente que resulte aplicable.

Izenpe dispone de la información referente a los tratamientos en la dirección www.izenpe.eus/datos

12 LEGISLACIÓN APLICABLE. MECANISMOS DE RESOLUCIÓN DE CONFLICTOS

12.1 Normativa aplicable

La ley española de firma electrónica se aplica en todo lo referente a la ejecución, elaboración, interpretación y validez de esta Declaración de Prácticas de Certificación. La normativa aplicable al presente documento, y a las operaciones que derivan de ellas, es la siguiente:

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 39-2015 Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40-2015 Régimen Jurídico Sector Público
- 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/).
- Reglamento Europeo 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).

12.2 Reclamaciones y resolución de disputas.

Izenpe está sometida al sistema arbitral de consumo en los términos previstos en la legislación aplicable como medio para atender y resolver con carácter vinculante y ejecutivo para ambas partes, las quejas o reclamaciones de los solicitantes o suscriptores en el caso de los certificados de ciudadanos.

A tales efectos se considerará que el solicitante o suscriptor se acoge a dicho sistema desde el momento de la formalización de la solicitud de arbitraje ante la Junta Arbitral de Consumo que corresponda.

Cualquier otra cuestión litigiosa que pudiera surgir de los solicitantes o suscriptores en el ámbito de los certificados de ciudadanos no sometidos al sistema arbitral de consumo, quedará sometida a la jurisdicción competente.

13 AUDITORÍAS, CERTIFICACIONES Y SELLOS DE CONFIANZA DE LA AC Y LOS REPOSITORIOS

Con el objetivo de desarrollar e implantar eficazmente los servicios, Izenpe ha implementado un sistema de gestión de seguridad de la información para los procesos relacionados con los servicios de confianza, según el estándar ISO 27001.

Izenpe además sigue las indicaciones de los estándares de ETSI (Instituto Europeo de Estándares de Telecomunicaciones) y ha conseguido la certificación bajo las especificaciones técnicas de la norma EN 319 411-2 para la emisión de certificados cualificados, de la norma EN 319 411-1 para la emisión de certificados de clave pública, y de la norma EN ETSI EN 319 422 para la emisión de los sellos de tiempo. Estas normas son las exigidas por el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS)

Para los certificados de servidor seguro que siguen la política de certificados de validación extendida (EVCP), para los certificados de servidor seguro que siguen la política de validación de la organización (OVCP) y para los certificados de servidor seguro que siguen la política de validación del dominio (DVCP) se siguen además las guías aprobadas por el CA/Browser Forum, disponibles en www.cabforum.org.

Todas las acreditaciones están disponibles para su consulta en www.izenpe.eus

14 CONTROL DE VERSIONES

14.3 Control de cambios _Versión 1. 0

Requerimientos adicionales	➢ Adecuación al *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*.
Requerimientos actualizados	
Aclaraciones	
Editorial	
Requerimientos eliminados	➢ Condiciones de uso. ➢ Contrato de suscriptor.

14.4 Control de cambios _De la versión 1. 0 a la 1.1

Actualizaciones respecto a la versión anterior	➢ Actualización la denominación del documento. ➢ Apartado 2, se incluye un apartado específico de definiciones. ➢ Apartado 3, se diferencia entre el uso de los medios de identificación como atención y como firma. ➢ Apartado 4, se incluye una nueva clasificación de las obligaciones de las partes. ➢ Apartado 5, se actualizan las Responsabilidades de la autoridad de certificación.
Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	➢ Apartado 2 Se elimina el apartado 2 referente a los tipos de certificados y a los soportes en lo que se emiten.

14.5 Control de cambios _De la versión 1. 1 a la 1.2

Actualizaciones respecto a la versión anterior	
Aclaraciones	➢ Añadida aclaración de cumplimiento de política en el apartado 4.3 Obligaciones del Suscriptor de Certificado
Actualizaciones de formato.	
Eliminaciones.	

14.6 Control de cambios _De la versión 1. 2 a la 2.0

Actualizaciones respecto a la versión anterior	➢ Con la finalidad de facilitar al usuario la información relativa a los términos y condiciones de uso de los medios de identificación, se fusiona en un único documento el Acuerdo de Divulgación de PKI (PDS) versión 1.0 y el documento de Términos y Condiciones de Uso de Medios Electrónicos para autenticación y firma versión 1.2.
Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	

14.7 Control de cambios _De la versión 2.0 a la 2.1

Actualizaciones respecto a la versión anterior	➢ Se ha corregido el nivel eIDAS del perfil corporativo en contenedor ➢ Se ha añadido el perfil de dispositivo
Aclaraciones	
Actualizaciones de formato.	
Eliminaciones.	