

Declaración de Prácticas de Certificación

Referencia: IZENPE-DPC
Nº Versión: v 6.4
Fecha: 03 de Junio de 2020

© IZENPE 2020

Este documento es propiedad de IZENPE. Únicamente puede ser reproducido en su totalidad



Índice

Contenido

1	Introducción	12
1.1	Presentación	13
1.2	Identificación	18
1.3	Participantes de la infraestructura de clave pública PKI	18
1.3.1	Autoridades de Certificación	18
1.3.2	Entidades de Registro	27
1.3.3	Entidades finales usuarias de certificados	27
1.3.4	Terceras partes de confianza	28
1.4	Usos del certificado	28
1.4.1	Usos apropiados del certificado	28
1.4.2	Usos prohibidos del certificado	30
1.5	Políticas	30
1.5.1	Entidad responsable de la gestión de la documentación	30
1.5.2	Datos de contacto	30
1.5.3	Responsables de adecuación de la Declaración de Prácticas de Certificación	30
1.5.4	Procedimiento de aprobación de la Declaración de Prácticas de Certificación	30
1.6	Definiciones y acrónimos	31
1.6.1	Definiciones	31
1.6.2	Acrónimos	35
2	Publicación y responsables del repositorio de información	37
2.1	Repositorio de información	37
2.2	Publicación de información de certificación	37



2.2.1	Política de publicación y notificación	37
2.2.2	Elementos no publicados en la Declaración de Prácticas de Certificación	37
2.3	Frecuencia de publicación	37
2.4	Control de acceso al repositorio	38
3	Nombres	39
3.1.1	Tipos de nombres	39
3.1.2	Reglas para la Interpretación de formatos de nombres	39
3.1.3	Unicidad de los nombres	40
3.1.4	Resolución de conflictos relativos a nombres y tratamiento de marcas registradas	40
3.2	Validación de la identidad	40
3.2.1	Métodos para probar la posesión de la clave privada	40
3.2.2	Autenticación de la identidad de la organización	40
3.2.3	Autenticación de la identidad de la persona física solicitante	41
3.3	Identificación y autenticación para peticiones de reemisión de claves	41
3.4	Identificación y autenticación para peticiones de revocación	41
4	Requisitos operativos del ciclo de vida de los certificados	42
4.1	Solicitud de certificado	42
4.1.1	Comprobación de la solicitud	42
4.1.2	Proceso de inscripción y responsabilidades.	42
4.2	Procesamiento de las solicitudes	43
4.2.1	Realización de funciones de identificación y autenticación	43
4.2.2	Aprobar o rechazar solicitudes	43
4.3	Emisión del certificado	43
4.3.1	Acciones de la CA durante la emisión	44
4.3.2	Notificación al suscriptor de la emisión	44
4.4	Aceptación del certificado	44



4.4.1	Proceso de aceptación del certificado	44
4.4.2	Publicación del certificado por la CA	44
4.4.3	Notificación de la emisión del certificado por la CA a otras entidades	44
4.5	Par de claves y usos del certificado	45
4.5.1	Clave privada del suscriptor y uso del certificado	45
4.5.2	Uso de la clave pública y del certificado por terceros que confían en los certificados	46
4.6	Renovación del certificado	47
4.6.1	Circunstancias para la renovación del certificado	47
4.6.2	Quién puede solicitar la renovación	47
4.6.3	Tratamiento de peticiones de renovación de certificado	47
4.6.4	Notificación al suscriptor	47
4.6.5	Procedimiento de aceptación de un certificado renovado	47
4.6.6	Publicación del certificado	47
4.6.7	Notificación a otras entidades	48
4.7	Renovación con regeneración de las claves del certificado	48
4.7.1	Circunstancias para regenerar las claves del certificado	48
4.7.2	Quien lo puede pedir	48
4.7.3	Tratamiento de las peticiones de renovación con regeneración de claves	48
4.7.4	Notificación al suscriptor	48
	Se debe usar el mismo proceso de notificación que para peticiones de nuevo certificado.	48
4.7.5	Procedimiento de aceptación del certificado renovado	48
4.7.6	Publicación del certificado	49
4.7.7	Notificación a otras entidades	49
4.8	Modificación del certificado	49
4.9	Revocación	49
4.9.1	Circunstancias para la revocación	49



4.9.2	Quién puede solicitar la revocación	50
4.9.3	Tratamiento de las peticiones de revocación	50
4.9.4	Tiempo de plazo de la CA para procesar la revocación	50
4.9.5	Obligación de verificación de las revocaciones por terceros de confianza	51
4.9.6	Frecuencia de generación de CRLs	51
4.9.7	Tiempo transcurrido entre la generación y la publicación de las CRLs	51
4.9.8	Disponibilidad del sistema de verificación online del estado de los certificados	51
4.9.9	Requisitos de comprobación de revocación online	51
4.9.10	Otras formas de avisos de revocación disponibles	52
4.9.11	Requisitos especiales clave comprometida	52
4.10	Servicios de estado de los certificados	52
4.10.1	Características operativas	52
4.10.2	Disponibilidad del servicio	52
4.11	Finalización de la suscripción	52
4.12	Custodia y recuperación de claves	53
5	Controles de seguridad física, de procedimiento y de personal	54
5.1.1	Localización y construcción de las instalaciones	54
5.1.2	Acceso físico	54
5.1.3	Electricidad y aire acondicionado	55
5.1.4	Exposición al agua	55
5.1.5	Prevención y protección de incendios	55
5.1.6	Almacenamiento de soportes	55
5.1.7	Tratamiento de residuos	55
5.1.8	Copia de respaldo fuera de las instalaciones	55
5.2	Controles de procedimientos	55
5.2.1	Funciones fiables	55



5.2.2	Número de personas por tarea	56
5.2.3	Identificación y autenticación para cada rol	56
5.2.4	Separación de tareas en los diferentes roles	56
5.3	Controles de personal	56
5.3.1	Requisitos de historial, calificaciones, experiencia y autenticación	56
5.3.2	Procedimientos de investigación de historial	56
5.3.3	Requisitos de formación	56
5.3.4	Requisitos y frecuencia de actualización formativa	57
5.3.5	Secuencia y frecuencia de rotación laboral	57
5.3.6	Sanciones para acciones no autorizadas	57
5.3.7	Requisitos de contratación de personal	57
5.3.8	Suministro de documentación al personal	57
5.4	Audit	58
5.4.1	Tipo de eventos registrados	58
5.4.2	Frecuencia de procesamiento de logs	58
5.4.3	Periodo de retención del audit log	58
5.4.4	Protección del audit log	58
5.4.5	Procedimiento de backup del audit log	59
5.4.6	Recolección de logs	59
5.4.7	Notificación de la acción causante de los logs	59
5.4.8	Análisis de vulnerabilidades	59
5.5	Archivado de registros	59
5.5.1	Tipo de registros archivados	59
5.5.2	Periodo de retención del archivo	59
5.5.3	Protección del archivo	59
5.5.4	Procedimientos de backup del archivo	59



5.5.5	Requisitos para el sellado de tiempo de los registros	59
5.5.6	Sistema de archivo	60
5.5.7	Procedimientos para obtener y verificar la información del archivo	60
5.6	Cambio de claves	60
5.7	Plan de contingencias	60
5.7.1	Procedimientos de gestión de incidencias	60
5.7.2	Plan de actuación ante datos y software corruptos	61
5.7.3	Procedimiento ante compromiso de la clave privada	61
5.7.4	Continuidad de negocio después de un desastre	62
5.8	Terminación de la CA o RA	62
5.8.1	Entidad de Certificación	62
5.8.2	Entidad de Registro	63
6	Controles de seguridad técnica	64
6.1	Generación e instalación del par de claves	64
6.1.1	Generación del par de claves	64
6.1.2	Distribución de la clave privada al suscriptor	64
6.1.3	Distribución de la clave pública al emisor del certificado	64
6.1.4	Distribución de la clave pública de la Entidad de Certificación a los usuarios de certificados	65
6.1.5	Tamaños de claves y algoritmos utilizados	65
6.1.6	Algoritmos de firma de certificados	65
6.1.7	Usos admitidos de las claves (KeyUsage field X.509v3)	66
6.2	Protección de la clave privada	66
6.2.1	Estándares de módulos criptográficos	66
6.2.2	Control por más de una persona (n de m) sobre la clave privada	66
6.2.3	Custodia de la clave privada	66
6.2.4	Copia de respaldo de la clave privada	67



6.2.5	Archivado de la clave privada	67
6.2.6	Trasferencia de la clave privada a o desde el módulo criptográfico	67
6.2.7	Almacenamiento de la clave privada en el módulo criptográfico	67
6.2.8	Método de activación de la clave privada	68
6.2.9	Método de desactivación de la clave privada	68
6.2.10	Método de destrucción de la clave privada	68
6.2.11	Calificación del módulo criptográfico	68
6.3	Otros aspectos de gestión del par de claves	68
6.3.1	Archivo de la clave pública	68
6.3.2	Periodos de operación del certificado y periodos de uso del par de claves	68
6.4	Datos de activación	69
6.4.1	Generación e instalación de datos de activación	69
6.4.2	Protección de datos de activación	69
6.4.3	Otros aspectos de los datos de activación	69
6.5	Controles de seguridad informática	69
6.5.1	Requisitos técnicos específicos de seguridad informática	69
6.5.2	Evaluación del nivel de seguridad informática	70
6.6	Controles técnicos del ciclo de vida	70
6.6.1	Controles de desarrollo de sistemas	70
6.6.2	Controles de gestión de la seguridad	71
6.6.3	Controles de seguridad del ciclo de vida	71
6.7	Controles de seguridad de red	71
6.8	Fuente de tiempo	71
7	Perfiles de certificados y listas de certificados revocados	72
7.1	Perfil de certificado	72
7.1.1	Número de versión	72



7.1.2	Extensiones de certificado	72
7.1.3	Identificadores de objeto de algoritmos	72
7.1.4	Formatos de nombres	72
7.1.5	Restricciones de nombres	72
7.1.6	Identificador de objeto de política de certificado	72
7.1.7	Empleo de la extensión restricciones de política	73
7.1.8	Sintaxis y semántica de los calificadores de política	73
7.1.9	Tratamiento semántico para la extensión "certificate policy"	73
7.2	Perfil de la lista de revocación de certificados	73
7.2.1	Número de versión	73
7.2.2	Lista de revocación de certificados y extensiones de elementos de la lista	74
7.3	Perfil OCSP	74
7.3.1	Número de versión	74
7.3.2	Extensiones del OCSP	74
7.3.3	Otros aspectos del OCSP	74
8	Auditorías de cumplimiento	75
8.1	Frecuencia de auditoría	75
8.2	Cualificación del auditor	75
8.3	Relación del auditor con la empresa auditada	75
8.4	Elementos objetos de auditoría	75
8.5	Toma de decisiones como resultado de deficiencias	75
8.6	Comunicación de los resultados	76
9	Otros asuntos legales y de actividad	77
9.1	Tarifas	77
9.1.1	Tarifas de emisión o renovación de certificados	77
9.1.2	Tarifas de acceso a la información de estado de los certificados	77



9.1.3	Tarifas para otros servicios	77
9.1.4	Política de reintegro	77
9.2	Responsabilidad financiera	77
9.3	Confidencialidad de la información	77
9.3.1	Alcance de la información confidencial	77
9.3.2	Información que no está dentro del alcance	78
9.3.3	Responsabilidad para proteger la información confidencial	79
9.4	Protección de datos de carácter personal	79
9.5	Derechos de propiedad intelectual	80
9.5.1	Propiedad de los certificados	80
9.5.2	Propiedad de la Práctica de Certificación	80
9.5.3	Propiedad de la información relativa a nombres	80
9.5.4	Propiedad de claves y material relacionado	80
9.6	Obligaciones y garantías	80
9.6.1	Obligaciones de prestación del servicio	80
9.6.2	Obligaciones de operación fiable	81
9.6.3	Obligaciones de identificación	82
9.6.4	Obligaciones de información a usuarios	82
9.6.5	Obligaciones relativas a los programas de verificación	83
9.6.6	Obligaciones relativas a la regulación jurídica del servicio de certificación	83
9.6.7	Obligaciones de la Entidad de Registro	84
9.6.8	Obligaciones del solicitante del certificado	84
9.6.9	Obligaciones del suscriptor del certificado	84
9.6.10	Obligaciones del usuario verificador de certificados	85
9.6.11	Obligaciones del Servicio de Publicación	86
9.7	Responsabilidades	86



9.7.1	Responsabilidades de la autoridad de certificación	86
9.7.2	Responsabilidades de la autoridad de registro	87
9.7.3	Responsabilidades de los suscriptores	87
9.7.4	Responsabilidades de los terceros que confían en certificados	88
9.8	Indemnizaciones	88
9.9	Periodo de validez	88
9.9.1	Plazo	88
9.9.2	Terminación	89
9.9.3	Efectos de la finalización	89
9.10	Notificaciones individuales y comunicación con los participantes	89
9.11	Enmiendas	89
9.11.1	Procedimiento para los cambios	89
9.11.2	Periodo y mecanismo de notificación	89
9.11.3	Circunstancias por la cual un OID debe cambiarse	90
9.12	Reclamaciones y resolución de disputas	90
9.13	Normativa aplicable	90
9.14	Cumplimiento de la normativa aplicable	91
9.15	Estipulaciones diversas	91



1 Introducción

La administración pública del País Vasco como impulsores de la Sociedad de la Información y con la pretensión de garantizar la plena incorporación de las tecnologías de la información y comunicación a las actividades económicas y sociales de la ciudadanía, han arbitrado los instrumentos que permitan a los ciudadanos relacionarse con las distintas administraciones, organismos y empresas con la pretensión de garantizar la privacidad de la información, la intimidad de las personas y la salvaguarda de sus derechos, siempre con las máximas garantías de seguridad.

Con estas premisas, el Gobierno Vasco y las Diputaciones Forales, a través de sus respectivas sociedades informáticas resolvieron desarrollar, en un marco de colaboración, un sistema propio y común de certificación y firma electrónica garante de la interoperabilidad, de forma que los certificados emitidos puedan ser válidos en aplicaciones y procedimientos de las diferentes administraciones.

Esta voluntad de colaboración tuvo su primera expresión en la constitución en junio de 2002 de la sociedad mercantil “Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, IZENPE, S.A.” (en adelante, IZENPE) participada en su totalidad por las mencionadas sociedades informáticas.

IZENPE se constituye como el instrumento o la organización de la que se han dotado las Sociedades Informáticas de las Administraciones Públicas vascas para la gestión de su común interés en el desarrollo de la certificación electrónica, revelándose como medio idóneo para avanzar en la simplificación de las relaciones ciudadanos/administración.

El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE contempla la posibilidad de erigirse como Prestador Cualificado de Servicios de Confianza. En adelante eIDAS.

En tal sentido IZENPE se constituye como Prestador Cualificado de Servicios de Confianza dependiente de las Administraciones vascas cuyo objeto social es:

- El fomento del uso y potenciación del desarrollo del gobierno electrónico sobre redes de telecomunicaciones con las necesarias garantías de seguridad, confidencialidad, autenticidad e irrevocabilidad de las transacciones.
- Así como la prestación de servicios de seguridad, técnicos y administrativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos.

Los mecanismos de identificación ofrecidos por Izenpe están definidos siguiendo las directrices del Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.



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

IZENPE sigue las indicaciones de los estándares de ETSI (Instituto Europeo de Estándares de Telecomunicaciones) para la emisión de certificados cualificados y no cualificados, y para la emisión de los sellos de tiempo. En el caso de los certificados de servidor seguro (SSLs) se siguen además las guías aprobadas por el CA/Browser Forum, disponibles en www.cabforum.org.

Las especificaciones técnicas (ETSI TS) que se definen en estas normas marcan los requisitos básicos en los que se refieren a la gestión y prácticas de certificación de entidades certificadoras que emiten certificados cualificados y no cualificados y sellos de tiempo dentro del marco legal de la directiva 1999/93/EC del Parlamento y Consejo Europeo incorporada al régimen jurídico español en la ley de firma electrónica 59/2003, y que actualmente han sido convenientemente actualizadas en unas nuevas normas europeas, EN 319 411-1 para la emisión de certificados, EN 319 411-2 para la emisión de certificados cualificados según el reglamento 910/2014 y EN 319 421 para la emisión de sellos de tiempo según se recoge en el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).

En cumplimiento de ETSI EN 319 401 por el que se exige la accesibilidad a los servicios de confianza y productos de usuario final, Izenpe trabaja para garantizar que todos los ciudadanos, con especial atención a las personas con algún tipo de discapacidad y mayores que se relacionen con Izenpe, puedan acceder a la información y los servicios electrónicos en igualdad de condiciones, con independencia de sus circunstancias personales, medios o conocimientos. A estos efectos se tendrán en cuenta las recomendaciones de ETSI EN 301 549.

En todo caso, cualquier consulta en relación con la accesibilidad del sitio web de Izenpe, de sus productos o servicios puede presentarla a través del correo electrónico info@izenpe.com o del formulario disponible en www.izenpe.eus.

Esta Declaración de Prácticas de Certificación (DPC) está estructurada según la RFC 3647.

1.1 Presentación

IZENPE opera una infraestructura al objeto de prestar los siguientes servicios cualificados:

- a) Expedición de certificados electrónicos cualificados de firma electrónica
- b) Expedición de certificados electrónicos cualificados de sello electrónico
- c) Expedición de certificados electrónicos cualificados de autenticación de sitios web
- d) Servicio de expedición de sellos electrónicos cualificados de tiempo

Y los siguientes servicios no cualificados:

- a) Expedición de certificados electrónicos no cualificados de firma electrónica
- b) Expedición de certificados electrónicos no cualificados de autenticación de sitios web
- c) Entrega electrónica certificada
- d) Validación de firmas electrónicas
- e) Validación de sellos electrónicos



En el ámbito de la presente Declaración de Prácticas de Certificación y de la *Política específica para cada certificado*, IZENPE emite los siguientes tipos de certificado:

CIUDADANO						
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS		Tipo firma eIDAS
B@K	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Bajo		Básica
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada
Certificado Ciudadano	Chip criptográfico	QCP-n-qscd	Perfil eIDAS 1.3.6.1.4.1.14777.2.18.1	Alto		Cualificada
			Perfil anterior a eIDAS 1.3.6.1.4.1.14777.2.6	Alto		Cualificada
Mobile	Contenedor APP	NCP	1.3.6.1.4.1.14777.5.2.5.4	Sustancial		n/a (para firmar se usa el de BAKQ)
Seudónimo o NQC	Software	NCP	1.3.6.1.4.1.14777.5.2.7.2	Sustancial		Avanzada

REPRESENTANTE ENTIDAD						
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS		Tipo firma eIDAS
Representante entidad	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada
	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.2.12	Alto		Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.16	Sustancial		Avanzada



REPRESENTANTE ENTIDAD SPJ						
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS		Tipo firma eIDAS
Representante Entidad SPJ	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada
	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.2.13	Alto		Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.17	Sustancial		Avanzada

PROFESIONAL						
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS		Tipo firma eIDAS
Personal de Entidad Pública	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.4.14.1	Alto		Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.4.14.2	Sustancial		Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada
Personal de Entidad Pública con seudónimo	Chip criptográfico	QCP-n-qscd	Firma 1.3.6.1.4.1.14777.4.13.1.1	Alto		Cualificada
		NCP+	Autenticación 1.3.6.1.4.1.14777.4.13.1.2	Alto		n/a
		n/a	Cifrado 1.3.6.1.4.1.14777.4.13.1.3	Alto		n/a
Corporativo cualificado	Chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.2.19.1	Alto		Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.19.2	Sustancial		Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Alto (con tarjeta virtual)	Sustancial (con Giltza)	Avanzada
Corporativo no cualificado	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a (no cualificado)		Avanzada
Personal de las Entidades	Chip	QCP public +	1.3.6.1.4.1.14777.4.1	n/a		Reconocida



públicas (pre-eIDAS)	criptográfico	SSCD			
Personal del Gobierno Vasco (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.7.1	n/a	Reconocida
Corporativo público reconocido (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	n/a	Reconocida
Corporativo público no reconocido (pre-eIDAS)	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a	Reconocida
Corporativo privado reconocido (pre-eIDAS)	Chip criptográfico	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	n/a	Reconocida
Corporativo privado no reconocido (pre-eIDAS)	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.5.2.2	n/a	Reconocida
SELLO DE ENTIDAD					
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS	Tipo firma eIDAS
Sello de entidad	Contenedor software de Izenpe	QCP-I	1.3.6.1.4.1.14777.2.11	Sustancial	Avanzada
	HSM	QCP-I	1.3.6.1.4.1.14777.2.20	Sustancial	Avanzada

SELLO DE ADMINISTRACIÓN					
Breve descripción	Soporte	Identificador de política	OID política	Nivel identificación eIDAS	Tipo firma eIDAS
Sello de administración	Contenedor software de Izenpe	QCP-I	1.3.6.1.4.1.14777.4.11.2	Sustancial	Avanzada
	HSM	QCP-I	1.3.6.1.4.1.14777.4.11.3	Sustancial	Avanzada
Sello de administración nivel medio	HSM	NCP+	1.3.6.1.4.1.14777.4.4	n/a	Reconocida



(pre-eIDAS)					
-------------	--	--	--	--	--

SERVIDOR SEGURO (SSL/TLS)			
BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.1.2.1
SSL EV	Software	EVCP	1.3.6.1.4.1.14777.6.1.1
SEDE	Software	OVCP	1.3.6.1.4.1.14777.1.1.3
SEDE EV	Software	EVCP	1.3.6.1.4.1.14777.6.1.2
SSL cualificado	Software	EVCP	1.3.6.1.4.1.14777.6.1.3
Sede cualificado	Software	EVCP	1.3.6.1.4.1.14777.6.1.4

APLICACIÓN			
BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA
Aplicación	Contenedor software de Izenpe	NCP	1.3.6.1.4.1.14777.1.2.2

FIRMA DE CÓDIGO			
BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA
Firma de código	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.1.3.1

DISPOSITIVO IOT			
BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA
Dispositivo	Software	NCP	1.3.6.1.4.1.14777.1.3.2

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



1.2 Identificación

Con el objeto de identificar de forma individual cada tipo de certificado emitido por IZENPE de acuerdo con la presente Declaración de Prácticas de Certificación, se asignan a cada tipo un identificador de objeto (OID). Pueden consultarse en el documento de perfiles disponible en www.izenpe.com. Además, según la definición de ETSI EN 319 412-5, se incluyen los siguientes identificadores:

- QcCompliance: certificado cualificado según eIDAS
- QcSSCD: certificado emitido en un dispositivo cualificado de creación de firma
- QcRetentiodPeriod: periodo de retención de la documentación
- QcPDS: ruta a las condiciones de uso
- Qctype: indica el tipo de firma según eIDAS (sello, firma, web)

1.3 Participantes de la infraestructura de clave pública PKI

Los roles que intervienen en la administración y operación de la Entidad de Certificación son los siguientes:

- Autoridades de Certificación.
- Entidades de Registro.
- Usuarios de los certificados.

1.3.1 Autoridades de Certificación

IZENPE dispone de las siguientes Autoridades de Certificación,

- Autoridad de Certificación raíz
- Autoridades de Certificación subordinadas

AUTORIDAD DE CERTIFICACIÓN RAÍZ

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

CA raíz

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)



AUTORIDADES de Certificación subordinadas





Son Autoridades de Certificación que expiden certificados electrónicos a Entidades finales.

- CA Ciudadanos /Entidades Cualificados
- CA Ciudadanos /Entidades NO Cualificados
- CA AAPP NO Cualificados
- CA AAPP Cualificados
- CA SSL EV
- CA SSL EV 2018

CA Ciudadanos /Entidades Cualificados

Herritar eta Erakundeen Ciudadanos y Entidades (4)	
Campo / extensión	Contenido
version	Versión 3
serialNumber	2145c8d9b105500e4cbea542553af2c3
signature	sha256WithRSAEncryption
issuer	Igual al campo subject del certificado de la CA emisora
CN	izenpe.com
O	IZENPE S.A.
C	ES
validity	13 de diciembre de 2037
subject	
CN	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)
OU	NZZ Ziurtagiri publikoa - Certificado publico SCI
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	a4171d4e65d7ef87952e7f8eb875cb058bd38c7d
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/ari2
keyUsage	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)
Huella digital	08d8d62a1a1536c53a0f9a1835bf82c9f0968323

CA Ciudadanos /Entidades NO Cualificados

Herritar eta Erakundeen Ciudadanos y Entidades (3)	
Campo / extensión	Contenido
version	Versión 3
serialNumber	72eb2bad7d8b65e34cbea5bf9f2ac3d9
signature	sha256WithRSAEncryption
issuer	
CN	izenpe.com
O	IZENPE S.A.
C	ES
validity	13 de diciembre de 2037
subject	
CN	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3)
OU	NZZ Ziurtagiri publikoa - Certificado publico SCI
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	ecb204f691bd8b523806b3f4007fb137dbbc5197
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	875660a35cb103d7e0bb004424f16dbfbf21e0b4

CA AAPP Cualificados

EAEko HAetako langileen CA - CA personal de AAPP vascas (2)	
Campo / extensión	Contenido
version	Versión 3
serialNumber	693a966783e23bdf4cbea6d0d9543fd7
signature	sha256WithRSAEncryption
issuer	
CN	izenpe.com
O	IZENPE S.A.
C	ES
validity	13 de diciembre de 2037
subject	
CN	EAEko HAetako langileen CA - CA personal de 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	c6af966850be6fa1e514dcb99d973d8d73e77e9a
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	93a1446b61994b5b0e99d05b14cddb322e6c1764

CA AAPP no Cualificados

EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	
Campo / extensión	Contenido
version	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	c0a94af7472587ffbc5a689ce82d246a889eba3
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 SSL EV 2010

CA de Certificados SSL EV	
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 SSL EV 2018

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 Entidades de Registro

Esta Declaración de Prácticas de Certificación se aplica a las Entidades de Registro que IZENPE emplee en los procedimientos de emisión y gestión de certificados.

Las Entidades de Registro realizan las tareas de identificación de los solicitantes, suscriptores y poseedores de claves de los certificados, comprobación de la documentación acreditativa las circunstancias que constan en los certificados, así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los certificados.

Serán Entidad de Registro IZENPE o las Entidades Usuarias con las que IZENPE suscriba el correspondiente instrumento legal.

1.3.3 Entidades finales usuarias de certificados

Las Entidades finales usuarias de los certificados son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales

Serán Entidades finales usuarias del sistema de certificación:

- Solicitantes de certificados
- Firmante del certificado
- Suscriptores de certificados
- Poseedores de claves

Para cada tipo de certificado las especificidades están definidas en la *Documentación específica para cada certificado*.

Solicitantes de certificados, todo certificado debe ser solicitado por una persona, en su propio nombre o en nombre de una organización.

Firmante, el firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Suscriptores de certificados, los suscriptores son las personas físicas o jurídicas identificadas en el certificado.

Poseedores de claves, los poseedores de claves son las personas físicas que poseen o responden de la custodia de las claves de firma digital.



1.3.4 Terceras partes de confianza

Dentro de esta Declaración de Prácticas de Certificación, las personas físicas o jurídicas que reciben certificados y sellos de tiempo emitidos por IZENPE son terceros que confían en certificados y sellos de tiempo emitidos por IZENPE y, como tales, les es de aplicación lo establecido por la presente Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados o sellos de tiempo.

Se considera que los terceros confían en los certificados y sellos de tiempo en función del empleo objetivo que de los mismos realicen en sus relaciones con los suscriptores.

Cuando se haya dado este uso, se atenderá especialmente a la inexistencia de toda declaración por la cual el tercero afirme no confiar en los certificados o las firmas digitales adjuntados a los mensajes, para establecer que el tercero confió efectivamente en los certificados y las firmas digitales, siempre y cuando se trate de certificados válidos, firmas creadas durante el periodo operativo de los certificados y se hayan cumplido los restantes requisitos que determinan la confianza en un certificado.

Los terceros deberán guardar la diligencia debida en el empleo de cada tipo de certificado y actuar con base en los principios de buena fe y lealtad, absteniéndose de realizar conductas fraudulentas o negligentes cuyo fin sea repudiar mensajes emitidos dentro del ámbito de confianza asociado a la categoría del certificado o sello de tiempo.

1.4 Usos del certificado

Se establecen a continuación los usos permitidos y prohibidos de los certificados emitidos por IZENPE.

1.4.1 Usos apropiados del certificado

Certificados cualificados

Los certificados cualificados de firma electrónica garantizan la identidad del suscriptor y del poseedor de la clave privada. Cuando se empleen con dispositivos seguros de creación de firma, resultan idóneos para ofrecer soporte a la firma electrónica reconocida; esto es, la firma electrónica avanzada que se basa en certificado cualificado y que ha sido generada empleando un dispositivo seguro, por lo que, de acuerdo con eIDAS, se equipara a la firma manuscrita por efecto legal, sin necesidad de cumplir requisito adicional alguno.

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

Adicionalmente, dichos certificados pueden dar soporte a diversas formas de autenticación y a la firma electrónica avanzada, utilizados en conjunción con aplicaciones informáticas que protegen de forma fiable la clave privada de firma.

El certificado de sello electrónico vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona. Permiten generar sellos electrónicos, que sirven



como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento.

Los certificados de sello electrónico que emite Izenpe cumplen con los requisitos del anexo III de eIDAS para ser considerados cualificados.

Los certificados de autenticación de sitio web permiten autenticar un sitio web y vinculan el sitio web con la persona física o jurídica a quien se ha expedido el certificado. Los certificados web expedidos por Izenpe cumplen con los requisitos del anexo IV de eIDAS para ser considerados cualificados.

Los certificados de sede y sello electrónico se emiten a las administraciones públicas para la identificación de la sede electrónica y el sellado electrónico de documentos, según lo previsto en la *Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos*.

Los certificados cualificados de Izenpe siguen la norma técnica ETSI EN 319 411-2.

Certificado no cualificado

Los certificados no cualificados no garantizan fehacientemente la identidad del suscriptor y, en su caso, del poseedor de la clave privada; en cualquier caso, en caso de emplearse para firmar, se debe usar en conjunción con un dispositivo de generación de firma razonablemente seguro. En este caso no se equipará a la firma manuscrita del firmante.

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

Los certificados cualificados de Izenpe siguen la norma técnica ETSI EN 319 411-1.

Ámbito de uso de los certificados

En cuanto a su ámbito de uso se distinguen dos supuestos:

- Los certificados emitidos por IZENPE y dirigidos al público en general serán utilizados por los suscriptores, o en su caso los poseedores de claves, en las relaciones que mantengan con las Entidades Usuarías e Instituciones Públicas y Privadas en general que hayan admitido su uso.

Consultar las especificidades en cuanto al ámbito de uso de cada certificado en la *Documentación específica para cada certificado*.

- Los certificados emitidos por IZENPE y solicitados por las Entidades Usuarías serán utilizados en el ámbito de sus características como persona física o jurídica, según especificaciones de eIDAS. No obstante los poseedores de claves podrán utilizar estos certificados para otros usos siempre que se respeten los límites de uso señalados en el apartado anterior.

Consultar las especificidades en cuanto al ámbito de uso de cada certificado en la *Documentación específica para cada certificado*.



1.4.2 Usos prohibidos del certificado

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

Del mismo modo, 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.

1.5 Políticas

1.5.1 Entidad responsable de la gestión de la documentación

IZENPE, con domicilio social en la Avenida Mediterráneo 14 Vitoria-Gasteiz y NIF A-01337260, es la Entidad de Certificación que expide los certificados a los que aplica esta Declaración de Prácticas de Certificación.

1.5.2 Datos de contacto

Consultar el apartado “4.9.3 Tratamiento de las peticiones de revocación” para conocer los canales de revocación.

1.5.3 Responsables de adecuación de la Declaración de Prácticas de Certificación

El Comité de Seguridad de IZENPE es el órgano responsable de la aprobación de la presente Declaración de Prácticas de Certificación así como los posibles cambios a la misma.

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
Teléfono	900 840 123

1.5.4 Procedimiento de aprobación de la Declaración de Prácticas de Certificación

Las modificaciones finales del presente documento son aprobadas por el Comité de Seguridad de IZENPE, tras comprobar el cumplimiento de los requisitos establecidos.



1.6 Definiciones y acrónimos

1.6.1 Definiciones

- **Agencia de Protección de Datos (APD):** es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y cuya principal finalidad es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.
- **Autoridad de Certificación (CA):** la Autoridad de Certificación es la entidad que emitirá, a petición de la Autoridad de Registro, los Certificados que se precisen, de forma automatizada y previa confirmación de la Autoridad de Registro Local.
- **Autoridad de Registro (RA):** la autoridad de registro es la entidad encargada de realizar las tareas de identificación de los solicitantes, suscriptores y poseedores de claves de los certificados, comprobar la documentación acreditativa de las circunstancias que constan en los certificados así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los certificados. El usuario se debe dirigir a la autoridad de registro para solicitar un certificado con la garantía de la autoridad certificadora asociada a la autoridad de registro.
- **Autoridad de Sellado de Tiempo (TSA):** autoridad que emite sellos de tiempo
- **Certificado:** es un documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- **Certificado Raíz:** certificado cuyo suscriptor es una Autoridad de Certificación perteneciente a la jerarquía de IZENPE, y que contiene los Datos de Verificación de firma de dicha Autoridad firmado con los datos de creación de Firma de la misma como Prestador de Servicios de Certificación. Las entidades emisoras de IZENPE forman una jerarquía, de forma que hay una entidad raíz común para cualquier tipo de certificado y varias entidades subordinadas, para los diferentes tipos de certificados.
- **Certificado cualificado:** son los certificados electrónicos expedidos por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en eIDAS, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.
- **Certificados no cualificados:** son certificados ordinarios, sin la consideración legal de certificado cualificado.
- **Clave:** secuencia de símbolos empleados para controlar las operaciones de cifrado y descifrado.
- **Confidencialidad:** la confidencialidad es la capacidad de mantener un documento electrónico inaccesible a todos los usuarios, salvo a una determinada lista de personas. De este modo, podemos conseguir que las comunicaciones no sean escuchadas por otros y enviar documentos que solo puedan ser leídos por el destinatario indicado.
- **Criptografía:** la criptografía es una rama de las Matemáticas que estudia la transformación de información legible en información que no se puede leer directamente, es decir, que tiene que ser descifrada para ser leída.



- **Datos de creación de firma (Clave Privada):** una clave privada es un número único y secreto que pertenece a una única persona de manera que se puede identificar a la persona por medio de su clave privada. Esta clave es asimétrica a su clave pública. Una clave puede verificar y descifrar lo que la otra ha firmado o cifrado.
- **Datos de Verificación de firma (Clave Pública):** una clave pública es un número único que pertenece a una única persona pero que, a diferencia de la clave privada, puede ser conocida por todos. A través de procedimientos matemáticos se relaciona con la clave privada y sirve para encriptar y verificar firmas digitales.
- **Declaración de Prácticas de Certificación (DPC):** declaración que IZENPE pone a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita. Tendrá la consideración de documento de seguridad en el que se detallarán, en el marco de eIDAS, las obligaciones que los Prestadores de Servicios de Certificación 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 y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.
- **Directorio de Certificados:** repositorio de información que sigue el estándar X.500 del ITU-T. De este modo, IZENPE mantiene un directorio actualizado de certificados en el que se indicarán los certificados expedidos.
- **Dispositivo cualificado de creación de firma:** dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II de eIDAS.
- **Firma electrónica:** los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- **Firma electrónica avanzada:** firma electrónica que cumple los requisitos contemplados en el artículo 26 de eIDAS.
- **Firma electrónica cualificada:** firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- **Firmante:** es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
- **Hash o huella digital:** resultado de tamaño fijo que se obtiene tras aplicar una Función hash a un mensaje y que se encuentra asociado unívocamente a los datos iniciales.
- **HSM (Módulo de seguridad criptográfico):** es un dispositivo de seguridad que genera y protege claves criptográficas.
- **Infraestructura de Claves Públicas (PKI, Public Key Infrastructure):** una PKI determina qué entidades entran a formar parte del sistema de certificación, qué papel juegan dichas entidades, qué normas y protocolos se deben seguir para poder operar dentro del sistema, cómo se codifica y se transmite la información digital, y qué información



contendrán los objetos y documentos gestionados por la infraestructura. Todo esto basado en la tecnología de Clave Pública (dos claves).

- **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 (RGPD):** Reglamento Europeo que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
- **Listas de Certificados Revocados (CRLs):** es aquella lista donde figura la relación de certificados revocados que IZENPE emite desde el momento en que se produce una revocación con carácter inmediato. Existe también un servicio Web disponible de forma permanente que permite consultar la actualización incremental telemática de certificados revocados por IZENPE. En cuanto a la publicación de las Listas de Certificados Revocados, se garantiza un acceso a los usuarios y suscriptores de los certificados de forma segura y rápida
- **Número de serie del Certificado:** es un valor entero y único asociado inequívocamente con un certificado expedido por cualquier Prestador de Servicios de Certificación.
- **OCSP (Online Certificate Status Protocol):** es un protocolo informático que permite la comprobación del estado de un certificado electrónico.
- **OID (Object Identifier):** valor que comprende una secuencia de componentes variables constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que poseen la propiedad de ser únicos entre el resto de OID.
- **PIN (Personal Identification Number):** Secuencia de caracteres que únicamente puede ser conocido por el sujeto que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- **Política de Certificación:** es un documento anexo a la Declaración de Prácticas de Certificación que recoge el ámbito de aplicación, los caracteres técnicos de los diferentes tipos de certificados, el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación, así como sus condiciones de uso.
- **Poseedores de claves:** son las personas físicas que poseen o responden de la custodia de las claves de autenticación y firma digital.
- **Prestador cualificado de servicios de confianza (TSP):** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados según eIDAS y al que el organismo de supervisión ha concedido la cualificación
- **Servicio de Verificación Avanzada:** servicio que permite a la Entidad Usuaria del servicio beneficiarse de la utilización de los certificados emitidos por IZENPE mediante la comprobación del estado de los certificados basándose en el protocolo OCSP (Online Certificate Status Protocol).



- **Servicio de Publicación:** es el servicio en el que se publica la documentación relacionada con el sistema de certificación que debe ser accesible a los usuarios de los certificados.
- **Servicio de Sellos de Tiempo:** es el servicio que permite a la Entidad Usaria obtener una garantía referente a que cierta información existía en un momento concreto de tiempo.
- **Servidor Seguro:** es un servidor Web en el que la comunicación viaja encriptada de extremo a extremo, de forma segura. Para poder realizar esta operación, se necesita que el servidor disponga de un Certificado.
- **Solicitante del certificado:** es aquella persona que, en su propio nombre o en nombre de una organización, solicita la emisión de un certificado.
- **SSL (Secure Socket Layer):** es un protocolo que permite la transmisión de información cifrada entre un navegador de internet y un servidor.
- **Suscriptor del certificado:** es la persona cuya identidad personal queda vinculada a los datos firmados electrónicamente, a través de una Clave Pública certificada por el Prestador de Servicios de Certificación.
- **Tarjeta Criptográfica:** es aquella tarjeta considerada como Dispositivo Seguro de Creación de Firma empleada por el Suscriptor para: almacenar claves privadas de firma y autenticación, para generar firmas electrónicas y descifrar mensajes de datos.
- **Terceros que confían en terceros:** son las personas físicas o jurídicas que reciben certificados emitidos por IZENPE. Son terceros que confían en certificados y, como tales, les es de aplicación lo establecido por la Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados.
- **Usuarios de los certificados:** las entidades finales usuarias de los certificados son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales.
- **Creador de un sello:** persona jurídica que crea un sello electrónico
- **Sello electrónico:** datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos
- **Sello electrónico avanzado:** sello electrónico que cumple los requisitos contemplados en el artículo 36 de eIDAS
- **Sello electrónico cualificado:** sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico
- **Datos de creación del sello electrónico:** datos únicos que utiliza el creador del sello electrónico para crearlo
- **Certificado de sello electrónico:** declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona



- **Certificado cualificado de sello electrónico:** certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III de eIDAS
- **Dispositivo de creación de sello electrónico:** equipo o programa informático configurado que se utiliza para crear un sello electrónico
- **Dispositivo cualificado de creación de sello electrónico:** dispositivo de creación de sellos electrónicos que cumple mutatis mutandis los requisitos enumerados en el anexo II de eIDAS
- **Sello de tiempo electrónico:** datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante
- **Sello cualificado de tiempo electrónico:** sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 de eIDAS

1.6.2 Acrónimos

ARL: Lista de Revocación de Autoridades de Certificación

CA: Autoridad de Certificación

CN: Common Name (Nombre común)

CRL: Certificate Revocation List (Lista de Certificados Revocados)

DN: Distinguished Name (Nombre distintivo)

DPC: Declaración de Prácticas de Certificación

QSCD: Dispositivo Cualificado de Creación de Firma

ETSI: European Telecommunications Standards Institute

GN: nombre propio del poseedor en un certificado

HSM: Hardware Security Module (Módulo de Seguridad Criptográfico)

LRA: Autoridad de Registro Local

OCSP: Online Certificate Status Protocol (Servicio de Publicación de Certificados Revocados a partir de una fecha y una hora)

OID: Object Identifier (Identificador de objeto único)

PIN: Personal Identification Number (Número de identificación personal)

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

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

PSC: Prestador de Servicios de Certificación

RA: Autoridad de Registro

SSL: Secure Socket Layer

TSA: Servidor de la Autoridad de Sellado de Tiempo



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 la que se deroga la Directiva 1999/93/CE



2 Publicación y responsables del repositorio de información

2.1 Repositorio de información

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

2.2 Publicación de información de certificación

IZENPE garantiza la disponibilidad de la DPC, políticas específicas de certificados y términos y condiciones de uso de los certificados en www.izenpe.eus.

IZENPE garantiza el acceso a la información de estado del certificado a usuarios y suscriptores de forma segura, rápida y gratuita. Dicho acceso se puede realizar de dos formas:

- Consulta online (OCSP): Izenpe facilita la utilización de un servicio rápido y seguro de consulta del estado de los certificados emitidos, a disposición de los terceros que confían en los certificados.
- Consulta offline (CRL): mediante la publicación de listas de Certificados Revocados (CRLs)

Izenpe mantiene sitios web de test para que proveedores de software puedan probar sus productos con certificados SSL/TLS en entorno de producción. Izenpe mantiene sitios diferentes con al menos un certificado final vivo, caducado y revocado. Consultar en la Política específica la ruta de cada uno de ellos.

2.2.1 Política de publicación y notificación

Los cambios en las especificaciones o en las condiciones del servicio serán comunicados por IZENPE a los usuarios a través de www.izenpe.com. IZENPE podrá establecer canales adicionales de comunicación para situaciones específicas.

En el caso de DPC, Políticas específicas de certificados y Términos y Condiciones de Uso se mantendrán en www.izenpe.com de forma indefinida la versión vigente y todas las anteriores.

2.2.2 Elementos no publicados en la Declaración de Prácticas de Certificación

La relación de componentes, subcomponentes y elementos que existen pero que por su carácter confidencial no están a disposición del público son los referidos en el apartado “9.3.2 Información que no está dentro del alcance” de la presente Declaración de Prácticas de Certificación.

2.3 Frecuencia de publicación

La Declaración de Prácticas de Certificación se publica en el momento de su aprobación. Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en el presente documento.

La información sobre el estado de los certificados se publica de acuerdo con lo establecido en los apartados “4.9.6 más adelante y “4.9.9 Requisitos de comprobación de revocación online” del presente documento.



2.4 Control de acceso al repositorio

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 están disponibles para su consulta.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.



3 Nombres

3.1.1 Tipos de nombres

Todos los certificados de entidad final contienen un nombre distinguido en el campo Subject Name.

Los atributos que componen el nombre diferenciado del campo subject son los recogidos en el apartado correspondiente al perfil del certificado

El valor autenticado del campo *Common Name* es el nombre del suscriptor y en su caso del poseedor de las claves.

Adicionalmente el campo *subjectAltName* es utilizado en ocasiones para contener un nombre que pueda ser utilizado para identificar al sujeto, distinto del que aparece en el campo Subject Name.

Emisor

Este campo contiene la identificación de IZENPE, la Entidad de Certificación que ha firmado y emitido el certificado.

El campo no puede estar en blanco y contiene obligatoriamente un nombre diferenciado (DN) compuesto por un conjunto de atributos, consistentes en un nombre o etiqueta y un valor asociado.

El campo issuer de las CAs subordinadas coincide con el campo subject de la CA que ha emitido dichos certificados.

Asunto

Este campo contiene la identificación del suscriptor o titular del certificado emitido por IZENPE (la CA identificada en el campo Issuer del mismo).

El campo no puede estar en blanco y contiene obligatoriamente un nombre diferenciado (DN). Un nombre diferenciado se compone de un conjunto de atributos, que consisten en un nombre o etiqueta y un valor asociado.

La *Documentación específica para cada certificado* establece el perfil detallado de cada certificado.

3.1.2 Reglas para la Interpretación de formatos de nombres

El subject y el nombre del emisor en un certificado identifica a la persona (física o jurídica) o dispositivo, y deberán tener significado en el sentido de que la RA dispone de la evidencia de la asociación entre estos nombres o pseudónimos y las entidades a las que están asignados. Los nombres no podrán ser engañosos. Esto no excluye a los certificados de pseudónimo definidos en el apartado "3.1.3 Unicidad de los nombres".



3.1.3 Unicidad de los nombres

Los nombres de los suscriptores y, en su caso, los poseedores de claves son únicos para cada tipo de certificado. En el common name (CN) se deben cumplir los requisitos de unicidad y de espacios en el nombre. Izenpe podrá emitir certificados de pseudónimo, pero éstos no pueden ser certificados de CA o CA subordinada. Los detalles de perfil de cada tipo de certificado se pueden consultar en www.izenpe.eus.

3.1.4 Resolución de conflictos relativos a nombres y tratamiento 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 de la identidad

3.2.1 Métodos para probar la posesión de la clave privada

Cuando el par de claves es generado,

- Por una Entidad de Registro y las claves están alojadas en una tarjeta criptográfica, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación de la tarjeta criptográfica y del correspondiente certificado y par de claves almacenados en su interior.
- Por una Entidad de Registro y las claves están alojadas en un HSM, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de custodia en el HSM y del acceso exclusivo a las claves por parte del suscriptor.
- Por el propio poseedor de claves del certificado, la demostración de posesión de la clave privada consiste en la correcta utilización del certificado.
- Por el contenedor de claves del navegador, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de generación del par de claves y de emisión del certificado.
- Por el contenedor de claves del dispositivo móvil, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de generación del par de claves y de emisión del certificado.

3.2.2 Autenticación de la identidad de la organización

Izenpe se basa en las especificaciones del Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de



confianza para las transacciones electrónicas en el mercado interior. Consultar Política correspondiente.

3.2.3 Autenticación de la identidad de la persona física solicitante

Izenpe se basa en las especificaciones del Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Consultar Política correspondiente.

3.3 Identificación y autenticación para peticiones de reemisión de claves

Las condiciones de identificación y autenticación de una petición de reemisión se desarrollan en la Política correspondiente

3.4 Identificación y autenticación para peticiones de revocación

Las condiciones de autenticación de una petición de revocación se desarrollan en la Política correspondiente.



4 Requisitos operativos del ciclo de vida de los certificados

La presente Declaración de Prácticas de Certificación regula los requisitos operativos comunes a los certificados emitidos. En el caso de que Izenpe realice cross-certification con una CA externa, exigirá a dicha CA el cumplimiento de todos los requisitos definidos en la presente Declaración de Prácticas de Certificación y las políticas de certificado relacionadas.

La regulación específica para cada tipo de certificado deberá consultarse en la Política correspondiente.

4.1 Solicitud de certificado

No será necesaria nueva *Solicitud de Emisión* en el caso de emisiones realizadas como consecuencia de una revocación debida a fallos técnicos en la emisión y/o distribución del certificado o documentación relacionada.

Se recogen con exactitud, (dentro de los límites técnicos establecidos en el contenido del certificado), los datos identificativos correspondientes a cada tipo de certificado. Consultar *Política específica de cada certificado*.

4.1.1 Comprobación de la solicitud

IZENPE de forma previa a la emisión del certificado comprobará los datos que constan en la solicitud según Política de certificado correspondiente.

4.1.2 Proceso de inscripción y responsabilidades.

Las tareas de identificación y acreditación de la información que consta en el certificado, así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los mismos serán realizados por Entidades de Registro propias o Entidades usuarias con las que Izenpe suscriba el correspondiente instrumento legal. Éstas últimas deberán asumir las siguientes obligaciones:

- Comprobar la identidad y aquellas otras circunstancias personales del solicitante, suscriptor y poseedor de claves que consten en los certificados o sean relevantes para el fin de los certificados, conforme a los presentes procedimientos.
- Conservar toda la información y documentación relativa a los certificados, cuya emisión, renovación, revocación o reactivación gestiona.
- Comunicar a IZENPE, con la debida diligencia, las solicitudes de revocación de los certificados de forma rápida y fiable.
- Permitir a IZENPE el acceso a los archivos y la auditoría de sus procedimientos en la realización de sus funciones y en el mantenimiento de la información necesaria para las mismas.



- Informar a IZENPE de las solicitudes de emisión, renovación, reactivación y cualquier otro aspecto que afecte a los certificados emitidos por la misma.
- Comprobar, con la diligencia debida, las causas de revocación que pudieran afectar a la vigencia de los certificados.
- Cumplir en el desempeño de sus funciones de gestión de emisión, renovación y revocación de los certificados los procedimientos establecidos por IZENPE y la legislación vigente en esta materia.
- En caso de que el tipo de certificado lo exija podrá asumir la función de poner a disposición del suscriptor y/o poseedor de claves los procedimientos técnicos de creación y de verificación de firma electrónica.

4.2 Procesamiento de las solicitudes

4.2.1 Realización de funciones de identificación y autenticación

Es responsabilidad de IZENPE realizar la identificación del suscriptor de forma adecuada. Este proceso deberá ser realizado previamente a la emisión del certificado.

En todo caso es necesario consultar las especificidades de cada tipo de certificado en la *Política específica para cada certificado*.

4.2.2 Aprobar o rechazar solicitudes

Una vez realizada la solicitud de certificado, la RA deberá verificar la información proporcionada por el solicitante, incluyendo la validación de la identidad del suscriptor.

Si la información no es correcta, la RA denegará la petición, contactando con el solicitante para comunicarle el motivo. Si es correcta, se procederá entonces a la emisión del certificado.

Cuando esta solicitud sea para un certificado que incluya un nombre de dominio para la autenticación de un servidor, Izenpe examinará el registro de la CAs autorizadas, CAA, según la RFC 6844, y si esos registros CAA están presentes y no permiten a Izenpe emitir esos certificados porque no se encuentra registrado, Izenpe no emitirá ese certificado, pero permitirá a los solicitantes volver a realizar la solicitud una vez Izenpe haya podido subsanar esa posible incidencia.

En todo caso es necesario consultar las especificidades de cada tipo de certificado en la *Política específica para cada certificado*.

4.3 Emisión del certificado

La emisión de un certificado implica la aprobación final y completa de una solicitud. IZENPE emitirá el certificado y procederá a su entrega según condiciones de Política de Certificado correspondiente. Además, Izenpe entregará al poseedor los códigos de desbloqueo en los casos en los que Izenpe genere las claves.

Si en el plazo de 1 mes desde la solicitud de emisión el solicitante no ha recibido el certificado, deberá ponerse en contacto con IZENPE.



4.3.1 Acciones de la CA durante la emisión

Consultar las especificidades para la emisión de cada tipo de certificado en la *Política específica para cada certificado*.

4.3.2 Notificación al suscriptor de la emisión

IZENPE notifica al suscriptor la emisión del certificado

4.4 Aceptación del certificado

La aceptación del certificado supone que el suscriptor reconoce estar de acuerdo con los términos y condiciones contenidos en el contrato que rige los derechos y obligaciones de IZENPE y del suscriptor y conocer la presente Declaración de Prácticas de Certificación, que rige técnica y operativamente los servicios de certificación digital prestados por IZENPE.

El suscriptor/poseedor de claves dispone de un plazo de 15 días, desde la entrega del certificado, para comprobar el correcto funcionamiento del mismo y en caso de que fuera necesario devolverlo a Izenpe.

Si la devolución se debiese a defectos de funcionamiento por causas técnicas (entre otras: mal funcionamiento del soporte del certificado, problemas de compatibilidad de programas, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado, IZENPE revocará el certificado emitido y procederá a emitir un nuevo certificado.

4.4.1 Proceso de aceptación del certificado

Con la firma del documento de solicitud del certificado se aceptan también los términos y condiciones de uso, disponibles en www.izenpe.com.

4.4.2 Publicación del certificado por la CA

Una vez que el certificado ha sido aceptado por el suscriptor y generado, el certificado será publicado en repositorios internos de Izenpe. Cualquiera puede acceder a la información de estado del certificado mediante consulta a la VA o a la CRL.

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

Los certificados de Servidor Seguro (SSL) son publicados en el servicio Certificate Transparency Log Server (CT), según política de Google. El resto de certificados no se notifican a ninguna entidad.



4.5 Par de claves y usos del certificado

4.5.1 Clave privada del suscriptor y uso del certificado

El suscriptor que custodia sus claves,

- Garantizará el buen uso y la conservación de los soportes de los certificados.
- Empleará adecuadamente el certificado y, en concreto, cumplirá con las limitaciones de uso de los certificados.
- Será diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la Declaración de Prácticas de Certificación.
- Notificará a IZENPE y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida, el robo o el compromiso potencial de su clave privada.
 - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo criptográfica) o por cualquier otra causa.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, instando la revocación del certificado cuando dicha modificación constituya causa de revocación del mismo.
- Dejará de emplear la clave privada transcurrido el periodo de validez del certificado.
- Transferirá a los poseedores de claves las obligaciones específicas de los mismos.
- No monitorizará, manipulará o realizará actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de la Entidad de Certificación.
- No comprometerá intencionadamente la seguridad de los servicios de certificación.
- No empleará las claves privadas correspondientes a las claves públicas contenidas en los certificados, con el propósito de firmar ningún certificado, como si se tratase de una Entidad de Certificación.
- El suscriptor de certificados cualificados que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado, debe reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se emplee dispositivo criptográfico, conforme a lo indicado por eIDAS.

El suscriptor que tiene sus claves albergadas en Izenpe,

- Empleará adecuadamente el certificado y, en concreto, cumplirá con las limitaciones de uso de los certificados.



- Será diligente en la custodia de su clave de activación, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la Declaración de Prácticas de Certificación.
- Notificará a IZENPE y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, instando la revocación del certificado cuando dicha modificación constituya causa de revocación del mismo.
- Dejará de emplear la clave privada transcurrido el periodo de validez del certificado.
- Aceptará las obligaciones indicadas en la presente Declaración de Prácticas de Certificación
- No monitorizará, manipulará o realizará actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de la Entidad de Certificación.
- No comprometerá intencionadamente la seguridad de los servicios de certificación.
- El suscriptor de certificados cualificados que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado, debe reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se emplee un dispositivo cualificado de creación de firma, conforme a lo preceptuado en eIDAS.

4.5.2 Uso de la clave pública y del certificado por terceros que confían en los certificados

El usuario verificador de certificados queda obligado a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Conocer las condiciones de utilización de los certificados conforme a lo previsto en la Declaración de Prácticas de Certificación
- Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de verificador.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.



- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de IZENPE
- No comprometer intencionadamente la seguridad de los servicios de certificación.
- Reconocer que tales firmas electrónicas son equivalentes a firmas manuscritas, de acuerdo con eIDAS.

4.6 Renovación del certificado

La renovación del certificado consiste en la emisión de un nuevo certificado al suscriptor sin cambiar ninguna información del suscriptor (u otros participantes) o cualquier otra información que aparezca en el certificado. Dependiendo del tipo de certificado el periodo de validez puede ser diferente. Los costes de emisión están indicados en www.izenpe.com. Se podrán mantener las claves en los casos indicados según Política específica del certificado.

4.6.1 Circunstancias para la renovación del certificado

Izenpe realiza esfuerzos razonables para notificar a los suscriptores la próxima expiración del certificado. La notificación se realizará normalmente durante el periodo de 60 días previos a la caducidad del certificado.

4.6.2 Quién puede solicitar la renovación

Cualquier suscriptor podrá pedir la renovación de su certificado si se cumplen las circunstancias descritas en la Política de certificado específica. Izenpe no renueva automáticamente ningún certificado.

4.6.3 Tratamiento de peticiones de renovación de certificado

El suscriptor podrá contactar con IZENPE y solicitar su renovación. IZENPE le informará de cómo formalizar su solicitud. Se aplicarán las directrices de la Política de certificado correspondiente.

4.6.4 Notificación al suscriptor

Se debe usar el mismo proceso de notificación que para peticiones de nuevo certificado.

4.6.5 Procedimiento de aceptación de un certificado renovado

Se debe usar el mismo proceso que para peticiones de nuevo certificado.

4.6.6 Publicación del certificado

Una vez el certificado haya sido renovado, el nuevo certificado se publicará en el mismo repositorio interno que los nuevos certificados.



4.6.7 Notificación a otras entidades

Según lo recogido en el punto 4.4.3

4.7 Renovación con regeneración de las claves del certificado

El proceso de “re-key” consiste en crear un nuevo certificado con una clave pública diferente (y número de serie) mientras se mantiene el contenido del subject del antiguo certificado. El nuevo certificado contendrá nueva información de validez y un nuevo par de claves, pero mantendrá el mismo subject.

Se renovarán las claves durante la renovación del certificado según Política específica del certificado.

4.7.1 Circunstancias para regenerar las claves del certificado

La regeneración de las claves del certificado tendrá lugar como parte de la renovación del certificado, según se indica en la sección 3.2 de la DPC. También se podrán regenerar las claves del certificado cuando éstas se vean comprometidas.

4.7.2 Quien lo puede pedir

Izenpe puede regenerar las claves de los certificados de las CAs, según documento de ceremonia de generación de nueva CA o subCA. Izenpe también puede regenerar las claves de los certificados del servicio de VA y TSA según procedimiento interno.

Cualquier suscriptor podrá pedir la renovación de su certificado si se cumplen las circunstancias descritas en la Política de certificado específica.

4.7.3 Tratamiento de las peticiones de renovación con regeneración de claves

El suscriptor podrá contactar con IZENPE y solicitar su renovación. IZENPE le informará de cómo formalizar su solicitud. Se aplicarán las directrices de la Política de certificado correspondiente.

4.7.4 Notificación al suscriptor

Se debe usar el mismo proceso de notificación que para peticiones de nuevo certificado.

4.7.5 Procedimiento de aceptación del certificado renovado

Se debe usar el mismo proceso que para peticiones de nuevo certificado.



4.7.6 Publicación del certificado

Una vez el certificado haya sido renovado, el nuevo certificado podrá ser publicado en los repositorios de certificados que se consideren necesarios.

4.7.7 Notificación a otras entidades

Según lo recogido en el punto 4.4.3.

4.8 Modificación del certificado

En caso de necesidad de modificar algún dato del certificado, IZENPE procederá a la revocación del certificado y a la emisión de uno nuevo.

4.9 Revocación

4.9.1 Circunstancias para la revocación

IZENPE revocará los certificados en los siguientes casos:

- Cuando la revocación sea solicitada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- Cuando se produzca la violación o puesta en peligro de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por el firmante o por un tercero.
- Cuando lo ordene una resolución judicial o administrativa.
- Fallecimiento o extinción de la personalidad jurídica del firmante, fallecimiento o extinción de la personalidad jurídica del representado, incapacidad sobrevenida total o parcial, del firmante o de su representado, terminación de la representación, disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- Cese en la actividad de IZENPE salvo que, previo consentimiento del firmante, la gestión de los certificados electrónicos expedidos por aquel sean transferidos a otro prestador de servicios de certificación.
- Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del mismo.
- Cuando se produzca la pérdida, robo o se inutilice el certificado por daños en el soporte del certificado o en el caso de modificación del soporte a otro soporte no previsto en la política de certificación.
- Cuando alguna de las partes incumpla sus obligaciones.
- Cuando se haya producido un error en la emisión del certificado debido a una falta de adecuación al procedimiento establecido o a problemas técnicos durante el proceso de emisión del certificado.



- Cuando por circunstancias diferentes al compromiso de los datos de creación de firma, la seguridad de los sistemas y la fiabilidad de los certificados emitidos por IZENPE pueda verse afectada.
- Cuando se produzcan fallos técnicos en la emisión y/o distribución del certificado o documentación relacionada.
- Cuando solicitado el certificado transcurran tres meses hasta que el solicitante recoja el mismo.
- Cuando IZENPE reciba una solicitud de emisión de certificado, existiendo un certificado vigente de la misma política y con el mismo criterio de unicidad, se procederá a la revocación del certificado vigente previa solicitud de revocación del solicitante.

4.9.2 Quién puede solicitar la revocación

Podrán solicitar la revocación del certificado,

- El suscriptor.
- Representante Legal de la entidad suscriptora o tercero autorizado.
- Responsable de Personal o tercero autorizado.
- El solicitante.
- Izenpe en los casos de causa técnica contemplados en este documento.

4.9.3 Tratamiento de las peticiones de 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.com
 - O ante la organización suscriptora con la que Izenpe haya suscrito el instrumento legal pertinente.
- Online, en la dirección www.izenpe.com
- Por correo electrónico, enviando el formulario de solicitud de revocación firmado con un certificado cualificado

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

4.9.4 Tiempo de plazo de la CA para procesar la revocación

Una vez realizado lo indicado en el apartado “4.9.3 Tratamiento de las peticiones de revocación”, y la revocación debidamente tramitada por la RA (o por Izenpe en los casos



indicados en el apartado “4.9.1 Circunstancias para la revocación”), la revocación se hará efectiva inmediatamente.

4.9.5 Obligación de verificación de las revocaciones por terceros de confianza

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

IZENPE suministra información a los verificadores acerca de cómo y dónde encontrar la CRL y/o OCSP correspondiente.

4.9.6 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.

4.9.7 Tiempo transcurrido entre la generación y la publicación de las CRLs

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

4.9.8 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.

4.9.9 Requisitos de comprobación de revocación online

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.

4.9.10 Otras formas de avisos de revocación disponibles

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

4.9.11 Requisitos especiales clave comprometida

En caso de compromiso de la clave privada del certificado el suscriptor/poseedor de claves deberá notificar la circunstancia a IZENPE para que se proceda a solicitar la revocación del certificado y cesar el uso del certificado.

En caso de compromiso de la clave privada de una CA de IZENPE, se procederá de acuerdo a lo establecido en la sección 5.7.3 del presente documento.

4.10 Servicios de estado de los certificados

4.10.1 Características operativas

IZENPE ofrece un servicio gratuito de publicación de Listas de Certificados Revocados (CRL) sin restricciones de acceso. Adicionalmente, ofrece servicios de validación de certificados mediante el protocolo OCSP (Online Certificate Status Protocol).

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).

4.11 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

IZENPE no ofrece ese servicio.



5 Controles de seguridad física, de procedimiento y de personal

Izenpe dispone de controles de seguridad física en todos aquellos lugares en los que IZENPE presta servicios.

5.1.1 Localización y construcción de las instalaciones

Las instalaciones en las que se procesa información cumplen los siguientes requisitos físicos:

- El edificio que contiene las instalaciones de procesamiento de información es físicamente sólido, los muros externos del emplazamiento son de construcción sólida y está permanentemente vigilado por cámaras de seguridad, permitiendo únicamente el acceso a personas debidamente autorizadas.
- Todas las puertas y ventanas están cerradas y protegidas contra accesos no autorizados.

5.1.2 Acceso físico

Centro de Proceso de Datos

Las instalaciones de IZENPE disponen de un completo sistema de control de acceso físico compuesto por:

- Un perímetro de seguridad que se extiende desde el suelo real hasta el techo real para evitar accesos no autorizados.
- Control de acceso físico a las instalaciones,
 - Únicamente está permitido el acceso a personal autorizado.
 - Los derechos de acceso al área segura son revisados y actualizados periódicamente.
 - Se requiere que todo el personal porte algún elemento de identificación visible y se fomenta que el personal requiera dicha identificación a cualquiera que no disponga de la misma.
 - El personal ajeno a la operación de IZENPE que se encuentre trabajando en sus instalaciones es supervisado.

Se mantiene de forma segura un fichero log de los accesos.

Las puertas de entrada a IZENPE están dotadas con mecanismos de acceso.

Un circuito cerrado de televisión que monitoriza los elementos con los que IZENPE presta el servicio de certificación.

Autoridades de Registro (RAs)

Las RAs cumplen los criterios de seguridad necesarios, definidos tanto en la Política de Seguridad como en la Política de Seguridad de Proveedores de Izenpe.



5.1.3 Electricidad y aire acondicionado

El Centro de Proceso de Datos cuenta con sistemas de energía y aire acondicionado adecuados para garantizar un entorno operativo fiable.

Así mismo las instalaciones de IZENPE disponen de una funcionalidad de alimentación ininterrumpida (SAI y grupo electrógeno) que mantiene los equipos en funcionamiento durante el tiempo necesario para el cierre ordenado de los sistemas en el caso en que un fallo de energía o aire acondicionado provocara la caída de los mismos.

5.1.4 Exposición al agua

IZENPE ha adoptado las medidas necesarias para minimizar los riesgos derivados de los daños por agua.

5.1.5 Prevención y protección de incendios

El Centro de Procesos de Datos de IZENPE dispone de barreras físicas, desde el suelo real hasta el techo real, así como de sistemas de detección automática de incendios con la finalidad de:

- Avisar del inicio de un incendio al servicio de vigilancia y al personal de IZENPE.
- Cumplir con las misiones de desconexión del sistema de ventilación, cierre de las compuertas contrafuego, corte de la energía eléctrica y el disparo de la instalación automática de extinción.

5.1.6 Almacenamiento de soportes

Los soportes de las copias de seguridad se almacenan de forma segura.

5.1.7 Tratamiento de residuos

Se ha establecido una política reguladora de los procedimientos de destrucción de los soportes de información.

Los soportes que contengan información confidencial se destruyen de tal manera que la información sea irre recuperable con posterioridad a su desecho.

5.1.8 Copia de respaldo fuera de las instalaciones

IZENPE almacena los soportes de las copias de seguridad de forma que se encuentren protegidos frente a accidentes y a una distancia suficiente para evitar que resulten dañados en el caso de un desastre en el emplazamiento principal.

5.2 Controles de procedimientos

5.2.1 Funciones fiables

Se define “rol de confianza” como aquel al que se le asignan funciones que pueden dar lugar a problemas de seguridad si no se realizan adecuadamente, bien por accidente o de forma malintencionada.



Con la finalidad de incrementar la probabilidad de que las funciones correspondientes a un “rol de confianza” se realicen correctamente, se contemplan dos enfoques:

- El primero es el diseño y configuración de la tecnología, de forma que se eviten errores y se prohíba un comportamiento inadecuado.
- El segundo es la distribución de las funciones entre varias personas de forma que la actividad malintencionada requiera la connivencia de varias de ellas.

IZENPE dispone de una completa definición de los roles desarrollados en la organización. Para todos ellos, están definidas las funciones y responsabilidades de cada uno de ellos.

5.2.2 Número de personas por tarea

Para reforzar la seguridad del sistema, se asignan personas diferentes para cada rol con la excepción del rol de operador que puede ser asumido por el administrador.

Además, se pueden asignar múltiples individuos a un mismo rol.

5.2.3 Identificación y autenticación para cada rol

Los roles de confianza exigen la autenticación con un medio suficientemente seguro, y en cualquier caso siempre con usuarios personales.

IZENPE dispone de documentación específica en el que se especifican los roles de cada uno.

5.2.4 Separación de tareas en los diferentes roles

IZENPE sigue la política de seguridad CIMC (Certificate Issuing and Management Component) y está definida en su modelo de seguridad.

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autenticación

IZENPE emplea personal que posee la experiencia y calificación necesarias para los servicios que debe realizar.

Todo el personal con roles fiables está libre de intereses que puedan perjudicar la imparcialidad de las operaciones de IZENPE.

5.3.2 Procedimientos de investigación de historial

Izenpe dentro de sus procedimientos de Recursos Humanos realiza las investigaciones pertinentes antes de la contratación de cualquier persona. Por limitaciones legales no se incluye la comprobación de antecedentes penales.

5.3.3 Requisitos de formación

El personal de IZENPE recibe la formación requerida para asegurar su competencia en la realización de sus funciones. Se realiza al menos una vez al año una formación que incluye como mínimo los siguientes puntos:



- Entrega de una copia de la Declaración de Prácticas de Certificación.
- Concienciación sobre la seguridad
- Operación del software y hardware para cada rol específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimiento de operación y administración para cada rol específico.
- Procedimientos para la recuperación de desastres.
- Procedimiento de gestión de incidencias

Se realizará una formación y concienciación específica para los operadores de RA al menos durante su alta, y posteriormente con una periodicidad definida por Izenpe.

5.3.4 Requisitos y frecuencia de actualización formativa

Cualquier cambio significativo en la operación de IZENPE requerirá un plan de formación y la ejecución del plan será documentada. El personal perteneciente a “Trusted Roles” debe recibir al menos una formación anual, que les permita mantener sus niveles de capacitación. Dicha formación siempre debe incluir la revisión del contenido.

5.3.5 Secuencia y frecuencia de rotación laboral

La rotación de empleados en un puesto se realiza según necesidades del propio puesto, o por solicitud del propio empleado.

5.3.6 Sanciones para acciones no autorizadas

Incidentes de seguridad de la información

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

Proceso punitivo

Existe un régimen disciplinario interno que define el proceso punitivo.

5.3.7 Requisitos de contratación de personal

Todo el personal subcontratado por Izenpe para realizar funciones relacionadas con la operación de servicios de Izenpe está sujeto a los requerimientos de la Política de Seguridad de Proveedores de Izenpe.

5.3.8 Suministro de documentación al personal

Todo el personal relacionado con roles fiables recibe:

- Una copia de la Declaración de Prácticas de Certificación
- La documentación que define las obligaciones y procedimientos de cada rol.
- Tiene acceso a los manuales relativos a la operación de los diferentes componentes del sistema.



5.4 Audit

Se utilizarán los ficheros de log para reconstruir los eventos significativos que han sido realizados por el software de IZENPE y las Entidades de Registro y el usuario o evento que los originó. Podrá ser utilizado como un medio de arbitraje en posibles disputas mediante la comprobación de la validez de una firma en un momento determinado.

5.4.1 Tipo de eventos registrados

Se almacenan los siguientes logs:

- Nuevas peticiones de certificado
- Peticiones de certificado rechazadas
- Violaciones de acceso a cuentas
- Firma de certificados
- Revocación de certificados
- Logon de cuentas
- Firma de CRLs
- Modificaciones en CAs
- Caducidad de certificados

Esta lista es no inclusiva, y está limitada a los eventos que están relacionados directamente a la gestión de certificados o funciones administrativas. En particular, no se incluyen eventos técnicos que están registrados en otros sitios.

Para grabar la fecha y hora de cada evento, se utiliza una base de tiempos fiable.

5.4.2 Frecuencia de procesamiento de logs

Los logs son procesados continuamente y auditados con una periodicidad mensual por el Responsable de Seguridad. El informe de auditoría incluye los siguientes aspectos:

- Lista de intentos de acceso no autorizados
- Errores generados en cada CA
- Certificados SSL emitidos a rangos de IP no confiables

5.4.3 Periodo de retención del audit log

La información generada en el fichero log se mantiene en línea hasta el momento de ser archivada. Una vez archivados, los ficheros log son mantenidos durante 7 años.

5.4.4 Protección del audit log

Se asigna a acceso a la información de log a todo el personal que requiera el acceso como parte de su función. El rol de Auditor puede acceder. El diario está almacenado en la base de datos, y el acceso está protegido a diferentes niveles.

Está impedido el borrado no autorizado de los registros de log y la modificación de los mismos. Existen medidas de contingencia para evitar la pérdida de los datos de log.



5.4.5 Procedimiento de backup del audit log

Los logs están alojados en la base de datos, por lo que se incluye en el backup diario de la base de datos, según política de copias de seguridad.

5.4.6 Recolección de logs

Los archivos de log de CAs y RAs son almacenados en los sistemas internos de IZENPE.

5.4.7 Notificación de la acción causante de los logs

No está contemplada la notificación de la acción de los ficheros log al origen del evento.

5.4.8 Análisis de vulnerabilidades

Se realiza con una periodicidad trimestral un análisis de vulnerabilidades tanto externo como interno en los sistemas internos de IZENPE. Además anualmente se realiza un test de penetración.

5.5 Archivado de registros

5.5.1 Tipo de registros archivados

Los tipos de datos o ficheros que son archivados, entre otros, son los siguientes:

- Datos relacionados con el procedimiento de registro y solicitud de certificados;
- Los registros de auditoría de la sección anterior;
- Histórico de claves

5.5.2 Periodo de retención del archivo

Toda la información y documentación relativa a los certificados cualificados se conserva durante 15 años (a partir de la fecha de emisión), y la relativa al resto de certificados, durante 7 años (a partir de la fecha de finalización del certificado).

5.5.3 Protección del archivo

El Procedimiento de Gestión de Archivo indica las medidas de protección que se adoptarán para que tanto los registros en papel como en formato electrónico no puedan ser manipulados ni destruido su contenido.

5.5.4 Procedimientos de backup del archivo

Existe una política de copias de seguridad y Plan de Contingencias que define los criterios y estrategias de actuación ante una incidencia. El diseño de toda la estrategia de actuación ante incidencias se basa en el correspondiente inventario de activos y análisis de riesgos.

5.5.5 Requisitos para el sellado de tiempo de los registros

Los sistemas de información empleados por IZENPE garantizan el registro de los instantes de tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura de fecha y hora. Todos los sistemas sincronizan su instante de tiempo con esta fuente.



5.5.6 Sistema de archivo

El sistema de archivo se encuentra ubicado en las instalaciones de IZENPE y en las entidades que participan en la prestación del servicio.

5.5.7 Procedimientos para obtener y verificar la información del archivo

El acceso a esta información está restringido al personal autorizado a tal efecto, protegiéndose frente a accesos físicos y lógicos según lo establecido en las secciones 5 y 6 de la presente Declaración de Prácticas de Certificación.

5.6 Cambio de claves

Para minimizar el riesgo de compromiso de la clave privada de una CA, la clave debe ser cambiada en función del nivel de seguridad de los algoritmos utilizados. Una vez cambiada, la nueva clave sólo debe ser utilizada para funciones de firma. La antigua, aunque siga siendo válida, deberá estar disponible para verificar firmas antiguas hasta que todos los certificados firmados con ella hayan caducado. Únicamente se debe mantener la clave privada antigua en el caso de que se utilice para firmar CRLs que contienen certificados firmados con esta clave, y se protegerá con el mismo nivel de protección que la nueva. El procedimiento para la generación de una nueva clave de CA está definido en el Documento de Ceremonia de Generación de nueva CA y migración de antigua CA. El apartado 6.1.5 define los tamaños de clave y algoritmos utilizados

5.7 Plan de contingencias

5.7.1 Procedimientos de gestión de incidencias

Existe un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por IZENPE.

Los principales objetivos del Plan de Contingencia son:

- Maximizar la efectividad de las operaciones de recuperación mediante el establecimiento de tres fases:
 - Fase de Notificación/Evaluación/Activación para detectar, evaluar los daños y activar el plan.
 - Fase de Recuperación para restablecer temporal y parcialmente los servicios hasta la recuperación de los daños provocados en el sistema original.
 - Fase de Reconstitución para restaurar el sistema y los procesos a su operativa habitual.
- Identificar las actividades, recursos y procedimientos necesarios para la prestación parcial de los servicios de certificación en un CPD alternativo durante interrupciones prolongadas de la operativa habitual.



- Asignar responsabilidades al personal designado de IZENPE y facilitar una guía para la recuperación de la operativa habitual durante largos periodos de interrupción.
- Asegurar la coordinación de todos los agentes (departamentos de la entidad, puntos de contacto externos y vendedores) que participen en la estrategia de contingencia planificada.

El Plan de Contingencias de IZENPE es de aplicación al conjunto de funciones, operaciones y recursos necesarios para restaurar la prestación de servicios de certificación. Dicho plan se aplica al personal de IZENPE asociado a la prestación de los servicios de certificación.

El Plan de Contingencias establece la participación de ciertos grupos en la recuperación de las operaciones de IZENPE.

La evaluación de los daños y el plan de acción se describen en el Plan de Contingencias.

En el caso de producirse la circunstancia de que el algoritmo, la combinación de los tamaños de clave utilizados o cualquier otra circunstancia técnica que mermara significativamente la seguridad técnica del sistema se aplicará dicho Plan de Contingencia. Se realizará un análisis de impacto. En ese análisis se estudiará la criticidad del problema de seguridad, su ámbito y la estrategia de recuperación ante la incidencia. Los puntos que se deben definir como mínimo en el informe de análisis de impacto son:

- Descripción detallada de la contingencia, ámbito temporal, etc
- Criticidad, ámbito
- Solución o soluciones propuestas
- Plan de despliegue de la solución elegida, que incluirá al menos:
 - Notificación a los usuarios por el medio considerado más eficaz. Se incluirá tanto a los solicitantes como a los suscriptores y verificadores (terceras partes confiables) de los certificados.
 - Se informará en la web de la contingencia producida
 - Revocación de los certificados afectados
 - Estrategia de renovación

5.7.2 Plan de actuación ante datos y software corruptos

El Plan de Contingencias de IZENPE recoge la estrategia de actuación ante este tipo de situaciones.

5.7.3 Procedimiento ante compromiso de la clave privada

La CA Raíz revocará el certificado de una CA emisora en el caso que la clave privada de esa CA haya sido comprometida.

En el caso que la CA Raíz deba revocar el certificado de la CA emisora, lo notificará inmediatamente a:

- La CA emisora



- Todas las RA's autorizadas para el registro de esa CA
- Todos los signatarios titulares de certificados emitidos por esa CA.

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

Después de resolver los factores que indujeron la revocación, la CA Raíz puede:

- Generar un nuevo certificado para la CA emisora.
- Asegurar que todos los nuevos certificados y CRL emitidos por la CA son firmados utilizando la nueva clave.

La CA emisora podrá emitir certificados a todas las entidades finales afectadas.

En caso de que la clave comprometida sea la de la CA raíz, se eliminará el certificado de todas las aplicaciones y se distribuirá uno nuevo.

5.7.4 Continuidad de negocio después de un desastre

Se suspenderá la operación de la CA hasta el momento en que se haya completado el procedimiento de recuperación de desastre y se encuentre funcionando correctamente en el centro principal o alternativo.

Se activará el Plan de Contingencias y de Continuidad de Negocio de IZENPE.

5.8 Terminación de la CA o RA

5.8.1 Entidad de Certificación

IZENPE dispone de un Plan de Finalización de la CA que detalla el procedimiento que se ejecutaría ante esta circunstancia.

En caso de cese de su actividad, IZENPE comunicará al suscriptor por cualquier medio que garantice el envío y la recepción de la notificación, con un plazo mínimo de antelación de 2 meses a su fecha de su extinción, su intención de cesar como prestador de servicios de certificación.

De la misma manera, se notificará a TSPs, fabricantes de navegadores y cualquier entidad con la que IZENPE mantenga alguna relación contractual de uso de sus certificados.

Izenpe mantendrá durante el tiempo necesario según especificaciones de la presente DPC toda la información sobre registro, estado de revocación y archivo de logs. En el caso de transferencia a otra entidad se tomarán las medidas para que dicho traspaso se realice con todas las garantías necesarias.

La responsabilidad de esta notificación corresponde a la Dirección General de IZENPE o persona/as designadas por el Consejo de Administración, quien decidirá el mecanismo más adecuado.

En el supuesto de que IZENPE decidiera transferir la actividad a otro prestador de servicios de confianza, comunicará al Ministerio de Industria, Energía y Turismo y al suscriptor de sus certificados los acuerdos de transferencia. A tal efecto IZENPE enviará el documento explicativo de las condiciones de transferencia así como de las condiciones de utilización que regularán las relaciones entre el suscriptor y el TSP al cual se transfieren los certificados. Esta comunicación se realizará a través de la plataforma de envío de notificaciones de la sede



electrónica del Ministerio (<https://sede.minetur.gob.es/ES/procedimientoselectronicos/Paginas/ley592003.aspx>), con una antelación mínima de 2 meses previo al cese de su actividad.

El suscriptor deberá consentir de forma expresa la transferencia de los certificados, aceptando las condiciones del TSP al que se transfieren. Transcurrido el plazo de dos meses, sin que exista acuerdo de transferencia o sin que el suscriptor acepte expresamente la misma, los certificados serán revocados.

En el supuesto de que no existieran acuerdos con otros PSC, finalizado el plazo de los 2 meses de antelación en la comunicación, todos los certificados serán revocados de manera automática.

Se dará por finalizado cualquier autorización de terceros con los que Izenpe mantenga un contrato de prestación de servicios (identificación, emisión, albergue, etc.)

Izenpe o una entidad con la que Izenpe acuerde traspasar el servicio ofrecerá información de validez de todos sus certificados cualificados incluso cuando el certificado haya caducado.

5.8.2 Entidad de Registro

Una vez la Entidad de Registro cese en el ejercicio de las funciones que asuma transferirá los registros que mantenga a IZENPE, mientras exista obligación de mantener archivada la información dado que en otro caso, será cancelada y destruida.



6 Controles de seguridad técnica

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Las claves criptográficas de la CA raíz y subordinadas deben ser generadas en un módulo hardware criptográfico (HSM) que cumpla con FIPS 140-2 nivel 3 (o superior) y Common Criteria EAL 4+ sobre el perfil de protección correspondiente.

Las claves criptográficas de las RAs deben ser generadas en un módulo criptográfico que cumpla con FIPS 140-2 nivel 2 (o superior).

Las claves criptográficas de la VA deben ser generadas en un módulo hardware criptográfico (HSM) que cumpla con FIPS 140-2 nivel 3 (o superior).

Las claves criptográficas de la TSA deben ser generadas en un módulo hardware criptográfico (HSM) que cumpla con FIPS 140-2 nivel 3 (o superior).

Todas las claves criptográficas deben ser generadas siguiendo las recomendaciones de algoritmo y longitud de clave mínimas definidas en ETSI TS 119 312. En los casos en los que Izenpe genera las claves, éstas serán generadas en tarjeta / token criptográfico.

En los casos en los es el usuario final el que genera las claves, éstas podrán ser generadas en los siguientes dispositivos:

- Contenedor de certificados del navegador del usuario
- Contenedor de claves de cliente (ej: servidor web)
- Contenedor seguro de Izenpe
- Contenedor de la app de Izenpe para teléfono móvil

6.1.2 Distribución de la clave privada al suscriptor

Método de entrega de la clave privada varía en función de tipo de certificado y dispositivo. Consultar Política de certificado correspondiente.

6.1.3 Distribución de la clave pública al emisor del certificado

El método de entrega de la clave pública de las diferentes entidades que componen o colaboran con IZENPE al emisor de certificados correspondiente es el siguiente:

- Claves generadas por Izenpe (tarjeta, token, HSM): albergadas en el propio dispositivo criptográfico o contenedor seguro.
- Claves generadas en navegador: almacenadas en el contenedor de certificados del navegador.
- Claves generadas en teléfono móvil: almacenadas en el contenedor de la app de Izenpe
- Claves de certificado de servidor seguro (SSL): Izenpe envía por correo electrónico el certificado en formato X.509 al suscriptor o se pone a disposición del usuario en la aplicación de gestión de SSL.



- Claves públicas cuya clave privada ha sido generada por el suscriptor en el contenedor seguro: Izenpe envía por correo electrónico el certificado en formato X.509

6.1.4 Distribución de la clave pública de la Entidad de Certificación a los usuarios de certificados

Las claves públicas de las CA de IZENPE se distribuyen a través de varios medios, entre ellos la web de IZENPE. En la presente Declaración de Prácticas de Certificación, apartado 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.

El tamaño de las claves dependiendo de los casos es:

- Al menos 2048 bits para claves de personas físicas, jurídicas y de dispositivo, servidor OSCP, servidor TSA y certificados técnicos.
- Al menos 4096 bits para aquellas CAs emitidas a partir de 2007

6.1.6 Algoritmos de firma de certificados

El identificador de algoritmo (AlgorithmIdentifier) que emplea IZENPE para firmar los certificados es SHA2 (algoritmo de hash) con RSA (algoritmo de firma) que corresponde al identificador para "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc.". El esquema de padding utilizado es emsa-pkcs1-v2.1 (según RFC 3447 sección 9.2)".

Los certificados de usuario final están firmados con RSA con SHA-256. IZENPE recomienda a los usuarios finales que utilicen RSA con SHA-256 o superior a la hora de firmar con el certificado.

IZENPE utiliza un algoritmo cualificado por la industria y adecuado para el propósito de firma reconocida. Se tendrá en cuenta para ello el periodo de vigencia del certificado además sigue las recomendaciones indicadas por el CAB/Forum y por los diferentes estándares de ETSI.

En el caso de producirse la circunstancia de que el algoritmo, la combinación de los tamaños de clave utilizados o cualquier otra circunstancia técnica que mermará significativamente la seguridad técnica del sistema se aplicará dicho Plan de Contingencia. Se realizará un análisis de impacto. En ese análisis se estudiará la criticidad del problema de seguridad, su ámbito y la estrategia de recuperación ante la incidencia. Los puntos que se deben definir como mínimo en el informe de análisis de impacto son:

- Descripción detallada de la contingencia, ámbito temporal, etc
- Criticidad, ámbito
- Solución o soluciones propuestas
- Plan de despliegue de la solución elegida, que incluirá al menos:



- Notificación a los usuarios por el medio considerado más eficaz. Se incluirá tanto a los solicitantes como a los suscriptores y verificadores (terceras partes confiables) de los certificados.
- Se informará en la web de la contingencia producida
- Revocación de los certificados afectados
- Estrategia de renovación

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

6.2.1 Estándares de módulos criptográficos

Un módulo de seguridad criptográfico (HSM) es un dispositivo de seguridad que genera y protege claves criptográficas. Se requiere que los HSM cumplan el criterio FIPS 140-2 Nivel 3 como mínimo o Common Criteria EAL 4+ para el perfil de protección correspondiente.

IZENPE mantiene protocolos para comprobar que un HSM no ha sido manipulado durante su transporte y almacenamiento

En cuanto a los dispositivos criptográficos con certificados para firma electrónica cualificada, aptas como dispositivos cualificados de creación de firma (QSCD), cumplen el nivel de seguridad CC EAL4+, aunque también son admisibles las certificaciones equivalentes ITSEC E3 o FIPS 140-2 Nivel 2 como mínimo.

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

IZENPE, en cualquier caso, mantiene el control sobre la preparación, almacenamiento y distribución de los dispositivos de suscriptor en los que IZENPE genera las claves.

6.2.2 Control por más de una persona (n de m) sobre la clave privada

La utilización de las claves privadas de las CAs requiere la aprobación de al menos dos personas.

6.2.3 Custodia de la clave privada

La clave privada de la CA raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3 y/o CC EAL4+, garantizando que la clave privada nunca está fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente.



Las claves privadas de las CA Subordinadas están custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3.

En los casos en los que el suscriptor custodie la clave privada éste será el responsable de mantenerla bajo su exclusivo control.

6.2.4 Copia de respaldo de la clave privada

Existe un procedimiento de recuperación de claves de los módulos criptográficos de la CA (raíz o subordinadas) que se puede aplicar en caso de contingencia.

Existe un procedimiento de recuperación de claves de los módulos criptográficos de los suscriptores a los que Izenpe les custodia las claves, que se puede aplicar en caso de contingencia.

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

6.2.5 Archivado de la clave privada

IZENPE no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de la CA para comunicarse entre sí, firmar y cifrar la información serán archivadas, después de la emisión del último certificado.

Las claves privadas custodiadas por los suscriptores pueden ser archivadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación.

Las claves privadas de suscriptores gestionadas por Izenpe no se archivan una vez caducado o revocado el certificado.

6.2.6 Trasferencia de la clave privada a o desde el módulo criptográfico

La clave privada de la CA raíz, CAs subordinadas, VA y TSA son generadas en un HSM según lo especificado en el punto 6.2.1, y no es posible la exportación. Como medida de contingencia es posible la recuperación de las claves privadas según apartado 6.2.4.

En los siguientes dispositivos utilizados para la emisión de certificados de usuario final las claves son generadas en el módulo criptográfico, y no es posible la exportación de la clave privada:

- ✓ Tarjeta / Token criptográfico

En los casos en los que es el propio suscriptor el que genera las claves, será también el responsable de su custodia.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Existe un documento de ceremonia de claves de la CA raíz y CAs subordinadas donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

Izenpe sigue para la generación de las claves de las CAs las recomendaciones de ETSI EN 319 411-1, y CABForum Baseline Requirement Guidelines.



Izenpe sigue para la generación de las claves de suscriptores en tarjeta criptográfica las recomendaciones de la Comisión Europea (eIDAS) y de EN 319 411-1.

En los casos en los que se almacenen claves privadas fuera de los módulos criptográficos, éstas estarán protegidas de forma que se asegure el mismo nivel de protección que si estuviesen físicamente en el interior de los módulos criptográficos.

6.2.8 Método de activación de la clave privada

Las Claves privadas de las Autoridades de Certificación son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS PUB 140-2 Level 3.

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

6.2.9 Método de desactivación de la clave privada

Una persona con el rol de administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación mediante la detención del sistema. Para su reactivación se actuará según lo descrito en el apartado “6.2.8 Método de activación de la clave privada”.

En cuanto a la desactivación de las Claves privadas de los Certificados de entidad final se describe en la Política específica de cada certificado.

6.2.10 Método de destrucción de la clave privada

Existe un procedimiento de destrucción de claves de la CA.

En el caso de retirar el HSM que alberga las claves de la CA, éstas serán destruidas.

Este procedimiento no se aplica a las claves de firma o autenticación de usuario emitidas en tarjeta criptográfica salvo, en el caso de renovación de claves reutilizando el mismo dispositivo criptográfico, en el cual se destruirá la clave anterior y se generarán nuevas claves sobre el mismo soporte.

6.2.11 Calificación del módulo criptográfico

Según indicado en el apartado 6.2.1 del presente documento

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

Los certificados generados por la CA, y por lo tanto las claves públicas, son almacenados por la CA durante el periodo de tiempo obligado por la legislación vigente.

6.3.2 Periodos de operación del certificado y periodos de uso del par de claves

Los periodos de uso de los certificados emitidos por Izenpe son:

- ✓ El certificado de la CA raíz es válido durante 30 años.



- ✓ El certificado de la CA subordinada que emite los EVs es válida durante 10 años, el resto de CAs subordinadas son válidas hasta la caducidad de la CA raíz.
- ✓ El cambio de claves de los certificados de las CAs (raíz y subordinadas) se realizará a demanda, en función de los estándares determinados por la industria.
- ✓ Los certificados de usuario final tienen una duración diferente en cada caso, consultar la Política específica. En todos los certificados de persona física y jurídica la renovación implica regeneración de claves.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación, tanto de las claves de la CA raíz como de las claves de las CAs subordinadas que expiden los Certificados de entidad final, se generan durante la ceremonia de claves de creación de dichas Autoridades de Certificación.

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

6.4.2 Protección de datos de activación

Los datos de activación de las claves de la CA raíz están distribuidas en múltiples tarjetas físicas, siendo necesarias al menos dos personas para realizar cualquier operación. Las claves de las tarjetas están custodiadas en diferentes cajas fuertes.

Los datos de activación de las claves de las CAs subordinadas están distribuidas en múltiples tarjetas físicas, siendo necesarias al menos dos personas para realizar cualquier operación. Las claves de las tarjetas están custodiadas en diferentes cajas fuertes.

Las claves de la TSA y VA están generadas y gestionadas en mismo HSM que las claves de las CAs subordinadas. Aplican las mismas reglas.

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

6.4.3 Otros aspectos de los datos de activación

Ver Política específica de cada tipo de certificado.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

Existen una serie de controles en el emplazamiento de los diferentes elementos del sistema de prestación de servicio de certificación de IZENPE (CAs, BBDD de IZENPE, Servicios Internet de IZENPE, Operación CA y Gestión de Red):

- Controles operacionales.
 - Todos los procedimientos de operación están debidamente documentados en los correspondientes manuales de operación.

Existe un Plan de Contingencias.
 - Están implantadas herramientas de protección contra virus y códigos malignos.



- Se lleva a cabo un mantenimiento continuado del equipamiento, con el fin de asegurar su disponibilidad e integridad continuadas.
- Existe un procedimiento de salvado, borrado y eliminación segura de soportes de información, medios removibles y equipamiento obsoleto.
- Intercambios de datos. Los siguientes intercambios de datos van cifrados para asegurar la debida confidencialidad.
 - Transmisión de datos de registro entre las RAs y la base de datos de registro.
 - Transmisión de datos de prerregistro.
 - La comunicación entre las RAs y las CAs.
- El servicio de publicación de revocaciones posee las funcionalidades necesarias para que se garantice un funcionamiento 24x7.
- Control de accesos.
 - Se utilizarán IDs de usuario únicos, de forma que los usuarios son relacionados con las acciones que realizan y se les puede responsabilizar de sus acciones.
 - La asignación de derechos se lleva a cabo siguiendo el principio de concesión mínima de privilegios.
 - Eliminación inmediata de los derechos de acceso de los usuarios que cambian de puesto de trabajo o abandonan la organización.
 - Revisión trimestral del nivel de acceso asignado a los usuarios.
 - La asignación de privilegios especiales se realiza “caso a caso” y se suprimen una vez terminada la causa que motivó su asignación.
 - Existen directrices de calidad en las contraseñas
 - Todas las cuentas de operador con capacidad de emitir certificados tienen control de acceso basado en doble factor

Izenpe dispone de política de seguridad y procedimientos específicos para garantizar la seguridad a diferentes niveles.

6.5.2 Evaluación del nivel de seguridad informática

Los productos utilizados para la prestación de servicios de certificación disponen del certificado internacional basado en ISO/IEC 15408.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Se controla la implantación de software en los sistemas de producción.

Para evitar posibles problemas en dichos sistemas, se consideran los siguientes controles:

- La política de Izenpe incluye reglas para el desarrollo seguro de aplicaciones y sistemas



- Existe un procedimiento formal para el control de cambios. Se limitan a los necesarios, y son objeto de un control riguroso
- Cuando se cambian sistemas operativos se revisan las aplicaciones de negocio consideradas críticas según Plan de Continuidad de Negocio
- Se establecen principios de ingeniería de sistemas seguros
- El entorno de desarrollo está debidamente protegido
- El desarrollo externalizado es supervisado y controlado por Izenpe
- Se realizan pruebas de seguridad funcional durante el desarrollo
- Se establecen programas de pruebas de aceptación para nuevos sistemas de información, actualizaciones y versiones
- Los datos de prueba son seleccionados, y están protegidos y controlados

6.6.2 Controles de gestión de la seguridad

Izenpe monitoriza de forma continua para asegurar que los sistemas y comunicaciones operan según la Política de Seguridad de Izenpe. Todos los procesos son logueados y auditados de acuerdo con la legislación y normativa vigentes.

6.6.3 Controles de seguridad del ciclo de vida

La realización de pruebas requiere un volumen importante de datos, tan próximos a los datos de producción como sea posible. Se evita el uso de bases de datos de producción que contengan información personal.

6.7 Controles de seguridad de red

La seguridad de red está basada en el concepto de zonificación multi-nivel utilizando múltiples firewalls redundantes. La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL/TLS. Se dispone de sistemas IPS para el tráfico interno y externo.

6.8 Fuente de tiempo

IZENPE obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada siguiendo el protocolo NTP a través de la conexión establecida con el Gobierno Vasco. La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905.

Basándose en este servicio interno, Izenpe ofrece un servicio de sellado de tiempo (TSA) que puede ser utilizado para crear sellos de tiempo sobre documentos arbitrarios, según IETF RFC 3161 y ETSI EN 319 421. Más información en la Declaración de Prácticas de Sellado de Tiempo de Izenpe.



7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

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
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework.
- ETSI TS 101 867 Qualified Certificate Profile.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile.

7.1.1 Número de versión

Los certificados emitidos bajo la presente Declaración de Prácticas de Certificación utilizan el estándar X.509 versión 3 (populate version field with integer "2").

7.1.2 Extensiones de certificado

Indicadas en el documento de perfiles, disponible en www.izenpe.com.

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

Los formatos están indicados en el documento de perfiles, disponible en www.izenpe.com. Los perfiles de las CAs están en el punto 1.3.1 de este documento.

7.1.5 Restricciones de nombres

No se incluye la extensión "name constraints" en el perfil de los certificados de Autoridad Subordinada de Izenpe, por lo tanto no se da este tipo de restricción.

7.1.6 Identificador de objeto de política de certificado

De acuerdo a lo especificado en la sección 1.2 de la presente Declaración de Prácticas de Certificación.



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 lista de revocación de certificados

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.

Según se describe en RFC 6962, un precertificado no será considerado un certificado con las características definidas en la RFC 5280.

7.2.1 Número de versión

Versión 2 (populate version field with integer "1").



7.2.2 Lista de revocación de certificados y extensiones de elementos de la lista

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. Invalidation Date	Sí	No

7.3 Perfil 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 3.

7.3.2 Extensiones del OCSP

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

7.3.3 Otros aspectos del OCSP

- El servicio OCSP soporta el método GET
- La información de estado del certificado está permanentemente actualizada
- Las respuestas OCSP tienen una caducidad de 48 horas
- En las peticiones de estado de certificados que no han sido emitidos por Izenpe la respuesta es REVOKED.
- En las peticiones de estado de certificados emitidos por Izenpe, en el caso de que sea REVOKED, se incluye en la respuesta OCSP la extensión id-pkix-ocsp-extended-revoke
- En el caso de los certificados que no son de Izenpe se devuelve la respuesta obtenida de @Firma.
- Izenpe no soporta OCSP Stapling.



8 Auditorías de cumplimiento

La verificación de la conformidad con los requisitos de seguridad, también conocida como auditoría de seguridad o revisión de la seguridad, es una actividad que se desarrolla para asegurar el cumplimiento y adecuación con el plan de seguridad del sistema de prestación de certificación de IZENPE y se encuentra definido en un Plan de Auditoría.

Se realizan verificaciones in situ para determinar si el personal de IZENPE sigue los procedimientos y las salvaguardas específicas.

8.1 Frecuencia de auditoría

La verificación de la conformidad con los requisitos de seguridad es realizada periódicamente, planificada e integrada con otras actividades previstas.

8.2 Cualificación del auditor

El auditor tiene cualificación y experiencia probadas en la ejecución de auditorías de sistemas seguros de producción, en especial de sistemas de certificación digital. Debe estar acreditado según ETSI EN 319 403.

8.3 Relación del auditor con la empresa auditada

Se emplean auditores internos o externos, pero en todo caso independientes funcionalmente del servicio de producción objeto de auditoría.

8.4 Elementos objetos de auditoría

Los elementos objeto de auditoría son los siguientes:

- Procesos de PKI.
- Sistemas de Información.
- Protección del centro de proceso de datos.
- Documentos.

Los detalles de cómo se lleva a cabo la auditoría de cada uno de estos elementos están detallados en el Plan de Auditoría de IZENPE.

8.5 Toma de decisiones como resultado de deficiencias

Izenpe implementa un modelo de mejora continua, y los resultados de una auditoría de cumplimiento son tratados según este modelo. Dependiendo de la severidad y urgencia, todas las observaciones, mejoras y no conformidades son introducidas en un sistema de seguimiento, y tratadas como incidencias o problemas. Mediante una herramienta de apoyo Izenpe asegura que todos los problemas son tratados en plazo.



8.6 Comunicación de los resultados

Los informes de auditoría serán entregados al Comité de Seguridad, para su análisis.



9 Otros asuntos legales y de actividad

9.1 Tarifas

IZENPE recibirá las contraprestaciones económicas correspondientes de acuerdo con las tarifas aprobadas por su Consejo de Administración.

9.1.1 Tarifas de emisión o renovación de certificados

Las tarifas que los usuarios deben abonar en contraprestación de la emisión o renovación de certificados están recogidas en el apartado 10.1.

9.1.2 Tarifas de acceso a la información de estado de los certificados

IZENPE ofrece servicios de información del estado de los certificados a través de CRLs o del OCSP de forma gratuita.

9.1.3 Tarifas para otros servicios

Las tarifas aplicables a otros servicios se acordarán entre IZENPE y los clientes de los servicios ofrecidos.

9.1.4 Política de reintegro

IZENPE no dispone de una política de reintegro.

9.2 Responsabilidad financiera

IZENPE, las Entidades de Registro y las Entidades Usuarias disponen de suficientes recursos para mantener sus operaciones y realizar sus tareas.

IZENPE mantiene un seguro de responsabilidad civil que cubre los riesgos de error y/u omisión en la generación del certificado y que se extiende a las actividades que realiza exclusivamente. La relación que se establece entre IZENPE y las Entidades de Registro, cuando intervengan, y los suscriptores y usuarios de los certificados no es de mandato, ni de agente y principal. Ni los suscriptores ni los usuarios de los certificados pueden obligar a IZENPE ni a las Entidades de Registro a prestación alguna, ni por contrato ni por otros medios en este ámbito.

9.3 Confidencialidad de la información

9.3.1 Alcance de la información confidencial

Para la prestación del servicio, IZENPE y las Entidades de Registro precisan recabar y almacenar cierta información, que incluye datos de carácter personal. Tal información es recabada directamente de los afectados, obteniendo su consentimiento explícito, o sin consentimiento del afectado en aquellos casos en los que la legislación de protección de datos permita recabar de esta forma la información.



IZENPE y las Entidades de Registro recaban los datos exclusivamente necesarios para la expedición y el mantenimiento de los certificados y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

IZENPE desarrolla una política de intimidad, de acuerdo con la legislación de protección de datos de carácter personal vigente.

IZENPE y las Entidades de Registro no divulgan ni ceden datos de carácter personal, excepto en aquellos supuestos previstos en las secciones correspondientes de esta Declaración de Prácticas de Certificación y en la sección correspondiente en caso de terminación de la actividad de IZENPE y las Entidades de Registro.

Las siguientes informaciones son mantenidas de forma confidencial por IZENPE y las Entidades de Registro:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto la información indicada en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por IZENPE
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por IZENPE o las Entidades de Registro y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.

9.3.2 Información que no está dentro del alcance

La siguiente información es considerada no confidencial, y de esta forma es reconocida por los afectados, en el instrumento jurídico vinculante con IZENPE:

- Los certificados emitidos o en trámite de emisión.
- La vinculación de un suscriptor persona física a un certificado emitido por IZENPE
- El nombre y los apellidos del suscriptor del certificado, en caso de certificados en los que el suscriptor y el firmante sea una persona física, o del poseedor de claves, en caso de certificados en los que el suscriptor sea una persona jurídica u órgano administrativo, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- En el supuesto en que se incluya, la dirección de correo electrónico del suscriptor del certificado, en caso de certificados en los que el suscriptor y el firmante sea una persona física, o del poseedor de claves, en caso de certificados en los que el suscriptor sea una persona jurídica u órgano administrativo, o la dirección de correo electrónico asignada por el suscriptor, en caso de certificados para dispositivos.
- Los usos y límites económicos reseñados en el certificado.



- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las Listas de Certificados Revocados (CRLs), así como las restantes informaciones de estado de revocación.
- La información contenida en el Servicio de Publicación de IZENPE.
- Toda otra información que no esté indicada en la sección de informaciones confidenciales de la Declaración de Prácticas de Certificación.

9.3.3 Responsabilidad para proteger la información confidencial

IZENPE o las Entidades de Registro divulgarán la información confidencial únicamente en los supuestos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

Los certificados serán objeto de publicación de acuerdo con lo establecido en el artículo 18.c) de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.4 Protección de datos de carácter personal

El régimen aplicable a los tratamientos de los datos de carácter personal que Izenpe lleva a cabo será el previsto en el *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (en adelante, RGPD) y en su normativa de desarrollo y aquella otra normativa vigente que resulte aplicable.

Izenpe tiene la consideración de responsable del tratamiento respecto a los datos que el usuario proporciona para la solicitud de los medios de identificación regulados en esta Declaración y dispone de la certificación ISO 27001:2013 sobre su Sistema de Gestión de la Seguridad de la Información, disponible en www.izenpe.com.

Además Izenpe cumple con las medidas exigidas por el Esquema Nacional de Seguridad definido en el Real Decreto 3/2010, y con la normativa ETSI vigente aplicable a un Prestador de Servicios de Confianza según eIDAS.

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



9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados

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

Quedan excluidos los derechos de propiedad intelectual e industrial derivados de aplicaciones que integran el sistema de certificación digital y que sean propiedad de un tercero.

Las mismas reglas son de aplicación al sistema de información de revocación de certificados.

9.5.2 Propiedad de la Práctica de Certificación

IZENPE es la propietaria de la presente Declaración de Prácticas de Certificación.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, el poseedor de claves, conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor y, en su caso, el poseedor de claves, es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3 de la Declaración de Prácticas de Certificación.

9.5.4 Propiedad de claves y material relacionado

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

9.6 Obligaciones y garantías

IZENPE, como Entidad de Certificación que expide certificados de acuerdo con la presente Declaración de Prácticas de Certificación asume las siguientes obligaciones,

9.6.1 Obligaciones de prestación del servicio

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

- No copiar los datos de creación de firma de la persona a la que haya prestado sus servicios.
- Mantener un sistema en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida.



- Conservar registrada por cualquier medio seguro toda la información y documentación relativa a los certificados cualificados y a las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo y la relativa al resto de certificados, durante 7 años.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.
- Cumplir la normativa y estándares de seguridad (RGPD, ISO, ETSI y Política de Seguridad de Izenpe).
- Exigir a proveedores de albergue el cumplimiento de la normativa y estándares de seguridad (RGPD, ISO, ETSI, CABForum y Política de Seguridad de Proveedores de Izenpe).

9.6.2 Obligaciones de operación fiable

IZENPE garantiza:

- Que la identidad contenida en el certificado se corresponde de forma unívoca con la clave pública contenida en el mismo.
- La rapidez y seguridad en la prestación del servicio. En particular, se permite la utilización de un servicio rápido y seguro de consulta de validez de los certificados y se asegura que se informa de la extinción de los certificados de forma segura e inmediata, de acuerdo con lo previsto en la presente Declaración de Prácticas de Certificación. El servicio está disponible 24 horas x 7 días a la semana.
- El cumplimiento de los requisitos técnicos y de personal exigidos por la legislación vigente en materia de firma electrónica:
 1. Demostrar la fiabilidad necesaria para prestar servicios de certificación.
 2. Garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado o se extinguió su vigencia.
 3. Emplear el personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y gestión adecuados en el ámbito de la firma electrónica.
 4. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte, de acuerdo con la Política de Seguridad.
 5. Tomar medidas contra la falsificación de certificados y garantizar la confidencialidad en el proceso de generación de acuerdo con lo indicado en el apartado 6 y su entrega por un procedimiento seguro al firmante.
 6. Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticación e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.



- La correcta gestión de su seguridad, gracias a la implementación de un Sistema de Gestión de la Seguridad de la Información de acuerdo a los principios establecidos por la ISO/IEC 27001 y que incluye, entre otras, las siguientes medidas:
 1. Realizar de forma periódica comprobaciones regulares de la seguridad, con el fin verificar la conformidad con los estándares establecidos.
 2. Llevar a cabo una completa gestión de los sucesos de seguridad, con el fin de garantizar su detección, resolución y optimización.
 3. Mantener los contactos y relaciones apropiadas con grupos de especial interés en materia de seguridad, como especialistas, foros de seguridad y asociaciones profesionales relacionadas con la seguridad de la información.
 4. Planificar adecuadamente el mantenimiento y evolución de los sistemas, con el fin de garantizar en todo momento un rendimiento adecuado y un servicio que cumpla con todas las garantías las expectativas de los usuarios y clientes.

9.6.3 Obligaciones de identificación

En el caso de certificados cualificados, IZENPE identifica al suscriptor del certificado, de acuerdo con los niveles de aseguramiento definidos en el Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 y la presente Declaración de Prácticas de Certificación.

9.6.4 Obligaciones de información a usuarios

- Antes de la emisión y entrega del certificado al suscriptor, IZENPE le informa mediante referencia al documento “Términos y Condiciones de uso y Acuerdo de Divulgación de Infraestructura de clave pública (PKI - PDS)” disponible en www.izenpe.com de los términos y condiciones relativos al uso del certificado, de su precio – cuando se establezca – de sus limitaciones de uso y de los instrumentos jurídicos vinculantes a los que hace referencia la sección 2.1.1.6 de la presente Declaración de Prácticas de Certificación.
- IZENPE informará al poseedor de claves acerca de la extinción de la vigencia de su certificado de manera previa o simultánea a la extinción de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en la que el certificado quedará sin efecto.
- IZENPE comunicará a los firmantes el cese de sus actividades de prestación de servicios de certificación con dos meses de antelación e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados. Las comunicaciones a los firmantes se efectúan conforme a lo previsto en el presente documento.
- IZENPE dispone de un plan de finalización del cese de su actividad en el que se especifican las condiciones en las que se realizaría.



9.6.5 Obligaciones relativas a los programas de verificación

IZENPE ofrece mecanismos de verificación de la validez de los certificados de acceso público, mediante los sistemas descritos en la presente Declaración de Prácticas de Certificación.

9.6.6 Obligaciones relativas a la regulación jurídica del servicio de certificación

IZENPE asume todas las obligaciones incorporadas directamente en el certificado o incorporadas por referencia. La incorporación por referencia se logra incluyendo en el certificado un identificador de objeto u otra forma de enlace a un documento.

El instrumento jurídico que vincula a IZENPE y al solicitante, suscriptor o poseedor de claves y al tercero que confía en el certificado está en lenguaje escrito y comprensible, teniendo los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 2.1.4, 2.1.5, 2.1.6, 2.2, 2.3 y 2.4 de la presente Declaración de Prácticas de Certificación.
- Indicación de la Declaración de Prácticas de Certificación aplicable, con indicación, en su caso, de que los certificados se expiden al público y de la necesidad de empleo de dispositivo seguro de creación de firma o descifrado de mensajes.
- Cláusulas relativas a la emisión, revocación, renovación y, en su caso, recuperación de claves privadas.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión de un dispositivo criptográfico y para la cesión de dicha información a terceros, en caso de terminación de operaciones de IZENPE sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.3.2.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales IZENPE acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si IZENPE ha sido declarada conforme con las Políticas de Certificación de alguna o algunas de las Entidades Públicas y, en su caso, de acuerdo con qué sistema.
- Forma en la que se garantiza la responsabilidad patrimonial de IZENPE



9.6.7 Obligaciones de la Entidad de Registro

Antes de que IZENPE autorice la delegación de las funciones de Entidad de Registro con un tercero, éste deberá asumir formalmente mediante el correspondiente instrumento legal las siguientes obligaciones:

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

9.6.8 Obligaciones del solicitante del certificado

El solicitante del certificado está obligado a:

- Garantizar la veracidad, totalidad y actualidad de la información aportada en la solicitud de los certificados y que haya de constar en los mismos.
- Cumplir el procedimiento de solicitud establecido en la documentación específica.
- Abonar en un plazo máximo de tres meses el importe correspondiente al tipo de certificado, en las condiciones indicadas por Izenpe.

9.6.9 Obligaciones del suscriptor del certificado

- Facilitar a IZENPE información completa y adecuada, conforme a los requerimientos de la Declaración de Prácticas de Certificación en especial en lo relativo al procedimiento de registro.
- Garantizar la veracidad, totalidad y actualidad de la información que haya de constar en los certificados.
- Conocer y aceptar las condiciones de utilización de los certificados, así como las modificaciones que se realicen sobre las mismas.



- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Garantizar el buen uso y la conservación de los soportes de los certificados.
- Emplear adecuadamente el certificado y, en concreto, cumplir con las limitaciones de uso de los certificados.
- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la Declaración de Prácticas de Certificación.
- Notificar a IZENPE y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida, el robo o el compromiso potencial de su clave privada.
 - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo criptográfica) o por cualquier otra causa.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, instando la revocación del certificado cuando dicha modificación constituya causa de revocación del mismo.
- Dejar de emplear la clave privada transcurrido el periodo de validez del certificado.
- Transferir a los poseedores de claves las obligaciones específicas de los mismos.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de la Entidad de Certificación.
- No comprometer intencionadamente la seguridad de los servicios de certificación.
- No emplear las claves privadas correspondientes a las claves públicas contenidas en los certificados, con el propósito de firmar ningún certificado, como si se tratase de una Entidad de Certificación.

El suscriptor de certificados cualificados que genere firmas digitales empleando la clave privada correspondiente a su certificado, debe reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se emplee dispositivo criptográfico, conforme a lo preceptuado en eIDAS.

9.6.10 Obligaciones del usuario verificador de certificados

El usuario verificador de certificados queda obligado a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Conocer las condiciones de utilización de los certificados conforme a lo previsto en la Declaración de Prácticas de Certificación y el contrato de prestación de servicios de certificación entre el verificador e IZENPE
- Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.



- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de verificador.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de IZENPE
- No comprometer intencionadamente la seguridad de los servicios de certificación.

El usuario de certificados cualificados queda obligado a reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con eIDAS.

9.6.11 Obligaciones del Servicio de Publicación

No aplicable por no ser el Servicio de Publicación una entidad independiente.

9.7 Responsabilidades

9.7.1 Responsabilidades de la autoridad de certificación

IZENPE responderá por negligencia o falta de la debida diligencia en los servicios de certificación descritos en la presente Declaración de Prácticas de Certificación así como cuando incumpla las obligaciones impuestas en la legislación sobre firma electrónica, excepto en los siguientes supuestos:

- IZENPE no será responsable por los daños causados por las informaciones contenidas en los Certificados, siempre que el contenido de los mismos cumpla sustancialmente con la Declaración de Prácticas de Certificación.
- IZENPE no será responsable por los daños causados por la extinción de la eficacia de los certificados, siempre que cumpla sustancialmente con las obligaciones de publicación previstas en la Declaración de Prácticas de Certificación.
- IZENPE no será responsable de ningún daño directo e indirecto, especial, incidental, emergente, de cualquier lucro cesante, pérdida de datos, daños punitivos, fuesen o no previsibles, surgidos en relación con el uso, entrega, licencia, funcionamiento o no funcionamiento de los Certificados, las firmas digitales, o cualquier otra transacción o servicio ofrecido o contemplado en la Declaración de Prácticas de Certificación en caso de uso indebido.
- IZENPE no será responsable por los daños y perjuicios ocasionados al suscriptor o terceros de buena fe, por la inexactitud de los datos que consten en el certificado, si éstos le han sido acreditados mediante documento público notarial, judicial o administrativo, salvo en el caso del documento aportado por la Entidad de Registro.
- IZENPE tampoco será responsable por los daños y perjuicios ocasionados al suscriptor o a terceros de buena fe, por el incumplimiento de los deberes inherentes a la condición de suscriptor o terceros que confían en los certificados.



IZENPE responderá por los daños y perjuicios que cause a cualquier persona por la falta o retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados o de la extinción de la vigencia de los certificados.

Asimismo, asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que delegue para el ejercicio de las funciones necesarias para la prestación de servicios de certificación. En este sentido se ha constituido un seguro de responsabilidad civil para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados.

9.7.2 Responsabilidades de la autoridad de registro

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

Cuando las funciones de identificación sean realizadas por las Administraciones Públicas suscriptoras de los certificados, será de aplicación la responsabilidad patrimonial de las Administraciones Públicas, según se establece la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

9.7.3 Responsabilidades de los suscriptores

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

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

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

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



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

- Proporcionar a IZENPE o a la Entidad de Registro información veraz, completa y exacta sobre los datos que deban constar en el certificado o que sean necesarios para la expedición o revocación de éste, cuando su inexactitud no haya podido ser detectada por el prestador de servicios.
- Comunicar sin demora a IZENPE o a la Entidad de Registro cualquier modificación de las circunstancias reflejadas en el certificado.
- Conservar con diligencia sus datos de creación de firma con el fin de asegurar su confidencialidad y protegerlos de todo acceso o revelación.
- Solicitar la revocación del certificado en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- Abstenerse de utilizar los datos de creación de firma desde el momento en que haya expirado el período de validez del certificado o el prestador de servicios le notifique su pérdida de vigencia.
- Respetar los límites que figuren en el certificado en cuanto a sus posibles usos y utilizarlo conforme a las condiciones establecidas y comunicadas al firmante de servicios de certificación.

9.7.4 Responsabilidades de los terceros que confían en certificados

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

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

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

9.8 Indemnizaciones

IZENPE incluye, en los instrumentos jurídicos que le vinculan con el suscriptor y el verificador, cláusulas de indemnidad en caso de infracción de sus obligaciones o de la legislación aplicable.

9.9 Periodo de validez

9.9.1 Plazo

La DPC entra en vigor en el momento de su publicación.



9.9.2 Terminación

La DPC actual será derogada en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente el documento anterior.

9.9.3 Efectos de la finalización

Para los certificados vigentes emitidos bajo una DPC anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.10 Notificaciones individuales y comunicación con los participantes

IZENPE establece en el instrumento jurídico vinculante con el suscriptor los medios y plazos para las notificaciones.

De modo general, se utilizará la página web de IZENPE, www.izenpe.eus para realizar cualquier tipo de notificación y comunicación.

9.11 Enmiendas

9.11.1 Procedimiento para los cambios

Las modificaciones de este documento serán aprobadas por el Comité de Seguridad de IZENPE. Estas modificaciones estarán recogidas en un documento de Actualización de la Declaración de Prácticas de Certificación cuyo mantenimiento está garantizado por IZENPE.

Las versiones actualizadas de la Declaración de Prácticas de Certificación junto con la relación de modificaciones realizadas pueden ser consultadas en la dirección www.izenpe.com.

IZENPE podrá modificar, de forma unilateral, la Declaración de Prácticas de Certificación siempre y cuando proceda según el siguiente procedimiento:

- La modificación estará justificada desde el punto de vista técnico, legal o comercial, debiendo estar avalada por la dirección de IZENPE.
- Se deberán contemplar todas las implicaciones técnicas y legales de la nueva versión de especificaciones.
- Se establecerá un control de modificaciones, para garantizar, que las especificaciones resultantes cumplen con los requisitos que se intentaban cumplir y que dieron pie al cambio.
- Se deberá establecer las implicaciones que el cambio de especificaciones tiene sobre el usuario, contemplando la necesidad de notificarle dichas modificaciones.

9.11.2 Periodo y mecanismo de notificación

El Comité de Seguridad de IZENPE revisará anualmente la DPC y en cualquier caso cuando haya que realizar cualquier modificación de la misma. Esta revisión se realizará de forma conjunta entre las áreas responsables y participantes de su elaboración y mantenimiento.



IZENPE podrá realizar modificaciones de este documento sin necesidad de informar previamente a los usuarios, como por ejemplo:

- Correcciones de errores tipográficos en el documento
- Cambios en la información de contacto.

Modificaciones que pudieran requerir informar a los usuarios, como por ejemplo:

- Cambios en las especificaciones o condiciones del servicio.
- Modificaciones de URLs

9.11.3 Circunstancias por la cual un OID debe cambiarse

Se procederá al cambio de OID en aquellas circunstancias que se altere alguno de los procedimientos descritos en el presente documento.

9.12 Reclamaciones y resolución de disputas

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

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

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

9.13 Normativa aplicable

La ley española de firma electrónica se aplica en todo lo referente a la ejecución, elaboración, interpretación y validez de esta Declaración de Prácticas de Certificación.

La normativa aplicable al presente documento, y a las operaciones que derivan de ellas, es la siguiente:

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Reglamento No 910/2014 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
- Ley 39/2015 Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40-2015 Régimen Jurídico Sector Público
- Ley 15/99 Orgánica de Protección de Datos (LOPD)
- Reglamento (UE) 2016/679 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 (RGPD)
- Reglamento Europeo 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS)



9.14 Cumplimiento de la normativa aplicable

La jurisdicción competente será aquella a la que en cada momento remita la legislación procesal española.

En cualquier caso, IZENPE manifiesta el cumplimiento de las normativas indicadas en el apartado 10.13

En caso de conflicto entre los requerimientos de los CABForum Baseline Requirements o EV Guidelines con la legislación aplicable, se especificará en la presente DPC, y será notificada a CABForum a través de los canales previstos en los Baseline Requirements o EV Guidelines.

9.15 Estipulaciones diversas

Cada cláusula de esta Declaración de Prácticas de Certificación es válida en sí misma y no invalida al resto. La cláusula inválida o incompleta puede ser sustituida por otra equivalente.

Ninguno de los términos de esta Declaración de Prácticas de Certificación que afecte directamente a los derechos y obligaciones de IZENPE y que no afecte al resto de las partes, puede ser corregido, renunciado, suplementado, modificado o eliminado si no es mediante documento escrito autenticado de IZENPE, que no supone en ningún caso novación extintiva, sino meramente modificativa, y no afecta al resto de derechos y obligaciones de las restantes partes.

Las comunicaciones escritas a IZENPE deben ser enviadas a la siguiente dirección:

IZENPE, S.A.
c/ Beato Tomás de Zumárraga, nº 71, 1ª planta.
01008 Vitoria-Gasteiz