

Declaración de Prácticas de Confianza Global

© Izenpe 2025

■ Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.eus
izenpe@izenpe.eus



Histórico de versiones

Los cambios de las versiones anteriores a la 7.0 se pueden consultar en el apartado “Actualizaciones y notificaciones acerca de la declaración de prácticas de certificación” de www.izenpe.eus



Versión	Fecha	Resumen de los cambios producidos
7.0	14/07/2021	Añadido el cuadro de cambios para sustituir el documento de actualizaciones Actualizado el apartado 4.9.12 de la DPC para indicar los métodos disponibles para demostrar el compromiso de clave privada
7.1	13/01/2022	Se actualizan los siguientes epígrafes, 6.2.1 Estándares de módulos criptográficos. 9.3.3 Responsabilidad para proteger la información confidencial: actualización normativa. 9.16.6: otras estipulaciones.
7.2	01/09/2022	Se actualizan los siguientes epígrafes, 1.1.1 Jerarquía CA raíz 2007 (CN=izenpe.com): se actualiza el valor de tipo de firma Cualificada a Avanzada en los OIDs en vigor en chip criptográfico.
7.3	21/10/2022	Se actualizan los siguientes epígrafes, 1.1.1 Jerarquía CA raíz 2007 (CN=izenpe.com): se actualiza el valor de identificador de política a QCP-n en los OIDs en vigor en chip criptográfico y se actualiza la política de los certificados SSL EV a QEVCP-w
7.4	13/09/2023	1.4.1 Corrección de erratas 1.6.2 Corrección de erratas 2.3 Actualización redaccion 6.1.2 Actualización FIPS 6.1.3 Actualización de los métodos de distribución 7.1 Actualización perfil de los certificados
7.5	08/11/2023	Actualización punto 4.9.8 Tiempo transcurrido entre la generación y la publicación de las CRLs Actualización punto 9.16.6 sobre prevalencia de la guía de directrices
8.0	19/06/2025	Adecuación de la Declaración de Practicas de Certificación a la modificación del Reglamento (UE) N° 910/2014.
8.1	06/10/2025	1.2.2.4: incorporación: jerarquía 2025 1.4: OIDs certificado cualificado en dispositivo seguro creación de firma 6.1.5: actualización longitud de claves



8.2	18/11/2025	Actualización del epigrafe 4.6
-----	------------	--------------------------------



Índice

Contenido

1	Introducción	11
1.1	Presentación	11
1.2	Nombre del documento e identificación	12
1.2.1	Identificación	12
1.2.2	Identificadores de certificados	13
1.3	Participantes de la infraestructura de clave pública PKI	17
1.3.1	Autoridades de Certificación	17
1.3.2	Entidades de Registro	22
1.3.3	Suscriptores de los certificados	22
1.3.4	Terceras partes de confianza	22
1.3.5	Otros participantes	23
1.4	Usos del certificado	23
1.4.1	Usos apropiados del certificado	23
1.4.2	Usos prohibidos del certificado	32
1.5	Administración de Políticas	32
1.5.1	Entidad responsable de la gestión de la documentación	32
1.5.2	Datos de contacto.	33
1.5.3	Responsables de adecuación de la DPCG	33
1.5.4	Procedimiento de aprobación de la DPCG.	33
1.6	Definiciones y acrónimos.	33
1.6.1	Definiciones.	33
1.6.2	Acrónimos	37
2	Publicación y responsables del repositorio de información	40
2.1	Repositorio de información	40
2.2	Publicación de información de certificación	40
2.2.1	Política de publicación y notificación.	40
2.2.2	Elementos no publicados en la Declaración de Prácticas de Certificación Global.	40
2.3	Frecuencia de publicación	40
2.4	Control de acceso al repositorio	41
3	Identificación y autenticación	42
3.1	Nombres	42
3.1.1	Tipos de nombres	42
3.1.2	Significado de los nombres	42
3.1.3	Seudónimos	42
3.1.4	Reglas para la Interpretación de formatos de nombres	42
3.1.5	Unicidad de los nombres	42
3.1.6	Resolución de conflictos relativos a nombres y tratamiento de marcas registradas	42
3.1.7	Emisor (Issuer)	43
3.1.8	Asunto (Subject)	43
3.2	Validación de la identidad	43
3.2.1	Métodos para probar la posesión de la clave privada	43
3.2.2	Autenticación de la identidad de la organización	43
3.2.3	Autenticación de la identidad de la persona física solicitante	44
3.2.4	Información no verificada del suscriptor	44
3.2.5	Validación de la autoridad	44
3.2.6	Criterios de interoperación	44



3.3	Identificación y autenticación para peticiones de reemisión de claves	45
3.3.1	Renovación rutinaria	45
3.3.2	Renovación después de una revocación	45
3.4	Identificación y autenticación para peticiones de revocación	45
4	Requisitos operativos del ciclo de vida de los certificados	46
4.1	Solicitud de certificado	46
4.1.1	Comprobación de la solicitud	46
4.1.2	Proceso de inscripción y responsabilidades	46
4.2	PGestión de las solicitudes	47
4.2.1	Realización de funciones de identificación y autenticación	47
4.2.2	Tiempo en procesar la solicitud	47
4.3	Emisión del certificado	47
4.3.1	Acciones de la CA durante la emisión	47
4.3.2	Izenpe procederá a la emisión del certificado según lo determinado al efecto en ca DPCP o PDS. Notificación de al sla emisión	47
4.3.3	Verificación del certificado	47
4.4	Aceptación del certificado	48
4.4.1	Proceso de aceptación del certificado.	48
4.4.2	Publicación del certificado por la CA.	48
4.4.3	Notificación de la emisión del certificado por la CA a otras entidades.	48
4.5	Par de claves y usos del certificado	48
4.5.1	Clave privada del suscriptor y uso del certificado	48
4.5.2	Uso de la clave pública y del certificado por terceros que confían en los certificados	50
4.6	Renovación del certificado	50
4.6.1	Circunstancias para la renovación del certificado	50
4.6.2	Quién puede solicitar la renovación	50
4.6.3	Tratamiento de peticiones de renovación de certificado	51
4.6.4	Notificación al suscriptor	51
4.6.5	Procedimiento de aceptación de un certificado renovado	51
4.6.6	Publicación del certificado	51
4.6.7	Notificación a otras entidades	51
4.7	Renovación con regeneración de las claves del certificado	51
4.7.1	Circunstancias para regenerar las claves del certificado	51
4.7.2	Quien lo puede pedir	51
4.7.3	Tratamiento de las peticiones de renovación con regeneración de claves	51
4.7.4	Procedimiento de aceptación del certificado renovado	51
4.7.5	Publicación del certificado	52
4.8	Modificación del certificado	52
4.8.1	Circunstancias para la modificación del certificado.	52
4.8.2	Quién puede solicitar la modificación del certificado	52
4.8.3	Procesamiento de solicitudes de modificación del certificado	52
4.8.4	Notificación de la modificación del certificado	52
4.8.5	Publicación del certificado modificado	52
4.8.6	Notificación de la modificación del certificado a otras entidades	52
4.9	Revocación	52
4.9.1	Circunstancias para la revocación	52
4.9.2	Quién puede solicitar la revocación	53
4.9.3	Tratamiento de las peticiones de revocación	53
4.9.4	Periodo de gracia de la solicitud de revocación	54
4.9.5	Tiempo de plazo de la CA para procesar la revocación	54
4.9.6	Obligación de verificación de las revocaciones por terceros de confianza	54



4.9.7	Frecuencia de generación de CRLs	54
4.9.8	Tiempo transcurrido entre la generación y la publicación de las CRLs	55
4.9.9	Requisitos de comprobación de revocación online	55
4.9.10	Otras formas de avisos de revocación disponibles	55
4.9.11	Requisitos especiales clave comprometida	55
4.9.12	Circunstancias para la suspensión	56
4.9.13	Quién puede solicitar la suspensión	56
4.9.14	Procedimiento para la petición de la suspensión	56
4.9.15	Límites sobre el periodo de suspensión	56
4.10	Servicios de estado de los certificados	56
4.10.1	Características operativas	56
4.10.2	Disponibilidad del servicio	56
4.10.3	Características opcionales	56
4.11	Finalización de la suscripción	56
4.12	Custodia y recuperación de claves	57
4.12.1	Prácticas y políticas de custodia y recuperación de claves	57
4.12.2	Prácticas y políticas de protección y recuperación de la clave de sesión	57
5	Controles de seguridad física, de procedimiento y de personal	58
5.1	Controles de seguridad física	58
5.1.1	Localización y construcción de las instalaciones	58
5.1.2	Acceso físico	58
5.1.3	Electricidad y aire acondicionado	58
5.1.4	Exposición al agua	59
5.1.5	Prevención y protección de incendios	59
5.1.6	Almacenamiento de soportes	59
5.1.7	Tratamiento de residuos	59
5.1.8	Copia de respaldo fuera de las instalaciones	59
5.2	Controles de procedimientos	59
5.2.1	Roles de confianza	59
5.2.2	Número de personas por tarea	60
5.2.3	Identificación y autenticación para cada rol	60
5.2.4	Separación de tareas en los diferentes roles	60
5.3	Controles de personal	60
5.3.1	Requisitos de historial, calificaciones, experiencia y autenticación	60
5.3.2	Procedimientos de investigación de historial	60
5.3.3	Requisitos de formación	60
5.3.4	Requisitos y frecuencia de actualización formativa	61
5.3.5	Secuencia y frecuencia de rotación laboral	61
5.3.6	Sanciones para acciones no autorizadas	61
5.3.7	Requisitos de contratación de personal	61
5.3.8	Suministro de documentación al personal	61
5.4	Audit	61
5.4.1	Tipo de eventos registrados	61
5.4.2	Frecuencia de procesamiento de logs	62
5.4.3	Periodo de retención del audit log	62
5.4.4	Protección del audit log	62
5.4.5	Procedimiento de backup del audit log	62
5.4.6	Recolección de logs	62
5.4.7	Análisis de vulnerabilidades	62
5.5	Archivado de registros	63
5.5.1	Tipo de registros archivados	63
5.5.2	Periodo de retención del archivo	63



5.5.3	Protección del archivo	63
5.5.4	Procedimientos de backup del archivo	63
5.5.5	Requisitos para el sellado de tiempo de los registros	63
5.5.6	Sistema de archivo	63
5.5.7	Procedimientos para obtener y verificar la información del archivo	63
5.6	Cambio de claves de la CA	63
5.7	Gestión de incidentes y Plan de contingencias	64
5.7.1	Procedimientos de gestión de incidentes	64
5.7.2	Plan de actuación ante datos y software corruptos	65
5.7.3	Procedimiento ante compromiso de la clave privada de la CA	65
5.7.4	Continuidad de negocio después de un desastre	65
5.8	Terminación de la CA o RA	66
5.8.1	Entidad de Certificación	66
5.8.2	Entidad de Registro	66
6	Controles de seguridad técnica	67
6.1	Generación e instalación del par de claves	67
6.1.1	Generación del par de claves	67
6.1.2	Distribución de la clave privada al suscriptor	67
6.1.3	Distribución de la clave pública al emisor del certificado	67
6.1.4	Distribución de la clave pública de la entidad de certificación a los usuarios de certificados	68
6.1.5	Tamaños de claves	68
6.1.6	Parámetros de generación de la clave pública y verificación de la calidad	68
6.1.7	Usos admitidos de las claves (KeyUsage field X.509 v3)	69
6.2	Protección de la clave privada	69
6.2.1	Estándares de módulos criptográficos	69
6.2.2	Control por más de una persona (n de m) sobre la clave privada	69
6.2.3	Custodia de la clave privada	69
6.2.4	Copia de respaldo de la clave privada	70
6.2.5	Archivado de la clave privada	70
6.2.6	Trasferencia de la clave privada a o desde el módulo criptográfico	70
6.2.7	Almacenamiento de la clave privada en el módulo criptográfico	70
6.2.8	Método de activación de la clave privada	71
6.2.9	Método de desactivación de la clave privada	71
6.2.10	Método de destrucción de la clave privada	71
6.2.11	Calificación del módulo criptográfico	71
6.3	Otros aspectos de gestión del par de claves	71
6.3.1	Archivo de la clave pública	71
6.3.2	Periodos de operación del certificado y periodos de uso del par de claves	71
6.4	Datos de activación	72
6.4.1	Generación e instalación de datos de activación	72
6.4.2	Protección de datos de activación	72
6.4.3	Otros aspectos de los datos de activación	72
6.5	Controles de seguridad informática	72
6.5.1	Requisitos técnicos específicos de seguridad informática	72
6.5.2	Evaluación del nivel de seguridad informática	73
6.6	Controles técnicos del ciclo de vida	73
6.6.1	Controles de desarrollo de sistemas	73
6.6.2	Controles de gestión de la seguridad	74
6.6.3	Controles de seguridad del ciclo de vida	74
6.7	Controles de seguridad de red	74
6.8	Fuente de tiempo	74



7	Perfiles de certificados y listas de certificados revocados	75
7.1	Perfil de certificado	75
7.1.1	Número de versión	75
7.1.2	Extensiones de certificado	75
7.1.3	Identificadores de objeto de algoritmos	75
7.1.4	Formatos de nombres	76
7.1.5	Restricciones de nombres	76
7.1.6	Identificador de objeto de política de certificado	76
7.1.7	Empleo de la extensión restricciones de política	76
7.1.8	Sintaxis y semántica de los calificadores de política	76
7.1.9	Tratamiento semántico para la extensión “certificate policy”	76
7.2	Perfil de la lista de revocación de certificados	76
7.2.1	Número de versión	77
7.2.2	Lista de revocación de certificados y extensiones de elementos de la lista	77
7.3	Perfil OCSP	77
7.3.1	Número de versión	77
7.3.2	Extensiones del OCSP	77
7.3.3	Otros aspectos del OCSP	78
8	Auditorías de cumplimiento	79
8.1	Frecuencia de auditoría	79
8.2	Cualificación del auditor	79
8.3	Relación del auditor con la empresa auditada	79
8.4	Elementos objetos de auditoría	79
8.5	Toma de decisiones como resultado de deficiencias	79
9	Otros asuntos legales y de actividad	80
9.1	Tarifas	80
9.1.1	Tarifas de emisión o renovación de certificados	80
9.1.2	Tarifas de acceso a los certificados	80
9.1.3	Tarifas de acceso a la información de estado de los certificados	80
9.1.4	Tarifas para otros servicios	80
9.1.5	Política de reintegro	80
9.2	Responsabilidad financiera	80
9.2.1	Seguro de responsabilidad civil	80
9.2.2	Otros activos	80
9.2.3	Seguros y garantías para entidades finales	80
9.2.4	Alcance de la información confidencial	81
9.2.5	Información que no está dentro del alcance	81
9.2.6	Responsabilidad para proteger la información confidencial	82
9.3	Protección de datos de carácter personal	82
9.3.1	Plan de privacidad	82
9.3.2	Información tratada como privada	82
9.3.3	Información no considerada privada	82
9.3.4	Responsabilidad de proteger la información privada	82
9.3.5	Aviso y consentimiento para usar información privada	84
9.3.6	Divulgación conforme al proceso judicial o administrativo	84
9.3.7	Otras circunstancias de divulgación de información	84
9.4	Derechos de propiedad intelectual	84
9.4.1	Propiedad de los certificados	84
9.4.2	Propiedad de la DPCG	84
9.4.3	Propiedad de la información relativa a nombres	84
9.4.4	Propiedad de claves y material relacionado	84
9.5	Obligaciones y garantías	84



9.5.1	Obligaciones de la CA	84
9.5.2	Obligaciones de la entidad de registro	88
9.5.3	Obligaciones de los titulares	88
9.5.4	Obligaciones de las partes que confían	89
9.5.5	Obligaciones de otros participantes	90
9.6	Renuncia de garantías	90
9.7	Limitaciones de responsabilidad	90
9.7.1	Responsabilidades de la autoridad de certificación	90
9.7.2	Responsabilidades de la autoridad de registro	91
9.7.3	Responsabilidades de los suscriptores	91
9.7.4	Responsabilidades de los terceros que confían en certificados	92
9.8	Indemnizaciones	92
9.9	Periodo de validez	92
9.9.1	Entrada en vigor	92
9.9.2	Terminación	93
9.9.3	Efectos de la finalización	93
9.10	Notificaciones individuales y comunicación con los participantes	93
9.11	Modificaciones de este documento	93
9.11.1	Procedimiento para los cambios	93
9.11.2	Periodo y mecanismo de notificación	93
9.11.3	Circunstancias por la cual un OID debe cambiarse	94
9.12	Reclamaciones y resolución de disputas	94
9.13	Normativa aplicable	94
9.14	Cumplimiento de la normativa aplicable	95
9.15	Estipulaciones diversas	95
9.15.1	Acuerdo íntegro	95
9.15.2	Asignación	95
9.15.3	Divisibilidad	95
9.15.4	Cumplimiento	95
9.15.5	Fuerza Mayor	95
9.15.6	Otras estipulaciones	96



1 Introducción

1. Las administraciones públicas vascas como impulsoras 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.
2. 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.
3. 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). El objetivo de esta colaboración es el desarrollo de los servicios de confianza, como medios idóneos para avanzar en la simplificación de las relaciones entre la ciudadanía y la administración.

1.1 Presentación

4. El Reglamento eIDAS¹ contempla la posibilidad de erigirse como Prestador Cualificado de Servicios de Confianza.
5. 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.
6. 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 eIDAS.

¹ 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital



7. Así mismo con el objetivo de desarrollar e implantar eficazmente los servicios, Izenpe ha implementado un sistema de gestión de la seguridad de la información para los procesos relacionados con los servicios de confianza, según el estándar ISO 27001.
8. Izenpe para la prestación de los servicios de confianza sigue las indicaciones de los estándares de ETSI (Instituto Europeo de Estándares de Telecomunicaciones) 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.
9. Las especificaciones técnicas (ETSI TS) que se definen en estas normas marcan los requisitos básicos a los que se refieren a la gestión y prácticas de prestadores de servicios de confianza que emiten certificados cualificados y no cualificados y sellos de tiempo dentro del marco legal del Reglamento eIDAS incorporado al régimen jurídico de la "Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza", 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 eIDAS y EN 319 421 para la emisión de sellos de tiempo según se recoge en el Reglamento eIDAS.
10. En cumplimiento con la norma 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.
11. Izenpe incorpora la identificación remota por vídeo para la expedición de certificados de acuerdo con la "Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados y con la Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo".
12. En todo caso, cualquier consulta en relación con la accesibilidad del sitio web de Izenpe, de sus productos o servicios puede presentarse a través del correo electrónico info@izenpe.com o del formulario disponible en www.izenpe.eus.
13. Además de los servicios de confianza cualificados, Izenpe dispone de otros servicios no cualificados de confianza, entre los que destacar:
 - Expedición de certificados electrónicos no cualificados de firma electrónica.
 - Expedición de certificados electrónicos no cualificados de autenticación de sitios web.
 - Validación de firmas no cualificado.

1.2 Nombre del documento e identificación

1.2.1 Identificación

14. El presente documento se denomina "Declaración Prácticas de Confianza Global de Izenpe" e internamente será citado por su acrónimo DPCG. Este documento está estructurado según la RFC 3647.



15. El Comité de Seguridad de Izenpe revisa regularmente los riesgos a los que se expone la organización y aprueba los planes de tratamiento necesarios para garantizar la seguridad de los servicios definidos tanto en esta DPCG como las concreciones en los textos de divulgación (PDS).
16. Las condiciones de uso, limitaciones, responsabilidades, propiedades y cualquier otra información que se considere específica de cada tipo de certificado, vendrán reflejadas en las PDS dependientes de esta DPCG, y, cuando existan, de las DPC particulares.
17. Estos procedimientos se basan principalmente en las normas del European Telecommunications Standards Institute (ETSI).
18. Con el objeto de identificar de forma individual cada tipo de certificado emitido por Izenpe de acuerdo con la presente DPCG, se asignan a cada tipo un identificador de objeto (OID). Pueden consultarse en el documento de perfiles disponible en www.izenpe.eus. 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 los textos de divulgación (PDS).
 - Qctype: indica el tipo de firma según eIDAS (sello, firma, web).

1.2.2 Identificadores de certificados

19. Izenpe opera una infraestructura al objeto de prestar los siguientes servicios cualificados:
 - Expedición de certificados electrónicos cualificados de firma electrónica.
 - Expedición de certificados electrónicos cualificados de sello electrónico.
 - Expedición de certificados electrónicos cualificados de autenticación de sitios web.
 - Servicio de expedición de sellos electrónicos cualificados de tiempo.
20. En el ámbito de la presente DPCG y de las PDSs, Izenpe expide los siguientes tipos de certificado:

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

1.2.2.1.1 Certificados cualificados eIDAS.

Descripción	Política	OID
Certificados de ciudadano		
Ciudadano (chip)	QCP-n	1.3.6.1.4.1.14777.2.18.1
BaKQ (HSM)	QCP-n	1.3.6.1.4.1.14777.2.18.3



Certificados de Representante de Entidad		
Representante (software)	QCP-n	1.3.6.1.4.1.14777.2.12
Representante (chip)	QCP-n	1.3.6.1.4.1.14777.2.16
Representante (chip)-firma cualificada	QCP	1.3.6.1.4.1.14777.2.12.5
Certificados de Representante de Entidad SPJ		
Representante Entidad SPJ (HSM)	QCP-n	1.3.6.1.4.1.14777.2.15
Representante Entidad SPJ (chip)	QCP-n	1.3.6.1.4.1.14777.2.13
Representante Entidad SPJ (chip)-firma cualificada	QCP	1.3.6.1.4.1.14777.2.13.5
Representante Entidad SPJ (software)	QCP-n	1.3.6.1.4.1.14777.2.17
Certificados empleado público (PEP)		
Empleado público (chip)	QCP-n	1.3.6.1.4.1.14777.4.14.1
Empleado público (software)	QCP-n	1.3.6.1.4.1.14777.4.14.2
Empleado público (HSM)	QCP-n	1.3.6.1.4.1.14777.4.14.3
Certificados de personal de Empleado Público (PEP) con seudónimo		
Personal Entidad Pública con seudónimo (chip) FIRMA	QCP-n	1.3.6.1.4.1.14777.4.13.1.1
Personal Entidad Pública con seudónimo (software)	QCP-n	1.3.6.1.4.1.14777.4.13.2
Certificados de Profesional		
Corporativo cualificado (chip)	QCP-n	1.3.6.1.4.1.14777.2.19.1
Corporativo cualificado (software)	QCP-n	1.3.6.1.4.1.14777.2.19.2
Corporativo cualificado (HSM)	QCP-n	1.3.6.1.4.1.14777.2.19.3
Certificados de Sello electrónico de Entidad		
Sello de entidad (contenedor)	QCP-l	1.3.6.1.4.1.14777.2.11
Sello de entidad (HSM)	QCP-l	1.3.6.1.4.1.14777.2.20
Certificados de Sello electrónico de Administración		
Sello de administración (software)	QCP-l	1.3.6.1.4.1.14777.4.11.2
Sello de administración (HSM)	QCP-l	1.3.6.1.4.1.14777.4.11.3
Certificados de Autenticación web		
SSL cualificado	QEVCP-w	1.3.6.1.4.1.14777.50.3.2
SSL cualificado	QEVCP-w	1.3.6.1.4.1.14777.6.1.3

1.2.2.1.2 Certificados no cualificados.

Descripción	Política	OID
-------------	----------	-----



Certificados no cualificados de ciudadano		
BaK	NCP	1.3.6.1.4.1.14777.5.2.5
Izenpe Mobile (APP)	NCP	1.3.6.1.4.1.14777.5.2.5.4
Autónomo (software)	NCP	1.3.6.1.4.1.14777.5.2.7.2
Certificados no cualificados de Profesional		
Personal empleado público con seudónimo (chip) para Autenticación	NCP+	1.3.6.1.4.1.14777.4.13.1.2
Personal empleado público con seudónimo (chip) para Cifrado	N/A	1.3.6.1.4.1.14777.4.13.1.3
Corporativo no cualificado (chip)	NCP+	1.3.6.1.4.1.14777.1.1.1
Corporativo público no reconocido (chip)		
Corporativo privado no reconocido (chip)	NCP+	1.3.6.1.4.1.14777.5.2.2
Certificados no cualificados de Autenticación web		
SSL DV	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	OVCP	1.3.6.1.4.1.14777.1.2.1
Certificados no cualificados de Aplicación		
Aplicación (software)	NCP	1.3.6.1.4.1.14777.1.2.2
Certificados no cualificados de Dispositivo IOT		
Dispositivo (software)	NCP	1.3.6.1.4.1.14777.1.3.2

1.2.2.2 Jerarquía CA raíz 2020

1.2.2.2.1 Certificados SSL.

Descripción	Política	OID
Certificados de Autenticación web		
SSL DV	DVCP	1.3.6.1.4.1.14777.14.1.2

1.2.2.2.2 Certificados de sellado de tiempo.

Descripción	Política	OID
Certificados de sellado de tiempo		
TSA		1.3.6.1.4.1.14777.10.1



1.2.2.3 Jerarquía CA raíz 2024

1.2.2.3.1 Certificados cualificados Eidas.

Descripción	Política	OID
Certificados de Autenticación web		
SSL cualificado	QEVCP-w	1.3.6.1.4.1.14777.50.3.2

1.2.2.3.2 Certificados no cualificados

Descripción	Política	OID
Certificados no cualificados de Autenticación web		
SSL DV	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	OVCP	1.3.6.1.4.1.14777.50.2.2

1.2.2.4 Jerarquía CA raíz 2025

Descripción	Política	OID
Certificados de ciudadano		
Ciudadano (chip)	QCP-n	1.3.6.1.4.1.14777.51.1.1
BaKQ (HSM)	QCP-n	1.3.6.1.4.1.14777.51.1.3
Certificados de Representante de Entidad		
Representante (software)	QCP-n	1.3.6.1.4.1.14777.51.3.2
Representante (chip)	QCP-n	1.3.6.1.4.1.14777.51.3.1
Representante (chip)-firma cualificada	QCP	1.3.6.1.4.1.14777.51.3.5
Certificados de Representante de Entidad SPJ		
Representante Entidad SPJ (chip)	QCP-n	1.3.6.1.4.1.14777.51.4.1
Representante Entidad SPJ (chip)-firma cualificada	QCP	1.3.6.1.4.1.14777.51.4.5
Representante Entidad SPJ (software)	QCP-n	1.3.6.1.4.1.14777.51.4.2
Certificados empleado público (PEP)		
Empleado público (chip)	QCP-n	1.3.6.1.4.1.14777.52.1.1
Empleado público (software)	QCP-n	1.3.6.1.4.1.14777.52.1.2
Empleado público (HSM)	QCP-n	1.3.6.1.4.1.14777.52.1.3
Certificados de personal de Empleado Público (PEP) con seudónimo		
Personal Entidad Pública con seudónimo (chip) FIRMA	QCP-n	1.3.6.1.4.1.14777.52.2.1.1



Personal Entidad Pública con seudónimo (software)	QCP-n	1.3.6.1.4.1.14777.52.2.2
Certificados de Profesional		
Corporativo cualificado (chip)	QCP-n	1.3.6.1.4.1.14777.51.2.1
Corporativo cualificado (software)	QCP-n	1.3.6.1.4.1.14777.51.2.2
Corporativo cualificado (HSM)	QCP-n	1.3.6.1.4.1.14777.51.2.3
Certificados de Sello electrónico de Entidad		
Sello de entidad (contenedor)	QCP-l	1.3.6.1.4.1.14777.51.5.2
Sello de entidad (HSM)	QCP-l	1.3.6.1.4.1.14777.51.5.3
Certificados de Sello electrónico de Administración		
Sello de administración (software)	QCP-l	1.3.6.1.4.1.14777.52.3.2
Sello de administración (HSM)	QCP-l	1.3.6.1.4.1.14777.52.3.3
Certificados de Sello de Tiempo		
Certificado sello de tiempo		1.3.6.1.4.1.14777.53.1.3

1.3 Participantes de la infraestructura de clave pública PKI

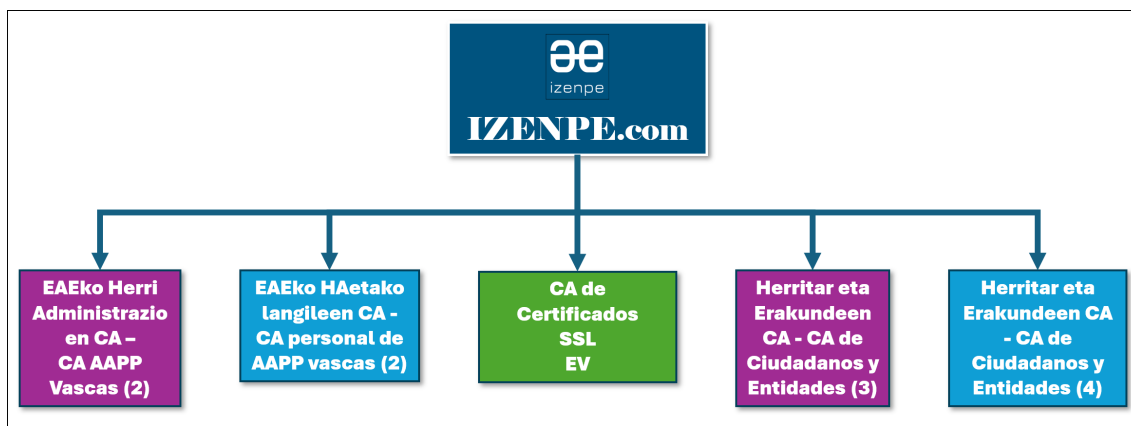
21. Los roles que intervienen en la administración y operación de la Entidad de Certificación son los siguientes:

- Autoridades de Certificación.
- Entidades de Registro.
- Suscriptores y firmantes de los certificados.
- Partes que confían.
- Otros participantes.

1.3.1 Autoridades de Certificación

22. Izenpe dispone de las siguientes Autoridades de Certificación:

1.3.1.1 Jerarquía Izenpe.com creada el 2007



Certificado CA Raíz

CN	izenpe.com
VALIDEZ	13/12/2007 hasta el 13/12/2037
HASH SHA256	25:30:CC:8E:98:32:15:02:BA:D9:6F:9B:1F:BA:1B:09:9E:2D:29:9E:0F:45:48:BB:91:4F:36:3B:C0:D4:53:1F
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA

Certificado CA Subordinada

CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)
VALIDEZ	20/10/2010 hasta el 13/12/2037
HASH SHA256	CD:6E:B9:37:EE:17:A9:FC:FF:60:A7:90:F8:BD:E0:CA:9A:BC:A0:7B:3E:F4:60:74:DD:19:78:F0:BC:A4:D4:49
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA

Certificado CA Subordinada

CN	EAEko HAetako langileen CA - CA personal de AAPP vascas (2)
VALIDEZ	20/10/2010 hasta el 13/12/2037
HASH SHA256	25:30:3C:FD:0B:F1:BA:A1:EF:24:8C:29:F0:73:FF:FC:2E:7C:81:58:2E:E2:3B:45:C7:F1:C3:B3:2E:34:1A:D8
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA



Certificado CA Subordinada

CN	CA de Certificados SSL EV
VALIDEZ	6/7/2018 hasta el 6/7/2028
HASH SHA256	DB:47:63:39:CC:BF:CC:9E:4B:D1:D6:CB:60:6C:A2:7F:00:67:9E:1E:F8:A5:81:E7:23:63:09:B9:D6:3F:FE:37
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA

Certificado CA Subordinada

CN	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3)
VALIDEZ	20/10/2010 hasta el 13/12/2037
HASH SHA256	5A:49:B1:5A:E6:0F:F6:27:DA:27:2A:87:43:D6:71:62:BA:CA:10:96:16:82:03:21:3A:CF:82:27:AF:4C:49:42
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA

Certificado CA Subordinada

CN	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)
VALIDEZ	20/10/2010 hasta el 13/12/2037
HASH SHA256	7E:D1:93:61:AD:73:4D:70:3F:BA:DF:02:9F:52:EC:3B:66:48:D8:DD:56:BA:BA:08:84:ED:4F:85:9B:5B:93:75
TIPO CLAVE	RSA 4096 bits / SHA-256 with RSA

1.3.1.2 Jerarquía creada el 2020.





Certificado CA RAIZ 2020

CN		ROOT CA QC IZENPE
VALIDEZ		23/09/2045
HASH SHA256		[d4a81325ebf2e5c19c779192c63db76404c8dafd] (CRT)
TIPO CLAVE		SHA2

Certificado CA Subordinada

CN		SUBCA QC IZENPE - TSA
VALIDEZ		23/09/2045
HASH SHA256		[fa6cf62e148806df05f536bc71dfe34b364023e8] (CRT)
TIPO CLAVE		SHA2

1.3.1.3 Jerarquía creada el 2024



Certificado CA RAIZ 2024

CN		ROOT CA SSL IZENPE 2024
VALIDEZ		24/09/2049
HASH SHA256		68E93296DEEB4254C18C49C4E80F5D8FA3D38A93
TIPO CLAVE		ECC(384 Bits)



Certificado CA Subordinada

CN	SUBCA SSL 2024
VALIDEZ	23/09/2045
HASH SHA256	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18
TIPO CLAVE	ECC(384 Bits)

1.3.1.4 Jerarquía creada el 2025

Certificado CA RAIZ 2025

CN	ROOT CA QC IZENPE 2025
VALIDEZ	25/09/2050
HASH SHA256	D2A934AE739B8B8B0C1D3857C324DE595EEB1DCAFD086A4A7E99DC08D77AF0C A
TIPO CLAVE	ECC(384 Bits)

Certificado CA Subordinada.

CN	CA ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA 2025
VALIDEZ	25/09/2045
HASH SHA256	7E4E551152F06C51DB576236162514BAFD7ABCE1A3A4141A1A7949BDCFE1A432
TIPO CLAVE	ECC(384 Bits)

Certificado CA Subordinada.

CN	CA HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA 2025
VALIDEZ	25/09/2045
HASH SHA256	D852490ED91838B06F6885E17153738DEBFE9A5FF9DDB96BA0E36E5D4572EFEE
TIPO CLAVE	ECC(384 Bits)

Certificado CA Subordinada.

CN	CA QC IZENPE-TSA 2025
VALIDEZ	25/09/2045



HASH SHA256	9850D9462094CD18854E39B9241DBA89FA4AFB4084AB942F0D3ABCEBA8FA3529
TIPO CLAVE	ECC(384 Bits)

1.3.2 Entidades de Registro

23. Esta DPCG se aplica a las Entidades de Registro que Izenpe emplee en los procedimientos de expedición y gestión de certificados.
24. Las Entidades de Registro realizan las tareas de identificación de los solicitantes, suscriptores y firmantes de los certificados, comprobación de la documentación acreditativa de las circunstancias que constan en los certificados, así como la validación y aprobación de las solicitudes de expedición, revocación y renovación de los certificados.
25. Serán Entidad de Registro: Izenpe y/o las Entidades Usuarias con las que Izenpe suscriba el correspondiente instrumento legal.

1.3.3 Suscriptores de los certificados

26. Tendrá la condición de suscriptor la persona que solicite un certificado.
27. Los **firmantes** son las personas físicas que mantienen bajo su uso exclusivo los datos de creación de firma asociados a los certificados de los que son titulares.
28. En ocasiones, la figura del suscriptor y firmante no coinciden: las personas jurídicas pueden solicitar certificados para sus empleados, socios, trabajadores en los que en éstos certificados las personas físicas se consideran “firmantes” y la persona jurídica se considera “suscriptor”.
29. Los **creadores de sellos** son las personas jurídicas que crean sellos electrónicos en los que se consta la identidad de dicha persona jurídica (Empresa mercantil, Fundación, Administración Pública...)

1.3.4 Terceras partes de confianza

30. Dentro de esta DPCG, las personas físicas o jurídicas que reciben servicios prestados por Izenpe son terceros que confían en estos servicios de confianza y, como tales, les es de aplicación lo establecido por la presente DPCG
31. Antes de confiar en los certificados y las firmas y sellos que creen, las terceras partes deben verificarlos, como se establece en esta DPCG: Para ello se comprobará que se ha usado un certificado válido, que se han creado las firmas o sellos durante el periodo de validez del certificado y que se ha cumplido con las indicaciones y directrices de esta DPCG.
32. 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 entre otros repudiar mensajes emitidos dentro del ámbito de confianza asociado a la categoría del certificado o sello de tiempo.



1.3.5 Otros participantes

33. Izenpe es Autoridad de Sellado de Tiempo cuando provee el Servicio de Confianza de creación de sellos de tiempo electrónicos, bajo su correspondiente DPCP.

1.4 Usos del certificado

34. Se establecen a continuación los usos permitidos y prohibidos de los certificados expedidos por Izenpe

1.4.1 Usos apropiados del certificado

1.4.1.1 Certificados cualificados

35. Los certificados cualificados de firma electrónica garantizan la identidad del suscriptor y del firmante . Cuando se empleen con dispositivos seguros de creación de firma, resultan idóneos para ofrecer soporte a la firma electrónica cualificada; esto es, la firma electrónica avanzada que se basa en certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo que, de acuerdo con el Reglamento eIDAS, se equipara a la firma manuscrita por efecto legal, sin necesidad de cumplir requisito adicional alguno.
36. Los certificados cualificados de firma electrónica son cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento eIDAS.
37. 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, cifrado sin recuperación de claves u otros. Esta firma electrónica tiene el efecto de garantizar la identidad del suscriptor del certificado de firma.
38. 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.
39. El certificado de sello electrónico es una declaración electrónica que 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.
40. Los certificados cualificados de sello electrónico son cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento eIDAS.
41. 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 del Reglamento eIDAS para ser considerados cualificados.
42. Los certificados de sello electrónico de órgano se emiten a las administraciones públicas para la identificación del órgano y el sellado electrónico de documentos, según lo previsto en la “Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público”.
43. Los certificados cualificados de Izenpe siguen la norma técnica ETSI EN 319 411-2.



1.4.1.2 Certificado no cualificado

44. Los certificados no cualificados no garantizan fehacientemente la identidad del suscriptor y, en su caso, del firmante 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.
45. 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, , cifrado sin recuperación de claves, u otros.
46. Los certificados no cualificados de Izenpe siguen la norma técnica ETSI EN 319 411-1.

1.4.1.3 Ámbito de uso de los certificados

47. En cuanto a su ámbito de uso se distinguen dos supuestos:
 - Los certificados expedidos por Izenpe y dirigidos al público en general serán utilizados por los suscriptores, o en su caso por los firmantes, en las relaciones que mantengan con las entidades usuarias e instituciones públicas y privadas en general que hayan admitido su uso.
48. Consultar las especificidades en cuanto al ámbito de uso de cada certificado en la PDS y cuando existan, las DPC particulares.
 - Los certificados emitidos por Izenpe y solicitados por las entidades usuarias serán utilizados en el ámbito de sus características como persona física o jurídica, según especificaciones de eIDAS. No obstante, los firmantes podrán utilizar estos certificados para otros usos siempre que se respeten los límites de uso señalados en el apartado anterior.

1.4.1.4 Certificado de persona física ciudadano

1.4.1.4.1 Certificados cualificados

- **Descripción:** certificado de persona física.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en tarjeta o en HSM (firma remota).

Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Certificado Ciudadano	Tarjeta	QCP-n	Perfil eIDAS	Avanzada
			1.3.6.1.4.1.14777.2.18.1	
Certificado Ciudadano BakQ	HSM	QCP-n	1.3.6.1.4.1.14777.51.1.1	Avanzada
			1.3.6.1.4.1.14777.2.18.3	
			1.3.6.1.4.1.14777.51.1.3	



1.4.1.4.2 Certificados no cualificados

49. Certificado BaK.

- **Descripción:** permite la identificación y firma de personas físicas.
Está formado por un número de referencia coincidente con el DNI/NIE/pasaporte de la persona usuaria y una contraseña.
Es un certificado no cualificado emitido en un repositorio centralizado de Izenpe que servirá para los actos de firma. La política ETSI LCP que incorpora Bak, implica que su expedición no requiere identificación presencial.
- **Validez:** hasta 4 años.
- **Soporte:** expedidos en HSM (firma remota).

50. Certificado Izenpe Mobile

- **Descripción:** medio que permite la identificación de personas físicas y autoriza el uso de un certificado cualificado almacenado en un repositorio centralizado seguro de Izenpe asociado a la persona. Está formado por:
 - Una aplicación instalada en un dispositivo móvil, vinculada a un certificado no cualificado que facilita procesos de comunicaciones seguras
 - Una contraseña o un factor biométrico que facilita el acceso a la aplicación.
- **Validez:** hasta 4 años.
- **Soporte:** emitidos en software.

51. Certificado de autónomo.

- **Descripción:** certificado de persona física expedido para las relaciones de la persona con la condición de autónomo con las Haciendas Forales vascas.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en software.

Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
BaK	HSM	LCP	1.3.6.1.4.1.14777.5.2.5	Básica
Izenpe Mobile	Contenedor APP	NCP	1.3.6.1.4.1.14777.5.2.5.4	NA (para firmar se usa el de BaKQ o profesional)
Autónomo	Software	LCP	1.3.6.1.4.1.14777.5.2.7.2	Básica

1.4.1.5 Certificado de persona física representante de entidad

1.4.1.5.1 Certificados cualificados



- **Descripción:** certificado expedido a una persona física con capacidad para actuar en nombre y representación de una persona jurídica.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en tarjeta, en contenedor software o en remoto en HSM.

Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Representante entidad	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.12 1.3.6.1.4.1.14777.51.3.1	Avanzada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.16 1.3.6.1.4.1.14777.51.3.2	Avanzada
	Chip criptográfico	QCP	1.3.6.1.4.1.14777.2.12.5 1.3.6.1.4.1.14777.51.3.5	Cualificada

1.4.1.6 Certificado de persona física representante de entidad sin personalidad jurídica

- **Descripción:** certificado expedido a una persona física) con capacidad para actuar en nombre y representación de una entidad sin personalidad jurídica.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en tarjeta, en contenedor software o en remoto en HSM.

1.4.1.6.1 Certificados cualificados.

Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Representante Entidad SPJ	HSM	QCP-n	1.3.6.1.4.1.14777.2.15 1.3.6.1.4.1.14777.51.4.3	Avanzada
	Chip criptográfico	QCP-n	1.3.6.1.4.1.14777.2.13 1.3.6.1.4.1.14777.51.4.1	Avanzada
	Chip criptográfico	QCP	1.3.6.1.4.1.14777.2.13.5 1.3.6.1.4.1.14777.51.4.5	Cualificada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.17 1.3.6.1.4.1.14777.51.4.2	Avanzada



1.4.1.7 Certificado de empleado público

1.4.1.7.1 Certificados cualificados

- **Descripción:** certificado expedido al personal al servicio de las administraciones públicas. Expedido en el ámbito de la “Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público”.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en tarjeta, en contenedor software o en remoto en HSM.

Sescripción	Soporte	Id de política	OID política	Tipo firma eIDAS
Empleado público	Tarjeta criptográfica	QCP-n	1.3.6.1.4.1.14777.4.14.1 1.3.6.1.4.1.14777.52.1.1	Avanzada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.4.14.2 1.3.6.1.4.1.14777.52.1.2	Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3 1.3.6.1.4.1.14777.52.1.3	Avanzada

1.4.1.8 Certificado de empleado público con seudónimo

1.4.1.8.1 Certificados cualificados

- **Descripción:** certificado expedido al personal al servicio de las administraciones públicas con la característica de no incluir datos personales del titular del certificado, sino estar emitido a un seudónimo de acuerdo con el documento de “Perfiles de Certificados electrónicos del Ministerio de Hacienda y Administraciones Públicas”, en el ámbito de la “Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público”.
- **Validez:** hasta 4 años.
- **Soporte:** expedidos en tarjeta o en contenedor software.

Breve descripción	Soporte	Id de política	OID política	Tipo firma eIDAS
Empleado público con seudónimo (firma)	Tarjeta criptográfica	QCP-n	1.3.6.1.4.1.14777.4.13.1.1 1.3.6.1.4.1.14777.52.2.1.1	Avanzada
Empleado público con seudónimo	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.4.13.2 1.3.6.1.4.1.14777.52.2.2	Avanzada

1.4.1.8.2 Certificados no cualificados



- **Descripción:** certificado para funciones de autenticación y cifrado que se emite junto al certificado cualificado de firma.
- **Validez:** hasta 4 años.
- **Soporte:** expedidos en tarjeta.

Breve descripción	Soporte	Id de política	OID política	Tipo firma eIDAS
Empleado público con seudónimo	tarjeta	NCP+	Autenticación 1.3.6.1.4.1.14777.4.13.1.2 1.3.6.1.4.1.14777.52.2.1.2	n/a
		n/a	Cifrado 1.3.6.1.4.1.14777.4.13.1.3 1.3.6.1.4.1.14777.52.2.1.3	n/a

1.4.1.9 Certificado de persona física profesional

1.4.1.9.1 Certificados cualificados

- **Descripción:** certificado expedido al personal de una organización.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en tarjeta, en contenedor software o en remoto en HSM.

Breve descripción	Soporte	Id de política	OID política	Tipo firma eIDAS
Profesional-Corporativo cualificado	Tarjeta	QCP-n	1.3.6.1.4.1.14777.2.19.1 1.3.6.1.4.1.14777.51.2.1	Avanzada
	Contenedor software de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.19.2 1.3.6.1.4.1.14777.51.2.2	Avanzada
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3 1.3.6.1.4.1.14777.51.2.3	Avanzada

1.4.1.9.2 Certificados no cualificados

52. Profesional-Corporativo no cualificado

- **Descripción:** certificado que identifica, con un grado medio de aseguramiento, la entidad actuante como suscriptora del certificado, así como a la persona que desempeña un cargo o puesto en la misma, como firmante.
- **Validez:** hasta 4 años.



- Soporte: expedido en tarjeta.

53. Profesional-Corporativo privado no cualificado

- **Descripción:** certificado que identifica, con un grado medio de aseguramiento, la entidad privada actuante como suscriptora del certificado, así como a la persona que desempeña un cargo o puesto en la misma, como firmante.
- **Validez:** hasta 4 años.
- **Soporte:** expedido en tarjeta.

Breve descripción	Soporte	Id de política	OID política	Tipo firma eIDAS
Corporativo no cualificado	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.1.1.1	Básica
Corporativo privado no reconocido	Chip criptográfico	NCP+	1.3.6.1.4.1.14777.5.2.2	Básica

1.4.1.10 Certificado de sello electrónico de entidad (persona jurídica y spj)

- **Descripción:** certificado que permite la identificación de la entidad, así como, en su caso, de la persona solicitante.

Permite probar que un documento electrónico ha sido expedido por ésta, aportando certeza sobre el origen y la integridad del documento.

Se emite a personas jurídicas y a entidades sin personalidad jurídica.

El suscriptor será la entidad. El solicitante la persona física, con capacidad para actuar en nombre de la entidad, que solicita el certificado.

Podrá constar en el certificado la información de la persona física en el caso que así lo determine de forma expresa.

- **Validez:** hasta 3 años.
- **Soporte:** expedido en software o remotos en HSM.

1.4.1.10.1 Certificados cualificados

Breve descripción	Soporte	Identificador de política	OID política	Tipo firma eIDAS
Sello de entidad	Contenedor software de Izenpe	QCP-I	1.3.6.1.4.1.14777.2.11 1.3.6.1.4.1.14777.51.5.2	Avanzada
	HSM	QCP-I	1.3.6.1.4.1.14777.2.20 1.3.6.1.4.1.14777.51.5.3	Avanzada



1.4.1.11 Certificado de sello electrónico de administración (sello de órgano)

- **Descripción:** certificado que permite la identificación de la administración, órgano, organismo público o entidad de derecho público, así como, en su caso, la identidad de la persona titular del órgano.

Se expide en el ámbito de la “Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público”.

Tendrá la consideración de suscriptor la administración, órgano, organismo público o entidad de derecho público.

Los certificados son de nivel medio.

- El certificado será utilizado por el suscriptor en aquellos servicios definidos por su organización como procedimientos de actuación automatizada y en los ofrecidos por terceros que admitan su uso con las condiciones y limitaciones definidas en esta DPCG.
- **Validez:** hasta 3 años.
- **SopORTE:** expedido en software o en remoto en HSM.

1.4.1.11.1 Certificados cualificados

Breve descripción	SopORTE	Identificador de política	OID política	Tipo firma eIDAS
Sello de administración	Contenedor software de Izenpe	QCP-I	1.3.6.1.4.1.14777.4.11.2 1.3.6.1.4.1.14777.52.3.2	Avanzada
	HSM	QCP-I	1.3.6.1.4.1.14777.4.11.3 1.3.6.1.4.1.14777.52.3.3	Avanzada

1.4.1.12 Certificado de autenticación de sitio web (servidor seguro)

1.4.1.12.1 Certificados cualificados

- **Descripción:** certificado de autenticación de sitio web.
- **Validez:** hasta 395 días².
- **SopORTE:** expedido en software.

² Validez de acuerdo con la normativa de Cabforum.org



Breve descripción	Soporte	Identificador de política	OID política
SSL cualificado	Software	QEVCP-w	1.3.6.1.4.1.14777.6.1.3
SSL cualificado	Software	QEVCP-w	1.3.6.1.4.1.14777.50.3.2

1.4.1.12.2 Certificados no cualificados

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 DV	Software	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.50.2.2
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.14.1.2

1.4.1.13 Certificado de aplicación

1.4.1.13.1 Certificado no cualificado

- **Descripción:** certificado empleado por una aplicación informática para asegurar la autenticidad e integridad de los datos electrónicos a los que va asociada la firma digital.
- **Validez:** hasta 3 años.
- **Soporte:** expedido en software.

Breve descripción	Soporte	Identificador de política	OID política
Aplicación	Contenedor software de Izenpe	NCP	1.3.6.1.4.1.14777.1.2.2

1.4.1.14 Certificado para dispositivo IOT

1.4.1.14.1 Certificado no cualificado

- **Descripción:** certificado que crea una identidad para objetos de un ecosistema IoT, que garantiza la integridad y el origen de los documentos firmados.
- **Validez:** hasta 10 años.
- **Soporte:** expedido en software.



Breve descripción	Soporte	Identificador de política	OID política
Dispositivo	Software	NCP	1.3.6.1.4.1.14777.1.3.2

1.4.1.15 Certificado para el sellado de tiempo TSA/TSU

1.4.1.15.1 Certificado timestamp

- **Descripción:** certificado de sello electrónico de persona jurídica con la activación del uso para el sellado de tiempo electrónico.
- **Validez:** hasta 5 años.
- **Soporte:** emitido en software.

BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA
Certificado de TSU	Software	NA	1.3.6.1.4.1.14777.10.1 1.3.6.1.4.1.14777.53.1.3

1.4.2 Usos prohibidos del certificado

54. Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.
55. Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la legislación aplicable.
56. 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.
57. Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados, ni para firmar peticiones de emisión, renovación, suspensión ni revocación de certificados

1.5 Administración de Políticas

1.5.1 Entidad responsable de la gestión de la documentación

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



1.5.2 Datos de contacto.

Nombre del prestador	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Dirección postal	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Dirección e-mail	izenpe@izenpe.eus
Teléfono	900 840 123

59. Para informar problemas de seguridad, tales como sospecha de compromiso clave, uso indebido de certificados, fraude u otros asuntos, comuníquese con incidencias@izenpe.eus
60. 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 DPCG

61. El Comité de Seguridad de Izenpe es el órgano responsable de la aprobación de la presente DPCG, así como de sus cambios y de las DPC particulares y PDS cuando existen.

1.5.4 Procedimiento de aprobación de la DPCG.

62. Las modificaciones finales del presente documento, las DPCP y las PDS 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.

- **Autoridad de Certificación (CA):** entidad que emite, a petición de la Autoridad de Registro, los certificados, de forma automatizada y previa confirmación de la Autoridad de Registro.
- **Autoridad de Registro (RA)** entidad encargada de realizar las tareas de identificación de los solicitantes, suscriptores y poseedores de claves de los certificados, comprueba la documentación acreditativa de la información que consta 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. Es el primer y principal certificado de una jerarquía PKI. Es autofirmado y sirve para firmar los certificados de las CA intermedias o subordinadas, emisoras de los certificados finales.

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:** certificado electrónico expedidos por un prestador de servicios de confianza 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 presta.
- **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 electrónicas.
- **Declaración de Prácticas de Confianza Global (DPCG):** declaración que Izenpe pone a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita. Se detallarán, en el marco de eIDAS, las obligaciones que los prestadores de servicios de confianza se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados 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 del Reglamento 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 del Reglamento 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 que 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 zenpe 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.
- **Poseedores de claves:** son las personas físicas que poseen o responden de la custodia de las claves de autenticación y firma electrónica.
- **Prestador cualificado de servicios de confianza (TSP):** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados según el Reglamento 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 Usuaria 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 web.
- **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 expedidos por Izenpe. Son terceros que confían en certificados y, como tales, les es de aplicación lo establecido por la DPCG 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 electrónicos.
- **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 del Reglamento 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 del Reglamento 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 del Reglamento 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 del Reglamento 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).
- **DPCG:** Declaración de Prácticas de Confianza Globalcertificación.
- **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 Confianza.
- Políticas de certificación que vienen definidas en la norma ETSI EN 319411-1 (*General requirements*):
 - **NCP:** Política de certificación normalizada que cumple las mejores prácticas reconocidas por los prestadores que emiten certificados usados para cualquier transacción.
 - **NCP+:** Política de certificación normalizada extendida que cumple las prácticas de la política NCP pero los certificados necesitan de un dispositivo criptográfico seguro para su uso.
 - **OVCP:** Política de certificación de organización validada para certificados de autenticación web con los requisitos de CABForum para la validación de organizaciones solicitantes.
 - **DVCP:** Política de certificación de dominio validado para certificados de autenticación web con los requisitos de CABForum para la validación de dominios.
- Políticas de Certificación Cualificadas, que vienen definidas en la norma ETSI EN 319411-2 (*Requirements for trust service providers issuing EU qualified certificates*)
 - **QCP-n:** Política de certificación cualificada que hace referencia a las firmas electrónicas avanzadas basadas en certificados cualificados de acuerdo con los artículos 26 y 28 del Reglamento eIDAS, para las personas físicas.
 - **QCP-l:** Política de certificación cualificada que hace referencia a los sellos electrónicos avanzados basados en certificados cualificados de acuerdo con los artículos 36 y 38 del Reglamento eIDAS, para las personas jurídicas.
 - **QCP-n-qscd:** Política de certificación cualificada que hace referencia a las firmas electrónicas cualificadas definidas en el artículo 3.12 del Reglamento eIDAS, para las personas físicas.
 - **QCP-l-qscd:** Política de certificación cualificada que hace referencia a los sellos electrónicos cualificados definidos en el artículo 3.27 del Reglamento eIDAS, para las personas jurídicas.
 - **QEVCP-w:** Política de certificación cualificada que hace referencia a los certificados de autenticación web cualificados definidos en el artículo 3.38 y 45 del Reglamento eIDAS, y descritos en la sección 4.2.2.5 de la norma ETSI EN 319 411-2.
- **RA:** Autoridad de Registro.



- SSL: Secure Socket Layer .
- TSA: Servidor de la Autoridad de Sellado de Tiempo.



2 Publicación y responsables del repositorio de información

2.1 Repositorio de información

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

2.2 Publicación de información de certificación

64. Izenpe garantiza la disponibilidad de la DPCG, las DPCP, PDS y , términos y condiciones de uso de los servicios de confianza en www.izenpe.eus.

65. 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)

66. 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 la DPC particular de certificados de autenticación web.

2.2.1 Política de publicación y notificación.

67. Los cambios en las especificaciones o en las condiciones del servicio serán comunicados por Izenpe a los usuarios a través de www.izenpe.eus. Podrá establecer canales adicionales de comunicación para situaciones específicas.

68. En el caso de DPCG, y Términos y Condiciones de Uso, izenpe mantendrá publicas en www.izenpe.eus el histórico de versiones .

2.2.2 Elementos no publicados en la Declaración de Prácticas de Certificación Global.

69. 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 “9.2.5 Información que no está dentro del alcance” de la presente DPCG.

2.3 Frecuencia de publicación

70. La DPCG se publica en el momento de su aprobación y si no hubiera cambios en la revisión anual. Los cambios se rigen por lo establecido en el presente documento.

71. La información sobre el estado de los certificados se publica de acuerdo con lo establecido en los apartados “4.9.7 Frecuencia de generación de CRLs” y “4.9.9 Requisitos de comprobación de revocación online” del presente documento.



2.4 Control de acceso al repositorio

72. 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.

73. 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 Identificación y autenticación

3.1 Nombres

3.1.1 Tipos de nombres

74. Todos los certificados de entidad final contienen un nombre distinguido en el campo Subject Name.
75. Los atributos que componen el nombre diferenciado del campo subject son los recogidos en el apartado correspondiente al perfil del certificado
76. El valor autenticado del campo *Common Name* es el nombre del suscriptor y en su caso del firmante.
77. En la extensión Subject Alternative Name se suelen incluir identidades alternativas de la misma persona que aparece como suscriptora del certificado.

3.1.2 Significado de los nombres

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

3.1.3 Seudónimos

79. Los certificados no permiten el uso de seudónimos para el firmante, a excepción de los certificados de empleado público con seudónimo.

3.1.4 Reglas para la Interpretación de formatos de nombres

80. El subject en un certificado identifica a la persona (física o jurídica) o dispositivo, y . Izenpe 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 “3.1.5 Unicidad de los nombres”.
81. En los certificados de autenticación de sitios web se deberá tener en cuenta los requerimientos del CABForum (Baseline Requirements y EV Guidelines).

3.1.5 Unicidad de los nombres

82. Los nombres de los suscriptores y, en su caso, los firmantes 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.

3.1.6 Resolución de conflictos relativos a nombres y tratamiento de marcas registradas

83. 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.
84. 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.



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

3.1.7 Emisor (Issuer)

86. Este campo contiene la identificación de Izenpe, la entidad de certificación que ha firmado y expedido el certificado.

87. 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.

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

3.1.8 Asunto (Subject)

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

90. 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.

3.2 Validación de la identidad

3.2.1 Métodos para probar la posesión de la clave privada

91. 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 o en su caso del firmante.
- Por el propio firmante del certificado: la demostración de posesión de la clave privada consiste en la correcta utilización 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

92. 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 eIDAS.

93. En www.izenpe.eus se publica la documentación que cada entidad deberá aportar en función de su configuración jurídica.



94. La identidad de la organización se acreditará mediante la documentación requerida según el tipo de entidad.

95. Más información: en las PDS.

3.2.2.1 Validación del dominio

96. La validación del dominio web en aquellos certificados de autenticación de sitio web se describe en la PDS correspondiente.

3.2.3 Autenticación de la identidad de la persona física solicitante

97. 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 eIDAS.

98. Más información en la Declaración de Prácticas del Servicio de Verificación de la Identidad y en las PDS.

99. Izenpe verificará la identidad del solicitante,

- De manera presencial.
- Legitimación de la firma de la Solicitud de Emisión por notario.
- Por medio de un certificado cualificado vigente
- Con identificación remota por vídeo.

3.2.4 Información no verificada del suscriptor

100. En general, la información de los certificados es verificada previamente a la emisión contrastándola con fuentes de información. Cuando existan PDSs se atenderá a lo determinado al respecto.

3.2.5 Validación de la autoridad

101. Se firmará el correspondiente instrumento legal en las que se especificarán las condiciones de la delegación del registro y las responsabilidades de los operadores.

102. Las Autoridades de Registro deberán :

- Acreditar a los operadores.
- Dotarles de un certificado cualificado expedido por Izenpe.
- Asegurar que han recibido la formación suficiente.
- Asegurar los envíos de documentación a Izenpe.

3.2.6 Criterios de interoperación

103. No existen relaciones de interactividad con autoridades de certificación externas a Izenpe.



3.3 Identificación y autenticación para peticiones de reemisión de claves

3.3.1 Renovación rutinaria

3.3.2 Renovación después de una revocación

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

3.4 Identificación y autenticación para peticiones de revocación

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



4 Requisitos operativos del ciclo de vida de los certificados

La presente PDCG regula los requisitos operativos comunes a los certificados expedidos.

En el caso de que Izenpe realizara cross-certification con una CA externa, exigirá a dicha CA el cumplimiento de todos los requisitos definidos en la DPCG, las PDS y la DPSV.

4.1 Solicitud de certificado

106. 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.

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

4.1.1 Comprobación de la solicitud

108. Izenpe de forma previa a la emisión del certificado comprobará los datos que constan en la solicitud según lo indicado en la DPCG, DPCP, PDS.

4.1.2 Proceso de inscripción y responsabilidades

109. 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 firmante 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 expedición, 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 firmante los procedimientos técnicos de creación y de verificación de firma electrónica.



4.2 PGestión de las solicitudes

4.2.1 Realización de funciones de identificación y autenticación

110. Es responsabilidad de Izenpe identificar el suscriptor de forma adecuada. según la DPSV. Aprobar o rechazar solicitudes.
111. Una vez realizada la solicitud de certificado, la RA deberá verificar la información aportada por el solicitante, incluyendo la validación de la identidad del suscriptor.
112. Si la información no es correcta, la RA denegará la petición, contactando con el solicitante para comunicarle el motivo. Si es correcta, se procederá a la emisión del certificado.
113. Cuando se solicite 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 este registro 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 hayan podido subsanar esa posible incidencia.

4.2.2 Tiempo en procesar la solicitud

114. Entre la aprobación de la solicitud y la expedición del certificado no puede transcurrir un periodo temporal superior a un mes. En todo caso cada DPCP o PDS concretará este aspecto.

4.3 Emisión del certificado

115. La emisión de un certificado implica la aprobación final y completa de una solicitud. Izenpe emitirá el certificado según lo determinado en esta DPCG, las DPCP cuando existan y las PDS. Además, Izenpe entregará al suscriptor (o al firmante en los certificados profesionales) los certificados y/o los códigos de desbloqueo en los casos en los que Izenpe genere las claves.
116. Si el solicitante no tuviera constancia de la expedición del certificado, deberá ponerse en contacto con Izenpe.

4.3.1 Acciones de la CA durante la emisión

117. Cumplirá lo determinado para la emisión de cada tipo de certificado en la DPCG, DPCP, en las DPSV.

4.3.2 Izenpe procederá a la emisión del certificado según lo determinado al efecto en ca DPCP o PDS. Notificación de al sla emisión

118. Izenpe notifica al suscriptor y/o firmante de la expedición del certificado.

4.3.3 Verificación del certificado

119. La persona firmante deberá verificará el correcto funcionamiento y, en caso de que fuera necesario, comunicará a Izenpe los defectos de funcionamiento.
120. Si los defectos de funcionamiento se debieran a causas técnicas (entre otras: mal funcionamiento del soporte del certificado, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado aplicables a Izenpe, Izenpe revocará el certificado y procederá a emitir uno nuevo asumiendo los costes derivados.



4.4 Aceptación del certificado

121. 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 DPCG, que rige técnica y operativamente los servicios de certificación prestados por Izenpe.

4.4.1 Proceso de aceptación del certificado.

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

4.4.2 Publicación del certificado por la CA.

123. Una vez que el certificado ha sido aceptado por el suscriptor y generado, el certificado será publicado en repositorios internos de Izenpe.

124. 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.

125. 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

126. 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 sus limitaciones de uso.
- 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 DPCG.
- 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 firmantes 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 electrónicas 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 elIDAS.

127. 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 DPCG.
- 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 DPCG.
- 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 electrónicas 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 elIDAS.



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

128. 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 DPCG.
- Verificar la validez o revocación de los certificados expedidos, 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 electrónica 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.
- 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 el Reglamento eIDAS.

4.6 Renovación del certificado

129. La renovación del certificado consiste en la emisión de un nuevo certificado al suscriptor sin cambiar ninguna 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.eus.

130. En el plazo de 30 días previos a la caducidad del certificado se podrá proceder a su renovación.

131. Izenpe tramitará la renovación según el procedimiento de emisión y entrega previsto en cada caso.

4.6.1 Circunstancias para la renovación del certificado

132. Izenpe realiza esfuerzos razonables para notificar a los suscriptores la próxima expiración del certificado. La notificación se realizará normalmente durante el periodo de 30 días previos a la caducidad del certificado.

4.6.2 Quién puede solicitar la renovación

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



4.6.3 Tratamiento de peticiones de renovación de certificado

134. El suscriptor podrá contactar con Izenpe y solicitar su renovación. Izenpe le informará de cómo formalizar su solicitud.

4.6.4 Notificación al suscriptor

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

4.6.5 Procedimiento de aceptación de un certificado renovado

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

4.6.6 Publicación del certificado

137. 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

138. Según lo recogido en el punto 4.4.3.

4.7 Renovación con regeneración de las claves del certificado

139. 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 certificado anterior. El nuevo certificado contendrá nueva información de validez y un nuevo par de claves, pero mantendrá el mismo subject.

140. Se renovarán las claves durante la renovación del certificado según DPS.

4.7.1 Circunstancias para regenerar las claves del certificado

141. 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 DPCG. También se podrán regenerar las claves del certificado cuando éstas se vean comprometidas.

4.7.2 Quien lo puede pedir

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

143. Cualquier suscriptor podrá pedir la renovación de su certificado si se cumplen las circunstancias descritas en esta DPCG.

4.7.3 Tratamiento de las peticiones de renovación con regeneración de claves

144. El suscriptor podrá contactar con Izenpe y solicitar su renovación. Izenpe e informará de cómo formalizar su solicitud. Notificación al suscriptor.

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

4.7.4 Procedimiento de aceptación del certificado renovado

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



4.7.5 Publicación del certificado

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

148. Notificación a otras entidades.

149. Según lo recogido en el punto 4.4.3

4.8 Modificación del certificado

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

4.8.1 Circunstancias para la modificación del certificado.

151. No se estipula la modificación.

4.8.2 Quién puede solicitar la modificación del certificado

152. No se estipula la modificación.

4.8.3 Procesamiento de solicitudes de modificación del certificado

153. No se estipula la modificación.

4.8.4 Notificación de la modificación del certificado

154. No se estipula la modificación.

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

156. No se estipula la modificación.

4.8.5 Publicación del certificado modificado

157. No se estipula la modificación.

4.8.6 Notificación de la modificación del certificado a otras entidades

158. No se estipula la modificación.

4.9 Revocación

4.9.1 Circunstancias para la revocación

159. 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 de sello electrónico de persona jurídica o de un SSL.
- 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, las gestiones 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 expedición del certificado debido a una falta de adecuación al procedimiento establecido o a problemas técnicos durante el proceso de expedición 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 expedición 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 expedición del 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

160. 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

161. El solicitante de la revocación tramitará ante Izenpe la solicitud de revocación.

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



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

- Presencialmente ante,
 - Izenpe solicitando cita previa a través de www.izenpe.eus.
 - O ante la organización suscriptora con la que Izenpe haya suscrito el instrumento legal pertinente.
- Online, Acceso aplicación de revocación on line disponible <https://servicios.izenpe.com/gestionCertificados/>
- Por correo electrónico, enviando el formulario de solicitud de revocación firmado con un certificado cualificado expedido por una CA incluida en la EU TSL (Trusted Service List) a la dirección izenpe@izenpe.eus.

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

4.9.4 Periodo de gracia de la solicitud de revocación

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

4.9.5 Tiempo de plazo de la CA para procesar la revocación

166. Izenpe revocará el certificado dentro de las 24 horas siguientes a la recepción de la solicitud de un día laborable e informará por correo electrónico a la persona solicitante y a la persona suscriptora del cambio de estado del certificado.

167. 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.

4.9.6 Obligación de verificación de las revocaciones por terceros de confianza

168. 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.

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

4.9.7 Frecuencia de generación de CRLs

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

171. En la CRL se indica 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 CRL se regenera diariamente.

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

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



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

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

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

176. El tiempo de publicación es inmediato pero el servidor que las expone puede cachearlas por un período de 1 hora.

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

178. 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.

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

4.9.9 Requisitos de comprobación de revocación online

180. 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.

181. 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.

182. 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

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

4.9.11 Requisitos especiales clave comprometida

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

185. La comunicación a Izenpe sobre el compromiso de una clave privada a través de la cuenta de correo incidencias@izenpe.eus indicada en el apartado 1.5.2, debe incluir en todo caso una prueba de dicho compromiso e indicar en el asunto del correo electrónico:



“Compromiso de claves”. Para demostrarlo, las partes pueden utilizar los siguientes métodos:

- Envío de la clave privada comprometida o una respuesta de desafío firmada por la clave privada y verificable por la clave pública, así como la propia clave pública.
- Proporcionar referencias a vulnerabilidades y / o fuentes de incidentes de seguridad a partir de las cuales el compromiso de la clave sea verificable.

186. Izenpe podrá aceptar otro tipo de evidencias que demuestren adecuadamente el compromiso de claves.

187. 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.

4.9.12 Circunstancias para la suspensión

188. Izenpe no permite la suspensión en ninguno de sus certificados.

4.9.13 Quién puede solicitar la suspensión

189. Izenpe no permite la suspensión en ninguno de sus certificados.

4.9.14 Procedimiento para la petición de la suspensión

190. Izenpe no permite la suspensión de sus certificados.

4.9.15 Límites sobre el periodo de suspensión

191. Izenpe no permite la suspensión de sus certificados.

4.10 Servicios de estado de los certificados

4.10.1 Características operativas

192. Izenpe ofrece de manera gratuita 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

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

4.10.3 Características opcionales

194. No estipuladas.

4.11 Finalización de la suscripción

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



196. Los certificados cualificados pueden tener una vigencia máxima 5 años de acuerdo con la Ley³ Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

197. Los certificados de autenticación web tienen una vigencia de acuerdo con la normativa Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates⁴.

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de custodia y recuperación de claves

198. Izenpe no recuperará las claves privadas de los titulares de los certificados.

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

199. No estipulado.

³ Artículo 4.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

⁴ En la web <https://cabforum.org>



5 Controles de seguridad física, de procedimiento y de personal

5.1 Controles de seguridad física

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

5.1.1 Localización y construcción de las instalaciones

201. 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

5.1.2.1 Centro de Proceso de Datos

202. 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.

203. Se mantiene de forma segura un fichero log de los accesos. Las puertas de entrada a Izenpe están dotadas de mecanismos de acceso. Un circuito cerrado de televisión que monitoriza los elementos con los que Izenpe presta el servicio de certificación.

5.1.2.2 Autoridades de Registro (RAs)

204. 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

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

206. 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

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

5.1.5 Prevención y protección de incendios

208. 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

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

5.1.7 Tratamiento de residuos

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

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

5.1.8 Copia de respaldo fuera de las instalaciones

212. 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 Roles de confianza

213. 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.

214. 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.

215. 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

216. 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.

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

5.2.3 Identificación y autenticación para cada rol

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

219. 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

220. Izenpe sigue la política de seguridad CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures) y está definida en su modelo de seguridad.

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autenticación

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

222. 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

223. Izenpe dentro de sus procedimientos de Personal 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

224. 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 DPCG.
- 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
- Concienciación sobre privacidad y protección de datos.



225. 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

226. 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

227. 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

5.3.6.1 Incidentes de seguridad de la información

228. Izenpe dispone de un Plan de gestión de incidentes de seguridad.

5.3.6.2 Proceso punitivo

229. Existe un régimen disciplinario interno que define el proceso punitivo.

5.3.7 Requisitos de contratación de personal

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

5.3.8 Suministro de documentación al personal

231. Todo el personal relacionado con roles fiables recibe:

- Una copia de la DPCG.
- 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

232. 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

233. 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.

234. Modificaciones en Cas.

- Caducidad de certificados.

235. 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.

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

5.4.2 Frecuencia de procesamiento de logs

237. Los logs son procesados continuamente y auditados con una periodicidad trimestral 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.
- Listado usuarios administradores.
- Listado de software instalado en las máquinas Windows.

5.4.3 Periodo de retención del audit log

238. 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 15 años.

5.4.4 Protección del audit log

239. 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.

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

5.4.5 Procedimiento de backup del audit log

241. 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

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

243. Notificación de la acción causante de los logs.

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

5.4.7 Análisis de vulnerabilidades

245. 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

246. 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

247. Toda la información y documentación relativa a servicios cualificados se conserva durante 15 años a partir de la fecha de extinción del certificado o la finalización del servicio prestado y la relativa a certificados y servicios no cualificados durante 7 años (a partir de la fecha de extinción del certificado o de la finalización del servicio prestado).

5.5.3 Protección del archivo

248. 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

249. Existe una “Política de copias de seguridad” y un “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

250. 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 (ver Fuente de tiempo).

5.5.6 Sistema de archivo

251. 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

252. 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 DPCG.

5.6 Cambio de claves de la CA

253. 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 Gestión de incidentes y Plan de contingencias

5.7.1 Procedimientos de gestión de incidentes

254. 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, con el objetivo de que el tiempo de indisponibilidad sea el menor posible

255. 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.

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

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

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

259. 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

260. 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 de la CA

261. 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.

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

263. Esta contingencia está contemplada en el “Plan de contingencias y de continuidad de negocio de Izenpe”, y determina, entre otras, las siguientes acciones a tomar:

- Detener la prestación del servicio afectado.
- Revocar los certificados que pudieran verse afectados.
- Notificar a suscriptores, usuarios y terceras partes. De la misma manera, se incluirá la notificación a TSPs con convenios de confianza, fabricantes de navegadores y en general cualquier entidad con la que Izenpe mantenga alguna relación contractual de uso del servicio.
- Estudiar la necesidad de ejecutar el “Plan de Cese de Actividades del TSP” según la DPCG y legislación vigente.

5.7.4 Continuidad de negocio después de un desastre

264. 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.

265. 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

266. Izenpe dispone de un “Plan de cese” que detalla el procedimiento que se ejecutaría ante esta circunstancia.
267. 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. En esta comunicación se indicará que en el plazo de 2 meses se revocarán todos los certificados vigentes.
268. En caso de finalización de una CA por expiración o por revocación, se seguirá dando respuesta a las consultas de estado del certificado a través del servicio OCSP. Una vez finalizada la CA, las respuestas OCSP sobre los certificados emitidos por esa CA estarán firmadas por otra CA vigente de Izenpe. La CRLs de Izenpe no incluyen certificados caducados, según se indica en el apartado 4.9.7 Frecuencia de generación de CRLs esta DPCG.
269. En caso de cese de Izenpe, la información de revocación de los certificados se dará a través de una last CRL, con un nextUpdate de “99991231235959Z”, según especificaciones del apartado 6.3.9 de ETSI EN 319 411-1.
270. Se notificará a TSPs, fabricantes de navegadores y cualquier entidad con la que IZENPE mantenga alguna relación contractual de uso de sus certificados.
271. Izenpe mantendrá durante el tiempo necesario según especificaciones de la presente DPCG 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.
272. 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.
273. Izenpe comunicará al Organismo de supervisión el cese de su actividad, incluyendo la información relativa a los certificados cuya vigencia vaya a ser extinguida. Esta comunicación se realizará a través de la plataforma de envío de notificaciones de la sede electrónica del Ministerio competente en el ámbito de la prestación de servicios de confianza, con una antelación mínima de 3 meses previo al cese de su actividad.
274. Se dará por finalizada cualquier prestación de terceros con los que Izenpe mantenga un contrato de prestación de servicios (identificación, emisión, albergue, etc.).
275. 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 (hasta la fecha de caducidad de la CA subordinada que emitió el certificado).

5.8.2 Entidad de Registro

276. 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

277. 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.

278. 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).

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

280. 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 de certificados cualificados en los que Izenpe genera las claves, éstas serán generadas en tarjeta o hardware criptográfico.

281. En los casos de estos certificados cualificados en los es el usuario final es el que genera las claves, éstas podrán ser generadas en los siguientes dispositivos:

282. Contenedor de claves de cliente (ej: servidor web).

283. Contenedor seguro de Izenpe.

- Contenedor de la app de Izenpe para teléfono móvil.

6.1.2 Distribución de la clave privada al suscriptor

284. El método de entrega de la clave privada varía en función de tipo de certificado y dispositivo.. Consultar la PDS y o DPCP.

6.1.3 Distribución de la clave pública al emisor del certificado

285. La clave pública, generada junto a la Clave privada en un dispositivo de generación y custodia de claves, es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación.

286. 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.



6.1.4 Distribución de la clave pública de la entidad de certificación a los usuarios de certificados

287. Las claves públicas de las CA de Izenpe se distribuyen a través de varios medios, entre ellos la web de Izenpe. En la presente DPCG, 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

288. El tamaño de las claves dependiendo de los casos es:

289. Jerarquía 2007, 2020.

- Al menos 3072 bits para claves de personas físicas, jurídicas y de dispositivo, servidor OCSP, y certificados técnicos.
- Al menos 3072bits para aquellas CAs emitidas a partir de 2007.

290. El tamaño de claves del servidor de TSU se emite con 4096.

291. Jerarquía 2024.

292. ECC 256 o 384 bits.

293. Jerarquía 2025: ECC 256 o 384 bits.

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

294. El identificador de algoritmo (AlgorithmIdentifier) que emplea Izenpe para firmar los certificados en la jerarquía de 2007 y 2020 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)". En la jerarquía del 2024 y 2025 utiliza ECC256 o 384.

295. 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.

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

297. 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 el "Plan de contingencia y de continuidad de negocio de Izenpe" y 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) 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.509 v3)

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

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

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

6.2 Protección de la clave privada

6.2.1 Estándares de módulos criptográficos

301. 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.

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

303. En cuanto a los dispositivos criptográficos con certificados para firma electrónica cualificada, aptos 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.

304. En el caso de que dichos dispositivos perdieran la certificación de dispositivo seguro y esto supusiera la pérdida de la condición de firma cualificada, Izenpe procederá a la revocación del certificado; siempre según lo determinado por el órgano supervisor y/o normativa vigente.

305. 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.

306. 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

307. 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

308. 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.

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

310. 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

311. 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.

312. 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 los casos definidos en los procedimientos correspondientes.

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

6.2.5 Archivado de la clave privada

314. Izenpe podrá efectuar una copia de seguridad de las Claves Privadas, garantizando que el grado de seguridad de los datos duplicados es del mismo nivel que el de los datos originales y que el número de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio. No se duplican los datos de creación de firma para ninguna otra finalidad.

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

315. La clave privada de la CA raíz, CAs subordinadas, VA y TSA son generadas en un HSM según lo especificado en el punto 5.2.1, y no es posible la exportación. Como medida de contingencia es posible la recuperación de las claves privadas según apartado 5.2.4.

316. En el siguiente dispositivo utilizado 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.

317. 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

318. 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.

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

320. 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.

321. 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

322. Las claves privadas de las Autoridades de Certificación son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS140-2 Level 3.

323. Los mecanismos de activación y uso de las claves privadas de los certificados de entidad final se describen en la PDS y/o en DPCP, en su caso.

6.2.9 Método de desactivación de la clave privada

324. 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”.

325. En cuanto a la desactivación de las claves privadas de los certificados de entidad final se describe en la correspondiente PDS.

6.2.10 Método de destrucción de la clave privada

326. Existe un procedimiento de destrucción de claves de la CA.

327. En el caso de retirar el HSM que alberga las claves de la CA, se seguirá el procedimiento establecido al efecto.

328. Este procedimiento no se aplica a las claves de firma o autenticación de usuario emitidas en tarjeta criptográfica, contenedor seguro 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

329. Según indicado en el apartado 5.2.1 del presente documento.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

330. 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

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

- El certificado de la CA raíz de 2007 es válido durante 30 años.
- El certificado de la CA raíz de 2020 es válido durante 25 años
- El certificado de la CA raíz de 2024 es válido durante 25 años.
- El certificado de la CA raíz de 2025 es válido durante 25 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. Los certificados cualificados de persona física o sello electrónico su duración máxima es de cinco (5) años. Los certificados de autenticación web tienen una duración máxima de 365 días. En todos los certificados de persona física y de sello de persona jurídica la renovación implica regeneración de claves.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

332. 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.

333. En cuanto a los datos de activación de las claves de los certificados de entidad final, se describen, en su caso, en la DPS o en la DPCP.

6.4.2 Protección de datos de activación

334. 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.

335. 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.

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

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

6.4.3 Otros aspectos de los datos de activación

338. Ver las existentes así como los textos de divulgación (PDS).

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

339. 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, serviciosInternet de Izenpe, operación CA y gestión de red):

340. 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.

341. 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.

342. El servicio de publicación de revocaciones posee las funcionalidades necesarias para que se garantice un funcionamiento 24x7.

343. 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.

344. 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

345. 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

346. 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

347. 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

348. 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

349. 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

350. Izenpe obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada siguiendo el protocolo NTP. La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905.

351. 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

352. Los certificados emitidos por Izenpe son conformes a las siguientes normas:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) Mayo 2008.
- 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 EN 319 412.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile.

7.1.1 Número de versión

353. Los certificados emitidos bajo la presente DPCG utilizan el estándar X.509 versión 3 (populate version field with integer "2").

7.1.2 Extensiones de certificado

354. Indicadas en el documento de perfiles, disponible en www.izenpe.eus.

7.1.3 Identificadores de objeto de algoritmos

355. RSA.

356. Izenpe debe indicar que usa una clave RSA mediante el identificador de algoritmo rsaEncryption (OID: 1.2.840.113549.1.1.1). Los parámetros deben estar presentes y ser NULL explícitos.

357. Izenpe no debe utilizar un algoritmo diferente, como el identificador de algoritmo id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10), para indicar la presencia de una clave RSA.

358. Una vez codificado, el identificador de algoritmo para claves RSA DEBE ser idéntico byte a byte a los siguientes bytes codificados en hexadecimal: 300d06092a864886f70d0101010500 ECDSA.

359. La CA debe indicar que usa una clave ECDSA mediante el identificador del algoritmo id-ecPublicKey (OID: 1.2.840.10045.2.1). Los parámetros DEBEN usar la codificación namedCurve.

- Para claves P-256, namedCurve DEBE ser secp256r1 (OID: 1.2.840.10045.3.1.7).
- Para claves P-384, namedCurve DEBE ser secp384r1 (OID: 1.3.132.0.34).
- Para claves P-521, namedCurve DEBE ser secp521r1 (OID: 1.3.132.0.35). Una vez codificado, el identificador de algoritmo para las claves ECDSA DEBE ser idéntico byte a byte a los siguientes bytes hexadecimales.
- Para claves P-256: 301306072a8648ce3d020106082a8648ce3d030107.
- Para claves P-384: 301006072a8648ce3d020106052b81040022.



- Para claves P-521: 301006072a8648ce3d020106052b81040023.

7.1.4 Formatos de nombres

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

7.1.5 Restricciones de nombres

361. 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

362. De acuerdo a lo especificado en la sección 1.2 de la presente DPCG.

7.1.7 Empleo de la extensión restricciones de política

363. No se emplean restricciones de política.

7.1.8 Sintaxis y semántica de los calificadores de política

364. La extensión Certificate Policies contiene los siguientes calificadores de política:

- CPS Pointer: contiene un puntero a la DPCG de Izenpe www.izenpe.eus
- 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.

365. User Notice común a todos los certificados (excepto certificados SSL⁵):

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

7.1.9 Tratamiento semántico para la extensión “certificate policy”

366. 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

367. Los certificados emitidos por Izenpe son conformes a las siguientes normas:

⁵ El campo UserNotice está prohibido en certificados SSL desde la versión 2.0.0 de las BRG de Cabforum.



- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) Mayo 2008.
- 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.

368. 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

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

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

370. 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. Invalidity Date	Sí	No

7.3 Perfil OCSP

371. 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

372. 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

373. Izenpe define con carácter anual un plan de gestión de seguridad y privacidad de la información que facilita la verificación de la conformidad con los requisitos de seguridad establecidos. ,

8.1 Frecuencia de auditoría

374. 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

375. El auditor tiene cualificación y experiencia probadas en la ejecución de auditorías de Prestadores de Servicios de Confianza Debe estar acreditado según ETSI EN 319 403.

8.3 Relación del auditor con la empresa auditada

376. 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

377. Los elementos objeto de auditoría son los siguientes:

- Servicios de confianza..
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación relacionada.

8.5 Toma de decisiones como resultado de deficiencias

378. 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 en plazo mediante una herramienta de apoyo. Comunicación de los resultados.

379. Los informes de auditoría se entregan al Comité de Seguridad, para su análisis.



9 Otros asuntos legales y de actividad

9.1 Tarifas

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

381. Opciones de pago ofrecidas,

- Solicitud de emisión firmada electrónicamente: pago online a través de pasarela de pago.
- Carta de pago para presentar ante la entidad bancaria.
- Pago presencial ante la Entidad de Registro de Izenpe a través de tarjeta bancaria.

382. En el caso de entidades que pertenezcan al Sector Público vasco, se aplicaran los criterios definidos en el correspondiente marco regulador.

9.1.1 Tarifas de emisión o renovación de certificados

383. Las tarifas que los usuarios deben abonar en contraprestación de la emisión o renovación de certificados están recogidas en la web <https://www.izenpe.eus>

9.1.2 Tarifas de acceso a los certificados

384. No estipulado.

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

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

9.1.4 Tarifas para otros servicios

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

9.1.5 Política de reintegro

387. Izenpe no dispone de una política de reintegro.

9.2 Responsabilidad financiera

388. Izenpe, las Entidades de Registro y las entidades usuarias disponen de suficientes recursos para mantener sus operaciones y realizar sus tareas.

9.2.1 Seguro de responsabilidad civil

389. Izenpe dispone de un seguro de responsabilidad civil que cubre los riesgos de error y/u omisión derivados de su actividad con un límite de indemnización de 5.000.000 € por reclamación y periodo de seguro

9.2.2 Otros activos

390. No estipuladas.

9.2.3 Seguros y garantías para entidades finales

391. No estipuladas.



392. Confidencialidad de la información .

9.2.4 Alcance de la información confidencial

393. Para la prestación del servicio, Izenpe precisa 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.

394. Izenpe recabn los datos exclusivamente necesarios para la expedición y el mantenimiento de los certificados y la prestación de otros servicios de certificación, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

395. Izenpe desarrolla su actividad de acuerdo a lo establecido en el RGPD y en su normativo de desarrollo.

396. Izenpe divulga ni ceden datos de carácter personal, excepto en aquellos supuestos previstos en esta DPCG

397. 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,
- 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 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.

9.2.5 Información que no está dentro del alcance

398. 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.
- 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 esta DPCG.

9.2.6 Responsabilidad para proteger la información confidencial

399. Izenpe divulgará la información confidencial únicamente en los supuestos legalmente previstos para ello.

400. 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

401. Los certificados serán objeto de publicación de acuerdo con lo establecido en el Reglamento eIDAS y en la LSEC.

9.3 Protección de datos de carácter personal

402. Izenpe publica información referente a privacidad y protección de datos en el sitio web: www.izenpe.eus/datos.

9.3.1 Plan de privacidad

403. El tratamiento de datos de carácter personal que realiza Izenpe se alinea con lo dispuesto en el RGPD y en la LOPDGDG, así como en la normativa de desarrollo.

9.3.2 Información tratada como privada

404. Izenpe considera como privada toda la información personal sobre las personas físicas usuarias de los servicios de confianza

9.3.3 Información no considerada privada

405. No se considera información privada aquella que se incorpora a los certificados electrónicos, la información relativa al estado de vigencia de los mismos, la fecha de inicio de dicho estado (activo, revocado, caducado...), así como el motivo que provocó el cambio de estado. Por tanto, los certificados electrónicos, las Listas de Certificados Revocados y cualquier contenido de los mismos no es considerada información privada.

9.3.4 Responsabilidad de proteger la información privada

406. Izenpe adopta las medidas de seguridad requeridas de conformidad con el RGPD en cuanto al acceso y tratamiento que realiza sobre los datos personales de solicitantes y suscriptores de los certificados.

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

9.3.4.1 Persona delegada de protección de datos

408. Los datos de contacto de la DPD de Izenpe están publicados en www.izenp.eus/datos. Dichos datos de contacto incluyen la dirección de correo electrónico a la que los



interesados pueden dirigir todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos, de conformidad con el artículo 38.4 del RGPD

9.3.4.2 Registro de actividades de tratamiento

409. Izenpe cuenta con un registro de las actividades de tratamiento que realiza bajo su responsabilidad, entre los que se encuentra el de “Gestión de medios de identificación” relativo a la actividad que realiza esta Entidad como prestador de servicios de confianza. Dicho registro incluye, para cada tratamiento identificado, la siguiente información:

- Finalidad
- Entidad responsable
- Categorías de datos personales
- Quién proporciona los datos
- Quién es el afectado de los datos personales
- Quiénes son los encargados del tratamiento
- Comunicaciones de datos
- Transferencias internacionales de datos
- Plazo de supresión
- Medidas de seguridad

410. El documento de Registro de actividades de tratamiento puede consultarse en www.izenpe.eus/datos.

9.3.4.3 Derechos de los interesados

411. Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del RGPD, a través de:

- Medio postal: acompañando la solicitud con una copia del DNI/NIE.
- De manera electrónica firmando la solicitud mediante certificado cualificado de persona física.

9.3.4.4 Cooperación con las autoridades

412. Izenpe cooperará con las autoridades de protección de datos cuando sea requerida.

9.3.4.5 Notificaciones de violaciones de seguridad

413. Izenpe notificará a la Autoridad Vasca de protección de Datos (en adelante, AVPD) cualquier violación de seguridad en materia de datos personales, sin dilación posible y, en todo caso, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella, siempre que esta sea susceptible de constituir un riesgo para los derechos las libertades de las personas físicas afectadas.

414. En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la AVPD se complementará con una notificación dirigida a estos últimos, al objeto de permitirles la adopción de medidas para protegerse de sus consecuencias.



9.3.5 Aviso y consentimiento para usar información privada

415. La obtención de información privada de las personas físicas en los procesos ligados al ciclo de vida de los certificados (solicitud, acreditación de la identidad, renovación, revocación...) se realizará, mediante una manifestación del interesado o mediante una clara acción afirmativa.

9.3.6 Divulgación conforme al proceso judicial o administrativo

416. Izenpe no divulgará datos personales, salvo petición por parte de las autoridades administrativas o judiciales.

9.3.7 Otras circunstancias de divulgación de información

417. No estipuladas.

9.4 Derechos de propiedad intelectual

9.4.1 Propiedad de los certificados

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

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

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

9.4.2 Propiedad de la DPCG

421. Izenpe es la propietaria de la presente DPCG.

9.4.3 Propiedad de la información relativa a nombres

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

423. El suscriptor y, en su caso, el firmante, es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3 de la DPCG.

9.4.4 Propiedad de claves y material relacionado

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

9.5 Obligaciones y garantías

425. Izenpe como entidad de certificación que expide certificados de acuerdo con la presente DPCG asume las siguientes obligaciones:

9.5.1 Obligaciones de la CA

9.5.1.1 Obligaciones de prestación del servicio

426. Izenpe presta sus servicios de certificación conforme con la presente DPCG, 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.

427. Estas obligaciones 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 extinción, 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).

9.5.1.2 Obligaciones de operación fiable

428. 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 DPCG. El servicio está disponible 24 horas x 7 días a la semana.
- El cumplimiento de los requisitos técnicos y de personal exigidos por la legislación vigente en materia de firma electrónica:
 - Demostrar la fiabilidad necesaria para prestar servicios de certificación.
 - Garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado o se extinguió su vigencia.
 - 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.



- 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.
 - 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.
 - 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:
- Realizar de forma periódica comprobaciones regulares de la seguridad, con el fin verificar la conformidad con los estándares establecidos.
 - Llevar a cabo una completa gestión de los sucesos de seguridad, con el fin de garantizar su detección, resolución y optimización.
 - Mantener los contactos y relaciones apropiadas con grupos de especial interés en materia de seguridad, como especialistas, foros de seguridad y asociaciones profesionales relacionadas con la seguridad de la información.
 - Planificar adecuadamente el mantenimiento y evolución de los sistemas, con el fin de garantizar en todo momento un rendimiento adecuado y un servicio que cumpla con todas las garantías las expectativas de los usuarios y clientes.

9.5.1.3 Obligaciones de identificación

429. 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 DPCG.

9.5.1.4 Obligaciones de información a usuarios

430. Antes de la emisión y entrega del certificado al suscriptor, Izenpe le informa mediante referencia al documento 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 de la presente DPCG.

431. Izenpe informará al firmante 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.

432. 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.

433. Izenpe dispone de un plan de finalización del cese de su actividad en el que se especifican las condiciones en las que se realizaría.

9.5.1.5 Obligaciones relativas a los programas de verificación

434. Izenpe ofrece mecanismos de verificación de la validez de los certificados de acceso público, mediante los sistemas descritos en la presente DPCG.

9.5.1.6 Obligaciones relativas a la regulación jurídica del servicio de certificación

435. 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.

436. El instrumento jurídico que vincula a Izenpe y al solicitante, suscriptor o firmante 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 los apartados de la sección 2 de la presente DPCG.
- Indicación de la DPCG 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 expedición, 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 comunicación 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 1.4.
- 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.
- Legislación aplicable y jurisdicción competente.
- Forma en la que se garantiza la responsabilidad patrimonial de Izenpe.



9.5.2 Obligaciones de la entidad de registro

437. 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 firmante que consten en los certificados o sean relevantes para el fin de los certificados.
- Conservar toda la información y documentación relativa a los certificados, cuya expedición, 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.

9.5.3 Obligaciones de los titulares

438. 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 las correspondientes PDS

439. El suscriptor está obligado a:

- Facilitar a Izenpe información completa y adecuada, conforme a los requerimientos de la DPCG 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.
- Manifiestar su conformidad 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 DPCG.
- 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 firmante 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 Izenpe.
- 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.

440. El suscriptor de certificados cualificados que genere firmas electrónicas 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.

9.5.4 Obligaciones de las partes que confían

441. 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 DPCG 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 electrónica 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.

9.5.5 Obligaciones de otros participantes

442. Izenpe en la prestación de su servicio como Autoridad de Sellado de Tiempo, se responsabiliza de la variación de la referencia temporal, en relación a la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada, que introduce en los Sellos de tiempo electrónicos en el momento de la solicitud, más no de la veracidad ni de los contenidos representados por los datos electrónicos remitidos por las entidades usuarias del servicio, que son el objeto del Sello de tiempo electrónico emitido.

9.6 Renuncia de garantías

443. No estipulado.

9.7 Limitaciones de responsabilidad

9.7.1 Responsabilidades de la autoridad de certificación

444. Izenpe responderá por negligencia o falta de la debida diligencia en los servicios de certificación descritos en la presente DPCG, 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 Declaración de Prácticas de Certificación contenidas en los certificados, siempre que el contenido de los mismos cumpla sustancialmente con la esta DPCG
- 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 esta DPCG.
- 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 electrónicas, o cualquier otra transacción o servicio ofrecido o contemplado en esta DPCG 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.



445. 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.

446. 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.

9.7.2 Responsabilidades de la autoridad de registro

447. 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.

448. 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

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

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

451. 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 éstas 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.

452. 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

453. Un tercero que confíe en un certificado no válido o una firma electrónica 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.

454. 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.
- Comprobar el identificador del certificado cualificado en la Trusted Service List (TSL).

9.8 Indemnizaciones

455. 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 Entrada en vigor

456. La DPCG entra en vigor en el momento de su publicación.



9.9.2 Terminación

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

9.9.3 Efectos de la finalización

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

9.10 Notificaciones individuales y comunicación con los participantes

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

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

9.11 Modificaciones de este documento

9.11.1 Procedimiento para los cambios

461. 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 DPCG cuyo mantenimiento está garantizado por Izenpe.

462. Las versiones actualizadas de la DPCG junto con la relación de modificaciones realizadas pueden ser consultadas en la dirección www.izenpe.eus.

463. Izenpe podrá modificar, de forma unilateral, la DPCG 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 el Comité de Seguridad 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

464. El Comité de Seguridad de Izenpe revisará anualmente la DPCG 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.

465. 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.



466. 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

467. 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

468. Izenpe 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.

469. 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.

470. 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.

471. Las partes acuerdan resolver cualquier cuestión que surja entre ellas mediante un proceso de Derecho Colaborativo, pudiendo acudir a los Juzgados y Tribunales de la ciudad de Vitoria-Gasteiz, en caso de no llegar a un acuerdo.

9.13 Normativa aplicable

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

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

- 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”
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza..
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

474. Adicionalmente, las prácticas de los servicios de confianza provistos por Izenpe siguen los siguientes estándares:



- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- CABForum Baseline Requirements
- CABForum EV Certificate Guidelines.

9.14 Cumplimiento de la normativa aplicable

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

476. En cualquier caso, Izenpe manifiesta el cumplimiento de las normativas indicadas en el apartado 9.14.

9.15 Estipulaciones diversas

9.15.1 Acuerdo íntegro

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

9.15.2 Asignación

478. Izenpe no será responsable de la falta de servicio o anomalías en el mismo, así como de los daños y perjuicios que pudieran producirse directa o indirectamente, cuando el fallo o desastre tuviera su origen en causas de fuerza mayor, atentado terrorista, sabotajes o huelgas salvajes; todo ello, sin perjuicio de realizar las actuaciones necesarias para la subsanación y/o reanudación del servicio lo antes posible.

9.15.3 Divisibilidad

479. No estipulado.

9.15.4 Cumplimiento

480. No estipulado.

9.15.5 Fuerza Mayor

481. No estipulado.



9.15.6 Otras estipulaciones

482. Izenpe como prestador de servicios de confianza, prestará servicios a todo aquel interesado que lo solicite en las condiciones previstas en esta DPCG, las DP particulares Prácticas y Leyes de Emisión aplicables al objeto de la solicitud.
483. Los servicios de confianza de Izenpe utilizados y combinados adecuadamente permitirán a usuarios, suscriptores y titulares, entre otras, la dotación a los intercambios de información de las medidas de seguridad necesarias para la identificación, autenticación, no repudio y confidencialidad de las partes.
484. Izenpe gestiona sus servicios de certificación y emite certificados SSL de conformidad con la última versión de las BRG de la entidad CA/Browser Forum (que pueden consultarse en la dirección <https://cabforum.org/baseline-requirements-documents/>) y de conformidad con la última versión de los requisitos definidos por la entidad CA/Browser Forum en su “guía para la expedición y gestión de Certificados de Validación Extendida” (que pueden consultarse en la dirección <https://cabforum.org/extended-validation/>), así como en la DPC particular de expedición de certificados de autenticación web de IZENPE.
485. Izenpe revisará sus políticas y prácticas de certificación para mantenerlas acordes a los referidos requisitos. En caso de cualquier inconsistencia entre este documento y la “guía para la expedición y gestión de Certificados de Validación Extendida”, las directrices marcadas en la propia guía prevalecen sobre este documento.
486. Izenpe permite a terceros verificar y probar todos los tipos de certificados que expide. Para ello cuenta con un conjunto de certificados de prueba disponibles en www.izenpe.eus.