ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA
Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA
Fecha: 2026.10.30 10:16:01 +01'00'

1. INTRODUCCIÓN

El presente documento establece la política de certificación correspondiente a los certificados emitidos por Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios, IZENPE, S.A. (en adelante, IZENPE) para sitios web en sus distintas variantes.

Su finalidad es detallar y completar, para este tipo de certificado, lo definido de forma genérica en la Declaración de Prácticas de Certificación de IZENPE, en los documentos específicos del CA/Browser Forum Baseline Requirements (en adelante, BR), las guías EV (en adelante, EVBR) para la emisión de certificados de sitio web, así como en las especificaciones de ETSI (www.etsi.org). IZENPE adhiere a la última versión publicada de dichas normas.

De este modo, IZENPE sigue las siguientes políticas de certificación establecidas por ETSI:

- DVCP (Domain Validation Certificates Policy): para certificados SSL DV.
- OVCP (Organisational Validation Certificates Policy): para certificados SSL OV.
- QEVCP -(Organisational Validation Certificates Policy): para certificados SSL Cualificados EV.

Las Root CAs y las Sub CAs contempladas en este documento se detallan en el apartado

1.3.1. En función del tipo de validación realizada, IZENPE emite los siguientes tipos de

certificados:

- *SSL VALIDADO POR DOMINIO (SSL DV),*

Este certificado, considerado como no cualificado, se utilizará para la identificación de la titularidad del dominio que aloja el sitio web, y ofrece al usuario del navegador de Internet una garantía razonable sobre la legitimidad del dominio.

La validez de estos certificados es de 195 días.

- *SSL VALIDADO POR ORGANIZACIÓN (SSL OV),*

Este certificado, considerado como no cualificado, se utiliza para la identificación del dominio y la acreditación de la organización, y ofrece al usuario del navegador de Internet una garantía razonable de que el sitio web al que accede pertenece a la organización identificada en el certificado.

La validez de estos certificados es de 195 días.

- *SSL DE VALIDACIÓN EXTENDIDA CUALIFICADO (SSL EV),*

Este certificado se considera cualificado conforme al Reglamento (UE) n.º 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 23 de julio de 2014, modificado por el Reglamento

(UE) 1183/2024, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interno, y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS). Se utilizará para la identificación del dominio y la acreditación de la organización, ofreciendo al usuario del navegador de Internet una garantía robusta de que el sitio web al que accede pertenece a la organización identificada en el certificado.

La validez de estos certificados es de 195 días.

1.1 Visión general

El objeto de este documento es regular las condiciones y características de los servicios de confianza aplicables a los usuarios de los certificados de autenticación de sitios web emitidos por Izenpe y establecer las obligaciones que Izenpe asume en relación con:

La gestión de los certificados y las condiciones aplicables a la solicitud, emisión, uso y finalización de su vigencia.

La prestación del servicio de consulta del estado de vigencia de los certificados, así como las condiciones aplicables al uso del servicio y las garantías ofrecidas.

Asimismo, incluye —ya sea directamente o mediante referencias a los detalles del régimen de responsabilidad aplicable a las partes que utilizan y/o confían en los servicios descritos en el párrafo anterior— los controles de seguridad aplicados a sus procedimientos e instalaciones, en la medida en que puedan publicarse sin comprometer su eficacia, y las normas de secreto y confidencialidad, así como cuestiones relativas a la titularidad de sus bienes y activos, la protección de datos personales y otros asuntos de carácter informativo que considera de interés poner a disposición del público.

Izenpe se ajusta a la última versión publicada de los *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* (Requisitos de referencia para la emisión y gestión de certificados de servidor TLS de confianza pública) disponibles en https://www.cabforum.org, así como a la política de la CCADB, la política del Programa de Raíz de Apple, la política del Programa de Raíz de Chrome, la política del Almacén de Raíces de Mozilla y los requisitos del Programa de Raíz de Microsoft. En caso de discrepancia entre este documento y dichos requisitos, estos últimos prevalecerán sobre el presente documento.

Con efectos a partir del 15 de abril de 2026, esta Autoridad de Certificación (AC) ha cesado la emisión de nuevos certificados SSL/TLS bajo la AC Raíz de 2007. La presente Declaración de Prácticas de Certificación (CPS) permanece vigente únicamente para regular los servicios de gestión, revocación y validación de estado de los certificados emitidos antes de la fecha de cese, hasta su vencimiento natural.

1.2 Nombre e identificación del documento

El presente documento se denomina: «Política de Certificación - Declaración de Prácticas de Certificación para Certificados de Autenticación de Sitios Web».

- Versión: 3.2
- Fecha de emisión: 29/10/2026
- Ubicación:http://www.izenpe.eus/s15-content/es/contenidos/informacion/doc_especifica/es_def/index.shtml

Para la identificación de los certificados, IZENPE les ha asignado los siguientes identificadores de objeto (OID):

RAÍZ 2007:

CERTIFICADO	OID DE POLÍTICA
DV SSL	1.3.6.1.4.1.14777.1.2.4
OV SSL	1.3.6.1.4.1.14777.1.2.1
SSL Cualificado	1.3.6.1.4.1.14777.6.1.3

RAÍZ 2024:

CERTIFICADO	OID DE POLÍTICA
DV SSL	1.3.6.1.4.1.14777.50.1.2
OV SSL	1.3.6.1.4.1.14777.50.2.2
SSL Cualificado	1.3.6.1.4.1.14777.50.3.2

Control de versiones

VERSIÓN	CAMBIO
1.0	- Requisitos añadidos en la sección 2.2 – Requisitos actualizados en las secciones 2.1 y 2.2 – Requisitos actualizados en la sección 2.2 – Índice añadido. – Pie de página añadido. – Requisitos eliminados en las secciones 2.1 y 2.2. – Año eliminado de la portada
1.1	– Requisitos actualizados en la validación de dominio, en la sección 2.2. – Figuras eliminadas en las secciones 2.3 y 2.6.
1.2	– Requisitos actualizados en la validación CCA, en la sección 2.2.
1.3	- 1. Introducción En el marco del proyecto Google Certificate Transparency, los certificados EV S EV HQ emitidos serán publicados en el servicio CT de los Log Servers (servidore registro) con los que IZENPE mantiene un acuerdo. - 1.1. Descripción del certificado. * Actualización de la normativa relativa al certificado de sello electrónico. * Actualización de la validez de los certificados a 1 o 2 años. - 1.2. Identificación * Se incluyen los OIDs del CA/B FORUM. * Los números de serie de los certificados deberán tener al menos 64 bits de entro - Secciones 1.3 y siguientes. Adaptación de la terminología para la emisión de certificados EV a entidades privadas. - 14. Disposiciones generales, * Obligaciones de identificación. Se indica que, en todos los casos, IZENPE verif titularidad o el control del dominio. Obligaciones del suscriptor del certificado. Se incluyen aquellas determinadas er PDS. – Inclusión de aclaraciones sobre el cumplimiento de los Requisitos Básicos (BRs)
1.4	– Se ha actualizado el OID de política de los certificados EV SSL y EV HQ. –Se indica en la sección «1.1 Descripción de certificados» que los certificados Qualified EV SSL y Qualified EV HQ se consideran cualificados según el Reglam eIDAS. – Se especifica en la introducción que TODOS los certificados serán publicados er CTs. – Se han eliminado todas las referencias al certificado HQ.

1.5	- Se han añadido perfiles cualificados
1.6	Se han añadido los siguientes métodos de verificación de titularidad del dominio - Correo electrónico generado a contacto del dominio. - Correo electrónico al contacto DNS CAA. - Correo electrónico al contacto DNS TXT. - Consulta DNS (DNS Lookup). - Se detallan las causas y plazos de revocación tanto para certificados finales com para sub-CAs.
1.7	Se han añadido los siguientes elementos: - Rutas de prueba de certificados (vigente, revocado, caducado). - Verificación de los parámetros de clave RSA. - Inclusión de la definición de «precertificado». - obligación de incrementar el número de versión, incluso si no se han introducid cambios. Se han eliminado los siguientes elementos: - Los certificados EV de entre los perfiles actualmente emitidos por IZENPE. - Procedimiento de revocación, remitiéndose ahora a la Declaración de Prácticas Certificación (CPS) -Se especifica que las CAs públicas de IZENPE no emiten certificados para dom internos
1.8	El documento ha sido adaptado a la estructura del RFC 3647.
1.9	– La sección de control de cambios ha sido sustituida por esta tabla de historial de versior – Se ha actualizado la vigencia de todos los perfiles a 395 días. – Se ha eliminado el método DNS CAA. – Se ha añadido el método Whois para dominios .eus
2.0	– Eliminación de referencias a los certificados SSL, HQ y EV SSL cualificados. – Actualización de la dirección postal y de correo electrónico de IZENPE. - Revisión de la redacción general de la política.
2.1	– 3.2.2.1 Identidad: en relación con los certificados SSL cualificados Se incluye la de fuentes de verificación de entidades, conforme a CABFORUM. – Portada: Se elimina el pie de página del título del documento debido a un error e número de teléfono.
2.2	–Portada: Se elimina el pie de página del título del documento debido a un error número de teléfono.

	Secciones, -1 Corrección del párrafo de «Transparencia de Certificados». - Eliminado el párrafo relativo al RFC 6962 en la sección 3.1. - 3.2.2.1 Identidad: ampliación de la lista de fuentes de verificación. –3.2.2.1 Identidad: en relación con los certificados SSL cualificados Se incluye la de fuentes de verificación de entidades, conforme a CABFORUM. - 3.2.2.2.4. Los métodos de validación son correctos, pero la descripción «c» no corresponde con ningún caso; falta la descripción del método según CABFORUM 3.2.2.4.4. - 4.1.2 Eliminadas referencias a entidades cuya información de incorporación no puede ser verificada. - 4.6 Corrección de traducción: se decía «revocación» cuando debía ser «renovación». - 4.4.3 Corrección relativa a «Transparencia de Certificados». - 4.9.6 Reescrita. - 6.3.2 Error tipográfico, donde decía 395 debía decir 398. - 6.1.5. añadido el operador «≥» al valor 2048. - 9.1.3 Corrección, la «I» hace referencia a IZENPE.
2.3	- Homogeneización de formato. - Modificadas 1., 1.2 y 1.3.1 para añadir información sobre la nueva RAÍZ. - Corregidas referencias a CABFORUM. - 3.2.2.2. Estaba mal etiquetada como 3.2.2.2.2. - 3.2.2.4. Estaba mal etiquetada como 3.2.2.2.4. - 3.2.2.4. 3.2.2.4 Eliminada referencia a BR 3.2.2.4.1. - 7.1.8. Referencia obsoleta a «UserNotice». - Modificadas 6.1.5 y 7.1.3 para añadir nueva información sobre la RAÍZ.
2.4	- Reescritura de las secciones: 1.6.1, 1.6.2, 2.1, 2.2, 4.4.2 - Nuevas secciones incluidas: 1.6.3, 1.6.4, 4.2.4, 5.4.1.1, 4.3.1.1, 4.3.1.2, 4.3.1.3 7.1.2.1, 7.1.2.1.1, 7.1.2.2, 7.1.3.1,7.1.3.1.1, 7.1.3.1.2, 7.1.3.2, 7.1.3.2.1, 7.1.3.2.2 7.1.4.1, 7.1.4.2, '7.1.4.3','7.1.4.4'
2.5	- La Política de Certificación (CP) y la Declaración de Prácticas de Certificación (C han sido fusionadas – Todas las secciones marcadas anteriormente como «Ver la sección correspondi en la CPS» dentro de la CP < han sido reemplazadas por la sección correspondi de la CPS.
2.6	- Sección 3.2.2.4 modificada para eliminar el método 3.2.2.4.2. – Sección 3.2.2.1 modificada para añadir nuevas fuentes de verificación.
2.7	– Sección 7.2.2 modificada para establecer la extensión «Issuing Distribution Point como crítica.

2.8	5.7.1.2 Sección del plan de revocación masiva incluida.
2.9	Duración certificados SSL a 195 días.
3.0	1.1,4.3,5.8 Dejar de emitir certificados TLS el 15 de abril de 2026 bajo la CA raíz 2007.
3.1	Cumplimiento de la CCADB y de los programas de autoridades de certificación r (Root programs).
3.2	7.2.2 No se permitirá el valor «unspecified» (no especificado) en el campo CrlRe para las sub-CA (autoridades de certificación subordinadas).

1.3 Participantes en la PKI

Las partes implicadas en la gestión y uso de los servicios de confianza descritos:

1. Autoridad de Certificación
2. Autoridad de Registro
3. Suscriptores o titulares de certificados
4. Terceros de confianza
5. Otros participantes

1.3.1 Autoridades de certificación

En el marco de esta política, IZENPE dispone de las siguientes Autoridades de Certificación:

RAÍZ 2007

Tipo	CN	Huella SHA1
Raíz	IZENPE.com	2F783D255218A74A653971B52CA29C45156FE919
Subordinada	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	F79CDA11E7917419A0418DB84BA743C5313AD7F0
Subordinada	Certificate CA EV SSL	C68BADE5F069778A003074E619DAB2E7928342D5

AUTORIDAD DE CERTIFICACIÓN RAÍZ 2007

Campo / extensión	Contenido

version	Versión 3
serialNumber	00B0B75A16485FBFE1CBF58BD719E67D
Campo / extensión	**Contenido**
signature	sha256WithRSAEncryption
issuer	
CN	IZENPE.com
O	IZENPE S.A.
C	ES
validity	13 de diciembre de 2037
sujeto	
CN	IZENPE.com
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensiones	
subjectAltName	
rfc822Name	info@izenpe.com
nombreDirectorio	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05
keyUsage	Firma de certificados, firma offline de CRL, firma de listas de revocación de certificados (CRL) (06)

AUTORIDAD DE CERTIFICACIÓN SUBORDINADA: «EAEko Herri Administrazioen CA - CA AAPP Vascas (2)»

Campo / extensión	Contenido
version	Versión 3
serialNumber	24C5C8AA566F8EE84CBEA7055CE164A4
signature	sha256WithRSAEncryption
Campo / extensión	**Contenido**
issuer	
CN	IZENPE.com
O	IZENPE S.A.
C	ES
validity	13 de diciembre de 2037
sujeto	
CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)
OU	AZZ Ziurtagiri publikoa - Certificado publico SCA
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensiones	
subjectAltName	
rfc822Name	info@izenpe.com
nombreDirectorio	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	C0A94AF7472587FFBCB5A689CE82D246A889EBA3
authorityKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05
certificatePolicies	
policyIdentifier	Todas las directrices de emisión

Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
Alternative name	
Campo / extensión	**Contenido**
URL address	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Firma de certificados, firma offline de CRL, firma de listas de revocación de certificados (CRL) (06)
Digital footprint	F79CDA11E7917419A0418DB84BA743C5313AD7F0

AUTORIDAD DE CERTIFICACIÓN SUBORDINADA: «Certificate CA EV SSL»

Campo / extensión	**Contenido**
version	Versión 3
serialNumber	687DB7171744DA235B3F625A7393F8A5
signature	sha256WithRSAEncryption
issuer	
CN	IZENPE.com
O	IZENPE S.A.
C	ES
validity	6 de julio de 2028
sujeto	
CN	Certificate CA EV SSL
OU	BZ Ziurtagiri publikoa - Certificado publico EV
O	IZENPE S.A.

C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensiones	
subjectAltName	
rfc822Name	info@izenpe.com
nombreDirectorio	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
Campo / extensión	**Contenido**
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	C6EDFE77FB51564DFCABD5E3B10C13A3BF54E39B
authorityKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05
certificatePolicies	
policyIdentifier	Todas las directrices de emisión
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
Alternative name	
URL address	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Firma de certificados, firma offline de CRL, firma de listas de revocación de certificados (CRL) (06)
Digital footprint	C68BADE5F069778A003074E619DAB2E7928342D5

RAÍZ 2024

Tipo	CN	Huella SHA1

Raíz	RAÍZ CA SSL IZENPE 2024	68E93296DEEB4254C18C49C4E80F5D8FA3D38A93
Subordinada	SUBCA SSL 2024	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18

AUTORIDAD DE CERTIFICACIÓN RAÍZ 2024

Campo / extensión	Contenido
version	Versión 3
serialNumber	1BE568F081EDFEEE7776604E73FA081E
signature	sha384ECDSA
issuer	
Campo / extensión	**Contenido**
CN	RAÍZ CA SSL IZENPE 2024
O	IZENPE S.A.
C	ES
validity	24 de septiembre de 2049
sujeto	
CN	RAÍZ CA SSL IZENPE 2024
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	ECC(384 bits)
extensiones	
subjectKeyIdentifier	EADC1AEECBD319D1B12B4FDB12CB56795DB2B0EA
keyUsage	Firma de certificados, firma offline de CRL, firma de listas de revocación de certificados (CRL) (06)

AUTORIDAD DE CERTIFICACIÓN SUBORDINADA: «SUBCA SSL 2024»

Campo / extensión	Contenido

version	Versión 3
serialNumber	45C858662468EEA028BAEDB26E098D37
signature	sha384ECDSA
issuer	
CN	RAÍZ CA SSL IZENPE 2024
O	IZENPE S.A.
C	ES
validity	24 de septiembre de 2049
sujeto	
CN	SUBCA SSL 2024
IDENTIFICADORDELAORGANIZACIÓN	VATES-A01337260
Campo / extensión	**Contenido**
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	ECC(384 bits)
extensiones	
subjectKeyIdentifier	5730599CA33DA068ECB3DBCFD555C8AACC5D00A9
authorityKeyIdentifier	EADC1AEECBD319D1B12B4FDB12CB56795DB2B0EA
certificatePolicies	
policyIdentifier	Todas las directrices de emisión
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	calssuer

URL address	http://www.izenpe.eus/contenidos /informacion/cas_izenpe/es_cas/adjuntos/ izenpe_root_ssl_2024.crt
cRLDistributionPoints	http://crl.izenpe.eus/2024/izsslroot.crl
keyUsage	Firma de certificados, firma offline de CRL, firma de listas de revocación de certificados (CRL) (06)
Digital footprint	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18

1.3.2 Autoridades de registro

IZENPE es la única Autoridad de Registro que interviene en el proceso de emisión de estos certificados. Realiza las tareas de identificación y verificación de forma automatizada, con el objetivo de garantizar que el certificado emitido al Suscriptor corresponde con un control efectivo sobre el nombre de dominio incluido en el Certificado. Control exclusivo

Ninguna de las verificaciones sobre la identidad o el control del dominio será delegada a terceros.

1.3.3 Suscriptores

Los Suscriptores son las personas jurídicas a quienes se emiten los certificados y que quedan vinculadas conforme a lo establecido en el documento de Términos y Condiciones

1.3.4 Terceros de confianza

Los terceros de confianza son los usuarios de Internet que establecen conexiones a sitios web mediante protocolos TLS/SSL que incorporan dichos certificados y que deciden confiar en ellos.

1.3.5 Otros participantes

Sin estipulación.

1.4 Uso del certificado

1.4.1 Usos permitidos del certificado

Los certificados de autenticación de sitios web autentican un sitio web y lo vinculan con la persona jurídica a la que ha sido emitido.

Todos los certificados cualificados de autenticación de sitios web emitidos bajo esta Política son certificados cualificados, de acuerdo con el Reglamento eIDAS y los requisitos establecidos en las normas europeas ETSI EN 319 411-2 (Requisitos para los prestadores de servicios de confianza que emiten certificados cualificados de la UE) y ETSI EN 319 412-4 (Perfil de certificado para certificados de sitio web).

1.4.2 Usos prohibidos del certificado

Los certificados deben utilizarse exclusivamente para la función y el propósito para los que fueron emitidos, y no podrán ser utilizados para funciones o finalidades distintas.

Asimismo, deberán usarse únicamente conforme a la legislación vigente aplicable.

Estos certificados no están diseñados, no pueden ser utilizados ni están autorizados para su uso o reventa como equipos para la monitorización de situaciones peligrosas, ni para usos que requieran un funcionamiento a prueba de fallos, como la operación de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pueda derivar directamente en la muerte, lesiones personales o daños ambientales graves.

En caso de que una entidad usuaria o un tercero confíe en estos certificados sin consultar previamente el servicio de información sobre el estado de validez de los certificados emitidos bajo esta Política de Certificación, no estará amparado por esta Política y Prácticas de Certificación, y no tendrá legitimidad para reclamar ni emprender acciones legales contra IZENPE por daños, pérdidas o conflictos derivados del uso o confianza depositada en un certificado.

IZENPE prohíbe expresamente el uso de certificados emitidos bajo esta política para la intercepción ilegal o descifrado de comunicaciones cifradas (MITM), inspección profunda de paquetes (DPI) etc.

1.5 Administración de la política

1.5.1 Organización responsable del documento

IZENPE, con domicilio social en c/ Beato Tomás de Zumárraga, nº 71, 1ª planta, 01008 Vitoria-Gasteiz, y con NIF A-01337260, es la Autoridad de Certificación que emite los certificados a los que se aplica esta Política de Certificación.

1.5.2 Persona de contacto

Nombre del prestador	**Ziurtapen eta Zerbitzu Enpresa – Empresa de Certificación y Servicios, IZENPE, S.A.**

Dirección	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Correo electrónico	izenpe@izenpe.eus

Para informar de problemas de seguridad, como sospechas de vulneración de clave, uso indebido de certificados, fraude, solicitudes de revocación u otras incidencias, contacte a **incidencias@izenpe.eus**.

1.5.3 Órgano responsable de determinar la adecuación de la CPS a esta CP

El Comité de Seguridad de IZENPE es el órgano responsable de la aprobación de esta CP.

1.5.4 Procedimientos de aprobación de la CPS

IZENPE gestiona sus servicios de certificación y emite certificados de acuerdo con la versión vigente de los Requisitos Básicos para la Emisión y Gestión de Certificados de Confianza, establecidos por el CA/Browser Forum, los cuales pueden consultarse en la siguiente dirección: https:// cabforum.org/baseline-requirements-documents/

IZENPE revisa y actualiza anualmente esta CP, identificando y publicando nuevas versiones en www.izenpe.eus

1.6 Definiciones y acrónimos

1.6.1 Definiciones

- ***Solicitante:*** La persona física o jurídica que solicita (o busca renovar) un certificado. Una vez emitido el certificado, el solicitante pasa a denominarse Suscriptor (Subscriber). Para certificados emitidos a dispositivos, el solicitante es la entidad que controla u opera el dispositivo nombrado en el certificado, incluso si es el propio dispositivo quien envía la solicitud de certificado.
- ***CAA:*** Según el RFC 8659 (http://tools.ietf.org/html/rfc8659): «El registro de recursos DNS Certification Authority Authorization (CAA) permite al titular de un nombre de dominio especificar una o más Autoridades de Certificación (CAs) autorizadas para emitir certificados para ese dominio. Los registros CAA permiten a una CA pública implementar controles adicionales para reducir el riesgo de emisión errónea de certificados."
- ***Par de claves de la CA:*** Par de claves en el que la clave pública aparece como Subject Public Key Info en uno o más certificados de CA Raíz y/o CA Subordinada.
- ***Certificado:*** Documento electrónico que utiliza una firma digital para vincular una clave pública con una identidad.
- ***Política de certificación:*** Conjunto de reglas que indica la aplicabilidad de un

determinado certificado a una comunidad específica y/o a una implementación de PKI con requisitos de seguridad comunes.

- ***Informe de incidente de certificado:*** Reclamación o notificación de sospecha de Compromiso de clave, uso indebido de un Certificado, u otros tipos de fraude, mal uso o conducta inapropiada relacionada con Certificados.
- ***Perfil de certificado:*** Conjunto de documentos o archivos que define los requisitos del contenido del Certificado y sus extensiones, conforme a lo establecido en la Sección 7, por ejemplo, una sección dentro de la CPS de una CA o una plantilla de certificado utilizada por el software de la CA.
- ***Lista de revocación de certificados:*** Lista actualizada regularmente y con marca de tiempo, que contiene los certificados revocados, generada y firmada digitalmente por la CA que emitió dichos certificados.
- ***Transparencia de certificados (CT)***: marco abierto de supervisión de Certificados de autenticación de sitios web, que permite que, al emitirse uno de estos certificados, sea publicado en registros CT, facilitando así a los titulares de dominios la supervisión de la emisión de certificados para sus dominios y la detección de certificados emitidos erróneamente.
- ***Autoridad de certificación:*** Organización responsable de la creación, emisión, revocación y gestión de Certificados. El término aplica tanto a las CA raíz como a las CA subordinadas.
- ***Declaración de prácticas de certificación:*** Uno de los documentos que forman el marco de gobierno dentro del cual se crean, emiten, gestionan y utilizan los certificados.
- ***Contacto del dominio:*** Persona o Entidad registrada como Titular, contacto técnico o contacto administrativo del nombre de dominio, según figura en el registro WHOIS del Dominio Base o en el registro SOA DNS, o bien a través de contacto directo con el Registrador del Nombre de Dominio.
- ***Etiqueta de dominio:*** Según el RFC 8499 (http://tools.ietf.org/html/rfc8499): «Una lista ordenada de cero o más octetos que constituye una parte de un nombre de dominio. En términos de teoría de grafos, una etiqueta identifica un nodo dentro de una porción del grafo de todos los posibles nombres de dominio.»
- ***Nombre de dominio:*** Lista ordenada de una o más Etiquetas de Dominio asignadas a un nodo dentro del Sistema de Nombres de Dominio.
- ***Reglamento eIDAS:*** Hace referencia al Reglamento (UE) 910/2014, modificado por el Reglamento (UE) 1183/2024.
- ***CA emisora:*** En relación con un certificado determinado, es la CA que ha emitido el Certificado. Puede ser tanto una CA raíz como una CA subordinada.

- ***Compromiso de clave:*** Se considera que una clave privada está comprometida si su valor ha sido revelado a una persona no autorizada o si una persona no autorizada ha tenido acceso a ella.
- ***Par de claves:*** Conjunto formado por una clave privada y su correspondiente clave pública.
- ***Identificador de objeto:*** Identificador alfanumérico o numérico único, registrado conforme

al estándar aplicable de la Organización Internacional de Normalización (ISO), asignado a un objeto o clase de objeto específicos.

- ***Servidor OCSP:*** Servidor en línea operado bajo la autoridad de la CA y conectado a su Repositorio, encargado de procesar solicitudes sobre el estado de Certificados. Ver también: Online Certificate Status Protocol.
- ***Clave privada:*** Clave del par de claves que se mantiene en secreto por parte de su titular, y que se utiliza para generar Firmas digitales y/o descifrar registros electrónicos o archivos cifrados con la clave pública correspondiente.
- ***Clave pública:*** Clave del Par de claves que puede ser divulgada públicamente por el titular de la clave privada correspondiente, y que es utilizada por terceros de confianza para verificar Firmas digitales generadas con la clave privada correspondiente y/o cifrar mensajes que solo podrán ser descifrados por esa clave privada.
- ***Infraestructura de clave pública:*** Conjunto de hardware, software, personas, procedimientos, normas, políticas y obligaciones utilizadas para permitir la creación, emisión, gestión y uso de confianza de Certificados y claves basados en Criptografía de clave pública.
- ***Valor aleatorio:*** Valor especificado por una CA al solicitante, que presenta al menos 112 bits de entropía.
- ***Autoridad de registro (RA):*** Entidad jurídica responsable de la identificación y autenticación de los sujetos de los certificados, que no es una CA, y por tanto, no firma ni emite Certificados. Una RA puede colaborar en el proceso de solicitud o de revocación de certificados, o en ambos. Cuando se usa el término RA como adjetivo para describir un rol o función, no implica necesariamente una entidad separada; puede ser parte de la propia CA.
- ***Fuente de datos fiable:*** Documento de identificación o fuente de datos utilizada para verificar la Identidad del sujeto, que es reconocida como fiable por empresas y administraciones públicas, y que ha sido creada por un tercero para un propósito distinto al de Obtener un Certificado.
- ***Tercero de confianza:*** Persona física o Entidad jurídica que confía en un Certificado válido. Un Proveedor de software de aplicación no se considera un Tercero de confianza cuando el software que distribuye solo muestra información relacionada con el Certificado.

- ***Repositorio:*** Base de datos en línea que contiene documentos públicos de gobernanza de la PKI (como CP, CPS) y estado de certificados, ya sea en forma de una CRL o una respuesta OCSP.

- ***CA raíz:*** Autoridad de certificación de nivel superior, cuyo Certificado raíz es distribuido por Proveedores de software de aplicación y que emite certificados a CA subordinadas.
- ***Certificado raíz:*** Certificado autofirmado emitido por la CA raíz para identificarse a sí misma y facilitar la verificación de los Certificados emitidos a sus CA subordinadas.
- ***Sujeto:*** Persona física, dispositivo, sistema, unidad o Entidad jurídica identificada en un Certificado como el Sujeto. El Sujeto puede ser el Suscriptor o un dispositivo bajo su control y operación.
- ***Información de Identidad del sujeto:*** Información que identifica al Sujeto del certificado. No

incluye el Nombre de dominio listado en la extensión subjectAltName, ni el campo commonName del sujeto.

- ***CA subordinada:*** Autoridad de certificación cuyo Certificado es firmado por una CA raíz o por otra CA subordinada.
- ***Suscriptor:*** Persona física o Entidad jurídica a quien se le emite un Certificado y que queda legalmente vinculada por un Acuerdo de suscriptor o por los términos de uso.
- ***WHOIS:*** Información recuperada directamente del Registrador de nombres de dominio o del operador del registro, mediante el protocolo definido en RFC 3912, el protocolo RDAP definido en RFC 7482, o a través de un sitio web HTTPS.
- ***Certificado comodín:*** Certificado que contiene al menos un nombre de dominio comodín en el campo Subject Alternative Name del certificado.

1.6.2 Acrónimos

- **CA:** Autoridad de Certificación
- **CAA:** Autorización de la Autoridad de Certificación
- **CN:** Nombre Común
- **CP:** Política de Certificación
- **CPS:** Declaración de Prácticas de Certificación
- **CRL:** Lista de Revocación de Certificados
- **CT:** Transparencia de Certificados
- **DNS:** Sistema de Nombres de Dominio
- **DN:** Nombre Distinguido
- **EIDAS:** Reglamento eIDAS
- **ETSI:** Instituto Europeo de Normas de Telecomunicación
- **EV:** Validación Extendida
- **FQDN:** Nombre de Dominio Totalmente Cualificado
- **HSM:** Módulo de Seguridad de Hardware Dispositivo para generar y proteger claves criptográficas.
- **HTTP:** Protocolo de Transferencia de Hipertexto
- **ISO:** Organización Internacional de Normalización
- **OCSP:** Protocolo de Estado de Certificados en Línea
- **OID:** Identificador de Objeto
- **OV:** Validación de Organización
- **PDS:** Declaración de Divulgación de la PKI
- **PKI Public Key:** Infraestructura
- **PKCS:** Normas de Criptografía de Clave Pública
- **RA:** Autoridad de Registro
- **TLS/SSL:** Protocolo de Seguridad de la Capa de Transporte / Capa de Conexión Segura
- **UTC:** Tiempo Universal Coordinado

1.6.3 Referencias

Documento	Título
ETSI EN 319 401	Firmas e Infraestructuras Electrónicas (ESI); Requisitos generales de política para los Prestadores de Servicios de Confianza
ETSI EN 319 403	Firmas e Infraestructuras Electrónicas (ESI); Evaluación de conformidad del Prestador de Servicios de Confianza – Requisitos para organismos de evaluación
ETSI EN 319 411-1	Requisitos de política y seguridad para Prestadores de Servicios de Confianza emisores de certificados; Parte 1: Requisitos generales
ETSI EN 319 411-2	Requisitos de política y seguridad para Prestadores de Servicios de Confianza emisores de certificados; Parte 2: Certificados cualificados de la UE
ETSI EN 319 421	Requisitos de política y seguridad para Prestadores de Servicios de Confianza emisores de sellos de tiempo
RFC 2119	Palabras clave para utilizar en RFC para indicar niveles de obligatoriedad
RFC 3492	Punycode: Codificación Bootstring de Unicode para nombres de dominio internacionalizados (IDNA)
RFC 3647	Infraestructura de Clave Pública X.509 de Internet: Marco de políticas de certificación y prácticas de certificación
RFC 3986	Punycode: Identificadores Uniformes de Recursos (URI): Sintaxis general
RFC 5280	Perfil de certificados y listas de revocación (CRL) de la PKI X.509 de Internet
RFC 6960	Protocolo OCSP para la PKI X.509 de Internet
RFC 6962	Transparencia de Certificados
RFC 8737	Entorno Automatizado de Gestión de Certificados (ACME): Extensión ALPN del Protocolo de Aplicación TLS

1.6.4 Convenciones

Las palabras clave «debe», «no debe», «obligatorio», «deberá», «no deberá», «debería», «no debería», «recomendado», «puede» y «opcional» en este documento serán interpretadas como se

describe en RFC 2119.

2. PUBLICACIÓN Y RESPONSABILIDADES DEL REPOSITORIO

2.1 Repositorios

IZENPE dispone de un repositorio de información pública accesible en www.izenpe.eus, disponible las 24 horas del día, los 7 días de la semana, donde se puede consultar información sobre la CP/CPS, certificados raíz y certificados de subCA.

2.2 Publicación de la información de certificación

La información relativa a la emisión de certificados electrónicos cubiertos por esta CP está disponible a través del sitio web: www.izenpe.eus e incluye la siguiente información:

- Política de certificación y declaración de prácticas de certificación.
- Perfiles de certificados y listas de revocación.
- Declaraciones de Información PKI (PDS).
- Términos y condiciones de uso de los certificados, como instrumento legal vinculante.
- Descarga de los Certificados raíz de IZENPE y de las CAs subordinadas, junto con información adicional.

IZENPE adoptará todas las medidas necesarias para garantizar que este repositorio esté disponible

permanentemente. Los Proveedores de software de aplicación pueden probar sus desarrollos

utilizando las siguientes direcciones:

RAÍZ 2007 |Estado|URL| |-|-| |Válido|https://test-ev-qualified.izenpe.eus/| |Caducado|https://test-expired-ev.izenpe.eus/| |Revocado|https://test-revoked-ev.izenpe.eus/|

RAÍZ CA SSL IZENPE 2024 |Estado|URL| |-|-| |Válido|https://test-valid-ev-2024.izenpe.eus| |Caducado|https://test-expired-ev-2024.izenpe.eus| |Revocado|https://test-revoked-ev-2024.izenpe.eus|

2.3 Frecuencia o momento de publicación

IZENPE revisa sus políticas y prácticas de certificación y actualiza este documento anualmente, siguiendo las directrices establecidas en la sección «1.5.4 Procedimiento de aprobación» del

presente documento.

Cualquier cambio en la CP/CPS será publicado de forma inmediata.

La frecuencia de publicación de las CRL está definida en la sección 4.9.7 «Frecuencia de generación de CRL» de este documento.

2.4 Controles de acceso al repositorio

IZENPE permite el acceso de solo lectura a la información publicada en su repositorio, y establece controles para: evitar que personas no autorizadas puedan añadir, modificar o eliminar registros del Servicio y proteger la integridad y autenticidad de la información depositada. Para ello, IZENPE emplea sistemas fiables que aseguran que:

- Solo las personas autorizadas puedan realizar anotaciones o modificaciones.
- La autenticidad de la información publicada pueda ser verificada.
- Los certificados estén disponibles para su consulta pública.
- Se puedan detectar cambios técnicos que afecten a los requisitos de seguridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Asignación de nombres

La codificación de los certificados sigue el estándar RFC 5280, «Perfil de certificado X.509 de la Infraestructura de clave pública de Internet y la Lista de revocación decertificados (CRL)». Todos los campos definidos en el perfil de certificados en la CPS y en la CP, excepto aquellos en los que se indique explícitamente lo contrario, utilizan codificación UTF8String.

Adicionalmente, para los certificados SSL cualificados, IZENPE cumplirá con los requisitos establecidos en las últimas directrices de validación extendida, disponibles en: https://cabforum.org/working-groups/server/extended-validation/guidelines/.

3.1.1 Tipos de nombres

Los certificados electrónicos de entidad final cubiertos por esta CP contienen un nombre distinguido (DN) en el campo Subject Name, compuesto por la información establecida en el perfil de certificados (sección 7.1 de este documento). IZENPE cumple en este sentido con los requisitos establecidos en X.500, RFC 5280, y por el CA/Browser Forum (BRs y EVGs).

El campo Common Name define al suscriptor del certificado.

3.1.2 Necesidad de que los nombres sean significativos

Todos los nombres distinguidos (DN) incluidos en el campo Subject Name son significativos. La descripción de los atributos asociados al suscriptor del certificado es legible para personas (véase sección 7.1.4 «Formato de nombres» de este documento).

El campo Subject Distinguished Name también estará sujeto a los requisitos establecidos en la sección 9.2 del CA/Browser Forum, dentro de su guía para la emisión y gestión de certificados de validación extendida, consultable en: https://cabforum.org/extended-validation/.

IZENPE no emite Certificados comodín bajo políticas EV.

3.1.3 Anonimato o seudonimato de los suscriptores

Bajo esta Política de Certificación, IZENPE no permite el uso de seudónimos.

3.1.4 Reglas para interpretar las distintas formas de nombre

Se aplican los requisitos definidos por el estándar de referencia X.500 según ISO/IEC 9594.

3.1.5 Unicidad de los nombres

El nombre distinguido (DN) asignado al suscriptor del certificado dentro del dominio del Prestador de Servicios de Confianza deberá ser único.

3.1.6 Reconocimiento, autenticación y rol de las marcas comerciales

Los solicitantes de certificados no deben incluir nombres en sus solicitudes de emisión que puedan suponer una infracción de derechos de terceros por parte del futuro suscriptor.

IZENPE no determina si el solicitante de un certificado tiene derechos sobre el nombre que figura en la solicitud del mismo. Asimismo, IZENPE no actúa como árbitro ni mediador, ni resuelve disputas sobre la titularidad de nombres de personas, organizaciones o nombres de dominio.

IZENPE se reserva el derecho de rechazar una solicitud de certificado en caso de conflicto con el nombre propuesto.

3.2 Validación inicial de identidad

IZENPE realiza el proceso de validación de la información incluida en los certificados de autenticación de sitios web conforme a los «Requisitos Básicos para la emisión y gestión de certificados de confianza», establecidos por el CA/Browser Forum, accesibles en: https://cabforum.org/working-groups/server/baseline-requirements/requirements/.

Adicionalmente, antes de emitir un certificado SSL cualificado, IZENPE garantiza que toda la información incluida en este tipo de certificados relativa al suscriptor: cumple los requisitos definidos por el CA/Browser Forum en su «Guía para la emisión y gestión de certificados de validación extendida», sección 11 y ha sido verificada conforme a dichos requisitos. Dicha guía puede consultarse en: https://cabforum.org/working-groups/server/extended-validation/guidelines/

IZENPE registra todas las confirmaciones realizadas en esta sección como parte de los procesos de auditoría interna e independiente periódicos.

3.2.1 Método para demostrar la posesión de la clave privada

IZENPE recibe una solicitud de certificado en formato PKCS#10, firmada digitalmente con la clave privada generada por el representante del suscriptor en su propio entorno, e incluyendo la clave pública asociada a dicha clave privada.

3.2.2 Autenticación de la identidad de la organización

Antes de solicitar por primera vez cualquier certificado, IZENPE obliga a registrar previamente a la Organización en su sistema, con la autorización de un Representante. Durante este proceso, la información de la Organización y del Representante será validada contra una fuente fiable, según lo establecido en la sección 3.2.2.1, y esta información será utilizada posteriormente para la emisión de certificados OV y EV.

3.2.2.1 Identidad

IZENPE no emite certificados de autenticación de sitios web cuyo suscriptor sea una persona física.

- En el caso de certificados DV IZENPE no verifica la identidad ni ningún otro tipo de información sobre la organización suscriptora.
- En el caso de certificados OV
    - IZENPE verifica la dirección postal y la identidad de la organización suscriptora, dependiendo del tipo de entidad (privada o pública):
    - Si el suscriptor es una organización del sector privado, IZENPE verifica su identidad y dirección consultando el registro oficial correspondiente.

Si se trata de una entidad pública, la verificación se realiza mediante la consulta al Boletín Oficial correspondiente y otros registros públicos utilizados como referencia.

IZENPE valida que el nombre y la dirección postal de la organización solicitante del certificado coincidan con el nombre y la dirección registrados oficialmente, conforme a lo descrito anteriormente.

- En el caso de certificados SSL cualificados

IZENPE verifica la existencia, la dirección y la identidad de la organización, en función del tipo de entidad:

- Si el suscriptor es una organización del sector privado, IZENPE verifica su identidad y dirección consultando el registro oficial correspondiente.
- Si se trata de una entidad pública, la verificación se realiza mediante la consulta al Boletín Oficial correspondiente y otros registros públicos utilizados como referencia.

Las fuentes de verificación que IZENPE utilizará en estos casos son las siguientes:

VERSIÓN	FECHA
3	2025/06/19

DESCRIPCIÓN	URL	PAÍS	PROVINCIA
BOLETÍN OFICIAL DEL PAÍS VASCO	https://www.euskadi.eus/y22-bopv/es/bopv2/datos/Ultimo.shtml	ES	EUSKADI
DIARI OFICIAL DE LA GENERALITAT DE CATALUNYA	https://dogc.gencat.cat/es/inici/index.html	ES	CATALUNYA
REGISTRO DE ENTIDADES LOCALES DEL PAÍS VASCO	https://www.euskadi.eus/registro-de-entidades-locales/web01-a2tokiad/es/	ES	EUSKADI
Ministerio de Justicia – Registro de Entidades Religiosas	https://maper.mjusticia.gob.es/Maper/buscarRER.action	ES	
AGENCIA TRIBUTARIA	https://www10.agenciatributaria.gob.es/wlpl/BURT-JDIT/ws/VNifV2SOAP	ES	
REGISTRO MERCANTIL	https://sede.registradores.org/site/invitado/mercantil/busqueda#/	ES	
INVENTARIO DE ENTIDADES DEL	https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx/	ES	

SECTOR PÚBLICO			
BANCO DE ESPAÑA	www.bde.es	ES	
BOLETÍN OFICIAL DEL ESTADO	https://www.boe.es/buscar/boe.php	ES	
BOLETÍN OFICIAL DE BIZKAIA	https://apps.bizkaia.eus/BT00/	ES	BIZKAIA
BOLETÍN OFICIAL DE GIPUZKOA	https://egoitza.gipuzkoa.eus/es/bog	ES	GIPUZKOA
BOLETÍN OFICIAL DE ÁLAVA / ARABA	https://www.araba.eus/botha/	ES	ALAVA / ARABA
BOLETÍN OFICIAL DEL PAÍS VASCO	https://www.euskadi.eus/y22-bopv/es/p43aBOPVWebWar/	ES	EUSKADI
DESCRIPCIÓN	**URL**	**PAÍS**	**PROVINCIA**
PAÍS	buscarAvanzada.do?idioma=es&tipoBusqueda=2		
REGISTRO DE ASOCIACIONES DEL PAÍS VASCO	https://www.euskadi.eus/registro-asociaciones-buscador/ web01-a2aderre/es/	ES	EUSKADI
INVENTARIO DE ENTES DEL SECTOR PÚBLICO	https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx/	ES	
ENTIDADES LOCALES DE NAVARRA	https://www.navarra.es/es/buscador-de-entidades-locales	ES	NAVARRA
ORGANIZACIONES SINDICALES Y EMPRESARIALES	https://expinterweb.mites.gob.es/deose/publico/expedientes	ES	

IZENPE verifica que el nombre, la dirección y el número de identificación fiscal de la organización

suscriptora del certificado incluidos en la solicitud coincidan con los datos registrados oficialmente en los registros consultados, según lo descrito en las secciones anteriores.

IZENPE cumplirá con los requisitos definidos por la entidad CA/Browser Forum en su Guía para la emisión y gestión de Certificados de Validación Extendida (EV), la cual puede consultarse en: https://cabforum.org/extended-validation/

3.2.2.2 Nombre comercial o marca registrada

Si la información de identidad del sujeto incluye un nombre comercial o una marca registrada, IZENPE aplicará los mismos procedimientos y criterios de verificación descritos en la Sección 3.2.2.1 para comprobar el derecho del solicitante a utilizar dicho nombre o marca.

En el caso de los certificados SSL cualificados, se requiere una verificación exhaustiva de identidad, conforme a lo definido en la Sección 11.3 de la Guía para la emisión y gestión de Certificados de Validación Extendida del CA/Browser Forum.

3.2.2.3 Verificación del país

El país será verificado utilizando cualquiera de los métodos listados en la Sección 3.2.2.1.

3.2.2.4 Validación de autorización y control del dominio

Para validar el dominio en certificados de autenticación de sitios web, IZENPE utiliza uno de los siguientes métodos descritos en el documento de Requisitos básicos del CA/Browser Forum:

- 3.2.2.4.4 Correo electrónico construido al contacto del dominio
- 3.2.2.4.7 Cambio en DNS
- 3.2.2.4.14 Correo electrónico al contacto DNS TXT
- 3.2.2.4.18 Cambio acordado en el sitio web versión 2
- 3.2.2.4.19 Cambio acordado en el sitio web mediante ACME

IZENPE seguirá un procedimiento documentado para cada método empleado y conservará registros que indiquen qué método se utilizó en cada emisión de certificado. Los métodos restantes descritos en los Requisitos básicos del CA/Browser Forum no se utilizan para la validación de dominio.

- Correo electrónico construido al contacto del dominio(BR 3.2.2.4.4).

  Se enviará un correo electrónico con un valor aleatorio a una o varias de las siguientes direcciones del dominio solicitado: «admin», «administrator», «webmaster», «hostmaster» o «postmaster».

- Cambio acordado en DNS (BR 3.2.2.4.7) El solicitante realiza un cambio en el registro DNS del dominio para el que solicita el certificado SSL. Este cambio consiste en añadir un código aleatorio y único enviado por IZENPE, dentro de un campo CNAME, TXT o CAA. Una vez que el solicitante realice el cambio, IZENPE procederá a verificarlo.

IZENPE proporcionará un código único aleatorio para cada solicitud de certificado y no reutilizará dicho código después de 30 días.

Para este propósito, deberá existir una entrada CAA con tipo «contactemail» con una dirección de correo electrónico válida, por ejemplo: CAA 0 contactemail contacto@example.com

IZENPE proporcionará un código único aleatorio para cada solicitud de certificado y no reutilizará dicho código después de 30 días.

- Correo electrónico al contacto DNS TXT (BR 3.2.2.4.14): IZENPE envía al solicitante un código único y aleatorio por correo electrónico a la dirección que aparece en el registro TXT del DNS. Debe existir una entrada TXT en el subdominio «_validation-contactemail» con una dirección de correo electrónico válida, por ejemplo:

  _validation-contactemail.izenpe.eus. 299 IN TXT 'contacto@example.com'

  IZENPE proporcionará un código único aleatorio para cada solicitud de certificado y no reutilizará dicho código después de 30 días.

- Cambio acordado en DNS (BR 3.2.2.4.18) IZENPE exige que el solicitante publique, en la ruta «/.well-known/pki-validation», un archivo que contenga un código aleatorio y único enviado previamente por IZENPE. Una vez que el solicitante realice el cambio, IZENPE procederá a verificarlo.

- Cambio acordado en el sitio web mediante ACME:
  Consiste en confirmar el control del Solicitante sobre un FQDN mediante la validación del dominio utilizando el método ACME HTTP Challenge, tal como se define en la sección 8.3 del RFC 8555. A continuación se detallan los requisitos adicionales a lo establecido en RFC 8555 IZENPE debe recibir una respuesta HTTP satisfactoria a la petición, lo que implica la recepción de un código de estado HTTP 2xx. El token (según lo definido en la Sección 8.3 del RFC 8555) NO debe utilizarse durante más de 30 días desde su creación. El CPS puede definir un periodo de validez más corto para los valores aleatorios. En ese caso, la AC deberá atenerse a lo indicado en su CPS. IZENPE no sigue redirecciones.

IZENPE confirma que el representante del suscriptor tiene control sobre los nombres de dominio completos (FQDN) que se incorporan en los certificados de autenticación de sitios web que emite. Para ello: a través de la aplicación encargada de registrar las solicitudes de estos certificados, IZENPE verifica la identidad del representante del suscriptor y el nombre del FQDN. Posteriormente, comprueba que la solicitud proviene de un contacto que controla el dominio (según los métodos definidos en la sección anterior) o que ha sido autorizado por dicho contacto. También verifica que la solicitud del certificado haya sido realizada posteriormente al registro de la entidad correspondiente.

Adicionalmente, antes de emitir un certificado de autenticación de sitio web, IZENPE: verifica que el dominio a incluir sea público (es decir, que no se trate de un dominio interno) y consulta registros

públicos para asegurarse de que no se trate de un dominio de alto riesgo, como los identificados por Google Safe Browsing.

3.2.2.5 Autenticación mediante dirección IP

IZENPE no emite certificados destinados a la identificación de direcciones IP.

3.2.2.6 Validación de dominios comodín

La RA verificará que el suscriptor controle legítimamente todo el espacio de nombres del dominio en los certificados comodín de tipo OV.

En los casos en los que, en un certificado comodín, el asterisco se ubique en la etiqueta situada inmediatamente a la izquierda de un sufijo público o un registro controlado, IZENPE rechazará la emisión del certificado salvo que el solicitante demuestre el control legítimo de todo el espacio de nombres del dominio.

Para ello, IZENPE consultará la Lista de Sufijos Públicos, disponible en: https://publicsuffix.org/. Esta lista será descargada periódicamente por IZENPE para mantener su referencia actualizada.

3.2.2.7 Fiabilidad de las fuentes de datos

Antes de utilizar una fuente de datos como fuente de datos fiable, IZENPE evaluará su fiabilidad, precisión y resistencia a la alteración o falsificación. Los criterios que tendrá en cuenta para dicha evaluación son los siguientes:

1. Antigüedad de la información proporcionada.
2. Frecuencia con la que se actualiza la fuente de datos.
3. Identidad del proveedor de datos y propósito de la recopilación.
4. Accesibilidad pública de la fuente de información.
5. Dificultad relativa para falsificar o alterar los datos.

3.2.2.8 Registro CAA

Como parte del proceso de emisión de Certificados, IZENPE consultará y procesará los registros CAA de acuerdo con el estándar RFC 8659, para cada entrada dNSName presente en la extensión subjectAltName (excepto si se trata de un dominio tipo Onion).

Durante el procesamiento de los registros CAA IZENPE procesará las etiquetas de propiedad issue, issuewild e iodef, según lo especificado en el RFC 8659. Aunque iodef no requiere una acción obligatoria, IZENPE debe respetar la etiqueta si está presente. Se PUEDEN admitir etiquetas de propiedad adicionales, pero NO deben entrar en conflicto ni reemplazar las etiquetas obligatorias establecidas en el RFC. IZENPE RESPETARÁ el indicador «crítico», y no emitirá el certificado si encuentra una etiqueta no reconocida con este indicador activado.

Si IZENPE emite un certificado tras procesar un registro CAA, deberá hacerlo dentro del TTL del registro CAA o en un máximo de 8 horas, lo que sea mayor.

3.2.3 Autenticación de la identidad individual

IZENPE verifica que el representante del suscriptor coincida con la persona física que solicita un certificado de autenticación de sitio web, mediante la firma electrónica del formulario de solicitud utilizando un Certificado cualificado de firma electrónica, lo que garantiza la autenticidad de su identidad.

En el caso de certificados DV u OV, el representante del suscriptor puede delegar la capacidad de solicitud a otros solicitantes autorizados. Esta delegación debe firmarse electrónicamente a través de la aplicación de gestión de certificados SSL.

3.2.4 Información no verificada del suscriptor

Toda la información incluida en el certificado electrónico es verificada por la RA. Por lo tanto, no se incluye información no verificada en el campo ‘Subject’ de los certificados emitidos.

3.2.5 Validación de autoridad

IZENPE verifica que el solicitante tenga suficiente capacidad representativa mediante la firma electrónica del formulario de alta de cliente, tal como se describe en la sección 3.2.3 de esta política, aceptando el uso de un certificado de representante de IZENPE. Cuando dicho formulario se firma con un certificado cualificado distinto a los mencionados e la sección precedente, la RA de IZENPE verifica la capacidad representativa del firmante consultando registros oficiales (Registro Mercantil, Boletines Oficiales, etc., según el tipo de representación). Si dichas consultas no permiten comprobar la capacidad representativa, IZENPE contactará con el suscriptor para obtener evidencia adicional.

A través de la aplicación en línea de solicitud de certificados SSL, el representante de la entidad puede crear usuarios asociados para permitir la solicitud de certificados DV y OV en nombre de dicha entidad.

Para las solicitudes de certificados SSL cualificados, IZENPE cumplirá con los requisitos definidos por el CA/Browser Forum en su «Guía para la emisión y gestión de Certificados de Validación Extendida (EV)».

3.2.6 Criterios de interoperabilidad

No existen relaciones de interoperabilidad con Autoridades de certificación externas a IZENPE.

3.3 Identificación y autenticación para

reemisión de clave

3.3.1 Identificación y autenticación para reemisión de clave rutinaria

Los suscriptores pueden solicitar la reemisión de clave de cualquier certificado a través de la aplicación web de IZENPE. Esta nueva solicitud podrá requerir nuevas validaciones, en caso de que alguna haya caducado.

Las condiciones de autenticación para una solicitud de renovación se describen en la sección correspondiente del proceso de renovación de certificados de esta CP (ver sección 4.6 de este documento).

3.3.2 Identificación y autenticación para solicitud de revocación

El proceso de renovación del certificado tras su revocación será el mismo que el seguido para la emisión inicial del certificado.

3.4 Identificación y autenticación para solicitud de revocación

IZENPE podrá revocar cualquier certificado cubierto por esta CP a su entera discreción. Las condiciones de autenticación para una solicitud de revocación se detallan en la sección 4.9 de este documento.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud del certificado

4.1.1 Quién puede presentar una solicitud de certificado

Solo los Representantes del suscriptor o las personas debidamente autorizadas para solicitar el certificado en nombre del Suscriptor, que hayan acreditado tener control sobre el nombre de dominio

que se incluirá en el certificado, podrán solicitar certificados de autenticación de sitios web. Dicho control sobre el nombre de dominio será verificado por IZENPE tal como se describe en la sección «3.2 Validación inicial de identidad» de esta Política.

Además, para certificados cualificados, IZENPE cumplirá con los requisitos de la «Guía para la emisión y gestión de Certificados de Validación Extendida» establecida por el CA/Browser Forum.

4.1.2 Proceso de alta y responsabilidades

Previo a la emisión de un certificado, IZENPE deberá recopilar la siguiente documentación del Solicitante:

- Presentación de la solicitud de emisión y aceptación de los términos y condiciones aplicables. Con esta aceptación, los suscriptores garantizan que toda la información incluida en la solicitud del certificado es correcta.
- Presentación de la solicitud técnica (PKCS#10).
- Pago, si corresponde, de las tasas aplicables.

La RA de IZENPE verificará la Organización suscriptora y al representante del suscriptor, y comprobará que la Solicitud de certificado sea correcta, completa y debidamente autorizada, de acuerdo con los requisitos definidos en la sección «3.2 Validación inicial de identidad» de este documento. IZENPE podrá realizar comprobaciones adicionales a los procesos de validación descritos en dicha sección.

IZENPE compilará y conservará las evidencias correspondientes a las verificaciones realizadas.

Las responsabilidades de las partes en este proceso están recogidas en la sección 9.6 2 «Obligaciones y garantías» de este documento.

4.2 Tramitación de la solicitud de certificado

4.2.1 Realización de las funciones de identificación y autenticación

El Representante del suscriptor enviará a la RA de IZENPE un formulario firmado electrónicamente con un certificado electrónico cualificado, que contendrá toda la información que se incluirá en el certificado de autenticación de sitio web. Con base en esta información, la RA de IZENPE llevará a cabo las comprobaciones descritas en la sección «3.2 Validación inicial de identidad» de esta Política.

IZENPE verificará la veracidad de los datos incluidos en la solicitud y, cuando proceda, la capacidad del representante mediante las verificaciones correspondientes, conservando las evidencias oportunas.

La firma electrónica generada para la formalización del contrato será verificada por IZENPE.

El uso de datos o documentación de prevalidación, obtenidos de una fuente especificada en la sección 3.2, no podrá utilizarse transcurridos más de 12 meses desde la validación de dichos datos o documentación.

4.2.2 Aprobación o rechazo de solicitudes de certificado

La RA que actúa en el proceso de emisión de certificados de autenticación de sitios web es siempre IZENPE y, por tanto, no delega la validación de la propiedad del dominio en ninguna otra RA.
La RA de IZENPE realiza las comprobaciones relativas a: la prueba de posesión de la clave privada por parte del representante del suscriptor, la autenticación de la identidad de la organización y de la persona que solicita el certificado, y la validación del dominio, según lo descrito en la sección «3.2 Validación inicial de identidad» de esta CP, lo cual resultará en la aprobación o el rechazo de la solicitud.

IZENPE mantiene una base de datos interna de todos los certificados revocados, así como de todas las solicitudes de certificados previamente rechazadas por sospechas de phishing u otros usos fraudulentos. Esta información se utiliza para identificar solicitudes posteriores sospechosas antes de proceder a la aprobación de la emisión del certificado.

Además, IZENPE desarrolla, mantiene e implementa procedimientos documentados que permiten identificar y exigir actividades de verificación adicionales para solicitudes de certificados consideradas de alto riesgo, antes de su aprobación, siempre que sea razonablemente necesario para asegurar que dichas solicitudes se verifiquen adecuadamente conforme a estos requisitos.

Si alguna de estas validaciones no pudiera ser confirmada, IZENPE rechazará la solicitud del certificado, reservándose el derecho de no revelar los motivos de dicho rechazo. El representante del suscriptor cuya solicitud haya sido rechazada podrá presentar una nueva solicitud en una fecha posterior.

Toda solicitud de certificado OV o certificado cualificado será tramitada por personal de IZENPE con el rol de personal de confianza para este fin. El sistema de aprobación para la emisión de certificados cualificados requiere la intervención de al menos dos personas pertenecientes a la RA de IZENPE con rol de personal de confianza, una para validar la solicitud y otra para aprobarla.

Además, IZENPE comprueba si existe un registro CAA para cada nombre de dominio incluido en un certificado de autenticación de sitio web emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento establecidas en dicho estándar para los registros encontrados.

Si existe dicho registro CAA, no emitirá el Certificado a menos que determine que la solicitud es coherente con el conjunto de registros CAA aplicable.

4.2.3 Plazo de tramitación de las solicitudes de certificado

El plazo de tramitación de una solicitud de certificado depende, en gran medida, de que el Representante del suscriptor aporte la información y documentación necesarias conforme a los procedimientos aprobados por IZENPE. No obstante, IZENPE hará todo lo posible para que el proceso de validación que conlleve la aceptación o rechazo de la solicitud no exceda los cinco días laborables.

Este plazo podrá superarse ocasionalmente por causas ajenas al control de IZENPE. En tales casos, se intentará mantener informado al Representante del suscriptor que realizó la solicitud sobre las causas del retraso.

4.2.4 Autorización de la Autoridad de Certificación (CAA)

IZENPE admite CAA para la emisión de certificados TLS y certificados de Marca Verificada, tal y como se describe en la sección 3.2.2.8.

Los suscriptores que deseen autorizar a IZENPE a emitir certificados TLS para sus FQDN deben incluir un registro CAA con la propiedad issue o issuewild, y el valor «izenpe.com» o «izenpe.eus» en su zona DNS correspondiente.

4.3 Emisión de certificados

4.3.1 Acciones de la CA durante la emisión del certificado

Una vez aprobada la solicitud del certificado por la RA de IZENPE, el sistema de generación de certificados cuenta con una serie de controles previos a la emisión, que verifican el cumplimiento de los requisitos de RFC 5280 y del CA/Browser Forum (BRs y EVGs). Tras dicha verificación, el Certificado se emite de acuerdo con el perfil aprobado para cada tipo de Certificado.

Asimismo, IZENPE monitoriza periódicamente posibles desviaciones en los certificados emitidos.

Los procesos relacionados con la emisión de certificados electrónicos garantizan que todas las cuentas implicadas empleen autenticación multifactor.

4.3.1.1 Autorización manual para la emisión de certificados por las Root CAs

La emisión de certificados por la Root CA requerirá que una persona autorizada por IZENPE (por ejemplo, el operador del sistema de la CA, responsable de sistemas o administrador de PKI) emita deliberadamente un comando directo para que la Root CA lleve a cabo la operación de firma del certificado.

4.3.1.2 Linting del contenido del certificado antes de su firma

Debido a la complejidad que conlleva implementar perfiles de certificado conformes a estos requisitos, se considera una buena práctica que la CA implemente un proceso de Linting para probar la conformidad técnica de cada certificado pendiente de firma antes de proceder a su firma. Cuando un Precertificado ha pasado por el proceso de Linting, no será necesario aplicar Linting al certificado final, siempre que la CA disponga de un control técnico que verifique que el certificado a firmar corresponde al Precertificado, conforme a lo descrito en la RFC 6962, sección 3.2.
A partir del 15 de septiembre de 2024, se RECOMIENDA que la CA implemente este proceso de Linting. A partir del 15 de marzo de 2025, IZENPE DEBERÁ implementar obligatoriamente este proceso de Linting.

IZENPE DEBERÍA utilizar las herramientas de Linting ampliamente adoptadas por la industria, disponibles en: https://cabforum.org/resources/tools/. En particular, se recomienda el uso de zlint y pkimetal.

4.3.2 Notificación al suscriptor por parte de la CA sobre la emisión del certificado

Una vez emitido el Certificado, IZENPE envía una comunicación a la dirección de correo electrónico indicada en el formulario de alta de cliente firmado por el Representante del suscriptor, informando que el certificado está disponible para su descarga.

4.4 Aceptación del certificado

4.4.1 Hecho constitutivo de aceptación del certificado

Durante el proceso de solicitud del Certificado, el Representante del suscriptor acepta las condiciones de uso y manifiesta su voluntad de obtener el certificado, como requisitos necesarios para la generación del mismo.

4.4.2 Publicación del certificado por parte de la CA

Los certificados raíz y subordinados se publican en el repositorio general de IZENPE (ver Sección 2.2 de este documento).

IZENPE genera un precertificado por cada certificado emitido, conforme a la RFC 6962 (Transparencia de certificados). Este precertificado contiene la misma información que el certificado que se tiene la intención de emitir y se considerará como si hubiese sido emitido (aunque no lo haya sido). Dichos certificados pueden ser recuperados por cualquier persona que consulte los servidores de Transparencia de certificados.

4.4.3 Notificación de la emisión del certificado por la CA a

otras entidades

Antes de la emisión de Certificados de autenticación de sitio web, se envía un precertificado a los registros del servicio de Transparencia de certificados de aquellos proveedores donde esté incluido el Certificado raíz de IZENPE.

4.5 Uso del par de claves y del certificado

4.5.1 Uso de la clave privada y del certificado

IZENPE no genera ni almacena las claves privadas asociadas a los Certificados emitidos bajo esta CP. La custodia y el control de las claves del certificado corresponden a los Representantes del suscriptor que hayan acreditado el control del nombre de dominio que se incluirá en el certificado. Por lo tanto, la clave privada asociada a la clave pública será responsabilidad de dicho custodio.

4.5.2 Uso de la clave pública y del certificado por parte del tercero de confianza

Las entidades usuarias y los terceros que confíen en el certificado deben utilizar software compatible con los estándares aplicables al uso de certificados electrónicos (X.509, IETF, RFCs, etc.). Si la conexión al sitio web requiere medidas de seguridad adicionales, estas deben ser obtenidas por parte de las entidades usuarias.

Los terceros que confíen en el establecimiento de una conexión segura garantizada por un Certificado de autenticación de sitio web deben asegurarse de que dicha conexión: se haya creado dentro del período de validez del Certificado, que el Certificado se esté utilizando para el propósito para el que fue emitido conforme a esta CP, y que el Certificado esté actualmente activo, verificando su estado de revocación según lo dispuesto en la sección «4.10 Servicios de información sobre el estado de los certificados» de este documento.

4.6 Renovación del certificado

4.6.1 Circunstancia para la renovación del certificado

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.6.2 Quién puede solicitar la renovación

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.6.3 Tramitación de las solicitudes de renovación de certificados

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.6.4 Notificación de la emisión del nuevo certificado al suscriptor

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.6.5 Actuación que constituye aceptación del certificado renovado

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.6.6 Publicación del certificado renovado por parte de la CA

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.6.7 Notificación de la emisión del certificado por la CA a otras entidades

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados descrito en este documento.

4.7 Regeneración de clave del certificado

La renovación con regeneración de clave de los certificados de autenticación de sitio web se realiza siempre mediante la emisión de nuevas claves pública y privada, siguiendo el mismo proceso descrito para la emisión de un nuevo Certificado.

4.7.1 Circunstancia para la regeneración de claves del certificado

Las claves del certificado se renovarán en los siguientes casos:

- Por la expiración inminente de las claves actuales, a solicitud del solicitante de la renovación.
- Por vulneración de las claves o cualquier otra circunstancia recogida en la sección «4.9

Revocación y suspensión del certificado» de esta CP.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

Se seguirá el mismo proceso descrito para la emisión de un nuevo Certificado.

4.7.3 Tramitación de solicitudes de regeneración de clave

Se seguirá el mismo proceso descrito para la emisión de un nuevo Certificado.

4.7.4 Notificación de la emisión del nuevo certificado al suscriptor

Se seguirá el mismo proceso descrito para la emisión de un nuevo Certificado.

4.7.5 Actuación que constituye aceptación del certificado regenerado

Se seguirá el mismo proceso descrito para la emisión de un nuevo Certificado.

4.7.6 Publicación del certificado regenerado por parte de la CA

Se seguirá el mismo proceso descrito para la emisión de un nuevo Certificado.

4.7.7 Notificación de la emisión del certificado por la CA a otras entidades

Se seguirá el mismo proceso descrito para la emisión de un nuevo Certificado.

4.8 Modificación del certificado

No es posible realizar modificaciones sobre Certificados ya emitidos. Por tanto, cualquier necesidad de modificación implica la emisión de un nuevo certificado.

4.8.1 Quién puede solicitar la modificación del certificado

Modificación no estipulada.

4.8.2 Quién puede solicitar la modificación del certificado

Modificación no estipulada.

4.8.3 Tramitación de las solicitudes de modificación de certificados

Modificación no estipulada.

4.8.4 Notificación de la emisión del nuevo certificado al suscriptor

Modificación no estipulada.

4.8.5 Actuación que constituye aceptación del certificado modificado

Modificación no estipulada.

4.8.6 Publicación del certificado modificado por parte de la CA

Modificación no estipulada.

4.8.7 Notificación de la emisión del certificado por la CA a otras entidades

Modificación no estipulada.

4.9 Revocación y suspensión del certificado

Los certificados de autenticación de sitio web emitidos por IZENPE serán revocados en los siguientes casos:

1. Finalización del periodo de validez del certificado.
2. Cese de actividad de Izenpe como Prestador cualificado de servicios de confianza, salvo que, con el consentimiento expreso del suscriptor, los certificados emitidos por Izenpe se transfieran a otro Prestador de servicios de confianza.
   En los casos a) y b), la pérdida de efectividad de los certificados se producirá en el momento en que se den dichas circunstancias.
3. Revocación del certificado por cualquiera de los motivos indicados en este documento.

La expiración de la validez del certificado tendrá efecto desde la fecha en que IZENPE tenga conocimiento de cualquiera de los eventos determinantes y así lo indique en su Servicio de información y consulta sobre el estado de los Certificados.

IZENPE pone a disposición de suscriptores, terceros de confianza, proveedores de software y

terceros un canal de comunicación mediante la dirección: incidencias@izenpe.eus. Para que puedan comunicar cualquier incidencia relacionada con este tipo de certificados, respecto a la supuesta vulneración de la clave privada, uso indebido de los certificados u otros tipos de fraude, vulneración, uso indebido o conducta inapropiada.

IZENPE, como prestador cualificado de servicios de confianza, se reserva el derecho de no emitir o revocar este tipo de certificados si el suscriptor que tiene el control del nombre de dominio del sitio web incluido en el certificado no hace un uso adecuado del mismo, infringiendo los derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o sedes electrónicas que desea proteger con dichos certificados, o si su uso induce a error o confusión sobre la titularidad de dichas aplicaciones, sitios o contenidos.

IZENPE quedará indemne frente a los titulares o responsables de los equipos, aplicaciones, sitios web o sedes electrónicas que no cumplan lo previsto en esta sección y que estén relacionados con el certificado, quedando exonerada de cualquier reclamación o demanda por el uso inadecuado de dichos certificados.

4.9.1 Circunstancias para la revocación

4.9.1.1 Motivos de revocación de un certificado de entidad final

Además de lo previsto en el apartado anterior, serán causas de revocación de un certificado de autenticación de sitio web las siguientes:

1. Solicitud de revocación por parte de personas autorizadas. En todo caso, dicha solicitud deberá realizarse conforme a lo establecido por IZENPE.
    - Pérdida del soporte del certificado.
    - Uso por parte de un tercero de la clave privada asociada al certificado.
    - Violación o vulneración de la confidencialidad de la clave privada asociada al certificado.
    - No aceptación de las nuevas condiciones derivadas de la publicación de nuevas Declaraciones de Prácticas de Certificación (CPS), dentro del plazo de un mes desde su publicación.
2. Resolución judicial o administrativa que lo ordene.
3. Extinción, disolución o cierre del sitio web identificado por el certificado.
4. Extinción o disolución de la personalidad jurídica del suscriptor.
5. Cese de la forma de representación del representante del suscriptor del certificado.
6. Incapacidad total o parcial del Representante del suscriptor.
7. Inexactitudes en los datos facilitados por el Representante del suscriptor para la obtención del certificado, o modificación de los datos o circunstancias verificadas, de forma que el certificado

deje de ajustarse a la realidad.

8. Contravención de una obligación sustancial de esta CPS por parte del suscriptor, su representante o una Entidad de registro, si dicha contravención pudiera haber afectado al procedimiento de emisión.

9. Uso del certificado con la finalidad de generar dudas en los usuarios sobre el origen de productos o servicios ofrecidos, haciendo parecer que su procedencia es distinta a la real. Para ello, se seguirán los criterios establecidos en las normativas sobre consumidores y usuarios, comercio, competencia y publicidad.

10. Resolución del contrato entre el suscriptor o su representante e IZENPE, o impago de los servicios prestados.

11. Violación o vulneración de la confidencialidad de los datos de creación de firma/sello de IZENPE, con el cual firma/sella los certificados que emite.

12. Incumplimiento de los requisitos definidos por los esquemas de auditoría a los que está sujeta la Autoridad de certificación emisora de los certificados cubiertos por esta Política, con especial atención a aquellos relativos a algoritmos y tamaños de clave, que supongan un riesgo inaceptable para las partes que confían en dichos Certificados.

En ningún caso debe entenderse que IZENPE asume la obligación de comprobar los puntos "3" al "9" anteriormente indicados.

IZENPE solo será responsable por no haber revocado un Certificado en los siguientes casos:

- Que la revocación haya sido solicitada por el Representante del suscriptor conforme al procedimiento establecido.
- Que deba haberse revocado como consecuencia de la resolución del contrato con el Suscriptor.
- Que la solicitud de revocación o la causa de la misma haya sido notificada al Suscriptor mediante una resolución judicial o administrativa.
- Que los puntos «3» al «7» hayan sido acreditados fehacientemente, tras la identificación del solicitante de la revocación.

Acciones que constituyan delito o infracción penal sobre los datos o Certificados, de las cuales IZENPE no haya tenido conocimiento, así como inexactitudes o falta de diligencia en la comunicación de datos, exonerarán a IZENPE de cualquier responsabilidad.

Todas las solicitudes de revocación de certificados de entidad final serán tramitadas en un plazo máximo de 24 horas desde su recepción.

4.9.1.2 Motivos de revocación de un certificado de Sub CA

Los certificados de Sub CA deberán revocarse en un plazo máximo de 7 días por los siguientes

motivos:

1. La Sub CA lo solicita por escrito.
2. La Sub CA notifica que la solicitud original del certificado no fue autorizada y no permite su autorización retroactiva.
3. La CA emisora obtiene evidencia de que la clave privada correspondiente ha sido comprometida o ya no cumple los requisitos de las secciones 6.1.5 y 6.1.6 del BR.

4. La CA emisora obtiene evidencia de que el certificado fue emitido incorrectamente.
5. La CA emisora detecta que el certificado fue emitido sin cumplir con la CP o CPS.
6. La CA emisora determina que la información del certificado es inexacta o errónea.
7. La CA emisora o la Sub CA cesan su actividad y no han habilitado un acuerdo con otra CA para mantener el servicio de revocación.
8. Se revoca o termina el derecho de la CA emisora o Sub CA a emitir certificados conforme a los requisitos BR, salvo que exista acuerdo para mantener el repositorio CRL/OCSP.
9. Lo requiere la política de la CA emisora o su CPS.
10. El contenido o el formato técnico del certificado representa un riesgo inaceptable para los proveedores de software o terceros.
11. Proveedores o terceros (por ejemplo, el CA/Browser Forum) pueden determinar que un algoritmo criptográfico, firma o tamaño de clave supone un riesgo inaceptable, y que dichos certificados deben ser revocados y reemplazados dentro de un plazo determinado.

4.9.2 Quién puede solicitar la revocación

La revocación puede ser solicitada por el Suscriptor, la RA o la CA emisora. Adicionalmente, los Suscriptores, Terceros de confianza, Proveedores de software de aplicación u otros terceros pueden remitir Informes de Problemas de certificados informando a la CA emisora de una causa razonable para revocar el certificado.

4.9.3 Procedimiento para solicitar la revocación

El solicitante de la revocación deberá presentar la solicitud de revocación a IZENPE. En el caso de que la revocación sea solicitada por una persona distinta del solicitante, el suscriptor o el titular de la clave, IZENPE informará al titular de la clave y al suscriptor del certificado sobre la revocación y el motivo por el que se ha llevado a cabo, ya sea con anterioridad o de forma simultánea a la misma.

El solicitante podrá revocar el certificado a través de los siguientes canales:

- Presencialmente,
    - ante IZENPE mediante cita previa en www.izenpe.eus
    - A través de la entidad suscriptora, con la que IZENPE tenga firmado el correspondiente instrumento jurídico.

- En línea, en www.izenpe.eus
- Por correo electrónico, enviando el formulario de revocación firmado con el DNI electrónico o un certificado cualificado emitido por IZENPE.

La solicitud de revocación autenticada, así como la información justificativa, se registran y archivan.

Una vez IZENPE haya revocado el certificado de autenticación web, se publicará la correspondiente CRL en el Directorio seguro, incluyendo el número de serie del Certificado revocado, así como la fecha, hora y causa de la revocación. El Representante del suscriptor recibirá, en la dirección de correo electrónico especificada en la solicitud, una notificación del cambio de estado de validez del Certificado.

4.9.4 Periodo de gracia para la solicitud de revocación

No existe un periodo de gracia asociado a este proceso, ya que la revocación se lleva a cabo de forma inmediata una vez verificada la recepción de la solicitud.

4.9.5 Plazo de la CA para tramitar la solicitud de revocación

Todas las solicitudes de revocación de certificados de entidad final se procesan en un plazo máximo de 24 horas desde la recepción confirmada de la solicitud.

IZENPE procede a la revocación inmediata del certificado de autenticación web en el momento de realizar las comprobaciones descritas anteriormente o, en su caso, una vez verificada la veracidad de la solicitud mediante resolución judicial o administrativa.

4.9.6 Requisitos de comprobación de revocación para terceros de confianza

Los terceros que confían y aceptan el uso de certificados emitidos por IZENPE podrán verificar:

- que el certificado sigue siendo válido y activo, y
- el estado de los certificados incluidos en la cadena de certificación.

4.9.7 Frecuencia de emisión de CRL (si aplica)

IZENPE emite de forma inmediata una Lista de revocación de certificados (de aquí en adelante CRL) tan pronto como se produce una revocación.

La programación para la emisión de una nueva CRL está indicada en la propia CRL, aunque puede emitirse una antes del plazo si fuera necesario. Si no se producen revocaciones, la CRL se regenera

diariamente.

La CRL para certificados de entidad final se emite al menos cada 24 horas, o cuando se produce una revocación, con una validez de 10 días.

La CRL de certificados de CA (ARL) se emite cada 12 meses o cuando se produce una revocación.

Los certificados revocados que expiran se eliminan de la CRL. El registro de la revocación se conserva en el registro interno de IZENPE durante un período de 15 años.

4.9.8 Latencia máxima para CRLs (si aplica)

El tiempo máximo de latencia se establece en 30 segundos desde la generación de la CRL.

4.9.9 Disponibilidad de comprobación en línea de revocación/estado

IZENPE ofrece a las Entidades usuarias un servicio de verificación del estado del certificado en tiempo real utilizando el protocolo OCSP (Online Certificate Status Protocol), de forma que las aplicaciones usuarias puedan comprobar el estado del certificado.

Este servicio está disponible las 24 horas del día, los 7 días de la semana.

4.9.10 Requisitos para la comprobación en línea de revocación

El uso del servicio de CRLs, de acceso libre, requerirá:

- Comprobar en todo caso la última CRL emitida, la cual puede descargarse desde la dirección URL contenida en el propio certificado en la extensión «CRL Distribution Point».
- Que el usuario compruebe adicionalmente la(s) CRL(s) correspondiente(s) a la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse de que la respuesta está firmada por la CA que ha emitido el certificado a validar.
-

Los certificados revocados que hayan expirado serán eliminados de la CRL. No obstante, se seguirá proporcionando información sobre el estado del certificado mediante la consulta en línea, independientemente de que esté expirado.

El uso del servicio OCSP (también de libre acceso) requerirá:

- Comprobar la dirección URL contenida en el propio certificado en la extensión «Authority Info Access».
- El usuario deberá asegurarse de que la respuesta está firmada por la CA que ha emitido el certificado a validar.

4.9.11 Otros métodos de notificación de revocación disponibles

IZENPE envía un correo electrónico informativo al suscriptor del certificado cuando éste ha sido revocado.

4.9.12 Requisitos especiales en caso de vulneración de clave

No existen requisitos especiales en caso de revocación del certificado por vulneración de clave. Aplican los mismos requisitos que para el resto de causas de revocación.

4.9.13 Circunstancias para la suspensión

No se contempla la suspensión de certificados.

4.9.14 Quién puede solicitar la suspensión

No se contempla la suspensión de certificados.

4.9.15 Procedimiento para solicitar la suspensión

No se contempla la suspensión de certificados.

4.9.16 Límites del periodo de suspensión

No se contempla la suspensión de certificados.

4.10 Servicios de información de estado de certificados

4.10.1 Características operativas

El funcionamiento del Servicio de Información y Consulta del Estado de Certificados es el siguiente: El servidor OCSP recibe la solicitud OCSP realizada por un Cliente OCSP y verifica el estado de validez de los certificados incluidos en dicha solicitud. Si la solicitud es válida, se emite una respuesta OCSP que informa sobre el estado actual de los certificados consultados. Dicha respuesta se encuentra firmada/sellada con los Datos de Creación de Firma/Sello de IZENPE, garantizando así la integridad y autenticidad de la información proporcionada sobre el estado de revocación de los certificados.

Es responsabilidad de la Entidad Usuaria disponer de un Cliente OCSP que opere con el servidor OCSP puesto a disposición por IZENPE.

IZENPE opera y mantiene sus servicios de CRL y OCSP con los recursos suficientes para garantizar

un tiempo de respuesta adecuado bajo condiciones normales de operación.

4.10.2 Disponibilidad del servicio

IZENPE realiza todas las acciones necesarias para garantizar la disponibilidad ininterrumpida, en la medida de lo posible, de su servicio OCSP. IZENPE DEBERÁ operar y mantener su capacidad de CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez (10) segundos o menos en condiciones normales de operación.

4.10.3 Funcionalidades opcionales

No estipulado.

4.11 Fin de la suscripción

El certificado deja de ser válido para su uso tras la finalización del período de validez o cuando ha sido revocado.

La expiración de cada certificado se indica en la Política específica correspondiente.

4.12 Custodia y recuperación de claves

4.12.1 Política y prácticas de custodia y recuperación de claves

IZENPE no genera las claves privadas de los certificados de autenticación de sitio web y, por lo tanto, no las almacena ni puede recuperarlas.

4.12.2 Política y prácticas sobre encapsulación y recuperación de claves de sesión

No estipulado.

5. CONTROLES DE INSTALACIÓN, GESTIÓN Y OPERACIÓN

5.1 Controles físicos

5.1.1 Ubicación del sitio e infraestructuras

Las instalaciones donde se procesa la información cumplen con los siguientes requisitos:

- El edificio que alberga las instalaciones de procesamiento de información es físicamente sólido, con paredes exteriores reforzadas, monitorización continua por cámaras de videovigilancia, y el acceso está restringido exclusivamente a personal debidamente autorizado.
- Todas las puertas y ventanas están cerradas y protegidas para prevenir el acceso no autorizado.

5.1.2 Acceso físico

Centro de procesamiento de datos

La instalación de IZENPE dispone de un sistema completo de control de acceso físico que incluye:

- Seguridad perimetral desde suelo técnico hasta techo real, para evitar accesos no autorizados.
- Control del acceso físico a la instalación:
  - Solo se permite el acceso a personal autorizado.
  - Los derechos de acceso al área de seguridad se revisan y actualizan periódicamente.
  - Todo el personal debe portar algún tipo de identificación visible. Se anima a los empleados a preguntar a cualquier persona que no cumpla este requisito.
  - El personal ajeno a IZENPE que trabaje en las instalaciones está supervisado adecuadamente.
- Se mantiene un registro de accesos al sitio seguro.
- Mecanismos de control en las puertas perimetrales del edificio.
- Sistema de circuito cerrado de televisión que monitoriza los componentes utilizados por IZENPE para la prestación de sus servicios de certificación.

Autoridades de registro (RA)

Las RA cumplen con los criterios de seguridad necesarios definidos tanto en la Política de seguridad de IZENPE como en su Política de seguridad para proveedores.

5.1.3 Suministro eléctrico y aire acondicionado

El centro de procesamiento de datos dispone de suministro eléctrico y climatización suficientes para mantener un entorno de operación fiable.
Las instalaciones de IZENPE también cuentan con un Sistema de alimentación ininterrumpida (SAI) y un grupo electrógeno, que mantienen en funcionamiento los equipos el tiempo necesario para permitir un apagado ordenado en caso de fallo eléctrico o de climatización.

5.1.4 Exposición al agua

IZENPE ha adoptado las precauciones necesarias para minimizar el impacto de la exposición al agua.

5.1.5 Prevención y protección contra incendios

El centro de procesamiento de datos de IZENPE dispone de barreras físicas que se extienden del suelo técnico al techo real y sistemas automáticos de detección de incendios para:

- Notificar la activación a vigilancia y personal de IZENPE.
- Desconectar el sistema de ventilación, cerrar puertas ignífugas, cortar el suministro eléctrico y activar el sistema automático de extinción de incendios.

5.1.6 Almacenamiento de medios

Los soportes que contienen información de respaldo se almacenan de forma segura y protegida.

5.1.7 Eliminación de residuos

Existe una política para regular los procedimientos de destrucción de soportes de información.

Los soportes que contienen información confidencial son destruidos de forma que la información sea irrecuperable.

5.1.8 Respaldo fuera del sitio

IZENPE conserva copias de respaldo en un entorno seguro, protegido contra accidentes y a una distancia suficiente para evitar daños en caso de desastre en el sitio principal.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Un «rol de confianza» se define como una persona con responsabilidades que podrían generar problemas de seguridad si no se ejecutan adecuadamente, ya sea por error o intencionalmente.

Para garantizar el correcto desempeño de estos roles, se aplican las siguientes consideraciones:

- La tecnología está diseñada y configurada para prevenir errores o conductas indebidas.
- Las funciones están distribuidas entre varios individuos, de modo que cualquier acción indebida requiera complicidad.

IZENPE dispone de definiciones completas para todos los roles desempeñados en la organización. Los roles y responsabilidades están claramente definidos para cada uno.

5.2.2 Número de personas requeridas por tarea

Para reforzar la seguridad del sistema, se asigna más de una persona a cada rol, con la excepción del rol de operador, que puede ser desempeñado por el administrador.

Asimismo, varias personas pueden estar asignadas al mismo rol.

5.2.3 Identificación y autenticación para cada rol

Los roles de confianza requieren verificación de identidad por medios seguros; todos los roles de confianza son desempeñados por personas físicas.

IZENPE dispone de documentación específica con detalles adicionales de cada rol.

5.2.4 Roles que requieren separación de funciones

IZENPE sigue la política de seguridad CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures), lo cual está definido en su modelo de seguridad.

5.3 Controles del personal

5.3.1 Cualificaciones, experiencia y requisitos de habilitación

IZENPE emplea personal con la experiencia y las cualificaciones necesarias para desempeñar sus funciones.

Todo el personal con roles de confianza está libre de cualquier conflicto de intereses que pueda afectar a su imparcialidad respecto a las operaciones de IZENPE.

5.3.2 Procedimientos de verificación de antecedentes

A través de sus procedimientos de Recursos Humanos, IZENPE realiza investigaciones pertinentes antes de contratar personal. Debido a limitaciones legales, no se incluye una verificación de antecedentes penales.

5.3.3 Requisitos de formación

IZENPE proporciona a su personal la formación necesaria para que puedan desempeñar sus funciones de forma competente y satisfactoria. La formación se realiza al menos una vez al año e incluye, como mínimo, los siguientes contenidos:

- Copia de la Declaración de Prácticas de Certificación.
- Sensibilización en materia de seguridad.

- Funcionamiento del software y hardware para cada rol específico.
- Procedimientos de seguridad por rol específico.
- Procedimientos de gestión y operación por rol específico.
- Procedimientos de recuperación ante desastres. • Procedimientos de gestión de incidentes.

Los operadores de la RA recibirán formación y sensibilización específica al incorporarse y luego con la frecuencia definida por IZENPE.

5.3.4 Frecuencia y requisitos de cursos de perfeccionamiento

Cualquier cambio significativo en la operación de IZENPE requerirá un plan de formación, cuya ejecución será documentada. El personal con Roles de confianza deberá recibir formación al menos una vez al año para mantener su nivel de competencia. Esta formación debe incluir siempre una revisión de contenidos.

5.3.5 Frecuencia y secuencia de rotación de puestos

Los empleados rotan de puesto según las necesidades del rol o a solicitud del propio empleado.

5.3.6 Sanciones por acciones no autorizadas

Incidentes de seguridad de la información

IZENPE dispone de un plan de gestión de incidentes de seguridad.

Proceso sancionador

Existe un régimen disciplinario interno que define las sanciones aplicables al personal.

5.3.7 Requisitos para contratistas independientes

Todo el personal subcontratado por IZENPE para desempeñar funciones relacionadas con la operación de sus servicios está sujeto a los mismos requisitos establecidos en la Política de seguridad de Proveedores de IZENPE.

5.3.8 Documentación suministrada al personal

Todo el personal que desempeña Trusted Roles recibe:

- Copia de la Declaración de Prácticas de Certificación.
- Documentación que define las obligaciones y procedimientos asociados a cada rol.
- Acceso a los manuales de operación de los distintos componentes del sistema.

5.4 Procedimientos de registro de auditoría

Los registros de auditoría permiten reconstruir eventos significativos registrados en el software de IZENPE o de la Autoridad de Registro (RA), así como identificar al usuario o evento que originó el registro. También se utilizan en arbitrajes para resolver disputas y comprobar la validez de una firma en un momento determinado.

5.4.1 Tipos de eventos registrados

Se almacenan los siguientes eventos:

- Solicitudes de nuevos certificados
- Solicitudes de certificados rechazadas
- Violaciones de acceso a cuentas
- Firma de certificados
- Caducidad de certificados
- Inicio de sesión de cuentas
- Firma de listas CRL
- Modificaciones en la CA
- Caducidad de certificados

Esta lista no es exhaustiva y se limita a eventos directamente relacionados con la gestión de certificados o funciones administrativas. No se incluyen eventos técnicos registrados en otros sistemas.

Cada evento se registra con fecha y hora, utilizando una fuente horaria confiable.

5.4.1.1 Registros de actividad de routers y firewalls

Sin estipulación.

5.4.2 Frecuencia de procesamiento de registros

Los registros son procesados de forma continua y auditados trimestralmente por el área técnica. El informe de auditoría incluye:

- Listado de intentos de acceso no autorizado.
- Errores generados en cada CA.

5.4.3 Periodo de conservación de los registros de auditoría

La información del archivo de registro se mantiene en línea hasta que es archivada. Una vez archivados, los archivos de registro se conservan durante 7 años.

5.4.4 Protección del registro de auditoría

El acceso a la información del registro se asigna únicamente al personal que lo requiera como parte de sus funciones. El rol de Auditor puede acceder a dicha información. El registro se almacena en la base de datos, y el acceso está protegido en diferentes niveles.

Está bloqueada la eliminación o modificación no autorizada de los registros de auditoría. Existen métodos de contingencia para evitar la pérdida de los datos del registro.

5.4.5 Procedimientos de copia de seguridad de registro de auditoría

Los registros se alojan en la base de datos, por lo que se incluyen en la copia de seguridad diaria de la base de datos, conforme a la política de copias de seguridad.

5.4.6 Sistema de recopilación de auditoría (interno vs. externo)

Los archivos de registro de la CA y de la RA se almacenan en los sistemas internos de IZENPE.

5.4.7 Notificación al sujeto que genera el evento

No se contempla la notificación al sujeto que origina un evento registrado.

5.4.8 Evaluaciones de vulnerabilidad

Las vulnerabilidades, tanto externas como internas, en los sistemas internos de IZENPE, se evalúan de forma trimestral. Además, se realiza una prueba de penetración anual.

5.5 Archivo de registros

5.5.1 Tipos de registros archivados

Se archivan los siguientes datos o archivos, entre otros:

- Datos relacionados con el procedimiento de registro y solicitud de certificados.
- Los registros de auditoría descritos en la sección anterior.
- El registro de claves.

5.5.2 Periodo de conservación del archivo

Toda la información y documentación relacionada con certificados cualificados se conserva durante 15 años (desde la fecha de emisión). Los documentos relativos a otros tipos de certificados se conservan durante 7 años (desde la fecha de expiración del certificado).

5.5.3 Protección del archivo

El Procedimiento de gestión del archivo establece las medidas de protección adoptadas para que los registros, tanto en formato papel como electrónico, no puedan ser manipulados ni destruidos.

5.5.4 Procedimientos de copia de seguridad del archivo

Existe una política de copias de seguridad y un plan de contingencia que definen los criterios y estrategias de actuación ante incidentes. El diseño de la estrategia para actuar en caso de incidentes se basa en un inventario de activos y un análisis de riesgos.

5.5.5 Requisitos de sellado de tiempo de los registros

Los sistemas de información utilizados por IZENPE garantizan el registro exacto de la hora en que ocurre cada evento registrado. La hora utilizada proviene de una fuente de tiempo confiable. Todos los sistemas están sincronizados con esta fuente.

5.5.6 Sistema de recopilación de archivos (interno vs. externo)

El sistema de recopilación de archivos está ubicado en las instalaciones de IZENPE y en las instalaciones de las entidades que participan en la prestación de servicios.

5.5.7 Procedimientos para obtener y verificar la información archivada

El acceso a esta información está limitado a personal autorizado y está protegido frente al acceso físico y lógico conforme a las secciones 5 y 6 de esta Declaración de Prácticas de Certificación (CPS).

5.6 Cambio de clave

Para minimizar el riesgo de vulneración de la clave privada de la CA, la clave debe cambiarse de acuerdo con el nivel de seguridad del algoritmo utilizado. Una vez cambiada, la nueva clave solo debe usarse para firmar. La clave antigua, aunque siga siendo válida, debe mantenerse disponible para verificar firmas antiguas hasta que todos los certificados firmados con ella hayan expirado. La clave privada antigua solo debe conservarse si se utiliza para firmar CRLs de certificados firmados con dicha clave, y debe estar protegida con el mismo nivel de seguridad que la nueva clave. El procedimiento para generar una nueva clave de CA está definido en el Documento de Ceremonia de Generación para nuevas CAs y migraciones desde CAs anteriores. La sección 6.1.5 define los tamaños de clave y algoritmos utilizados.

5.7 Compromiso y recuperación ante desastres

5.7.1 Procedimientos de gestión de incidentes y vulneración

5.7.1.1 Respuesta a incidentes y plan de recuperación desastre.

Existe un Plan de contingencia que describe todas las acciones a realizar, así como los recursos y el personal involucrado, en caso de que un incidente, ya sea intencionado o accidental, dañe o inutilice los recursos de certificación o los servicios proporcionados por IZENPE. Los objetivos principales del Plan de contingencia son:

- Maximizar la eficacia de las operaciones de recuperación estableciendo tres fases:
  - Fase de Notificación/Evaluación/Activación para detectar y valorar los daños e iniciar la ejecución del plan.
  - Fase de Recuperación, orientada a restablecer de forma temporal y parcial los servicios hasta que se repare el daño en el sistema original.
  - Fase de Reconstitución, para restaurar las operaciones y procesos regulares.
- Identificar las actividades, recursos y procedimientos necesarios para ofrecer servicios de certificación de forma parcial en un CPD alternativo durante interrupciones prolongadas de las operaciones normales.
- Asignar responsabilidades al personal designado por IZENPE y proporcionar una guía para la recuperación de operaciones durante periodos largos de interrupción.
- Asegurar la coordinación entre todas las partes involucradas (departamentos de la entidad, puntos de contacto externos y proveedores) implicadas en la estrategia de contingencia planificada.

El Plan de contingencia de IZENPE se aplica a todas las funciones, operaciones y recursos necesarios para restablecer la prestación de servicios de certificación. También aplica al personal de IZENPE relacionado con dicha prestación.

El plan prevé la participación de ciertos grupos en la recuperación de las operaciones de IZENPE.

Las evaluaciones de daños y el plan de actuación están descritos en el propio Plan de contingencia.

En caso de que el algoritmo, la combinación de tamaños de claves utilizada, u otra circunstancia técnica reduzca significativamente la seguridad técnica del sistema, se activará el Plan de contingencia. Se llevará a cabo un análisis del impacto económico, el cual incluirá: El análisis abordará la naturaleza crítica del problema de seguridad, su alcance y la estrategia de recuperación para gestionar el incidente. En el informe de análisis de impacto deberán definirse los siguientes puntos:

- Descripción detallada de la contingencia, plazos temporales, etc.
- Naturaleza crítica del incidente, ámbito

- Solución o soluciones propuestas
- Plan de despliegue de la solución elegida, que incluirá al menos:
  - Notificación a los usuarios mediante los medios considerados más eficaces.
    Incluir a los solicitantes de certificados, suscriptores y verificadores (terceros de confianza).
  - Publicación de la contingencia en la página web.
  - Revocación de los certificados afectados.
  - Estrategia de renovación.

5.7.1.2Plan de revocación masiva

Desde el 1 de septiembre de 2025, Izenpe mantiene un plan integral y práctico para eventos de revocación masiva

para garantizar una respuesta rápida, coherente y fiable ante revocaciones de certificados a gran escala.

Este plan se pondrá a prueba, se revisará y se actualizará anualmente. También estará disponible para los auditores de Izenpe.

5.7.2 Recursos informáticos, software y/o datos están dañados

La estrategia para abordar este tipo de problemas está recogida en el Plan de contingencia de IZENPE.

5.7.3 Procedimientos ante la vulneración de la clave privada de la entidad

Una vez abordados los factores que dieron lugar a la revocación, la Autoridad de Certificación Raíz podrá:

- Generar un nuevo certificado para la CA emisora.
- Asegurar que todos los nuevos certificados y la CRL emitida por la CA estén firmados con la nueva clave.

La CA Raíz publicará el certificado revocado en la ARL (Lista de Revocación de Autoridades de Certificación).

Esta contingencia se incluirá en el Plan de continuidad de negocio de IZENPE, y determinará, entre otras, las siguientes acciones a tomar:

1. Cese de la prestación del servicio afectado.
2. Revocación de los certificados potencialmente comprometidos.
3. Notificación a suscriptores, usuarios y terceros. Igualmente, se enviará notificación a los TSP con los que existan acuerdos de confianza, fabricantes de navegadores y, en general, a cualquier entidad con la que IZENPE mantenga una relación contractual de prestación de

servicios.
4. Estudio de la necesidad de ejecutar el Plan de cese de actividad de TSP, de acuerdo con la CPS y la normativa vigente.

5.7.4 Capacidades de continuidad del negocio tras un desastre

La operación de la Autoridad de Certificación (CA) se suspenderá hasta que se haya completado el procedimiento de recuperación ante desastres y se restablezca de forma segura la operativa en la ubicación principal o en una instalación alternativa.

Se activará el Plan de contingencia y continuidad de negocio de IZENPE.

5.8 Cese de actividad de la CA o RA

IZENPE dispone de un Plan de terminación que especifica el procedimiento a seguir en caso de que ocurra dicha situación.

En caso de cese de actividad, IZENPE deberá notificar a los suscriptores con al menos dos meses de antelación a la finalización de sus operaciones, por cualquier medio que garantice una comunicación efectiva y la recepción de su intención de cesar la actividad como prestador de servicios de certificación. Dicha notificación indicará que todos los certificados en vigor serán revocados en un plazo de dos meses.

En caso de que una CA finalice por expiración o revocación, se seguirán atendiendo las consultas sobre el estado del certificado a través del servicio OCSP. Una vez finalizada la CA, las respuestas OCSP sobre los certificados emitidos por dicha CA serán firmadas por otra CA de IZENPE que permanezca vigente.

Las CRL de IZENPE no incluyen certificados expirados, conforme a lo indicado en el apartado 4.9.7 sobre la frecuencia de emisión de CRLs de este documento.

En caso de que IZENPE cese su actividad, se proporcionará la información sobre la revocación de certificados a través de una última CRL, con un valor de nextUpdate igual a «99991231235959Z», según lo especificado en el apartado 6.3.9 de la norma ETSI EN 319 411-1.

También se notificará a los TSP, fabricantes de navegadores y cualquier otra entidad con la que IZENPE tenga un acuerdo contractual para el uso de sus certificados.

Durante el periodo necesario, de acuerdo con lo especificado en esta CP/CPS, IZENPE mantendrá toda la información sobre registros, estado de revocación y archivos de registros. En caso de transferencia del servicio a otra entidad, se tomarán las medidas necesarias para que dicha transferencia se realice con todas las garantías requeridas.

El responsable de efectuar esta notificación será la Dirección General de IZENPE o la(s)

persona(s) designada(s) por el Consejo de Administración, quien(es) determinará(n) el mecanismo más adecuado para ello.

IZENPE notificará el cese de su actividad a la Autoridad Supervisora, incluyendo información sobre los certificados cuya validez expirará. Esta comunicación se realizará a través de la plataforma de notificaciones de la sede electrónica del Ministerio competente en materia de servicios de confianza, con un preaviso mínimo de 3 meses antes del cese de la actividad.

Cualquier autorización con terceros con los que IZENPE tenga un contrato de prestación de servicios (identificación, emisión, alojamiento, etc.) se considerará finalizada.

IZENPE, o la entidad a la que se haya transferido el servicio, deberá proporcionar información de validez sobre todos sus certificados cualificados, incluso cuando hayan expirado (hasta la fecha de expiración de la CA subordinada que emitió dicho certificado).

Izenpe ha iniciado un proceso formal de rescisión de sus servicios de emisión de certificados SSL/TLS bajo la certificación ROOT CA 2007. Se aplican las siguientes disposiciones:

Cesación de la emisión: La emisión de nuevos certificados se interrumpió el 15/04/2026.

Servicios de revocación continua: La CA mantendrá sus servicios de repositorio, emisión de CRL y respuesta OCSP de acuerdo con los plazos especificados en los Requisitos Básicos del Foro CA/B hasta que el último certificado emitido haya expirado o haya sido revocado.

Conservación de registros: Todos los registros de auditoría y la evidencia de validación de certificados se archivarán y conservarán durante un período mínimo de siete (7) años a partir de la fecha de expiración del último certificado emitido por esta CA.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e instalación de pares de claves

6.1.1 Generación de pares de claves

6.1.1.1 Generación de claves de la CA

Las claves criptográficas de las CA raíz y subordinadas deben generarse en un módulo de hardware criptográfico (HSM) que cumpla con el estándar FIPS 140-2 nivel 3 (o posterior) y con Common Criteria EAL 4+ para el perfil de protección correspondiente. Todas las claves criptográficas deben generarse de acuerdo con las recomendaciones mínimas de algoritmos y longitudes de claves establecidas en ETSI TS 119 312.

6.1.1.2 Generación de pares de claves de la RA

No aplica

6.1.1.3 Generación de pares de claves del suscriptor

Las claves privadas de los certificados de autenticación de sitio web son generadas y custodiadas por el suscriptor del certificado.

6.1.2 Entrega de la clave privada al suscriptor

La CA no genera ni entrega la clave privada al Suscriptor.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública, generada junto con la clave privada en el dispositivo de generación y custodia de claves, se entrega a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

6.1.4 Entrega de la clave pública de la CA a terceros de confianza

Las claves públicas de las CA de IZENPE se distribuyen por diversos medios, incluido el sitio web de IZENPE: www.izenpe.eus En el apartado 1.3.1 del CP/CPS se publican también las huellas digitales de las CA raíz y las CA emisoras.

6.1.5 Tamaños de clave

Los algoritmos utilizados son los siguientes:

JERARQUÍA RAÍZ 2007

Los algoritmos utilizados son los siguientes:

TIPOS DE NOMBRES	TIPO DE CLAVE
CA raíz	RSA 4096 bits
CA subordinada	RSA 4096 bits
TIPOS DE NOMBRES	**TIPO DE CLAVE**
Certificado de Autenticación de sitio web	RSA >=3072 bits

JERARQUÍA RAÍZ 2024

Los algoritmos utilizados son los siguientes:

TIPOS DE NOMBRES	TIPO DE CLAVE
CA raíz	ECC 384 bits
CA subordinada	ECC 384 bits
Certificado de Autenticación de sitio web	ECC 256384 bits

6.1.6 Generación de parámetros de clave pública y verificación de calidad

Las claves públicas de los certificados de autenticación de sitios web se codifican según RFC 5280 y PKCS#1.

6.1.7 Propósitos de uso de claves (según el campo «key usage» de X.509 v3)

Todos los certificados incluyen las extensiones Key Usage y Extended Key Usage, que indican los usos permitidos de las claves.

Las claves de la CA raíz se utilizan para firmar los certificados de las CA subordinadas, las ARL y el certificado de la TSA. Las claves de la CA subordinada o emisora se usan exclusivamente para firmar certificados de usuarios finales y CRLs.

Los usos de clave admitidos para los certificados finales se definen en el documento de perfiles de certificados disponible en www.izenpe.eus.

6.2 Protección de la clave privada y controles de ingeniería del módulo criptográfico

6.2.1 Estándares y controles del módulo criptográfico

Un módulo de seguridad hardware (HSM) es un dispositivo de seguridad que genera y protege claves criptográficas. Se requiere que dicho HSM cumpla, como mínimo, con los criterios FIPS 140-2 Nivel 3, o con Critero Común EAL 4+ para el perfil de protección correspondiente.

IZENPE dispone de protocolos para verificar que un HSM no ha sido manipulado durante su transporte y almacenamiento.

Los dispositivos criptográficos con certificados de firma electrónica cualificada, adecuados como dispositivos cualificados de creación de firma (DSCF), cumplen los requisitos del nivel de seguridad

CC EAL4+. No obstante, también se aceptan certificaciones que cumplan con un mínimo de ITSEC E3 o los criterios de seguridad FIPS 140-2 Nivel 2 o equivalente.

En caso de que estos dispositivos pierdan la certificación de dispositivo seguro y ello implique la pérdida de la condición de firma cualificada, IZENPE procederá a la revocación del certificado, siempre según lo determine el órgano de supervisión y/o la normativa vigente.

La norma de referencia europea para dispositivos de suscriptor utilizados es la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016.

En todo caso, IZENPE mantiene el control sobre la preparación, almacenamiento y distribución de los dispositivos de suscriptor cuando genera las claves.

6.2.2 Control multipersonal (n de m) para el uso de la clave privada

El uso de las claves privadas de la CA requiere la aprobación de al menos dos personas.

6.2.3 Custodia de clave privada

La clave privada de la CA raíz está almacenada en un dispositivo criptográfico hardware certificado según FIPS 140-2 Nivel 3 y/o CC EAL4+, lo que garantiza que la clave nunca sale del dispositivo criptográfico. La activación y uso de la clave privada requiere control multipersonal, tal como se indica en el punto anterior.

Las claves privadas de las CAs subordinadas están almacenadas en dispositivos criptográficos seguros certificados según FIPS 140-2 Nivel 3.

En los casos en que los suscriptores custodien su clave privada, será su responsabilidad mantenerla bajo su exclusivo control.

6.2.4 Copia de seguridad de la clave privada

Existe un procedimiento para la recuperación de las claves del módulo criptográfico de la CA (ya sea raíz o subordinada), que puede aplicarse en caso de contingencia.

También existe un procedimiento para la recuperación de las claves del módulo criptográfico del suscriptor bajo la custodia de IZENPE, que puede aplicarse en los casos definidos en las respectivas políticas.

En ambos casos, se aplican los mismos controles indicados en el punto 6.2.2.

6.2.5 Archivado de la clave privada

IZENPE puede realizar una copia de seguridad de las claves privadas, asegurando que la seguridad

de los datos duplicados sea del mismo nivel que la de los datos originales, y que la cantidad de datos duplicados no exceda el mínimo necesario para garantizar la continuidad del servicio. Los datos de creación de firma no se duplican con ningún otro propósito.

6.2.6 Transferencia de clave privada dentro o fuera de un módulo criptográfico

La clave privada de la CA raíz, de las CAs subordinadas, la VA y la TSA se generan en un HSM conforme al punto 6.2.1 y no es posible su exportación.

Como medida de contingencia, es posible la recuperación de las claves privadas según lo indicado en la sección 6.2.4.

6.2.7 Almacenamiento de clave privada en un módulo criptográfico

Existe un documento de ceremonia de claves de la CA raíz y de las CAs subordinadas que describe los procesos para generar la clave privada y su uso en hardware criptográfico.

En la generación de claves de CA, IZENPE sigue las recomendaciones de ETSI EN 319 411-1 y de las Guías de requisitos básicos del CA/B Forum.

Para la generación de claves del suscriptor en la tarjeta criptográfica, IZENPE sigue las recomendaciones de la Comisión Europea (eIDAS) y la norma EN 319 411-1.

En los casos en que las claves privadas se almacenen fuera de los módulos criptográficos, se protegerán de forma que se garantice el mismo nivel de seguridad que si estuvieran físicamente dentro del módulo.

6.2.8 Método de activación de la clave privada

Las claves privadas de las Autoridades de Certificación se generan y se custodian en un dispositivo criptográfico que cumple con los requisitos de seguridad FIPS 140-2 Nivel 3.

Los mecanismos de activación y uso de las claves privadas de los certificados de entidad final se describen en la Política específica de cada certificado.

6.2.9 Método de desactivación de la clave privada

Una persona con rol de administrador puede desactivar la clave de la CA deteniendo el sistema. Para volver a activarla, se deberá actuar conforme a lo descrito en la sección «6.2.8 Método de activación de la clave privada».

La desactivación de las claves privadas de certificados de entidad final se describe en la Política específica de cada certificado.

6.2.10 Método de destrucción de la clave privada

Existe un procedimiento para la destrucción de las claves de las CAs.
En caso de retirada del HSM que aloja las claves de la CA, se seguirá el procedimiento establecido.

Este procedimiento no se aplica a las claves de firma o autenticación del usuario emitidas en una tarjeta criptográfica o contenedor seguro, salvo en el caso de renovación de claves en el mismo dispositivo criptográfico.

6.2.11 Nivel de certificación del módulo criptográfico

Tal como se indica en la sección 6.2.1 de este documento.

6.3 Otros aspectos de la gestión de pares de claves

6.3.1 Archivado de la clave pública

Los Certificados de Autenticación de sitios web, y por tanto sus claves públicas asociadas, se conservan por IZENPE durante el período exigido por la legislación vigente, que actualmente es de 15 años.

6.3.2 Períodos operativos de los certificados y de uso del par de claves

Los períodos de validez de los certificados y de sus claves asociadas son:

- Certificado de la CA raíz y su par de claves: ver sección «1.3.1 Autoridad de Certificación» de esta CP.
- Certificado de la CA subordinada que emite los Certificados de Autenticación de sitio web y su par de claves: ver sección «1.3.1 Autoridad de Certificación» de esta CP.
- Certificados de Autenticación de sitio web y su par de claves: el período máximo de validez es de 398 días.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Los datos de activación, tanto de las claves de la CA raíz como de las CAs subordinadas emitidas por certificados de entidad final, se generan durante la ceremonia de creación de claves de dichas Autoridades de Certificación.

En cuanto a los datos de activación de las claves de Certificados de entidad final, se describen, en su caso, en la Política específica de cada certificado.

6.4.2 Otros aspectos de los datos de activación

Los datos de activación de la clave de la CA raíz se distribuyen en varias tarjetas físicas diferentes, y se requiere la participación de al menos dos personas para realizar cualquier operación. Las tarjetas que contienen las claves se custodian en cajas fuertes diferentes.

Los datos de activación de la clave de la CA subordinada también se distribuyen entre varias tarjetas físicas diferentes, con el mismo requisito de intervención de dos personas. Las tarjetas que contienen las claves se custodian en cajas fuertes diferentes.

Las claves de la TSA y VA se generan y gestionan en el mismo HSM que las claves de la CA subordinada, aplicando las mismas reglas.

Los suscriptores están obligados a mantener en secreto sus datos de activación.

6.4.3 Otros aspectos de los datos de activación

Consultar la Política específica correspondiente a cada tipo de certificado.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

Se aplican una serie de controles en los diferentes componentes que conforman el sistema de servicios de certificación de IZENPE (CA, bases de datos de IZENPE, servicios de Internet de IZENPE, operación de la CA y gestión de red):

- Controles operativos
  - Todos los procedimientos de operación están debidamente documentados en los correspondientes manuales operativos.
  - Existe un Plan de contingencia.
  - Se han implementado herramientas para la protección contra virus y códigos malignos
  - El equipo se mantiene de forma continua para garantizar la disponibilidad e integridad sin interrupciones.
  - Existe un procedimiento para el almacenamiento, borrado y eliminación segura de soportes de información, medios extraíbles y equipos obsoletos.
- Intercambio de datos. Los siguientes intercambios de datos están cifrados para garantizar la confidencialidad:
  - Transmisión de datos de registro entre las RAs y la base de datos de registro.
  - Transmisión de datos de pre-registro.
  - Comunicación entre las RAs y las CAs.

- El servicio de publicación de revocaciones dispone de las funciones necesarias para estar disponible 24 horas al día, 7 días a la semana.
- Control de acceso
    - Se utilizan identificadores únicos de usuario, de manera que los usuarios estén asociados a sus acciones y puedan ser responsables de las mismas.
    - Los derechos se asignan según el principio de proporcionar al usuario el mínimo privilegio necesario para realizar su labor.
    - Los derechos de acceso se cancelan de inmediato cuando los usuarios cambian de puesto o abandonan la organización.
    - El nivel de acceso asignado a los usuarios se revisa cada tres meses.
    - Los privilegios del sistema se asignan caso por caso, y se eliminan una vez que ya no exista motivo para su asignación.
    - Existen directrices de calidad para las contraseñas.
    - Todas las cuentas de operador con capacidad de emisión de certificados cuentan con control de acceso basado en doble factor.

IZENPE dispone de una política de seguridad y procedimientos específicos que garantizan la seguridad en los distintos niveles del sistema.

6.5.2 Clasificación de seguridad informática

Los productos utilizados para la prestación de los servicios de certificación cuentan con certificación internacional conforme al estándar ISO/IEC 15408.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo del sistema

La implementación del software en los sistemas de producción está controlada.

Para prevenir posibles problemas en estos sistemas, se aplican los siguientes controles:

- La política de IZENPE incluye normas para el desarrollo seguro de aplicaciones y sistemas.
- Existe un procedimiento formal para el seguimiento de los cambios. Los cambios se limitan a los estrictamente necesarios y están sujetos a un control riguroso.
- Cuando se realizan cambios en los sistemas operativos, se revisan las aplicaciones de negocio consideradas críticas según el Plan de continuidad de negocio.
- Se aplican principios de ingeniería de sistemas seguros.
- El entorno de desarrollo está debidamente protegido.
- El desarrollo subcontratado está supervisado y controlado por IZENPE.
- Se realizan pruebas de seguridad operativa durante el desarrollo.
- Se establecen programas de pruebas de aceptación para nuevos sistemas de información, actualizaciones y versiones.

- Los datos de prueba son seleccionados, protegidos y controlados.

6.6.2 Controles de gestión de la seguridad

IZENPE realiza un seguimiento constante para garantizar que los sistemas y comunicaciones funcionen conforme a la Política de seguridad de IZENPE. Todos los procesos se registran y auditan conforme a la legislación y normativa vigente.

6.6.3 Controles de seguridad del ciclo de vida

Para realizar pruebas, se requiere un volumen considerable de datos lo más similar posible a los datos de producción. Se evita el uso de bases de datos de producción que contengan información personal.

6.7 Controles de seguridad de red

La seguridad de la red se basa en el concepto de zonificación multinivel, con múltiples firewalls redundantes. La información confidencial transferida por redes no seguras se cifra utilizando protocolos SSL/TLS. Existen sistemas IPS para tráfico interno y externo.

6.8 Sellado de tiempo

IZENPE obtiene la hora de sus sistemas a través de una conexión con el Real observatorio de la Armada, siguiendo el protocolo NTP. . Una descripción del protocolo NTP se encuentra en la norma IETF RFC 5905.

A partir de este servicio interno, IZENPE ofrece un servicio de sellado de tiempo (TSA) que permite crear sellos de tiempo sobre documentos arbitrarios, de conformidad con la IETF RFC 3161 y la ETSI EN 319 421. Más información en la Declaración de prácticas de sellado de tiempo de IZENPE.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 Perfil de certificado

Los Certificados de Autenticación de sitio web cumplen con el estándar europeo ETSI EN 319 412-4, titulado «Perfil de certificado para certificados de sitio web».

Incluyen los siguientes identificadores de políticas del CA/B Forum:

CERTIFICADO	OID CA/B FORUM
DV SSL	2.23.140.1.2.1
OV SSL	2.23.140.1.2.2
EV SSL	2.23.140.1.1
SSL Cualificado	2.23.140.1.1

7.1.1 Número(s) de versión

Los certificados DEBEN ser del tipo X.509 versión 3.

7.1.2 Extensiones del certificado

En el siguiente sitio web se publica el documento que describe en detalle el perfil de los Certificados de Autenticación de sitio web, incluyendo todas sus extensiones: https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_def/adjuntos/Perfiles_de_Certificados.pdf

7.1.2.1 Certificado de la Autoridad de Certificación raíz

- basicConstraints
  - Esta extensión DEBE estar presente como una extensión crítica. El campo cA DEBE establecerse en true. El campo pathLenConstraint NO DEBERÍA estar presente.
- keyUsage
  - Esta extensión DEBE estar presente y DEBE marcarse como crítica. Los bits correspondientes a keyCertSign y cRLSign DEBEN estar activados. Si la clave privada de la CA Raíz se utiliza para firmar respuestas OCSP, entonces el bit digitalSignature DEBE estar activado.
- certificatePolicies
  - Esta extensión NO DEBERÍA estar presente.
- extKeyUsage
  - Esta extensión NO DEBE estar presente.

7.1.2.1.1 Validez del certificado CA de la raíz

CAMPO	MÍNIMO	MÁXIMO
notBefore	Un día antes del momento de la firma	El momento de la firma
notAfter	2922 días (aproximadamente 8 años)	9132 días (aproximadamente 25 años)

7.1.2.2 Certificado de la Autoridad de Certificación intermedia

1. ***basicConstraints***
   Esta extensión DEBE estar presente y DEBE marcarse como crítica. El campo cA DEBE establecerse en true. El campo pathLenConstraint PUEDE estar presente.
2. ***authorityKeyIdentifier***
   Esta extensión DEBE estar presente y NO DEBE marcarse como crítica. DEBE contener un campo keyIdentifier y NO DEBE contener authorityCertIssuer ni authorityCertSerialNumber.
3. ***subjectKeyIdentifier***
   Esta extensión DEBE estar presente y NO DEBE marcarse como crítica. Identifica de forma única una clave de CA en particular. Contiene el ID de la clave del Certificado de la CA
4. ***keyUsage***
   Esta extensión DEBE estar presente y DEBE marcarse como crítica. Los bits correspondientes a keyCertSign y cRLSign DEBEN estar activados. Si la clave privada de la CA subordinada se utiliza para firmar respuestas OCSP, el bit digitalSignature DEBE estar activado.
5. ***certificatePolicies***
   Esta extensión DEBE estar presente y NO DEBE marcarse como crítica. DEBE contener al menos un PolicyInformation.
6. ***extKeyUsage***
   Esta extensión DEBE estar presente y NO DEBE marcarse como crítica.
   Para Certificados de CA subordinada utilizados para emitir certificados de servidor TLS, el valor id-kp-serverAuth DEBE estar presente. I valor id-kp-clientAuth PUEDE estar presente. Los siguientes valores NO DEBEN estar presentes: id-kp-emailProtection [RFC5280], id-kp-codeSigning [RFC5280], id-kp- timeStamping [RFC5280], id-kp-OCSPSigning [RFC5280] and anyExtendedKeyUsage [RFC5280]. No se DEBERÍAN incluir otros valores.
7. ***authorityInformationAccess***
   Esta extensión DEBE estar presente y NO DEBE marcarse como crítica. DEBE contener un campo keyIdentifier y NO DEBE contener authorityCertIssuer ni authorityCertSerialNumber.
8. ***cRLDistributionPoints***
   Esta extensión DEBE estar presente y NO DEBE marcarse como crítica. DEBE contener la URL HTTP del servicio CRL de la CA.

7.1.3 Identificadores de algoritmos

IZENPE DEBERÁ utilizar uno de los siguientes algoritmos de firma y codificación:

Raíz CN	Identificador del algoritmo	Codificación
IZENPE.com (2007)	RSASSA-PKCS1-v1_5 con SHA-256	300D06092A864886F70D01010B0500

RAÍZ CA SSL IZENPE 2024	ecdsaWithSHA384	300A06082A8648CE3D040303

7.1.3.1 SubjectPublicKeyInfo

Los siguientes requisitos se aplican al campo ***subjectPublicKeyInfo*** dentro de un Certificado o Precertificado. No se permiten otras codificaciones.

7.1.3.1.1 RSA

IZENPE DEBE indicar una clave RSA utilizando el identificador de algoritmo rsaEncryption (OID: 1.2.840.113549.1.1.1). El campo de parámetros DEBE estar presente y DEBE ser un NULL explícito. IZENPE NO DEBE usar otro algoritmo como id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) para indicar una clave RSA.

El campo ***AlgorithmIdentifier*** de claves RSA codificado DEBE ser idéntico byte por byte al siguiente valor hexadecimal: ***300d06092a864886f70d0101010500***

7.1.3.1.2 ECDSA

La CA DEBE indicar una clave ECDSA utilizando el identificador de algoritmo id-ecPublicKey (OID: 1.2.840.10045.2.1). Los parámetros DEBEN usar el formato ***namedCurve***.

- Para las claves P-256 el ***namedCurve*** DEBE ser secp256r1 (OID: 1.2.840.10045.3.1.7).
- Para las claves P-384 el ***namedCurve*** DEBE ser secp384r1 (OID: 1.3.132.0.34).
- Para las claves P-521 el ***namedCurve*** DEBE ser secp521r1 (OID: 1.3.132.0.35).

El campo ***AlgorithmIdentifier*** de claves ECDSA codificado DEBE ser idéntico byte por byte al siguiente valor hexadecimal:

- Para las claves P-256, 301306072a8648ce3d020106082a8648ce3d030107
- Para las claves P-384, 301006072a8648ce3d020106052b81040022
- Para las claves P-521, 301006072a8648ce3d020106052b81040023

7.1.3.2 Identificador de algoritmo de firma

Todos los objetos firmados con la clave privada de una CA DEBEN cumplir con estos requisitos en cuanto al uso del campo ***AlgorithmIdentifier*** o del tipo ***AlgorithmIdentifier-derived*** en contextos de firmas.

7.1.3.2.1 RSA

IZENPE DEBERÁ utilizar uno de los siguientes algoritmos de firma y codificación: El campo AlgorithmIdentifier codificado DEBE ser idéntico byte por byte al valor hexadecimal especificado:

- RSASSA-PKCS1-v1_5 con SHA-256:

Codificación: 300d06092a864886f70d01010b0500
- RSASSA-PKCS1-v1_5 con SHA-384:
  Codificación: 300d06092a864886f70d01010c0500
- RSASSA-PKCS1-v1_5 con SHA-512:
  Codificación: 300d06092a864886f70d01010d0500
- RSASSA-PSS con SHA-256, MGF-1 con SHA-256 y una longitud de salt de 32 bytes:
  Codificación: 304106092a864886f70d01010a3034a00f300d060960864801650304020105
  00a11c301a06092a864886f70d010108300d060960864801650304020105
  00a203020120
- RSASSA-PSS con SHA-384, MGF-1 con SHA-384 y una longitud de salt de 48 bytes:
  Codificación: 304106092a864886f70d01010a3034a00f300d060960864801650304020205
  00a11c301a06092a864886f70d010108300d060960864801650304020205 00a203020130
- RSASSA-PSS con SHA-512, MGF-1 con SHA-512 y una longitud de salt de 64 bytes:
  Codificación: 304106092a864886f70d01010a3034a00f300d060960864801650304020305
  00a11c301a06092a864886f70d010108300d060960864801650304020305 00a203020140

7.1.3.2.2 ECDSA

IZENPE DEBE usar el algoritmo de firma correspondiente a la clave utilizada:

Si la clave para la firma es P-256, la firma DEBE usar el ECDSA con SHA-256. El campo AlgorithmIdentifier codificado DEBE ser idéntico byte por byte al siguiente valor hexadecimal: ***300a06082a8648ce3d040302***.

Si la clave para la firma es P-384, la firma DEBE usar el ECDSA con SHA-384. El campo AlgorithmIdentifier codificado DEBE ser idéntico byte por byte al siguiente valor hexadecimal: ***300a06082a8648ce3d040303***.

Si la clave para la firma es P-521, la firma DEBE usar el ECDSA con SHA-512. El campo AlgorithmIdentifier codificado DEBE ser idéntico byte por byte al siguiente valor hexadecimal: ***300a06082a8648ce3d040304***.

7.1.4 Formas de nombre

La codificación de los Certificados de Autenticación de sitios web sigue la recomendación del RFC 5280 «Perfil de certificado X.509 de la Infraestructura de clave pública de Internet y la Lista de revocación decertificados (CRL)». Todos los campos definidos en el perfil de estos Certificados, salvo aquellos que se indiquen específicamente de otro modo, utilizan codificación UTF8String.

7.1.4.1 Codificación del nombre

Para cada Ruta de certificación válida (según la Sección 6 del RFC 5280):
- En cada certificado de la Ruta de certificación, el contenido codificado del campo Issuer Distinguished Name debe ser idéntico byte por byte al contenido codificado del campo

Subject Distinguished Name del certificado de la CA emisora.

- En cada certificado de CA dentro de la ruta de certificación, el contenido codificado del campo Subject Distinguished Name debe ser idéntico byte por byte entre todos los certificados cuyos nombres distinguidos (DNs) puedan considerarse iguales según la Sección 7.1 del RFC 5280, incluyendo certificados expirados o revocados.

7.1.4.2 Codificación de atributos del sujeto

Sin estipulación.

7.1.4.3 Atributo nombre común del certificado del suscriptor

Sin estipulación.

7.1.4.4 Otros atributos del sujeto

Sin estipulación.

7.1.5 Restricciones de nombre

Las CAs subordinadas que emiten certificados bajo esta CP/CPS no están técnicamente restringidas.

7.1.6 Identificador del objeto de política del certificado

El identificador del objeto (OID) de la política de los Certificados de Autenticación es el definido en la sección «1.2 Nombre e identificación del documento» del presente documento.

7.1.7 Uso de la extensión Restricciones de política

No se utilizan restricciones de política.

7.1.8 Sintaxis y semántica de calificadores de política

La extensión Certificate Policies contiene los siguientes calificadores de política:

- CPS Pointer: Contiene un enlace al Certification Practice Statement (CPS) de IZENPE: http://www.izenpe.com/cps.

- Identificador de poítica: Indica el OID de la política asociada al certificado.

7.1.9 Semántica de procesamiento para la extensión crítica Política de certificación:

La extensión CP permite identificar la política que IZENPE asocia al certificado, así como el lugar

donde se puede consultar dicha política.

7.2 Perfil de la CRL

Los certificados emitidos por IZENPE se ajustan a los siguientes estándares:

- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile (abril de 2002)
- RFC 4325 – Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (diciembre de 2005)
- RFC 4630 – Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (agosto de 2006)

7.2.1 Número(s) de versión

Versión 2 (el campo de versión debe contener el entero «1»).

7.2.2 Extensiones de CRL y entradas de CRL:

Las extensiones utilizadas con las siguientes:

Campo	Obligatorio	Crítico
X.509v2 Extensions	Sí	NO
1. Authority key Identifier	Sí	NO
2. CRL Number	Sí	NO
3. Issuing Distribution Point	Sí	Sí
4. Reason Code	Sí	NO
5. Invalidity Date	Sí	NO

El motivo de revocación «no especificado» (0) NO debe utilizarse para certificados de CA revocados que se incluyan en listas de revocación de autoridades (ARL, por sus siglas en inglés). A cada certificado de CA revocado que figure en una ARL se le DEBE asignar un motivo de revocación específico y adecuado.

7.3 Perfil de la OCSP

Las respuestas OCSP de IZENPE cumplen con la RFC 6960 (Protocolo de Estado de Certificados en Línea de la Infraestructura de Clave Pública de Internet X.509 - OCSP) y están firmadas por el OCSP Responder, cuyo certificado ha sido emitido por la misma CA que firmó el certificado consultado.

7.3.1 Número(s) de versión

Versión 2,0

7.3.2 Extensiones OCSP

Campo	Obligatorio	Crítico
1. Issuer Alternative Name	NO	NO
2. Authority/Subject key Identifier	NO	NO
3. CRL Distribution Point	NO	NO
4. Key usage	Sí	Sí
5. Enhanced Key usage	Sí	Sí

8. AUDITORÍA DE CONFORMIDAD Y OTRAS EVALUACIONES

El sistema de emisión de certificados de autenticación de sitios web se somete a una auditoría anual de conformidad con:

- Las normas europeas ETSI EN 319 401 «Requisitos generales de política para los prestadores de servicios de confianza» y ETSI EN 319 411-1 «Requisitos de política y seguridad para los prestadores de servicios de confianza que emiten certificados».
- ETSI EN 319 411-2 «Requisitos para prestadores de servicios de confianza que emiten certificados cualificados de la UE».

Además, el sistema de emisión de certificados está sujeto a las siguientes auditorías:

- Auditoría del Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la norma UNE-ISO/IEC 27001 «Requisitos para los sistemas de gestión de la seguridad de la información».
- Auditoría conforme al Esquema Nacional de Seguridad (ENS), según el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.
- Auditoría conforme al 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 a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD/LOPD-GDD).

Asimismo, se realizan análisis de riesgos de acuerdo con lo establecido en el Sistema de Gestión de la Seguridad de la Información.

8.1 Frecuencia o circunstancias de la evaluación

En el caso de los certificados considerados como cualificados, la auditoría garantiza adicionalmente el cumplimiento de los requisitos establecidos en las normas europeas: ETSI EN 319 411-2: «Requisitos para prestadores de servicios de confianza que emiten certificados cualificados de la UE»y ETSI EN 319 412-4: «Perfil de certificados para certificados de sitio web».

La frecuencia del resto de auditorías adicionales se ajustará a lo establecido por las normativas vigentes correspondientes.

8.2 Identidad/cualificaciones del auditor

Los auditores están cualificados y han demostrado su competencia en la auditoría de sistemas seguros de producción, especialmente aquellos relacionados con sistemas de certificación digital. El auditor debe estar acreditado conforme a la norma ETSI EN 319 403.

8.3 Relación del auditor con la entidad evaluada

Se emplean tanto auditores internos como externos, pero en todos los casos estos son independientes del servicio de producción que está siendo auditado.

8.4 Temas cubiertos por la evaluación

La auditoría de cumplimiento cubrirá los siguientes temas:

- Procesos de la PKI.
- Sistemas de información.
- Protección del centro de procesamiento de datos.
- Documentación.

Los detalles sobre cómo se audita cada uno de estos temas se especifican en el Plan de auditoría de IZENPE.

8.5 Acciones tomadas como resultado de deficiencias

Los incidentes de seguridad son gestionados por el Comité de seguridad de IZENPE.

IZENPE abrirá una investigación en un plazo máximo de 24 horas desde la recepción del incidente, y decidirá las acciones a tomar considerando los criterios definidos en la sección 4.9.5 de los BRs.

Además, IZENPE informa de los casos que considera como incidentes (como fraudes, phishing, etc.) en el sitio web del Anti-Phishing Working Group (www.apwg.org) y verifica antes de la emisión que el solicitante o sus representantes no figuran en la base de datos interna de incidentes de seguridad de IZENPE.

En cualquier caso, IZENPE se reserva el derecho de emitir certificados en situaciones sospechosas.

8.6 Comunicación de resultados

Los informes de resultados de las auditorías se entregarán al Comité de seguridad para su análisis.

8.7 Autoevaluaciones

IZENPE supervisará el cumplimiento de esta CP/CPS y controlará la calidad de su servicio realizando autoevaluaciones al menos trimestralmente, sobre una muestra aleatoria compuesta por el mayor valor entre un certificado o al menos el tres por ciento (3%) de los certificados de confianza pública emitidos para SSL/TLS, incluidos los certificados EV.

IZENPE DEBERÁ completar y enviar una autoevaluación anual al CCADB que cubra, como mínimo, los requisitos de las siguientes políticas:

- Política del CCADB.
- Política del programa de raíz de Chrome.
- Política del almacén de raíces de Mozilla.
- Requisitos de seguridad de redes y sistemas de certificados.
- Requisitos básicos para certificados TLS de confianza pública.
- Guías de validación extendida para certificados TLS de confianza pública.

9. OTROS ASUNTOS COMERCIALES Y LEGALES

9.1 Tarifas

IZENPE recibirá la remuneración económica correspondiente de acuerdo con las tarifas aprobadas por su Consejo de Administración.

9.1.1 Tarifas por emisión o renovación de certificados

La determinación de las tarifas aplicables a la emisión o renovación de certificados seguirá lo dispuesto en la sección «9.1 Tarifas» de este documento.

9.1.2 Tarifas por acceso a certificados

No estipulado.

9.1.3 Tarifas por acceso a información de revocación o estado

IZENPE ofrece de forma gratuita servicios de información sobre el estado de los certificados mediante los protocolos CRL y OCSP.

9.1.4 Tarifas por otros servicios

Las tarifas aplicables a otros servicios son aprobadas anualmente por el Consejo de Administración de IZENPE.

9.1.5 Política de reembolsos

IZENPE no dispone de una política de reembolsos.

9.2 Responsabilidad financiera

IZENPE, las Autoridades de Registro (RA) y las Entidades usuarias dispondrán de los recursos financieros suficientes para mantener sus operaciones y desempeñar sus funciones.

9.2.1 Cobertura de seguros

IZENPE mantiene una póliza de seguro de responsabilidad civil para cubrir errores y omisiones derivados de la generación de certificados, que exclusivamente cubre las actividades realizadas por IZENPE. La relación entre IZENPE y las Autoridades de Registro, cuando intervienen, y los suscriptores y usuarios de certificados no es obligatoria ni fiduciaria. Los suscriptores y usuarios de certificados no pueden exigir a IZENPE ni a las Autoridades de Registro la prestación de ningún servicio, ya sea por contrato o por cualquier otro medio.

9.2.2 Otros activos

No estipulado.

9.2.3 Cobertura de seguros o garantías para entidades finales

No estipulado.

9.3 Confidencialidad de la información empresarial

9.3.1 Alcance de la información confidencial

Para poder prestar sus servicios, IZENPE y las Autoridades de Registro necesitan recopilar y almacenar ciertos tipos de datos, incluyendo información personal. Esta información es obtenida directamente de los interesados con su consentimiento expreso, o bien sin dicho consentimiento en los casos previstos por la legislación sobre protección de datos personales.

IZENPE y las Autoridades de Registro recopilan únicamente los datos necesarios para la emisión y gestión de certificados y para la prestación de otros servicios de firma electrónica; los datos no podrán utilizarse para otros fines sin el consentimiento expreso y por escrito del firmante.

La política de privacidad de IZENPE ha sido elaborada conforme a la legislación vigente en materia de protección de datos personales.
IZENPE y las Autoridades de Registro no divulgarán ni compartirán información personal, salvo en los supuestos descritos en las secciones de esta Declaración de Prácticas de Certificación (CPS) y en la sección relativa a la terminación de los servicios prestados por IZENPE y las Autoridades de Registro.

IZENPE y las Autoridades de Registro mantendrán de forma confidencial la siguiente información:

- Solicitudes de certificados, ya sean aprobadas o rechazadas, y toda otra información personal obtenida durante la emisión y mantenimiento de los certificados, salvo aquella especificada en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por IZENPE.
- Registros de transacciones, incluyendo los registros completos y las trazas de auditoría de las transacciones.
- Registros de auditorías internas y externas creados y/o conservados por IZENPE o por las Autoridades de Registro y sus respectivos auditores.
- Planes de continuidad de negocio y de recuperación ante desastres.
- Políticas y planes de seguridad.
- Registros de operaciones y otros planes operativos, tales como planes de archivo, monitorización y otros planes análogos.

9.3.2 Información no incluida dentro del ámbito de la información confidencial

La siguiente información no se considera confidencial y, por tanto, es reconocida por las partes interesadas en el instrumento legal firmado con IZENPE:

- Los certificados que hayan sido emitidos o estén en proceso de emisión.
- La información que vincula a la persona física suscriptora con un certificado emitido por IZENPE.
- El nombre y apellidos del titular del certificado, en el caso de certificados en los que el suscriptor y firmante es una persona física, o los nombres de los firmantes, en el caso de certificados en los que el suscriptor es una persona jurídica o un organismo administrativo,

así como cualquier otra circunstancia o dato personal del titular, si resulta significativa en función del objeto del certificado.
- En caso de estar incluida, la dirección de correo electrónico del titular del certificado, si el suscriptor y firmante es una persona física, o la dirección de correo electrónico del propietario de la clave, si el suscriptor es una persona jurídica o una entidad pública, o bien la dirección de correo electrónico asignada por el suscriptor para certificados de dispositivo.
- Los usos y limitaciones económicas indicados en los certificados.
- El período de validez, la fecha de emisión y la fecha de expiración del certificado.
- El número de serie del certificado.
- Las diferentes situaciones o estados del certificado y la fecha de inicio de cada uno, específicamente: pendiente de generación y/o emisión, válido, revocado, suspendido o caducado, así como el motivo del cambio de estado.
- Las Listas de Revocación de Certificados (CRLs) y otra información relacionada con el estado de revocación.
- La información contenida en el Repositorio de IZENPE.
- Cualquier otra información que no esté indicada en el apartado sobre información confidencial de esta Declaración de Prácticas de Certificación (CPS).

9.3.3 Responsabilidad de proteger la información confidencial

IZENPE o las Autoridades de Registro tendrán derecho a divulgar información confidencial en la medida en que así lo exija la ley.

En concreto, se podrán revelar los registros que certifiquen la veracidad de la información contenida en el certificado, si son requeridos como prueba de la certificación en procedimientos judiciales, incluso sin el consentimiento del titular del certificado.

Los certificados se publicarán conforme a lo dispuesto en los Reglamentos eIDAS1 y eIDAS2, así como en la Ley 6/2020, de 11 de noviembre, por la que se regulan determinados aspectos de los servicios electrónicos de confianza.

9.4 Privacidad de la información personal

IZENPE publica su Registro de Actividades de Tratamiento y otra información relativa a datos personales, para que los interesados puedan consultarla a través del siguiente sitio web: www.izenpe.eus/datos.

9.4.1 Plan de privacidad

El tratamiento de datos personales por parte de IZENPE se ajusta a lo establecido 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 a los requisitos aplicables derivados de la normativa nacional específica en esta materia.

9.4.2 Información no considerada privada

IZENPE considera como información personal privada toda aquella relativa a personas físicas usuarias de los Servicios de confianza que no deba ser incorporada a los certificados, así como la utilizada por los mecanismos del Servicio de consulta de información y estado de validez de los certificados.

En cualquier caso, se considera información privada toda aquella recopilada durante los procesos de solicitud, renovación y revocación de certificados electrónicos (excepto la indicada en la sección siguiente), las claves privadas en posesión del prestador de servicios de confianza, así como cualquier otra información claramente identificada como privada.

IZENPE aplica las garantías adecuadas para proteger esta información privada.

9.4.3 Información no considerada privada

No se considera información privada aquella incorporada en los certificados electrónicos, así como la información relativa al estado de validez de los certificados, la fecha de inicio de dicho estado (activo, revocado, expirado, etc.) y la causa del cambio de estado. Por tanto, los certificados electrónicos, las listas de certificados revocados y todo su contenido no se consideran información privada.

9.4.4 Responsabilidad sobre la protección de la información privada

IZENPE adopta las medidas de seguridad exigidas por el RGPD respecto al acceso y tratamiento de los datos personales de los solicitantes y suscriptores de certificados.

Las medidas técnicas y organizativas se establecerán teniendo en cuenta el estado de la técnica, los costes de aplicación, así como la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos para los derechos y libertades de las personas interesadas.

9.4.5 Notificación y consentimiento para el uso de información privada

La obtención de información privada de personas físicas durante los procesos del ciclo de vida de los Certificados (solicitud, acreditación de identidad, renovación, revocación, etc.) estará siempre sujeta al consentimiento inequívoco de dichas personas, entendiéndose como tal una declaración del interesado o una clara acción afirmativa.

9.4.6 Divulgación por requerimiento judicial o administrativo

IZENPE no compartirá datos personales, salvo en caso de requerimiento por parte de autoridades administrativas o judiciales.

9.4.7 Otras circunstancias de divulgación de información

No estipulado.

9.5 Derechos de propiedad intelectual

Derechos sobre los certificados

IZENPE es la única entidad que ostenta los derechos de propiedad intelectual sobre los certificados que emite.

Se excluyen los derechos de propiedad intelectual e industrial derivados del software usado en el sistema de certificación digital cuando sean propiedad de terceros.

Esta misma disposición se aplica al sistema de datos de revocación de certificados.

Derechos sobre la práctica de certificación

IZENPE ostenta todos los derechos de propiedad sobre esta Declaración de Prácticas de Certificación.

Derechos de propriedad sobre los nombres

El suscriptor, y en su caso el titular de la clave, conservará todos los derechos (si los hubiera) sobre cualquier marca comercial, nombre de producto o nombre comercial contenido en el certificado.

El suscriptor, y en su caso el titular de la clave, es el propietario del nombre distinguido del certificado, compuesto por la información especificada en la sección 3 de esta Declaración de Prácticas de Certificación.

Derechos de propiedad sobre claves y material criptográfico

Los pares de claves son propiedad de los suscriptores de los certificados.

9.6 Declaraciones y garantías

9.6.1 Declaraciones y garantías de la CA

Las obligaciones y responsabilidades de IZENPE, en calidad de Proveedor de servicios de

confianza, respecto del suscriptor del certificado y, en su caso, frente a los usuarios y terceros que confíen en el certificado, se determinarán en el documento de condiciones de uso o en el contrato de emisión del certificado, y, subsidiariamente, en esta Declaración de Prácticas y Políticas de Certificación.

IZENPE declara que cumple con los requisitos técnicos establecidos en la norma ETSI EN 319 411 para la emisión de certificados, y se compromete a continuar cumpliendo con dicha norma o con las que la sustituyan.
IZENPE emite certificados de autenticación de sitios web conforme a los requisitos de «Requisitos básicos para la emisión y gestión de certificados confiables», establecidos por el CA/Browser Forum, disponibles en: https://cabforum.org/. Asimismo, IZENPE adaptará sus prácticas de emisión de certificados a la versión vigente de dichos requisitos.

En caso de existir incoherencias entre dichos requisitos y esta Política, prevalecerán dichos requisitos.

Además, IZENPE se compromete a cumplir, en lo que respecta a la emisión de certificados cualificados, con los requisitos establecidos por la entidad CA/Browser Forum para este tipo de certificados (Directrices para certificados EV SSL), las cuales pueden consultarse en la siguiente dirección: https://cabforum.org/extended-validation/. Y del mismo modo, en caso de discrepancia con esta política, prevalecerán los requisitos del CA/Browser Forum.

Sin perjuicio de lo dispuesto en la normativa aplicable a este tipo de certificados, así como de las obligaciones descritas en la sección correspondiente de esta CPS, el Prestador de servicios de confianza se compromete, con carácter previo a la emisión del certificado, a:

- Verificar la identidad y circunstancias personales del solicitante del certificado y del suscriptor y/o su Representante, y recabar la declaración de que el solicitante está autorizado por el suscriptor para realizar dicha solicitud.
- Comprobar, en el proceso de registro, los datos relativos a la personalidad jurídica del suscriptor y la capacidad del Representante. Realizar todas estas comprobaciones de conformidad con lo dispuesto en este documento y en los protocolos y procedimientos de registro de IZENPE.
- En los procesos de verificación mencionados, IZENPE podrá llevar a cabo verificaciones a través de terceros con facultades notariales o mediante Registros competentes.
- Verificar que toda la información contenida en la solicitud del certificado se corresponde con la facilitada por el solicitante.
- Comprobar que el solicitante está en posesión de la clave privada asociada a la clave pública que se incluirá en el certificado a emitir.
- Garantizar que los procedimientos seguidos aseguran que las claves privadas correspondientes a los certificados de autenticación de sitio web se generan sin que IZENPE conserve o almacene copia alguna.
- Comunicar la información al suscriptor, representante y solicitante de manera que se garantice su confidencialidad.

- Poner a disposición del solicitante, suscriptor, Representante y demás partes interesadas la Declaración de Prácticas de Certificación de IZENPE, así como cualquier otra información relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los certificados regulados por esta Política de Certificación, de conformidad con la normativa aplicable.

9.6.2 Declaraciones y garantías de la RA

Las actividades relacionadas con la RA serán llevadas a cabo exclusivamente por IZENPE para todos los certificados de autenticación de sitio web.

La RA tiene las siguientes obligaciones:

- En general, seguir los procedimientos establecidos por IZENPE en la Política y Declaración de Prácticas de Certificación aplicables al desempeño de sus funciones de gestión, emisión y revocación de Certificados, y no alterar este marco.
- En particular, verificar la identidad, así como las circunstancias personales relevantes para el propósito determinado, de los solicitantes del certificado, suscriptores y sus Representantes, por cualquier medio permitido por la ley y conforme a las disposiciones generales de esta Política.
- Comprobar que la titularidad del nombre de dominio corresponde a la identidad del Suscriptor o, en su caso, obtener la autorización del Suscriptor, que se asociará al certificado de autenticación de sitio web, mediante los medios de los que disponga y que permitan acreditar dicha titularidad conforme al estado del arte.
-
- Manifestar expresamente la capacidad de decisión del suscriptor respecto a la titularidad del dominio objeto del certificado de autenticación.
- Conservar toda la información y documentación relativa a los certificados cuya solicitud, renovación o revocación gestione, durante un período de 15 años.
- Recibir y gestionar solicitudes a través de la aplicación de gestión de solicitudes publicada en www.izenpe.eus.
- Verificar con diligencia las causas de revocación que puedan afectar a la validez de los certificados.

9.6.3 Declaraciones y garantías del suscriptor

En lo que respecta a los certificados de autenticación de sitios web, los Suscriptores deben tener control sobre el nombre de dominio del sitio web incluido en dichos Certificados y mantener las claves privadas asociadas bajo su uso exclusivo. El solicitante y el Suscriptor de los Certificados

emitidos bajo esta Política de Certificación están obligados a:

- No utilizar el certificado fuera de los límites especificados en esta Política y Prácticas de Certificación.
- No utilizar el certificado en caso de que el Prestador de servicios de confianza haya cesado su actividad como Autoridad de Certificación emisora del mismo, especialmente en situaciones donde los Datos de creación del sello hayan podido ser comprometidos y dicha circunstancia haya sido comunicada.
- Proporcionar información veraz al solicitar los Certificados y mantenerla actualizada, suscribiendo los contratos mediante una persona con capacidad suficiente.
- No solicitar, como titular del certificado, signos distintivos, nombres o derechos de propiedad industrial o intelectual de los que no sea titular, licenciatario o tenga autorización demostrable para su uso.
- Actuar con diligencia en la custodia y conservación de los Datos de creación de firma/sello o cualquier otra información sensible como claves, códigos de activación del Certificado, contraseñas, números personales de identificación, etc., así como de los soportes del Certificado, no revelando en ningún caso dicha información.
- Conocer y cumplir las condiciones de uso de los certificados previstas en las condiciones de uso y en la Declaración de Prácticas de Certificación, en especial las limitaciones de uso.
- Conocer y cumplir las modificaciones realizadas a la Declaración de Prácticas de Certificación.
- Solicitar la revocación del Certificado correspondiente conforme al procedimiento descrito en este documento, notificando diligentemente a IZENPE cualquier circunstancia que motive dicha revocación o sospecha de pérdida de confidencialidad, 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, antes de confiar en los Certificados, la Firma electrónica avanzada o sello electrónico del Prestador de servicios de confianza emisor del Certificado.
- Notificar diligentemente a IZENPE cualquier modificación de los datos proporcionados en la solicitud del Certificado, solicitando, en su caso, la revocación del mismo.

El suscriptor será responsable del uso adecuado y la custodia diligente del Certificado, conforme al propósito y función para los cuales ha sido emitido, así como de informar a IZENPE de cualquier cambio en el estado o información reflejada en el Certificado, con el fin de proceder a su revocación y nueva emisión.

Asimismo, el suscriptor será responsable, en todo caso, frente a IZENPE, las Entidades usuarias y, en su caso, terceros, por el uso indebido del Certificado o por falsedades o errores en las declaraciones contenidas en el mismo o por actos u omisiones que causen daño o perjuicio a IZENPE o a terceros.

Será responsabilidad y, por tanto, obligación del suscriptor no utilizar el Certificado en caso de que el Prestador de servicios de confianza haya cesado su actividad como emisor del Certificado correspondiente y no se haya producido la subrogación prevista legalmente. En todo caso, el

suscriptor no deberá utilizar el certificado en aquellos supuestos en que los Datos de creación del sello del proveedor puedan estar amenazados y/o comprometidos, y esta circunstancia haya sido comunicada por el Proveedor o, en su caso, el suscriptor haya tenido conocimiento de la misma.

La relación entre IZENPE y el suscriptor se determinará, a efectos del régimen de uso de los Certificados, mediante el documento relativo a las condiciones de uso o, en su caso, el contrato de emisión del Certificado y de conformidad con los convenios, acuerdos o documento de relación entre IZENPE y la Entidad correspondiente.

9.6.4 Declaraciones y garantías de las partes de confianza

El usuario verificador del certificado se compromete a:

- Asegurar de forma independiente que el certificado es adecuado para el uso previsto.
- Comprender los términos y condiciones de uso de los certificados, conforme a lo establecido en la Declaración de Prácticas de Certificación y en el contrato de prestación del servicio de certificación suscrito con IZENPE.
- Verificar la validez o revocación de los certificados emitidos. Para ello, el usuario deberá consultar la información relativa al estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificación antes de confiar en la firma digital o en cualquiera de los certificados de dicha jerarquía.
- Tener en cuenta cualquier limitación de uso del certificado, con independencia de que esta figure en el propio certificado o esté recogida en el contrato de verificación.
- Atender a cualquier advertencia o precaución estipulada en un contrato u otro instrumento, cualquiera que sea su naturaleza jurídica.
- Notificar cualquier circunstancia o situación anómala en relación con el certificado que pudiera considerarse causa de revocación.
- Abstenerse de monitorizar, interferir o realizar ingeniería inversa sobre la implementación técnica de los servicios de certificación sin la autorización previa y por escrito de IZENPE.
- Abstenerse de comprometer intencionadamente la seguridad de los servicios de certificación.

9.6.5 Declaraciones y garantías de otras partes participantes

No estipulado.

9.7 Exclusión de garantías

No estipulado.

9.8 Limitaciones de responsabilidad

Responsabilidad de la Autoridad de Certificación

IZENPE será responsable por negligencia o falta de diligencia en la prestación de los servicios de certificación descritos en esta Declaración de Prácticas de Certificación, así como por el incumplimiento de las obligaciones legales previstas en la normativa de firma electrónica, salvo en los siguientes casos:

- En ningún caso IZENPE será responsable de los daños ocasionados por la información contenida en los certificados, siempre que el contenido de los mismos cumpla sustancialmente con lo establecido en esta Declaración de Prácticas de Certificación.
- En ningún caso será responsable de los daños derivados del vencimiento de un certificado, siempre que se cumplan sustancialmente las obligaciones de publicación previstas en este documento.
- IZENPE no será responsable por daños directos, indirectos, especiales, incidentales, consecuentes, lucro cesante, pérdida de datos, daños punitivos, previsibles o no, derivados del uso, entrega, licencia, operación o falta de operación de los Certificados, firmas digitales u otros servicios o transacciones contempladas en esta Declaración, en caso de uso indebido.
- IZENPE no asumirá responsabilidad por daños a suscriptores o terceros de buena fe cuando las inexactitudes en la información contenida en el certificado hayan sido certificadas mediante documentos oficiales, notariales o autorizados, salvo cuando dichos documentos hayan sido proporcionados por la Autoridad de Registro.
- No será responsable por daños derivados del incumplimiento de las obligaciones que competen a los suscriptores o a las partes de confianza.

IZENPE será responsable por perjuicios causados a cualquier persona como consecuencia de la falta de disponibilidad o del retraso en la actualización del servicio de consulta de validez de los certificados, o por la expiración de los mismos.

También responderá frente a terceros por las acciones de las personas a quienes haya delegado funciones necesarias para la prestación de los servicios de certificación. En este sentido, se ha suscrito una póliza de seguro de responsabilidad civil que cubre los daños y perjuicios que puedan derivarse del uso de los certificados.

Responsabilidad de la Autoridad de Registro

Cualquier entidad distinta de IZENPE que actúe como Autoridad de Registro será responsable ante IZENPE por los daños ocasionados en el ejercicio de las funciones asumidas, conforme a los términos establecidos en el correspondiente acuerdo legal.

Cuando las funciones de identificación sean llevadas a cabo por Administraciones públicas que suscriban los certificados, se aplicará el régimen de responsabilidad patrimonial de las Administraciones Públicas, conforme a lo establecido en la Ley del Régimen Jurídico del Sector Público y del Procedimiento Administrativo Común.

Responsabilidad del suscriptor

El Suscriptor será responsable de todas las transacciones electrónicas autenticadas mediante una firma digital generada con su clave privada, cuando el certificado haya sido validado a través de los servicios de verificación proporcionados por IZENPE.

Si no se ha recibido ninguna notificación de pérdida o robo del certificado, conforme a lo establecido en esta Declaración de Prácticas de Certificación, cualquier responsabilidad derivada del uso no autorizado y/o indebido de los certificados será, en todo caso, atribuible al Suscriptor.

Mediante la aceptación de los certificados, el Suscriptor se compromete a proteger y, en su caso, a indemnizar a IZENPE, a las Autoridades de Registro y a las Entidades usuarias por cualquier acto u omisión que pueda ocasionar daños, pérdidas, deudas, gastos legales u otros costes, incluidos los honorarios profesionales, en los que incurra IZENPE, las Autoridades de Registro o las Entidades usuarias, como consecuencia del uso o publicación de certificados, y que deriven de:

- el incumplimiento de los términos y condiciones establecidos en el instrumento legal que lo vincula con la Autoridad de Certificación,
- el uso de certificados digitales en transacciones electrónicas con personas no autorizadas,
- la falsedad o tergiversación de hechos por parte del Suscriptor,
- la omisión por parte del Suscriptor de hechos materiales en los certificados, cuando dicha omisión o tergiversación se haya realizado de forma negligente o con intención de engañar a IZENPE, a las Entidades Públicas Usuarias o a terceros que confíen en el certificado del Suscriptor, y
- el incumplimiento del deber de proteger la clave privada o de adoptar las precauciones razonables para evitar su pérdida, divulgación, modificación o uso no autorizado.

En este sentido, IZENPE no será responsable de los daños causados a suscriptores o a terceros de buena fe cuando se derive del incumplimiento por parte del Suscriptor de los siguientes deberes:

- Proporcionar a IZENPE o a la Autoridad de Registro información completa, veraz y precisa en relación con sus solicitudes de certificados y con cualquier otra información necesaria para su emisión o revocación, cuando las inexactitudes no hayan sido detectadas por el prestador del servicio.
- Notificar de forma inmediata a IZENPE o a la Autoridad de Registro cualquier cambio en la información suministrada para el certificado.
- Custodiar con diligencia los datos de creación de firma para garantizar su confidencialidad y protegerlos contra accesos o revelaciones no autorizadas.
- Solicitar la revocación del certificado ante cualquier sospecha sobre la pérdida de confidencialidad de los datos de creación de firma.
- Abstenerse de utilizar los datos de creación de firma a partir del momento en que expire el período de validez del certificado o cuando el prestador del servicio comunique su invalidez.

- Atenerse a las limitaciones de uso del certificado y utilizarlo conforme a las condiciones establecidas y comunicadas por el prestador del servicio de certificación.

Responsabilidad de terceros de confianza

Un tercero que confía en un certificado sin haberlo verificado asume todos los riesgos asociados a dicha confianza y, en ningún caso, podrá responsabilizar a IZENPE, a las Autoridades de Registro, a las Entidades usuarias ni a los Suscriptores por cualquier circunstancia derivada de su confianza en dichos certificados o firmas.

En este sentido, IZENPE no será responsable por daños causados a suscriptores o a terceros de buena fe, si el destinatario de los documentos firmados electrónicamente no cumple con alguna de las siguientes obligaciones de diligencia debida:

- Verificar y tener en cuenta las restricciones del certificado relativas a sus posibles usos y al importe máximo de las transacciones que pueden realizarse con el mismo.
- Comprobar la validez del certificado.
- Verificar el identificador digital del certificado cualificado en la Lista de servicios de confianza (TSL).

9.9 Indemnizaciones

En caso de incumplimiento por parte de IZENPE de sus obligaciones o de infracción de los requisitos legales, se incluirán cláusulas de indemnización en los instrumentos legales que vinculen a IZENPE con el suscriptor y con el verificador.

9.9.1 Indemnización a la CA

No estipulado.

9.9.2 Indemnización a los suscriptores

No estipulado.

9.9.3 Indemnización a los terceros de confianza

No estipulado.

9.10 Vigencia y terminación

9.10.1 Vigencia

Esta Política de certificación entrará en vigor en el momento de su publicación.

9.10.2 Terminación

Esta Política de certificación quedará derogada cuando se publique una nueva versión del documento.

La nueva versión sustituirá en su totalidad a la anterior. IZENPE se compromete a someter esta Política a un proceso de revisión anual.

9.10.3 Efectos de la terminación y subsistencia

Para los certificados vigentes emitidos conforme a esta Política de Certificación, prevalecerá la nueva versión en todo lo que no entre en conflicto con la anterior.

9.11 Notificaciones individuales y comunicaciones con los participantes

IZENPE establecerá los medios y plazos de notificación a través del instrumento legal vinculante.

Con carácter general, el sitio web de IZENPE (www.izenpe.eus) se utilizará para realizar cualquier tipo de notificación y comunicación.

9.12 Modificaciones

9.12.1 Procedimiento de modificación

Las modificaciones a esta Política de certificación serán aprobadas por el Comité de Seguridad de IZENPE, y quedarán reflejadas en el acta correspondiente, conforme al procedimiento interno aprobado.

9.12.2 Mecanismo y plazo de notificación

Cualquier modificación a esta Política de certificación será publicada de forma inmediata en la URL de acceso a la misma.

Si los cambios no implican modificaciones significativas en cuanto al sistema de obligaciones y responsabilidades de las partes, ni afectan a las políticas de prestación de servicios, IZENPE no notificará previamente a los usuarios, sino que simplemente publicará la nueva versión en su sitio web.

9.12.3 Circunstancias en las que debe modificarse el OID

Las modificaciones significativas en las condiciones del servicio, el régimen de obligaciones y responsabilidades, o las limitaciones de uso podrán dar lugar a un cambio en la política del servicio y en su identificación (OID), así como al enlace con la nueva declaración de política del servicio. En tal caso, IZENPE podrá establecer un mecanismo para informar de los cambios propuestos y, cuando corresponda, para recabar las opiniones de las partes interesadas.

9.13 Disposiciones sobre resolución de conflictos

IZENPE está sometida al sistema de arbitraje de consumo de conformidad con lo previsto en la legislación aplicable, como medio para resolver disputas o reclamaciones presentadas por solicitantes o suscriptores de certificados ciudadanos. Las resoluciones de este sistema se consideran firmes y vinculantes para ambas partes.

A estos efectos, se entiende que el solicitante o suscriptor acepta el sistema desde el momento en que presenta la reclamación ante la junta arbitral de consumo correspondiente.

Cualquier otra cuestión contenciosa planteada por solicitantes o suscriptores sobre certificados ciudadanos que no esté regulada por el sistema de arbitraje de consumo, se someterá a la jurisdicción competente.

9.14 Legislación aplicable

La ejecución, redacción, interpretación y validez de esta Declaración de Prácticas de Certificación se regirán conforme a la legislación española sobre firma electrónica.

Las normas aplicables a este documento y a las operaciones que de él se derivan son las siguientes:

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 910/2014 (eIDAS 1) sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, que deroga la Directiva 1999/93/CE.
- 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 relativo al establecimiento del marco de identidad digital europea (eIDAS 2).
- Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de Régimen Jurídico del Sector Público.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 (RGPD) 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.

La práctica de prestación de servicios de confianza de IZENPE sigue las siguientes normas técnicas:

- ETSI EN 319 401: Requisitos generales de política para los Prestadores de servicios de confianza.
- Declaración General de Prácticas de Servicios de Confianza y Certificación Electrónica, versión 5.7.
- ETSI EN 319 421: Requisitos de política y seguridad para Prestadores de servicios de confianza que emiten sellos de tiempo.
- ETSI EN 319 411-2: Requisitos para los prestadores que emiten certificados electrónicos cualificados en la UE.
- ETSI EN 319 412: Perfiles de certificados electrónicos.
- ETSI EN 319 421: Requisitos de política y seguridad para Prestadores de servicios de confianza que emiten sellos de tiempo.
- ETSI EN 319 422: Protocolo de sellado de tiempo y perfiles de tokens de sello de tiempo.
- Requisitos Básicos de CABForum.
- Guías de Certificados EV del CABForum.

9.15 Compromiso de cumplimiento con la ley

IZENPE declara su compromiso de cumplir con las regulaciones y requisitos aplicables a cada tipo de certificado de autenticación de sitios web, incluyendo las consideraciones recogidas en la sección «1.5.4. Procedimiento de aprobación del CPS» de este documento de CP.

9.16 Disposiciones misceláneas

9.16.1 Acuerdo íntegro

Cada cláusula contenida en esta Declaración de Prácticas de Certificación es válida por sí misma y no afecta a la validez del resto de las cláusulas. La cláusula que resulte inválida o incompleta podrá ser sustituida por otra cláusula equivalente.

Ninguno de los términos y disposiciones de esta Declaración de Prácticas de Certificación que afecte directamente a los derechos y obligaciones de IZENPE y que no afecte al resto de las partes podrá ser enmendado, renunciado, complementado, modificado o eliminado sin el consentimiento expreso y por escrito de IZENPE. En ningún caso dicho cambio supondrá una novación, sino una modificación que no afectará al resto de los derechos y obligaciones de las demás partes.

9.16.2 Cesión

IZENPE no será responsable por la falta de servicio o por anomalías en el mismo, ni por los daños y perjuicios que puedan derivarse directa o indirectamente cuando dicha interrupción o desastre sea causado por fuerza mayor, atentados terroristas, sabotajes o huelgas salvajes; todo ello sin perjuicio

de las actuaciones necesarias para remediar y/o restablecer el servicio con la mayor celeridad posible.

9.16.3 Divisibilidad

No estipulado.

9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)

No estipulado.

9.16.5 Fuerza mayor

No estipulado.

9.17 Otras disposiciones

Sin estipulación.