POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB.

ZIURTAPEN ETA ZERBITZU
ENPRESA-EMPRESA DE
CERTIFICACION Y SERVIC
2023.10.16 09:08:00 +02'00'

CONTROL DE CAMBIOS

VERSIÓN	CAMBIO
1.0	– Añadido requisitos en apartado 2.2 – Actualizados requisitos en apartados 2.1 y 2.2 – Actualizados requisitos en apartado 2.2 – Añadido índice. – Añadido pie de página. – Eliminados requisitos en apartados 2.1 y 2.2 – Eliminado año en portada
1.1	– Actualizados requisitos en validación del dominio, en el apartado 2.2 – Eliminadas gráficas en apartados 2.3 y 2.6.
1.2	– Actualizados requisitos en validación CAA, en el apartado 2.2.
1.3	– 1. Introducción. En el ámbito del proyecto de Google Certificate Transparency, los certificados SSL EV y Sede EV emitidos se publicarán en el servicio CT de los proveedores de Log Servers con los cuales Izenpe mantiene un acuerdo. – 1.1. Descripción de certificados. ▪ Actualización de la normativa referente a la regulación del certificado de sello. ▪ Actualización de la validez de los certificados que podrá ser de 1 o 2 años – 1.2. Identificación ▪ Se incluyen los OID CA/B FORUM ▪ Los números de serie de los certificados tendrán al menos 64 bits de entropía – Epígrafes 1.3 y siguientes. Adecuación de la terminología a la emisión de certificados de tipo EV a entidades privadas. – 14.Disposiciones generales, ▪ Obligaciones de identificación. Se indica que todos los casos Izenpe comprueba la titularidad o control sobre el dominio. ▪ Obligaciones del suscriptor del certificado. Se incluyen las determinadas en el Acuerdo de Divulgación de Clave Pública (PDS). – Apartados 1 ,2 y 3. Inclusión de aclaraciones sobre cumplimiento de las BR.
1.4	– Se ha actualizado el OID de política de los certificados SSL-EV y Sede-EV

	– Se indica en el apartado “1.1 Descripción de certificados” que los certificados SSL EV cualificado y Sede EV cualificado se consideran cualificados según eIDAS – Se indica en la introducción que se publicarán TODOS los certificados en los CT – Se han eliminado todas las referencias al certificado de sede
1.5	Se han añadido los perfiles cualificados
1.6	– Añadidos los siguientes métodos de comprobación de titularidad del dominio: – Email construido al contacto del dominio – Email a contacto DNS CAA – Email a contacto DNS TXT – DNS Lookup – Detalladas las causas y plazos de revocación tanto en finales como en subCAs
1.7	– Se añade, • Las rutas de los certificados de test (vivo, revocado, caducado) • la comprobación de parámetros de las claves RSA • Se añade la definición de “precertificado” • obligación de incrementar el número de versión aunque no haya habido cambios – Se elimina, • Los EV de entre los perfiles que Izenpe emite actualmente • Procedimiento de revocación, y se redirige a la DPC – Se especifica que las CAs públicas de Izenpe no emiten para dominios internos
1.8	Se ha adaptado el documento a la estructura de la RFC 3647
1.9	– Se sustituye el apartado de control de cambios por esta tabla de histórico de versiones – Se actualiza la duración de todos los perfiles a 395 días – Eliminado el método DNS CAA – Añadido el método whois para los .eus
2.0	– Eliminación de las referencias a certificados sede cualificado y SSL EV – Actualización de La dirección postal y electrónica de Izenpe. – Revisión de la redacción de la política.
2.1	Epígrafe, – 3.2.2.1 Identidad: en relación a los certificados SSL cualificados. Se incluye la lista de fuentes de comprobación de entidades según CABFORUM. – Portada: Se elimina el pie de página del título del documento por error en el número de teléfono.
2.2	Epígrafe,

	-3.2.2.1 Identidad: se amplía la lista de fuentes de comprobación de entidades. -1 Corrección párrafo “Certificate Transparency” -3.1 Eliminar párrafo referente a RFC 6962 -3.2.2.2.4. Los métodos de validación admitidos son correctos pero la descripción “c” no se corresponde y falta la descripción del método 3.2.2.4.4 de CABForum. -4.1.2 Eliminar referencia a entidades que no se pueden consultar en registros. -4.6 Error en la versión en Inglés. No es “revocation” sino “renewal” -4.4.3 Corrección respecto al “Certificate Transaparency” -4.9.6 Se cambia la redacción -6.3.2 se cambia 395 por 398 -6.1.5. Se añade un “>=” al 2048 -9.1.3 I=Izenpe

ÍNDICE

1. INTRODUCCIÓN

El presente documento recoge 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 diferentes variantes.

Su finalidad es detallar y completar para este tipo de certificados 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), EV guidelines (en adelante EVBR)* para la emisión de certificados para sitios web y en las especificaciones de ETSI (www.etsi.org). Izenpe se adhiere a la última versión publicada de dichas normas.

Así, Izenpe sigue las siguientes políticas de certificación establecidas por ETSI:

- DVCP (Domain Validation Certificates Policy): en los certificados "SSL DV"
- OVCP (Organizational Validation Certificates Policy): en los certificados "SSL OV"
- EVCP (Extended Validation Certificates Policy): en los certificados "SSL Cualificado"

En el ámbito del proyecto de Chrome Certificate Transparency, todos los certificados SSL emitidos se publicarán en el servicio CT de los proveedores de Log Servers en los que la raíz de Izenpe está incluida.

Izenpe mantiene sitios web de test para que proveedores de software puedan probar sus productos con certificados SSL/TLS en entornos de producción. Izenpe mantiene sitios diferentes con al menos un certificado final vivo, caducado y revocado:

- https://test-ev-qualified.izenpe.eus/
- https://test-expired-ev.izenpe.eus/
- https://test-revoked-ev.izenpe.eus/

Según la validación realizada, Izenpe expide los siguientes tipos de certificados

- *SSL DOMAIN VALIDATED (**SSL DV**),*

  Este certificado, con la consideración de no cualificado, será utilizado para la identificación de la titularidad del dominio que alberga el sitio web, proporcionando una garantía razonable al usuario de un navegador de Internet

  La validez de estos certificados es de 395 días.

- *SSL ORGANIZATION VALIDATED (**SSL OV**),*

  Este certificado, con la consideración de no cualificado, será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía razonable al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado.

- La validez de estos certificados es de 395 días.*SSL CUALIFICADO (**SSL CUALIFICADO**),*

  Este certificado tiene la consideración de cualificado según el Reglamento (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS). Será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía robusta al

usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado.

La validez de estos certificados es de 395 días.

1.1. Objeto

La finalidad 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 expedidos por Izenpe y establecer las obligaciones que Izenpe se compromete a cumplir en relación a:

- La gestión de los certificados y as condiciones aplicables a la solicitud, emisión, uso y extinción de su vigencia.
- La prestación del servicio de consulta del estado de validez de los certificados, así como las condiciones aplicables al uso del servicio y garantías ofrecidas.

Además, se recogen, bien directamente o con referencias a Declaración de Prácticas de Certificación de Izenpe, los detalles del régimen de responsabilidad aplicable a las partes usuarias y/o que confían en los servicios descritos en el párrafo anterior, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.

Esta Política forma parte de la DPC de Izenpe. En caso de que existiera contradicción entre el presente documento y lo dispuesto en la DPC, tendrá preferencia lo determinado en el presente documento.

1.2. Nombre del documento e identificación

El presente documento se denomina “Política de Certificación de certificados de autenticación de sitios web”.

- Versión: 2.2
- Fecha de expedición: 13/10/2023
- Localización:http://www.izenpe.eus/s15-content/es/contenidos/informacion/doc_especifica/es_def/index.shtml
- DPC relacionada: Declaración de Prácticas de Certificación de Izenpe.

Con el objeto de identificar los certificados, Izenpe les ha asignado los siguientes identificadores de política (OID).

CERTIFICADO	OID POLITICA
SSL DV	1.3.6.1.4.1.14777.1.2.4
SSL OV	1.3.6.1.4.1.14777.1.2.1
SSL Cualificado	1.3.6.1.4.1.14777.6.1.3

1.3. Partes intervinientes

Partes que intervienen en la gestión y uso de los servicios de confianza descritos:

1. Autoridad de Certificación
2. Autoridad de Registro
3. Suscriptores o titulares de los Certificados
4. Partes que confían
5. Otros participantes

1.3.1. Autoridad de Certificación

En el ámbito de la presente política, Izenpe dispone de las siguientes Autoridades de Certificación:

Tipo	CN	Huella SHA1
Raiz	Izenpe.com	2f783d255218a74a653971b52ca29c45156fe919
Subordinada	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	f79cda11e7917419a0418db84ba743c5313ad7f0
Subordinada	CA de Certificados SSL EV	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8
Subordinada	CA de Certificados SSL EV	c68bade5f069778a003074e619dab2e7928342d5

AUTORIDAD DE CERTIFICACIÓN RAÍZ

Es la Autoridad de Certificación que expide certificados para las Autoridades de Certificación subordinadas.

CA RAIZ	
Campo / extensión	**Contenido**
version	Versión 3
serialNumber	00b0b75a16485fbfe1cbf58bd719e67d
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	30 años
subject	

CN	Izenpe.com
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
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 CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)

AUTORIDAD DE CERTIFICACIÓN SUBORDINADA

EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	
Campo / extensión	**Contenido**
versión	Versión 3
serialNumber	24c5c8aa566f8ee84cbea7055ce164a4
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	13 de diciembre de 2037
subject	
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
extensions	
subjectAltName	
rfc822Name	info@izenpe.com

directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	c0a94af7472587ffbcb5a689ce82d246a889eba3
authorityKeyIdentifier	Id. de clave=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Todas las directivas de emisión
Id. de certificador de directiva	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Método de acceso	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
Nombre alternativo	
Dirección URL	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)
Huella digital	f79cda11e7917419a0418db84ba743c5313ad7f0

CA de Certificados SSL EV 2010	
Campo / extensión	Contenido
version	Versión 3
serialNumber	6d71e25b7bb6b6364cbea848e3a4a981
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	20 de octubre de 2020
subject	
CN	CA de Certificados SSL EV
OU	BZ Ziurtagiri publikoa - Certificado publico EV
O	IZENPE S.A.
C	ES

subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	a6ce69692ea621353b3acf0af12e3f15ac199027
authorityKeyIdentifier	Id. de clave=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Todas las directivas de emisión
Id. de certificador de directiva	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Método de acceso	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
Nombre alternativo	
Dirección URL	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)
Huella digital	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8

CA de Certificados SSL EV 2018	
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
subject	

CN	CA de Certificados SSL EV
OU	BZ Ziurtagiri publikoa - Certificado publico EV
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	c6edfe77fb51564dfcabd5e3b10c13a3bf54e39b
authorityKeyIdentifier	Id. de clave=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Todas las directivas de emisión
Id. de certificador de directiva	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Método de acceso	Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
Nombre alternativo	
Dirección URL	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)
Huella digital	c68bade5f069778a003074e619dab2e7928342d5

1.3.2. Autoridad de Registro

Izenpe es la única Autoridad de Registro que actúa en el proceso de expedición de estos certificados. Realiza las tareas de identificación y comprobación de manera automatizada, con la finalidad de garantizar que el certificado expedido al Suscriptor tiene el control del nombre de dominio incluido en el Certificado. Controlado exclusivamente

Ninguna de las verificaciones sobre la identidad o control de dominio se delegará en terceras partes.

1.3.3. Suscriptores de los certificados

Los suscriptores son las personas jurídicas a quienes se expiden los certificados, obligados según lo determinado en el documento de términos y Condiciones.

1.3.4. Partes que confían

Las partes que confían son aquellos usuarios de Internet que establecen conexiones a sitios web mediante el uso de protocolos TLS/SSL que incorporan este tipo de Certificados y deciden confiar en ellos.

1.3.5. Otros participantes

No estipulado

1.4. Uso de los certificados

1.4.1. Usos permitidos de los certificados

Los certificados de autenticación de sitio web permiten autenticar un sitio web y lo vinculan con la persona física o jurídica a quien se ha expedido.

Todos los certificados de autenticación de sitios web cualificados expedidos bajo la presente Política son certificados cualificados conforme al Reglamento eIDAS y y a los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” y ETSI EN 319 412-4 “Certificate profile for web site certificates”.

1.4.2. Restricciones en el uso de los certificados

Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Asimismo, los certificados deben emplearse únicamente de acuerdo con la legislación aplicable.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Si una entidad usuaria o un tercero confía en estos certificados sin acceder al servicio de información y consulta sobre el estado de validez de los certificados expedidos bajo esta Política de Certificación, no se obtendrá cobertura de las presentes Políticas y Prácticas de Certificación Particulares, y carecerá de legitimidad alguna para reclamar o emprender acciones legales contra Izenpe por daños, perjuicios o conflictos provenientes del uso o confianza en un Certificado.

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

1.5. Administración de Políticas

1.5.1. Entidad responsable

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

1.5.2. Datos de contacto

Nombre del prestador	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Dirección postal	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Dirección e-mail	izenpe@izenpe.eus

Para informar problemas de seguridad, tales como sospecha de compromiso de claves, uso indebido de certificados, fraude, solicitudes de revocación u otros asuntos, comuníquese con incidencias@izenpe.eus

1.5.3. Responsables de adecuación

El Comité de Seguridad de Izenpe es el órgano responsable de la aprobación de la presente Política.

1.5.4. Procedimiento de aprobación

Izenpe gestiona sus servicios de certificación y emite certificados de conformidad con la última versión de los Requisitos base para la emisión y gestión de certificados de confianza requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la siguiente dirección https://cabforum.org/baseline-requirements-documents/

Izenpe revisa y actualiza anualmente la presente Política identificando, publicando las nuevas versiones en www.izenpe.eus

1.6. Definiciones y Acrónimos

1.6.1. Definiciones

- Certificado de autenticación de sitio web: certificado que permite autenticar un sitio web y vincular el sitio web con la persona física o jurídica a quien se ha expedido el Certificado.
- Certificado OV*:* certificado de autenticación de sitio web expedido según la política de validación de Organización (OVCP), garantizando razonablemente al usuario de navegadores de Internet que el titular del sitio web al que accede coincide con la Organización identificada por el Certificado OV. Este Certificado cumple con los requisitos del estándar europeo ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”.
- Certificado Wildcard *OV*: certificado OV que incorpora un conjunto de subdominios ilimitado, a partir del tercer nivel, con un único Certificado de autenticación de sitio web.

- Certificado de autenticación Web cualificado: Este certificado tiene la consideración de cualificado según el eIDAS. Será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía robusta al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado.
- *Certificate Transparency (CT):* es un marco abierto para la supervisión de Certificados de autenticación de sitio web, de forma que cuando se expide uno de estos Certificados, se publica en registros CT, posibilitando así que los propietarios de dominios puedan supervisar la emisión de los mismos para sus dominios y detectar certificados emitidos erróneamente.
- *Declaración de Prácticas de Certificación (DPC*): declaración puesta a disposición del público fácilmente accesible, por vía electrónica de forma gratuita por parte de Izenpe. Tiene la consideración de documento de seguridad en el que se detallan, en el marco eIDAS, las obligaciones que los Prestadores de Servicios de Confianza se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los Certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los Certificados.
- *Política de certificado*: política que se aplica a la expedición de un conjunto determinado de certificados expedidos por Izenpe bajo las condiciones particulares recogidas en la misma.
- *Informe de incidencia con un certificado*: queja de sospecha de compromiso clave, mal uso del certificado u otros tipos de fraude, compromiso, mal uso o conducta inapropiada relacionada con los certificados
- *Organismo de supervisión*: organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el artículo 17 del Reglamento eIDAS. En España, actualmente es el Ministerio de Asuntos Económicos y Transformación Digital
- *Registro CAA (CAA records):* registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (CAA). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (CA) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de CAA permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada de un Certificado de autenticación de sitios web para su nombre de dominio.
- *Representante del Suscriptor*: persona física autoriza por el suscriptor para tramitar el certificado.
- *Suscriptor*: persona jurídica, órgano u organismo público destinatario de las actividades de Izenpe como Prestador de Servicios de Confianza, que suscribe los términos y condiciones del servicio. Bajo la presenta Política de Certificación, dicho servicio consiste en la expedición de Certificados de autenticación de sitios web. El Suscriptor se referencia en el campo Sujeto del Certificado y es el titular y responsable de su uso y posee el control exclusivo y la capacidad de decisión sobre el mismo.

1.6.2. Acrónimos

A los efectos de lo dispuesto en la presente CP, son de aplicación los siguientes acrónimos, cuyo significado es acorde con el estándar europeo ETSI EN 319 411 “Policy and security requirements for Trust Service Providers issuing certificates”:

CA: Autoridad de Certificación

RA: Autoridad de Registro

ARL: Lista de Revocación de Autoridades de Certificación

CN: Nombre común (Common Name)

CRL: Lista de Certificados revocados

DN: Nombre distintivo (Distinguished Name)

DPC: Declaración de Prácticas de Certificación

eIDAS: Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

EV: Validación extendida (Extended Validation).

ETSI: European Telecommunications Standards Institute

HSM: Módulo de seguridad criptográfico (Hardware Security Module). Es un dispositivo de seguridad que genera y protege claves criptográficas.

OCSP: Protocolo de internet usado para obtener el estado de un certificado en línea (Online Certificate Status Protocol)

OID: Identificador de Objeto (Object IDentifier)

OV: Validación de Organización (Organizational Validation).

PDS: Declaración informativa de la PKI (PKI Disclosure Statement).

PIN: Número de identificación personal (Personal Identification Number).

PKCS: Estándares PKI desarrollados por Laboratorios RSA (Public Key Cryptography Standards).

TLS/SSL: Protocolos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (Transport Layer Security/Secure Socket Layer protocol).

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. Repositorio

Izenpe dispone de un repositorio de información pública en www.izenpe.eus, disponible las 24 horas del día los 7 días de la semana.

2.2. Publicación de información de certificación

La información relativa a la expedición de certificados electrónicos objeto de la presente Política, está accesible a través de www.izenpe.eus e incluye las siguientes informaciones:

- ✓ Declaraciones de prácticas y políticas de Certificación.
- ✓ Perfiles de los Certificados y de las Listas de revocación.
- ✓ Las declaraciones informativas de la PKI (PDS).
- ✓ Los términos y condiciones de uso de los Certificados, como instrumento jurídico vinculante.
- ✓ Descarga de los Certificados raíz y de CAs subordinadas de Izenpe, así como a información adicional.

2.3. Frecuencia de publicación

Izenpe revisa sus políticas y prácticas de certificación y actualiza anualmente el presente documento siguiendo las pautas establecidas en el apartado "1.5.4. Procedimiento de aprobación " del presente documento.

Cualquier modificación en la DPC o en este documento será publicada de forma inmediata.

En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Frecuencia de generación de CRLs" de la DPC.

2.4. Control de acceso a los repositorios

Izenpe permite el acceso de lectura a la información publicada en su repositorio y establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros de este Servicio y para proteger la integridad y autenticidad de la información depositada.

Izenpe emplea sistemas fiables para el acceso al repositorio de información, de modo que:

- ✓ Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- ✓ Pueda comprobarse la autenticidad de la información.
- ✓ Los certificados estén disponibles para su consulta.
- ✓ Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Denominación

La codificación de los certificados sigue el estándar RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. Todos los campos definidos en el perfil de los Certificados en la DPC y en la política, excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

Adicionalmente, para los certificados SSL cualificados, Izenpe cumplirá con los requisitos establecidos en el apartado 9.2 de CABForum en su “guía para la expedición y gestión de Certificados de Validación Extendida” y que pueden consultarse en la dirección https://cabforum.org/extended-validation/

3.1.1. Tipos de nombres

Los certificados electrónicos de entidad final objeto de la presente Política contienen un nombre distintivo (DN) en el campo Subject Name, formado por la información relativa al perfil del Certificado (apartado 7.1 del presente documento). Izenpe cumple con los requisitos X.500, RFC 5280 y CA/Browser Forum (BRs and EVGs) a este respecto.

El campo Common Name define al suscriptor de certificado.

3.1.2. Significado de los nombres

Todos los nombres distintivos (DN) del campo Subject Name son significativos. La descripción de los atributos asociados al suscriptor del certificado es legible por humanos (véase el apartado 7.1.4 Formato de nombres del presente documento).

El campo Subject Distinguished Name estará también sujeto a los requisitos establecidos en el apartado 9.2 de CABForum en su “guía para la expedición y gestión de Certificados de Validación Extendida” y que pueden consultarse en la dirección https://cabforum.org/extended-validation/. Izenpe no emite Certificados Wildcard con políticas EV.

3.1.3. Seudónimos

Bajo la presente Política de Certificación Izenpe no admite el uso de seudónimos.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.5. Unicidad de los nombres

El nombre distintivo (DN) asignado al suscriptor del certificado dentro del dominio del Prestador de Servicios de Confianza será único.

3.1.6. Reconocimiento y autenticación de marcas registradas

Los solicitantes de certificados no deben incluir en las solicitudes de emisión nombres que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

Izenpe no determina si un solicitante de certificados tiene derecho alguno sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actúa como árbitro o mediador, ni de ningún otro modo resuelve disputa alguna concerniente a la propiedad de nombres de personas u organizaciones o nombres de dominio.

Izenpe se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

3.2. Validación inicial de la identidad

Izenpe realiza el proceso de validación de la información incluida en el certificado de autenticación de sitios web de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la dirección https://cabforum.org/baseline-requirements-documents

Adicionalmente, Izenpe, antes de expedir un Certificado SSL cualificado, asegura que toda la información incluida en estos tipos de certificados relativa al suscriptor, es conforme a (y se verifica de acuerdo a) los requisitos definidos por la entidad CA/Browser forum en su “guía para la expedición y gestión de Certificados de Validación Extendida”, (apartado 11) y que pueden consultarse en la dirección https://cabforum.org/extended-validation

Izenpe registra todas las confirmaciones realizadas en esta sección para los procesos periódicos de auditoría tanto interna como independiente

3.2.1. Métodos para probar la posesión de la clave privada

Izenpe recibe una solicitud de certificado, en formato PKCS#10, firmada digitalmente por la clave privada generada por el representante del suscriptor en su entorno. Antes de proceder a la expedición del certificado, Izenpe verifica dicha firma, garantizando que la clave pública incluida en la solicitud se corresponde con la clave privada generada por el responsable del certificado.

3.2.2. Autenticación de la identidad de la Organización

3.2.2.1 Identidad

Izenpe no expide certificados de autenticación de sitios web cuyo suscriptor sea una persona física.

- En el caso de certificados DV,

  Izenpe no comprueba la identidad ni ningún tipo de información de la organización.

- En el caso de certificados OV,

  Izenpe verifica la dirección postal y la identidad de la organización suscriptora en función del tipo de organización (carácter privado o público).

  - Cuando el suscriptor sea una organización perteneciente al sector privado, Izenpe verificará su dirección e identidad, mediante consulta al Registro oficial correspondiente.

  - Caso de entidades de carácter público, verificación realizada mediante consulta al Boletín Oficial correspondiente y otras fuentes consultadas.

- Si la naturaleza del suscriptor fuera distinta de los dos casos anteriores, las verificaciones relativas a la existencia, dirección y la identidad se realizará mediante consulta a la fuente oficial correspondiente.

Izenpe verifica que el nombre y la dirección postal de la organización suscriptora del certificado incorporados a la solicitud de este coinciden con el nombre y dirección inscritos formalmente en los registros consultados según se describe en los apartados anteriores.

– En el caso de certificados SSL cualificados,

Izenpe verifica la existencia, la dirección y la identidad de la organización, en función del tipo de organización.

- Cuando el suscriptor sea una organización perteneciente al sector privado, Izenpe verificará su dirección e identidad, mediante consulta al Registro oficial correspondiente.

- Caso de entidades de carácter público, verificación realizada mediante consulta al Boletín Oficial correspondiente y otros registros consultados.

- Si la naturaleza del suscriptor fuera distinta de los dos casos anteriores, las verificaciones relativas a la existencia, dirección y la identidad se realizará mediante consulta a la fuente oficial correspondiente.

Las fuentes de comprobación que Izenpe empleará en estos casos, son las que se incluyen a continuación:

Versión: 2

Fecha:13/10/2023

REGISTROS OFICIALES		JURISDICTION		
DESCRIPCION	**URL**	**COUNTRY**	**PROVINCE**	**LOCALITY**
BOPV	https://www.euskadi.eus/y22-bopv/es/bopv2/datos/Ultimo.shtml	ES	EUSKADI	
BOLETIN OFICIAL GENERALITAT DE CATALUNYA	https://dogc.gencat.cat/es/inici/index.html	ES	CATALUNYA	
REGISTRO ENTIDADES LOCALES DEL PAIS VASCO	https://www.euskadi.eus/registro-de-entidades-locales/web01-a2tokiad/es/	ES	EUSKADI	

Mº JUSTICIA 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 ENTES PÚBLICOS	https://www.hacienda.gob.es/es-ES/CDI/Paginas/Inventario/Inventario.aspx	ES		
BANCO DE ESPAÑA	www.bde.es	ES		
BOLETIN OFICIAL DEL ESTADO	https://www.boe.es/buscar/boe.php	ES		
BOLETIN OFICIAL DE BIZKAIA	https://apps.bizkaia.eus/BT00/	ES	BIZKAIA	
BOLETIN OFICIAL DE GIPUZKOA	https://egoitza.gipuzkoa.eus/es/bog	ES	GIPUZKOA	
BOLETIN OFICIAL DE ARABA/ALAVA	https://www.araba.eus/botha/	ES	ALAVA/ARABA	
BOLETIN OFICIAL DEL PAIS VASCO	https://www.euskadi.eus/y22-bopv/es/p43aBOPVWebWar/buscarAvanzada.do?idioma=es&tipoBusqueda=2	ES	EUSKADI	
REGISTRO ASOCIACIONES DEL PAIS VASCO	https://www.euskadi.eus/registro-asociaciones-buscador/web01-a2aderre/es/	ES	EUSKADI	

Izenpe verifica que el nombre, dirección y número de identificación fiscal de la organización suscriptora del certificado incorporados a la solicitud de este coinciden con el nombre, dirección y número de identificación fiscal inscritos formalmente en los registros consultados según se describe en los apartados anteriores.

Izenpe cumplirá con los requisitos definidos por la entidad CA/Browser Forum en su "guía para la expedición y gestión de Certificados de Validación Extendida" y que pueden consultarse en la dirección https://cabforum.org/extended-validation/

3.2.2.2 Nombre comercial o marca registrada

Si la información de la identidad del sujeto incluye un nombre comercial o marca registrada, Izenpe utilizará los mismos procedimientos y criterios de verificación que en la Sección 3.2.2.1 para verificar el derecho del Solicitante a usar el nombre comercial o marca registrada.

En el caso de Certificados SSL cualificados, se requiere una verificación de identidad exhaustiva según se define en la sección 11.3 de CABForum en su "guía para la expedición y gestión de Certificados de Validación Extendida.

3.2.2.3 Verificación del país

El país se verificará utilizando cualquiera de los métodos indicados en la Sección 3.2.2.1

3.2.2.4 Validación de la autorización y control sobre el dominio

Para validar el dominio de los certificados de autenticación de sitios web, Izenpe utiliza alguno de los siguientes métodos descritos en el documento CA/Browser Forum's Baseline Requirements:

- ✓ 3.2.2.4.2 Email to Domain Contact
- ✓ 3.2.2.4.4 Constructed Email to Domain Contact
- ✓ 3.2.2.4.7 DNS Change
- ✓ 3.2.2.4.14 Email to DNS TXT Contact
- ✓ 3.2.2.4.18 Agreed-Upon Change to Website v2

Para cada uno de los métodos empleados, Izenpe seguirá un proceso documentado y mantendrá registros que indiquen los métodos empleados para cada emisión. El resto de los métodos descritos en CA/Browser Forum's Baseline Requirements no se emplea para la validación de dominios.

a) Email al contacto del dominio (BR 3.2.2.4.2): Izenpe envía al solicitante un código único y aleatorio por correo electrónico a cualquiera de las direcciones que aparecen en el contacto de whois (Registrant, administrativo o técnico). La respuesta debe incluir el número aleatorio.

   Cada correo electrónico puede confirmar el control de varios nombres de dominio.

   Izenpe puede reenviar el correo electrónico en su totalidad, incluida la reutilización del código aleatorio, siempre que el contenido completo de la comunicación y los destinatarios se mantengan vigentes.

   Izenpe proporcionará un código aleatorio exclusivo para la solicitud del certificado y no utilizará el código aleatorio después de 30 días.

b) Email Construido al contacto del dominio (BR 3.2.2.4.4).

Se enviará un email con un código aleatorio a alguna o todas las siguientes direcciones de correo direcciones “admin”,”administrator”, “webmaster”, “hostmaster” o “postmaster” del dominio solicitado.

c) Cambio acordado en DNS (BR 3.2.2.4.7): El solicitante realiza un cambio en el registro DNS del dominio para el que peticiona el certificado SSL. El solicitante debe añadir el código aleatorio y único enviado por Izenpe en un campo CNAME, TXT o CAA, en su registro DNS. Una vez realizado el cambio por parte del solicitante, Izenpe lo verifica.

Izenpe proporcionará un código aleatorio exclusivo para la solicitud del certificado y no utilizará el código aleatorio después de 30 días.

Izenpe proporcionará un código aleatorio exclusivo para la solicitud del certificado y no utilizará el código aleatorio después de 30 días.

d) Email a 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 DNS TXT. Deberá existir una entrada en el subdominio “_validation-contactemail” de tipo TXT con una dirección de email:

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

Izenpe proporcionará un código aleatorio exclusivo para la solicitud del certificado y no utilizará el código aleatorio después de 30 días.

e) Cambio acordado en sitio web (BR 3.2.2.4.18): El solicitante debe publicar en la ruta "/.well-known/pki-validation" el fichero con un código aleatorio y único enviado por Izenpe. Una vez realizado el cambio por parte del solicitante, Izenpe lo verifica.

Izenpe confirma que el representante del suscriptor posee el control sobre los nombres completos de los dominios o FQDN (siglas en inglés de Fully Qualified Domain Name) que son incorporados a los certificados de autenticación de sitio web que expide. Para ello, Izenpe consulta, a través de la aplicación que registra las solicitudes de estos certificados, la identidad del representante del suscriptor y el nombre del citado FQDN. A continuación, verifica que la solicitud proviene del contacto que tiene el control sobre dicho dominio (según los métodos definidos en el apartado anterior) o tiene autorización por parte de este. Adicionalmente se comprueba que la solicitud del certificado ha sido realizada con posterioridad al alta en dichos registros.

Adicionalmente, antes de la emisión de un certificado de autenticación de sitio web, se verifica que el dominio a incluir en el certificado es público (no es un dominio interno) y se consulta a registros púbicos para verificar que no es un dominio de alto riesgo (Google Safe Browsing).

3.2.2.5 Autenticación para una dirección IP

Izenpe no emite certificados para identificar direcciones IP.

3.2.2.6 Validación de dominio Wildcard

La RA, verificará que todo el espacio de nombres de dominio en los Certificados Wildcard OV es controlado legítimamente por el Suscriptor.

Si en un certificado wildcar el asterisco estuviera dentro de la etiqueta inmediatamente a la izquierda de un sufijo público o un registro controlado, Izenpe rechazará la emisión de dicho certificado a menos que el solicitante demuestre el control legítimo de todo el espacio de nombres de dominio. Para ello consultará la “Public Suffix List” disponible en https://publicsuffix.org/, que se descargará periódicamente.

3.2.2.7 Fiabilidad de las fuentes de datos

Antes de utilizar cualquier fuente de datos como fuente de datos confiable, la RA evaluará la fuente en cuanto a su confiabilidad, precisión y resistencia a la alteración o falsificación.

3.2.2.8 Registro CAA

Previa a la emisión de todo certificado SSL, Izenpe valida la existencia de un registro CAA para cada nombre DNS de las extensiones CN y subjectAltName del certificado, según especificaciones de la RFC 6844. En el caso de que se emita el certificado, la validación se realizará antes del TTL del registro CAA, y en cualquier caso no superior a 8 horas. Izenpe procesa los tags "issue" e "issuewild".

Los registros CAA que identifican a dominios para los que se autoriza la emisión por parte de Izenpe son "izenpe.com" e "izenpe.eus".

3.2.3. Autenticación de la identidad de la persona física solicitante

Izenpe comprueba que el representante del suscriptor coincide con la persona física que solicita un certificado de autenticación de sitios web, mediante la firma electrónica del formulario de solicitud utilizando un Certificado cualificado de firma electrónica, garantizando así la autenticidad de su identidad.

En el caso de certificados DV u OV el representante del suscriptor puede delegar la capacidad de solicitud en solicitantes autorizados. El representante debe firmar electrónicamente esta delegación a través de la aplicación de gestión de certificados SSL.

3.2.4. Información no verificada del Suscriptor

Toda la información incorporada al certificado electrónico es verificada por la Autoridad de Registro, por tanto, no se incluye información no verificada en el campo “Subject” de los certificados expedidos.

3.2.5. Validación de la capacidad de representación

Izenpe verifica que el solicitante tiene suficiente capacidad de representación mediante la firma electrónica del formulario de solicitud de alta de cliente, según se describe en el apartado 3.2.3 de esta política, aceptando el uso de un certificado de Representante de Izenpe Cuando el citado formulario se firma mediante un certificado cualificado diferente de los mencionados en el apartado anterior la RA de Izenpe comprueba la facultad de representación del firmante de la solicitud mediante consulta a registros oficiales (Registro Mercantil, Boletines Oficiales, etc. en función de la naturaleza de la representación). Si del resultado de estas consultas no se obtuvieran evidencias de representación suficiente, Izenpe se pondrá en contacto con el suscriptor para recabar dichas evidencias.

A través de la aplicación online de solicitud de certificados SSL, el representante de la entidad podrá crear los usuarios asociados a los que permita la solicitud de certificados DV y OV para dicha entidad.

Para las solicitudes de certificados SSL cualificados, Izenpe cumplirá con los requisitos definidos por la entidad CA/Browser Forum en su "guía para la expedición y gestión de Certificados de Validación Extendida" (apartados 11.8 y 11.11).

3.2.6. Criterios de interoperación

No existen relaciones de interactividad con Autoridades de Certificación externas a Izenpe.

3.3. Identificación y autenticación para peticiones de renovación de claves

3.3.1. Identificación y autenticación para renovación rutinaria de claves

Los suscriptores de los certificados deberían solicitar la renovación de los mismos antes de que expire su período de vigencia. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado de esta CP correspondiente al proceso de renovación de Certificados (véase apartado 4.6 del presente documento).

La vigencia de la entidad y competencia del solicitante no será requerida en caso de haber sido comprobada por Izenpe en los últimos 13 meses.

3.3.2. Identificación y autenticación para renovación de claves después de una revocación

El proceso de renovación del certificado tras la revocación del mismo será el mismo que el que se sigue en la emisión inicial del mismo.

3.4. Identificación y autenticación para peticiones de revocación

Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado 4.9 del presente documento.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. Solicitud de Certificados

4.1.1. Quién puede solicitar un Certificado

Únicamente podrán solicitar certificados de autenticación de sitio web los Representantes del Suscriptor, o personas debidamente autorizados a solicitar el certificado en nombre del suscriptor, que hayan acreditado tener el control sobre el nombre del dominio a incluir en el certificado. El citado control sobre el nombre del dominio será verificado por Izenpe según se describe en el apartado "3.2 Validación inicial de la identidad" de la presente Política.

Adicionalmente, para certificados cualificados, Izenpe cumplirá los requisitos de la sección 11 de la "Guía para la emisión y gestión de Certificados de Validación Extendida" establecidos por la entidad CA/Browser fórum.

4.1.2. Proceso de registro y responsabilidades

Cada solicitante deberá presentar una solicitud de certificado y la información requerida antes de emitir un certificado.

El proceso de registro incluye las siguientes fases:

- ✓ Envío de la solicitud de emisión y aceptación de los términos y condiciones aplicables.

  Con esta aceptación, los suscriptores garantizan que toda la información contenida en la solicitud de certificado es correcta.
- ✓ Envío de la petición técnica (PKCS#10).
- ✓ Pago, en su caso, de las tarifas aplicables.

La RA de Izenpe verificará la organización suscriptora y del representante del Suscriptor, y comprueba que la solicitud del Certificado es correcta completa y debidamente autorizada, de conformidad con los requisitos definidos en el apartado "3.2 Validación inicial de la identidad" del presente documento. Izenpe podrá realizar comprobaciones adicionales a los procesos de validación descritos en el citado apartado.

Izenpe recopilará y custodiará las evidencias correspondientes a las comprobaciones realizadas

El apartado 9.6 "Obligaciones y garantías" del presente documento establece las responsabilidades de las partes en este proceso.

4.2. Procedimiento de solicitud de certificados

4.2.1. Realización de las funciones de identificación y autenticación

El Representante del Suscriptor remitirá a la RA de Izenpe un formulario firmado electrónicamente con un certificado electrónico cualificado, que recoge toda la información a incorporar en el certificado de autenticación de sitio web. A partir de dicha información, la RA de Izenpe llevará a cabo las comprobaciones descritas en el apartado "3.2 Validación inicial de la identidad" de la presente Política.

Izenpe comprobará la veracidad de los datos incluidos en la solicitud y, en su caso, la capacidad del representante a través de las verificaciones correspondientes, conservando las evidencias oportunas.

La firma electrónica generada para la suscripción del contrato será verificada por Izenpe.

El empleo de los datos o la documentación de validación previa, obtenidos de una fuente de las especificadas en la sección 3.2, no se puede utilizar más de 12 meses después de la validación de dichos datos o documentación.

4.2.2. Aprobación o rechazo de la solicitud del certificado

La RA que actúa en el proceso de expedición de certificados de autenticación de sitios web es siempre el propio Izenpe y, por tanto, no delega la validación de titularidad del dominio a 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, así como la validación del dominio, según se describe en el apartado "3.2 Validación inicial de la identidad" de la presente CP, que darán como resultado la aprobación o el rechazo de la solicitud del mismo.

Izenpe mantiene una base de datos interna de todos los certificados revocados y de todas las solicitudes de certificados rechazadas previamente debido a sospecha de phishing u otro uso fraudulento. Esta información es tenida en cuenta para identificar posteriores solicitudes de certificados sospechosos antes de proceder a la aprobación de la expedición de los mismos.

Adicionalmente, Izenpe desarrolla, mantiene e implementa procedimientos documentados que identifican y requieren actividad de verificación adicional para las solicitudes de certificados de alto riesgo antes de la aprobación de la expedición del certificado, según sea razonablemente necesario para garantizar que dichas solicitudes se verifican adecuadamente según estos requisitos.

Si alguna de estas validaciones no ha podido ser confirmada, Izenpe rechazará la solicitud del certificado, reservándose el derecho de no revelar los motivos de dicha denegación. El Representante del Suscriptor cuya solicitud haya sido rechazada podrá volver a solicitarlo posteriormente.

Cualquier solicitud de certificado OV o certificado cualificado será tramitada por personal de Izenpe con el rol de personal de confianza para tal efecto. El sistema de aprobación de expedición de los certificados cualificados requiere de la acción de al menos dos personas pertenecientes a la RA de Izenpe con rol de confianza, uno para validar la solicitud y otro para aprobarla.

Adicionalmente, Izenpe comprueba si hay un registro CAA para cada nombre de dominio que incluye en un certificado de autenticación de sitios web emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento establecidas en RFC 8659 para cualquier registro encontrado. Si existe dicho Registro CAA, no emitirá dicho Certificado a menos que determine que la solicitud del Certificado es consistente con el conjunto de registro de recursos CAA aplicable.

4.2.3. Tiempo en procesar la solicitud

El plazo de tiempo en procesar la solicitud de un certificado depende en gran medida de que el Representante del Suscriptor proporcione la información y la documentación necesarias de la forma prevista en los procedimientos aprobados por Izenpe para este fin. No obstante, esta entidad hará el esfuerzo necesario para que el proceso de validación que dará como resultado la aceptación o el rechazo de la solicitud no exceda de 5 días hábiles.

Este periodo de tiempo podrá, ocasionalmente, ser superado por motivos fuera del control de Izenpe. En estos casos, hará lo posible por mantener informado al Representante del Suscriptor que realizó la solicitud de las causas de tales retrasos.

4.3. Emisión del certificado

4.3.1. Acciones de la CA durante la emisión

Una vez aprobada la solicitud del Certificado por parte de la RA de Izenpe, el sistema de generación de certificados cuenta con una serie de controles, previos a la emisión del certificado que verifican el cumplimiento de requisitos de la RFC 5280 y CA/Browser Forum (BRs and EVGs). Tras esta verificación se procede a expedir el Certificado conforme al perfil aprobado para cada tipo de Certificado.

Así mismo, Izenpe monitoriza periódicamente posibles desviaciones en los certificados emitidos.

Los procesos relativos a la emisión de Certificados electrónicos garantizan que todas las cuentas que intervienen en los mismos tienen autenticación multi-factor.

4.3.2. Notificación de emisión de certificado

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

4.4. Aceptación del certificado

4.4.1. Proceso de aceptación

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

4.4.2. Publicación del certificado por la CA

Los Certificados generados son almacenados en un repositorio seguro de Izenpe.

4.4.3. Notificación de la emisión a otras entidades

Antes de la expedición de Certificados de autenticación de sitio web se envía un pre-certificado a los registros del servicio Certificate Transparency de aquellos proveedores con los que Izenpe mantiene un acuerdo para tal fin.

4.5. Par de claves y uso del certificado

4.5.1. Clave privada del suscriptor y uso del certificado

Izenpe no genera ni almacena las claves privadas asociadas a los Certificados expedidos bajo la presente Política de Certificación. Corresponde la condición de custodio y el control de las claves del certificado a los Representantes del Suscriptor que hayan acreditado tener el control sobre el nombre del dominio a incluir en el certificado. Por tanto, la clave privada asociada a la clave pública estará bajo la responsabilidad de dicho custodio.

4.5.2. Uso del certificado y la clave pública por terceros que confían

Las entidades usuarias y terceros que confían utilizarán software que sea compatible con los estándares aplicables al uso de Certificados electrónicos (X.509, IETF, RFCs…). Si la conexión al sitio web requiriese de adicionales medidas de aseguramiento, dichas medidas han de ser obtenidas por las entidades usuarias.

Los terceros que confían en el establecimiento de una conexión segura garantizada por un Certificado de autenticación de sitios web deben cerciorarse de que dicha conexión fue creada durante el periodo de validez del Certificado, que dicho Certificado está siendo usado con el propósito para el que se expidió de acuerdo con la presente CP, así como verificar que en ese momento el Certificado está activo, mediante la comprobación de su estado de revocación en la forma y condiciones que se expresan en el apartado "4.10 Servicios de información del estado de los certificados" del presente documento.

4.6. Renovación del certificado

4.6.1. Circunstancias para la renovación del certificado

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

4.6.2. Quién puede solicitar la renovación del certificado

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

4.6.3. Procesamiento de solicitudes de renovación del certificado

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

4.6.4. Notificación de la renovación del certificado

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

4.6.5. Conducta que constituye la aceptación de la renovación del certificado

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

4.6.6. Publicación del certificado renovado

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

4.6.7. Notificación de la renovación del certificado a otras entidades

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

4.7. Renovación con regeneración de las claves del certificado

La renovación con regeneración de claves de los certificados de autenticación de sitios web se realiza siempre emitiendo nuevas claves públicas y privadas, siguiendo el mismo proceso que el descrito para la emisión de un Certificado nuevo.

4.7.1. Circunstancias para la renovación con regeneración de claves

Las claves de los certificados se renovarán bajo los siguientes supuestos:

- ✓ Por caducidad próxima de las actuales claves a petición del solicitante de la renovación.
- ✓ Por compromiso de las claves u otra circunstancia de las recogidas en el apartado "4.9 Revocación y suspensión del certificado" de la presente CP.

4.7.2. Quién puede solicitar la renovación con regeneración de claves

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

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

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

4.7.4. Notificación de la renovación con regeneración de claves

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

4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves

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

4.7.6. Publicación del certificado renovado

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

4.7.7. Notificación de la renovación con regeneración de claves a otras entidades

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

4.8. Modificación del certificado

No es posible realizar modificaciones de los Certificados expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo Certificado.

4.8.1. Circunstancias para la modificación del certificado

No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

No se estipula la modificación.

4.8.5. Conducta que constituye la aceptación de la modificación del certificado

No se estipula la modificación.

4.8.6. Publicación del certificado modificado

No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

No se estipula la modificación.

4.9. Revocación y suspensión del certificado

Los certificados de autenticación de sitios web emitidos por Izenpe quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del certificado.

b) Cese en la actividad como Prestador de Servicios de Confianza de Izenpe, salvo que, previo consentimiento expreso del suscriptor, los certificados expedidos por Izenpe hayan sido transferidos a otro Prestador de Servicios de Confianza.

   En los casos a) y b), la pérdida de eficacia de los certificados tendrá lugar desde que estas circunstancias se produzcan.

c) Revocación del certificado por cualquiera de las causas recogidas en el presente documento.

La extinción de la vigencia del certificado surtirá efectos desde la fecha en que Izenpe tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo haga constar en su Servicio de información y consulta sobre el estado de los certificados.

Izenpe pone a disposición de los suscriptores, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de incidencias@izenpe.eus, para permitirles reportar cualquier asunto relacionado con este tipo de certificados, en cuanto a un supuesto compromiso de Clave Privada, uso indebido de los Certificados u otros tipos de fraude, compromiso, mal uso o conducta inapropiada.

Izenpe, como Prestador de Servicios de Confianza, se reserva el derecho de no expedir 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, conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o sedes electrónicas que se desean proteger con tales certificados, o su uso se presta a engaño o confusión sobre la titularidad de tales aplicaciones, sitios web o Sedes electrónicas y, por tanto, de sus contenidos.

Izenpe se mantendrá indemne por parte de los titulares o responsables de los equipos, aplicaciones, sitios web o sedes electrónicas que incumplan lo previsto en este apartado y que tengan relación con el certificado, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales certificados.

4.9.1. Circunstancias para la revocación

4.9.1.1 Causas de revocación de un Certificado de entidad final

Adicionalmente a lo previsto en el apartado anterior, serán causas de revocación de un certificado de autenticación de sitios web:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

   - La pérdida del soporte del certificado.
   - La utilización por un tercero de la clave privada asociada al certificado.
   - La violación o puesta en peligro del secreto de la clave privada asociada al certificado.
   - La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas Declaraciones de Prácticas de Certificación, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción, disolución o cierre del sitio web identificado por el certificado.

d) Extinción o disolución de la personalidad jurídica del suscriptor.

e) Terminación de la forma de representación del representante del suscriptor del certificado.

f) Incapacidad sobrevenida, total o parcial, del representante del Suscriptor.

g) Inexactitudes en los datos aportados por el Representante del Suscriptor para la obtención del certificado, o alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, de manera que éste ya no fuera conforme a la realidad.

h) Contravención de una obligación sustancial de esta Declaración de Prácticas de Certificación por parte del suscriptor, del representante del suscriptor o de una Entidad de Registro si, en este último caso, hubiese podido afectar al procedimiento de emisión del Certificado.

i) Utilizar el certificado con el propósito de generar dudas a los usuarios sobre la procedencia de los productos o servicios ofertados, haciendo ver que su origen es distinto del realmente ofertado. Para ello, se seguirán los criterios sobre actividad infractora de las normas sobre consumidores y usuarios, comercio, competencia y publicidad.

j) Resolución del contrato suscrito entre el suscriptor o su Representante, e Izenpe, o el impago de los servicios prestados.

k) Violación o puesta en peligro del secreto de los datos de creación de firma / sello de Izenpe, con los que firma / sella los certificados que emite.

l) Incumplimiento de los requisitos definidos por los esquemas de auditorías a los que se somete la Autoridad de Certificación que expide los certificados cubiertos por la presente Política, con especial atención a los de algoritmia y tamaños de clave, que supongan un riesgo inaceptable por parte de las partes que confían en estos Certificados.

En ningún caso se debe entender que Izenpe asume obligación alguna de comprobar los extremos mencionados en las letras c) a i) del presente apartado.

Izenpe únicamente será responsable de las consecuencias que se desprendan de no haber revocado un Certificado en los siguientes supuestos:

- Que la revocación le haya sido solicitada por el Representante del Suscriptor siguiendo el procedimiento establecido para este tipo de Certificados.

- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el Suscriptor.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que en las causas c) a g) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del Solicitante de la revocación.

Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento Izenpe que se realicen sobre los datos o el Certificado, las inexactitudes sobre los datos o falta de diligencia en su comunicación a Izenpe, producirán la exoneración de responsabilidad de Izenpe.

Todas las solicitudes de revocación de certificados de entidad final, son procesadas en el plazo máximo de 24 horas desde la recepción de la misma.

4.9.1.2 Causas de revocación de un Certificado de CA subordinada

En el caso de certificados de CAs subordinadas, éstas se revocarán en un plazo máximo de 7 días por las siguientes causas:

a) La subCA lo solicita por escrito

b) La subCA notifica a la CA emisora que la petición de certificado original no fue autorizada y no admite una autorización retroactiva

c) La CA emisora obtiene una evidencia de que la clave privada de la subCA correspondiente a la clave pública del certificado ha sufrido un compromiso de clave o ha dejado de cumplir con los requisitos de los apartados 6.1.5 y 6.1.6 de los BR

d) La CA emisora obtiene una evidencia de que el certificado fue emitido de forma incorrecta

e) La CA emisora detecta que el certificado no fue emitido de acuerdo con la Política de Certificado o la DPC

f) La CA emisora determina que algún dato que aparece en el certificado es impreciso o incorrecto

g) La CA emisora o la subCA cesa sus operaciones por cualquier razón y no se ha habilitado los acuerdos con otra CA para proporcionar el servicio de revocación

h) El derecho para emitir certificados por parte de la CA emisora o la subCA bajo los requisitos de BR finalizan o se revoca, a menos que la CA emisora haya habilitado los acuerdos para continuar manteniendo el repositorio de CRL/OCSP

i) Se requiere la revocación por parte de la política de la CA emisora y/o por la DPC

j) El contenido o formato técnico del certificado presenta un riesgo inaceptable para los proveedores de software o terceros

k) Proveedores o terceras partes (ej: el CA/Browser Forum podría determinar que un algoritmo/firma criptográfico o tamaño de clave presenta un riesgo inaceptable y que dichos certificados deberían ser revocados y reemplazados en un periodo concreto de tiempo)

4.9.2. Quién puede solicitar la revocación

La CA, la RA y los Suscriptores puede iniciar la revocación de un certificado

La revocación de un Certificado de autenticación de sitios web solamente podrá ser solicitada por la persona con facultades de representación del Suscriptor al que se ha expedido el Certificado.

Adicionalmente, estarán legitimados para solicitar la revocación de dicho certificado:

- El órgano directivo, organismo o entidad suscriptora del certificado o persona en quien delegue.
- La Oficina de Registro, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad de derecho público, Suscriptora del Certificado a revocar, cuando detecte que alguno de los datos consignados en el certificado
  - ✓ es incorrecto, inexacto o haya variado respecto a lo consignado en el Certificado, o
  - ✓ la persona física, custodio del Certificado, no se corresponda con el responsable máximo o designado para la gestión y administración de la dirección electrónica consignada en el Certificado objeto de la revocación

  siempre en el marco de los términos y condiciones aplicables a la revocación de este tipo de Certificados.

Adicionalmente, los suscriptores, las partes confiables, los proveedores de software de aplicaciones y otros terceros pueden informar a la CA emisora de una causa razonable para revocar el certificado, enviando un Informe de incidencia con un certificado.

No obstante, Izenpe podrá revocar de oficio los Certificados de autenticación de sitios web en los supuestos recogidos en la presente Declaración de Prácticas y Políticas de Certificación.

Además, en el caso de los certificados regulados en esta documentación específica Izenpe,

1. Presentará al suscriptor, a terceras partes y a los navegadores de Internet, instrucciones claras para la presentación de denuncias o sospechas de compromiso de la clave privada, de mal uso de certificados o de otros tipos de fraude, compromiso, mal uso, o conducta impropia en relación con los certificados.

2. Investigará los informes de problemas dentro de las veinticuatro horas siguientes a su recepción y decidirá sobre la revocación, atendiendo a los siguientes criterios:

   - La naturaleza del supuesto problema;
   - El número de informes recibidos de problemas de un certificado o página web.
   - La identidad de los denunciantes.
   - La legislación vigente.

4.9.3. Procedimiento de solicitud de la revocación

El solicitante de la revocación tramitará ante Izenpe la solicitud de revocación. En el caso de que la revocación fuera solicitada por persona distinta del solicitante, del suscriptor o del poseedor de claves, de forma previa o simultánea a la revocación, Izenpe comunicará al poseedor de claves y al suscriptor del certificado la revocación de su certificado y la causa por la que se ha llevado a cabo.

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

- Presencialmente ante,
    - Izenpe solicitando cita previa a través de www.izenpe.eus
    - O ante la organización suscriptora con la que Izenpe haya suscrito el instrumento legal pertinente.
- Online, en la dirección www.izenpe.eus

- Por correo electrónico, enviando el formulario de solicitud de revocación firmado con el DNI electrónico o un certificado cualificado expedido por Izenpe.

La solicitud de revocación autenticada, así como la información que justifica la revocación, es registrada y archivada.

Una vez que Izenpe ha procedido a la revocación del certificado de autenticación de sitios web, se publicará en el Directorio seguro la correspondiente Lista de Certificados Revocados, conteniendo el número de serie del Certificado revocado, así como la fecha, hora y la causa de revocación. El Representante del Suscriptor recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación del cambio de estado de vigencia del Certificado.

4.9.4. Periodo de gracia de la solicitud de revocación

No existe periodo de gracia asociado a este proceso, pues la revocación se realiza de forma inmediata a la recepción verificada de la solicitud de revocación.

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

Todas las solicitudes de revocación de certificados de entidad final, son procesadas en el plazo máximo de 24 horas desde el acuse de recepción de la misma.

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

4.9.6. Obligación de verificar las revocaciones por las partes que confían

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

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

4.9.7. Frecuencia de generación de CRLs

Izenpe emite con carácter inmediato una Lista de Revocación de Certificados (en adelante CRL) desde el momento en que se produce una revocación.

Se indica en la CRL el momento programado de emisión de una nueva CRL, si bien se podrá emitir una CRL antes del plazo indicado en la CRL anterior. Si no se producen revocaciones la Lista de Revocación de Certificados se regenera diariamente.

La CRL de los certificados de entidad final se emiten al menos cada 24 horas, o cuando se produzca una revocación, con una validez de 10 días.

La CRL de los certificados de las CAs (ARLs) se emite cada 12 meses o cuando se produzca una revocación.

Los certificados revocados que expiren son retirados de la CRL. A partir de ese momento se mantendrá la constancia de la revocación en el registro interno de Izenpe por un periodo de 15 años.

4.9.8. Periodo máximo de latencia de las CRLs

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

4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados

Izenpe proporciona a las Entidades Usuarias un servicio de verificación en tiempo real de certificados mediante el protocolo OCSP (Online Certificate Status Protocol), de forma que las aplicaciones usuarias verificarán el estado del certificado.

Este servicio está disponible 24 horas al día por 7 días a la semana.

4.9.10. Requisitos de comprobación en línea de la revocación

La utilización del servicio de CRLs, de libre acceso, requerirá,

- ✓ Comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión “CRL Distribution Point”.
- ✓ Comprobar por el usuario, adicionalmente, la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.
- ✓ Por el usuario asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.

Los certificados revocados que expiren serán retirados de la CRL, sin embargo, se seguirá ofreciendo información del estado del certificado a través de la comprobación online, independientemente de que esté caducado.

La utilización del servicio de OCSP, de libre acceso, requerirá:

- ✓ Comprobar la dirección URL contenida en el propio certificado en la extensión “Authority Info Access”.
- ✓ Que el usuario se asegure que la respuesta esté firmada por la CA que ha emitido el certificado que quiere validar.

4.9.11. Otras formas de aviso de revocación disponibles

Izenpe envía un email informativo al suscriptor del certificado cuando se produce la revocación de un certificado.

4.9.12. Requisitos especiales de revocación de claves comprometidas

No existen requisitos especiales para el caso de revocación de certificados causada por un compromiso de claves, siendo de aplicación lo descrito para el resto de las 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 la petición de la suspensión

No se contempla la suspensión de certificados.

4.9.16. Límites sobre el periodo de suspensión

No se contempla la suspensión de certificados.

4.10. Servicios de información del estado de los certificados

4.10.1. Características operativas

El funcionamiento del Servicio de información y consulta del estado de los certificados es el siguiente: el servidor OCSP recibe la petición OCSP efectuada por un Cliente OCSP y comprueba el estado de vigencia de los certificados incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los Certificados incluidos en la petición. Dicha respuesta es firmada / sellada con los Datos de Creación de Firma / Sello de Izenpe garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los Certificados consultados.

Será responsabilidad de la Entidad usuaria contar con un Cliente OCSP para operar con el servidor OCSP puesto a disposición por Izenpe.

Izenpe opera y mantiene sus capacidades de mantenimiento de sus CRL y servicio OCSP con recursos suficientes para proporcionar un tiempo de respuesta suficiente bajo condiciones normales de operación.

4.10.2. Disponibilidad del servicio

Izenpe proporciona a las Entidades Usuarias un servicio de revocación de 24x7 (24 horas al día por 7 días a la semana).

4.10.3. Características opcionales

No estipuladas.

4.11. Finalización de la suscripción

El certificado no es válido para su uso una vez finalizado el periodo de vigencia o cuando ha sido revocado.

En la Política específica se indica la caducidad de cada certificado.

4.12. Custodia y recuperación de claves

4.12.1. Prácticas y políticas de custodia y recuperación de claves

Izenpe no genera las claves privadas de los certificados de autenticación de sitios web y, por tanto, no las custodia ni puede recuperarlas.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DE PERSONAL

5.1. Controles de Seguridad Física

5.1.1. Ubicación de las instalaciones

Véase el apartado correspondiente en la DPC

5.1.2. Acceso Físico

Véase el apartado correspondiente en la DPC

5.1.3. Electricidad y Aire Acondicionado

Véase el apartado correspondiente en la DPC

5.1.4. Exposición al agua

Véase el apartado correspondiente en la DPC

5.1.5. Prevención y Protección contra incendios

Véase el apartado correspondiente en la DPC

5.1.6. Almacenamiento de Soportes

Véase el apartado correspondiente en la DPC

5.1.7. Eliminación de Residuos

Véase el apartado correspondiente en la DPC

5.1.8. Copias de Seguridad fuera de las instalaciones

Véase el apartado correspondiente en la DPC

5.2. Controles de Procedimiento

5.2.1. Roles de Confianza

Véase el apartado correspondiente en la DPC

5.2.2. Número de personas por tarea

Véase el apartado correspondiente en la DPC

5.2.3. Identificación y autenticación para cada rol

Véase el apartado correspondiente en la DPC

5.2.4. Roles que requieren segregación de funciones

Véase el apartado correspondiente en la DPC

5.3. Controles de Personal

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

Véase el apartado correspondiente en la DPC

5.3.2. Procedimientos de verificación de antecedentes

Véase el apartado correspondiente en la DPC

5.3.3. Requisitos de formación

Véase el apartado correspondiente en la DPC

5.3.4. Requisitos y frecuencia de actuación formativa

Véase el apartado correspondiente en la DPC

5.3.5. Secuencia y frecuencia de rotación laboral

Véase el apartado correspondiente en la DPC

5.3.6. Sanciones por acciones no autorizadas

Véase el apartado correspondiente en la DPC

5.3.7. Requisitos de contratación de personal

Véase el apartado correspondiente en la DPC

5.3.8. Suministro de documentación al personal

Véase el apartado correspondiente en la DPC

5.4. Procedimientos de auditoría

5.4.1. Tipos de eventos registrados

Véase el apartado correspondiente en la DPC

5.4.2. Frecuencia de procesamiento de registros

Véase el apartado correspondiente en la DPC

5.4.3. Periodo de conservación de los registros

Véase el apartado correspondiente en la DPC

5.4.4. Protección de los registros

Véase el apartado correspondiente en la DPC

5.4.5. Procedimientos de copias de seguridad de los registros auditados

Véase el apartado correspondiente en la DPC

5.4.6. Sistemas de recolección de registros

Véase el apartado correspondiente en la DPC

5.4.7. Notificación al sujeto causante de los eventos

Véase el apartado correspondiente en la DPC

5.4.8. Análisis de vulnerabilidades

Véase el apartado correspondiente en la DPC

5.5. Archivado de registros

5.5.1. Tipos de registros archivados

Véase el apartado correspondiente en la DPC

5.5.2. Periodo de retención del archivo

Véase el apartado correspondiente en la DPC

5.5.3. Protección del archivo

Véase el apartado correspondiente en la DPC

5.5.4. Procedimientos de copia de respaldo del archivo

Véase el apartado correspondiente en la DPC

5.5.5. Requisitos para el sellado de tiempo de los registros of Records

Véase el apartado correspondiente en la DPC

5.5.6. Sistema de archivo

Véase el apartado correspondiente en la DPC

5.5.7. Procedimientos para obtener y verificar la información archivada

Véase el apartado correspondiente en la DPC

5.6. Cambio de claves de la CA

Véase el apartado correspondiente en la DPC

5.7. Gestión de incidentes y vulnerabilidades

5.7.1. Gestión de incidentes y vulnerabilidades

Véase el apartado correspondiente en la DPC

5.7.2. Actuación ante datos y software corruptos

Véase el apartado correspondiente en la DPC

5.7.3. Procedimiento ante compromiso de la clave privada de la CA

Véase el apartado correspondiente en la DPC

5.7.4. Continuidad de negocio después de un desastre

Véase el apartado correspondiente en la DPC

5.8. Cese de la actividad del Prestador de Servicios de Confianza

Véase el apartado correspondiente en la DPC

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación de las Claves

6.1.1. Generación del par de claves

6.1.1.1 Generación del par de Claves de la CA

Véase el apartado correspondiente en la DPC

6.1.1.2 Generación del par de Claves de la RA

No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

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

6.1.2. Envío de la clave privada al suscriptor

No existe ninguna generación ni entrega de la clave privada al Titular por parte de la CA.

6.1.3. Envío de la clave pública al emisor del certificado

La Clave pública, generada junto a la Clave privada sobre el dispositivo de generación y custodia de claves, es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

6.1.4. Distribución de la clave pública de la CA a las partes que confían

Las claves públicas de las CA de IZENPE se distribuyen a través de varios medios, entre ellos la web de IZENPE www.izenpe.eus. En la DPC, apartados 1.3.1.1 y 1.3.1.2, se publican además las diferentes huellas de las CAs raíces y CAs emisoras.

6.1.5. Tamaños de claves y algoritmos utilizados

El algoritmo usado en todos los casos es el RSA con SHA2.

En cuanto al tamaño de las claves, dependiendo de cada caso, es:

- Claves de la CA raíz: RSA 4096 bits.
- Claves de las CA Subordinadas: RSA 4096 bits.
- Claves de los Certificados de autenticación de sitios web: RSA >=2048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

Las Claves públicas de los Certificados de autenticación de sitios web están codificadas de acuerdo con RFC5280 y PKCS#1.

6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3)

Todos los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de la claves.

Las claves de CA raíz se utilizan para firmar los certificados de las CAs subordinadas, las ARLs y el certificado de la TSA. Las claves de las CA subordinadas o emisoras únicamente se utilizan para firmar certificados de usuario final y CRLs.

Los usos admitidos de clave para certificados finales están definidos en documento de perfiles de certificado disponible en www.izenpe.eus.

6.2. Protección de la clave privada y controles de los módulos criptográficos

6.2.1. Estándares para los módulos criptográficos

Véase el apartado correspondiente en la DPC.

6.2.2. Control multi-persona (n de m) de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.3. Custodia de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.4. Copia de seguridad de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.5. Archivado de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.6. Transferencia de la clave privada a/o desde el módulo criptográfico

Véase el apartado correspondiente en la DPC.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

Véase el apartado correspondiente en la DPC.

6.2.8. Método de activación de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.9. Método de desactivación de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.10. Método de destrucción de la clave privada

Véase el apartado correspondiente en la DPC.

6.2.11. Clasificación de los módulos criptográficos

Véase el apartado correspondiente en la DPC.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Los Certificados de autenticación de sitios web y, por tanto, sus Claves públicas asociadas, son conservadas por Izenpe durante el periodo de tiempo exigido por la legislación vigente, que actualmente es de 15 años.

6.3.2. Periodos operativos del certificado y periodos de uso del par de claves

Los periodos de operación de los Certificados y sus Claves asociadas son:

- Certificado de la CA raíz y su par de claves: véase el apartado "1.3.1. Autoridad de Certificación" de la presente CP.
- El Certificado de la CA subordinada que expide los Certificados de autenticación de sitios web y su par de claves: véase el apartado "1.3.1. Autoridad de Certificación" de la presente CP.
- Los Certificados de autenticación de sitios web y su par de claves: el periodo máximo de vigencia es de 398 días.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Véase el apartado correspondiente en la DPC.

6.4.2. Protección de datos de activación

Véase el apartado correspondiente en la DPC.

6.4.3. Otros aspectos de los datos de activación

Véase el apartado correspondiente en la DPC.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

Véase el apartado correspondiente en la DPC.

6.5.2. Evaluación del nivel de seguridad informática

Véase el apartado correspondiente en la DPC.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Véase el apartado correspondiente en la DPC.

6.6.2. Controles de gestión de la seguridad

Véase el apartado correspondiente en la DPC.

6.6.3. Controles de seguridad del ciclo de vida

Véase el apartado correspondiente en la DPC.

6.7. Controles de seguridad de red

Véase el apartado correspondiente en la DPC.

6.8. Fuente de tiempo

Véase el apartado correspondiente en la DPC.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. Perfil del certificado

Los Certificados de autenticación de sitios web son de conformidad con el estándar europeo ETSI EN 319 412-4 “Certificate profile for web site certificates”.

Incluyen los siguientes identificadores de política de CABForum:

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

7.1.1. Número de versión

Los Certificados de autenticación de sitios web son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

En la página https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_def/adjuntos/Perfiles_de_Certificados.pdf se publica el documento que describe el perfil de los Certificados de autenticación de sitios web, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

El identificador de algoritmo (AlgorithmIdentifier) que emplea IZENPE para firmar el certificado es SHA-256/RSA que corresponde al identificador para “Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.”.

7.1.4. Formatos de nombres

La codificación de los Certificados de autenticación de sitios web sigue la recomendación RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. Todos los campos definidos en el perfil de estos Certificados, excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

7.1.5. Restricciones de nombres

Las Cas subordinadas que emiten los certificados bajo la presente CP no están restringidas técnicamente.

7.1.6. Identificador de objeto de política de certificado

El identificador de objeto (OID) de la política del Certificados de autenticación de sitios web es la definida en el apartado "1.2 Nombre del documento e identificación" del presente documento.

7.1.7. Empleo de la extensión restricciones de política

No se emplean restricciones de política.

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión Certificate Policies contiene los siguientes calificadores de política:

- **CPS Pointer**: contiene un puntero a la Declaración de Prácticas de Certificación de IZENPE, http://www.Izenpe.com/cps
- **User notice:** Nota de texto que se despliega en la pantalla, a instancia de una aplicación o usuario, cuando un tercero verifica el certificado.
- **Policy Identifier**: Indica el OID del certificado

User Notice común a todos los certificados (excepto certificados SSL):

USER NOTICE	Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik – Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado

7.1.9. Tratamiento semántico para la extensión "Certificate policy"

La extensión Certificate Policy permite identificar la política que IZENPE asocia al certificado y dónde se pueden encontrar dichas políticas.

7.2. Perfil de la CRL

Los certificados emitidos por IZENPE son conformes a las siguientes normas:

- ✓ Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) Abril 2002

- ✓ Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) Diciembre 2005

- ✓ Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) Agosto 2006.

7.2.1. Número de versión

Versión 2 (populate 54hishin field with integer "1").

7.2.2. CRL y extensiones

Las extensiones utilizadas son las siguientes:

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

7.3. Perfil de OCSP

Las respuestas OCSP de Izenpe son conformes a la norma RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP), y son firmadas por el OCSP Responder cuyo certificado ha sido firmado por la misma CA con la que se emitió el certificado por el que se está consultando.

7.3.1. Número de versión

Versión 2.0

7.3.2. Extensiones del OCSP

Véase el apartado correspondiente en la DPC

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	Si	Sí
5. Enhanced Key usage	Si	Sí

8. AUDITORÍAS DE CUMPLIMIENTO

El sistema de expedición de certificados de autenticación de sitios web es auditado anualmente conforme a,

- Los estándares europeos ETSI EN 319 401 “General Policy Requirements for Trust Service Providers” y ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates”.

- ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”.

Además, el sistema de expedición de certificados es objeto de las siguientes auditorías,

- ✓ Auditoría del Sistema de Gestión de la Seguridad de la Información conforme a UNE-ISO/IEC 27001 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”.

- ✓ Auditoría según lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).

- ✓ Auditoría conforme 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, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD / LOPD-GDD).

También se llevan a cabo análisis de riesgos, de acuerdo a lo dictado en el Sistema de Gestión de la Seguridad de la Información.

8.1. Frecuencia de las auditorías

En el caso de los certificados con la consideración de cualificados la auditoría garantiza adicionalmente el cumplimiento de los requisitos de los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” y ETSI EN 319 412-4 “Certificate profile for web site certificates”.

La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente.

8.2. Cualificación del auditor

Véase el apartado correspondiente en la DPC.

8.3. Relación del auditor con la empresa auditada

Véase el apartado correspondiente en la DPC.

8.4. Elementos objetos de auditoría

Véase el apartado correspondiente en la DPC.

8.5. Toma de decisiones frente a detección de deficiencias

Véase el apartado correspondiente en la DPC.

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, y se decidirán las acciones a adoptar teniendo en cuenta los criterios del apartado 4.9.5 de los BRs.

Además, Izenpe reporta aquellos casos que considere como incidentes (casos de fraude, 57hishing, etc.) en el sitio web del Anti-PhisingWorkGroup (www.apwg.org) y verifica de forma previa a la emisión que el solicitante o representantes no constan en la base de datos interna de incidentes de seguridad de Izenpe. En todo caso se reserva el derecho de emitir certificados ante situaciones sospechosas.

8.6. Comunicación de los resultados

Véase el apartado correspondiente en la DPC.

8.7. Autoevaluación

Véase el apartado correspondiente en la DPC.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. Tarifas

Véase el apartado correspondiente en la DPC.

9.1.1. Tarifas de emisión o renovación de certificados

La determinación de tarifas aplicables a la emisión o renovación de certificados seguirá lo establecido en el apartado “9.1 Tarifas” del presente documento.

9.1.2. Tarifas de acceso a los certificados

No estipulado

9.1.3. Tarifas de acceso a la información de estado o revocación

Izenpe ofrece servicios de información del estado de los certificados a través de CRL y del protocolo OCSP de forma gratuita.

9.1.4. Tarifas para otros servicios

Las tarifas aplicables a otros servicios se aprueban anualmente por el Consejo de Administración de Izenpe.

9.1.5. Política de reembolso

Izenpe no dispone de una política de reembolso.

9.2. Responsabilidad financiera

Véase el apartado correspondiente en la DPC.

9.2.1. Seguro de responsabilidad civil

Véase el apartado correspondiente en la DPC.

9.2.2. Otros activos

Véase el apartado correspondiente en la DPC.

9.2.3. Seguros y garantías para entidades finales

Véase el apartado correspondiente en la DPC.

9.3. Confidencialidad de la información

Véase el apartado correspondiente en la DPC.

9.3.1. Alcance de la información confidencial

Véase el apartado correspondiente en la DPC.

9.3.2. Información no incluida en el alcance

Véase el apartado correspondiente en la DPC.

9.3.3. Responsabilidad para proteger la información confidencial

Véase el apartado correspondiente en la DPC.

9.4. Protección de datos de carácter personal

Véase el apartado correspondiente en la DPC.

9.4.1. Plan de privacidad

Véase el apartado correspondiente en la DPC.

9.4.2. Información tratada como privada

Véase el apartado correspondiente en la DPC.

9.4.3. Información no considerada privada

Véase el apartado correspondiente en la DPC.

9.4.4. Responsabilidad de proteger la información privada

Véase el apartado correspondiente en la DPC.

9.4.5. Aviso y consentimiento para usar información privada

Véase el apartado correspondiente en la DPC.

9.4.6. Divulgación conforme al proceso judicial o administrativo

Véase el apartado correspondiente en la DPC.

9.4.7. Otras circunstancias de divulgación de información

Véase el apartado correspondiente en la DPC.

9.5. Derechos de propiedad intelectual

Véase el apartado correspondiente en la DPC.

9.6. Obligaciones y garantías

9.6.1. Obligaciones de la CA

Las obligaciones y responsabilidades de Izenpe, como Prestador de Servicios de Confianza, con el suscriptor del certificado y, en su caso, con las partes usuarias y terceros que confían, quedarán determinadas, principalmente, en el documento relativo a las condiciones de utilización o el contrato de expedición del certificado, y, subsidiariamente, por la presente Declaración de Prácticas y Políticas de Certificación.

Izenpe cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411 para la emisión de certificados y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

Izenpe emite los certificados de autenticación de sitios web de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser Forum que pueden consultarse en la dirección https://cabforum.org/. Asimismo, adaptará sus prácticas de expedición de certificados a la versión vigente de los citados requisitos. En caso de cualquier incoherencia con esta Política, dichos requisitos prevalecerán sobre este documento.

Adicionalmente, Izenpe se compromete a cumplir, en relación con la expedición de certificados cualificados, los requisitos establecidos por la entidad CA/Browser Fórum para este tipo de Certificados (EV SSL Certificate Guidelines), que pueden consultarse en la dirección https://cabforum.org/extended-validation/. En caso de cualquier incoherencia con esta Política dichos requisitos prevalecerán sobre este documento.

Sin perjuicio de lo dispuesto en la normativa de aplicación a este tipo de certificados, así como las obligaciones descritas en el apartado correspondiente de la DPC, el Prestador de Servicios de Confianza se obliga, con carácter previo a la expedición del certificado, a:

- ✓ Comprobar la identidad y circunstancias personales del solicitante del certificado y del suscriptor y/o su Representante y recoger la manifestación de que el solicitante está autorizado por el suscriptor para realizar la solicitud.

- ✓ En el proceso de registro, comprobar los datos relativos a la personalidad jurídica del suscriptor y a la capacidad del Representante. Todas estas comprobaciones se realizarán según lo dispuesto en este documento y los protocolos y procedimientos de registro de Izenpe.

- ✓ En los procesos de comprobaciones anteriores Izenpe podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de Registros competentes.

- ✓ Verificar que toda la información contenida en la solicitud del certificado se corresponde con la aportada por la persona solicitante.

- ✓ Comprobar que la persona solicitante está en posesión de la Clave Privada asociada a la Clave Pública que se incorpora al certificado a emitir.

- ✓ Garantizar que los procedimientos seguidos aseguran que las Claves Privadas correspondientes a los certificados de autenticación de sitios web son generadas sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de Izenpe.

- ✓ Realizar la comunicación de información al suscriptor, representante y solicitante de tal forma que se garantice su confidencialidad.

- ✓ Poner a disposición del solicitante, suscriptor, Representante y demás interesados (Declaración de Prácticas de Certificación de Izenpe y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los certificados objeto de esta Política de Certificación de conformidad con la normativa aplicable.

9.6.2. Obligaciones de la RA

Véase el apartado correspondiente en la DPC.

Las actividades relativas a la RA serán realizadas exclusivamente por Izenpe para todos los certificados de autenticación de sitios web.

La RA tiene las siguientes obligaciones:

- ✓ Con carácter general, seguir los procedimientos establecidos por Izenpe en la Política y Prácticas de Certificación de aplicación en el desempeño de sus funciones de gestión, expedición y revocación de Certificados y no alterar dicho marco de actuación.

- ✓ En particular, comprobar la identidad, y cualesquiera circunstancias personales relevantes para la finalidad determinada, de los solicitantes de los certificados, suscriptores y sus Representantes, mediante cualquier medios admitido en Derecho y conforme a lo previsto con carácter general en la DPC y con carácter particular en la presente Política.

- ✓ Comprobar que la titularidad del nombre de dominio se corresponde con la identidad del Suscriptor o, en su caso, obtener la autorización de éste, que se asociará al

- ✓ Certificado de autenticación de sitios web, por los medios a su alcance que, razonablemente, permitan acreditar tal titularidad, de conformidad con el estado de la técnica.

- ✓ Recoger expresamente el poder de decisión del suscriptor respecto a la titularidad del dominio del certificado de autenticación de sitios web.

- ✓ Conservar toda la información y documentación relativa a los sertificados, cuya solicitud, renovación o revocación gestiona durante 15 años.

- ✓ Realizar la recepción y gestión de las solicitudes a través de la aplicación de gestión de solicitudes publica en www.izenpe.eus

- ✓ Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los certificados.

9.6.3. Obligaciones de los suscriptores

Véase el apartado correspondiente en la DPC.

En cuanto a los certificados de autenticación de sitios web, los suscriptores deben tener el control del nombre de dominio de sitio web incluido en dichos Certificados y mantener bajo su uso exclusivo las Claves privadas asociadas.

El solicitante y el Suscriptor de los Certificados expedidos bajo la presente CP, tienen la obligación de:

- ✓ No usar el certificado fuera de los límites especificados en la presente Política y Prácticas de Certificación particulares.
- ✓ No usar el certificado en caso de que el Prestador de Servicios de Confianza haya cesado su actividad como Entidad emisora de Certificados que expidió el certificado en cuestión, especialmente en los casos en los que los Datos de Creación de Sello del prestador puedan estar comprometidos, y así se haya comunicado.
- ✓ Aportar información veraz en la solicitud de los Certificados y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- ✓ No solicitar para el Sujeto del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- ✓ Actuar con diligencia respecto de la custodia y conservación de los Datos de creación de Firma / Sello o cualquier otra información sensible como Claves, códigos de activación del Certificado, palabras de acceso, números de identificación personal, etc., así como de los soportes de los Certificados, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- ✓ Conocer y cumplir las condiciones de utilización de los Certificados previstas en las condiciones de uso y en la Declaración de Prácticas de Certificación y en particular, las limitaciones de uso de los Certificados
- ✓ Conocer y cumplir las modificaciones que se produzcan en la Declaración de Prácticas de Certificación.
- ✓ Solicitar la revocación del correspondiente Certificado, según el procedimiento descrito en el presente documento, notificando diligentemente a Izenpe las circunstancias para la revocación o sospecha de pérdida de la Confidencialidad, la divulgación, modificación o uso no autorizado de las Claves privadas asociadas,
- ✓ Revisar la información contenida en el Certificado, y notificar a Izenpe cualquier error o inexactitud.
- ✓ Verificar con carácter previo a confiar en los Certificados, la Firma electrónica o el Sello electrónico avanzados del Prestador de Servicios de Confianza emisor del Certificado.

- ✓ Notificar diligentemente a Izenpe cualquier modificación de los datos aportados en la solicitud del Certificado, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.

Será en todo caso responsabilidad del Suscriptor utilizar de manera adecuada y custodiar diligentemente el Certificado, según el propósito y función para el que ha sido expedido, así como informar a Izenpe acerca de cualquier variación de estado o información respecto de lo reflejado en el Certificado, para su revocación y nueva expedición.

Asimismo, será el Suscriptor quien deba responder, en todo caso, ante Izenpe, las Entidades usuarias y, en su caso, ante terceros, del uso indebido del Certificado, o de la falsedad o errores de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a Izenpe o a terceros.

Será responsabilidad y, por tanto, obligación del Suscriptor no usar el Certificado en caso de que el Prestador de Servicios de Confianza haya cesado en la actividad como Entidad emisora de Certificados que realizó la expedición del Certificado en cuestión y no se hubiera producido la subrogación prevista en la ley. En todo caso, el Suscriptor no usará el Certificado en los casos en los que los Datos de Creación de Firma del Prestador puedan estar amenazados y/o comprometidos, y así se haya comunicado por el Prestador o, en su caso, hubiera tenido noticia de estas circunstancias.

Las relaciones de Izenpe y el Suscriptor quedarán determinadas principalmente, a los efectos del régimen de uso de los Certificados, a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del Certificado y atendiendo a los acuerdos, convenios o documento de relación entre Izenpe y la Entidad correspondiente.

9.6.4. Obligaciones de las partes que confían

Será responsabilidad de la Entidad usuaria y de los terceros que confían en los certificados la verificación y comprobación del estado de los certificados, no pudiendo en ningún caso presuponer la validez de los certificados sin dichas comprobaciones.

Asimismo, será responsabilidad de la entidad usuaria observar lo dispuesto en la Declaración de Prácticas de Certificación y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los certificados en esta Política de Certificación.

Véase el apartado correspondiente en la DPC.

9.6.5. Obligaciones de otros participantes

No estipulado

9.7. Renuncia de garantías

No estipulado

9.8. Límites de responsabilidad

Véase el apartado correspondiente en la DPC.

9.9. Indemnizaciones

9.9.1. Indemnización de la CA

No estipulado

9.9.2. Indemnización de los Suscriptores

No estipulado

9.9.3. Indemnización de las partes que confían

No estipulado

9.10. Periodo de validez de este documento

9.10.1. Plazo

La presente Política de Certificación entrará en vigor en el momento de su publicación.

9.10.2. Terminación

La presente Política de Certificación será derogada en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente al documento anterior. Izenpe se compromete a someter esta Política a un proceso de revisión anual.

9.10.3. Efectos de la finalización

Para los certificados vigentes emitidos bajo esta Política de Certificación, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11. Notificaciones individuales y comunicación con los participantes

Véase el apartado correspondiente en la DPC.

9.12. Modificaciones de este documento

9.12.1. Procedimiento para las modificaciones

Las modificaciones de la presente Política de Certificación serán aprobadas por el Comité de Seguridad de Izenpe, que quedarán reflejadas en la correspondiente acta, de conformidad con el procedimiento interno aprobado.

9.12.2. Periodo y mecanismo de notificación

Cualquier modificación en la presente Política de Certificación será publicada de forma inmediata en la URL de acceso a la misma.

Si las modificaciones a realizar no conllevan cambios significativos en cuanto al régimen de obligaciones y responsabilidades de las partes o relativos a una modificación de las políticas de prestación de los servicios, Izenpe no informará previamente a los usuarios, limitándose a publicar una nueva versión de la declaración afectada en su página web.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

Las modificaciones significativas de las condiciones de los servicios, régimen de obligaciones y responsabilidades o limitaciones de uso pueden ocasionar un cambio de política del servicio y su identificación (OID), así como el enlace a la nueva declaración de política del servicio. En este caso, Izenpe podrá establecer un mecanismo de información de los cambios propuestos y, en su caso, de recogida de opiniones de las partes afectadas.

9.13. Reclamaciones y resolución de disputas

Véase el apartado correspondiente en la DPC.

9.14. Normativa de aplicación

Véase el apartado correspondiente en la DPC.

9.15. Cumplimiento de la normativa aplicable

Izenpe manifiesta su compromiso de cumplimiento de la normativa y de los requisitos de aplicación a cada tipo de Certificado de autenticación de sitios web, incluyendo las consideraciones establecidas en el apartado “1.5.4. Procedimiento de aprobación de la DPC” del presente documento de CP.

9.16. Estipulaciones diversas

9.16.1. Acuerdo íntegro

Véase el apartado correspondiente en la DPC.

9.16.2. Asignación

Véase el apartado correspondiente en la DPC.

9.16.3. Severabilidad

Véase el apartado correspondiente en la DPC.

9.16.4. Cumplimiento

Véase el apartado correspondiente en la DPC.

9.16.5. Fuerza Mayor

Véase el apartado correspondiente en la DPC.

9.17. Otras estipulaciones

Véase el apartado correspondiente en la DPC.