

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN **Civitana**

Versión: X.X

Vigente desde:_____

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1.0
Fecha edición:	[X]

Estado formal

Preparado por:	do por:	ado por:
re: [X] [X]	re: [X] [X]	re: [X] [X]

Estado formal

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	[X]	[X]

Índice

Contenido

Información general	2
Control documental	2
Estado formal	2
Estado formal	2
Índice	3
1. INTRODUCCIÓN	4
1.1. Presentación	4
1.2. Nombre del documento e identificación	4
1.2.1. Identificador del documento	4
1.2.2. Identificadores de certificados	4
1.3. Participantes en los servicios de certificación	5
1.3.1. Prestador de servicios de certificación	5
1.3.2. Autoridades de Registro	6
1.3.3. Suscriptores	7
1.3.4. Firmantes	7
1.3.5. Partes que confían	8
1.3.6. Proveedor de herramientas de identificación remota	8
1.4. Uso de los certificados	8
1.4.1. Usos permitidos de los certificados	8
1.4.2. Ámbito de uso de los certificados	10
1.4.3. Límites y prohibiciones de uso de los certificados	10
1.5. Administración de la política	11
1.5.1. Entidad Responsable	11
1.5.2. Datos de contacto	11
1.5.3. Responsables de adecuación de la Declaración de Prácticas de Certificación	11
1.5.4. Procedimientos de gestión del documento	11
1.6. Definiciones y acrónimos	12
1.6.1. Definiciones	12
1.6.2. Acrónimos	15
2. PUBLICACIÓN Y RESPONSABLES DEL REPOSITORIO DE INFORMACIÓN	16

Civitana: Declaración de Prácticas de Certificación

2.1.	Repositorio de información	16
2.2.	Publicación de información de certificación	16
2.3.	Política de publicación y notificación	16
2.4.	Frecuencia de publicación	16
2.5.	Control de acceso al repositorio	16
3.	Identificación y autenticación.	18
3.1.	Tipos de nombres	18
3.1.1.	Emisor	18
3.1.2.	Asunto	18
3.1.3.	Significado de los nombres	19
3.1.4.	Emisión de certificados de prueba	19
3.1.5.	Seudónimos	20
3.1.6.	Reglas para la Interpretación de formatos de nombres	20
3.1.7.	Unicidad de los nombres	20
3.1.8.	Resolución de conflictos relativos a nombres y tratamiento de marcas registradas	20
3.2.	Validación de la identidad	20
3.2.1.	Métodos para probar la posesión de la clave privada	21
3.2.2.	Métodos de validación de la identidad	21
3.2.3.	Validación de la identidad por medios electrónicos	21
3.2.4.	Autenticación de la identidad de la persona física solicitante	23
3.2.5.	Información no verificada del suscriptor	24
3.2.6.	Validación de la autoridad de registro	24
3.3.	Identificación y autenticación para peticiones de renovación	25
3.3.1.	Validación para la renovación rutinaria de certificados	25
3.3.2.	Identificación y autenticación de la solicitud de renovación	25
3.4.	Identificación y autenticación para peticiones de revocación	26
3.5.	Suspensión de certificados	26
4.	REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS	27
4.1.	Solicitud de emisión de certificado	27
4.1.1.	Legitimación para solicitar la emisión	27
4.1.2.	Comprobación de la solicitud	27
4.1.3.	Proceso de inscripción y responsabilidades.	27
4.2.	Procesamiento de las solicitudes	28
4.2.1.	Realización de funciones de identificación y autenticación	28

Civitana: Declaración de Prácticas de Certificación

4.2.2.	Aprobar o rechazar solicitudes	28
4.2.3.	Tiempo en procesar la solicitud	28
4.3.	Emisión del certificado	28
4.3.1.	Acciones de la CA durante la emisión	29
4.3.2.	Notificación al suscriptor de la emisión	29
4.4.	Entrega y Aceptación del certificado	29
4.4.1.	Responsabilidad de la CA	29
4.4.2.	Proceso de aceptación del certificado	30
4.4.3.	Publicación del certificado por la CA	30
4.4.4.	Notificación de la emisión del certificado por la CA a otras entidades	30
4.5.	Uso del par de claves y usos del certificado	31
4.5.1.	Clave privada del suscriptor y uso del certificado	31
4.5.2.	Uso de la clave pública y del certificado por terceros que confían en los certificados	31
4.6.	Renovación del certificado	32
4.6.1.	Circunstancias para la renovación del certificado	32
4.6.2.	Quién puede solicitar la renovación	33
4.6.3.	Tratamiento de peticiones de renovación de certificado	33
4.6.4.	Notificación al suscriptor	33
4.6.5.	Procedimiento de aceptación de un certificado renovado	34
4.6.6.	Publicación del certificado	34
4.6.7.	Notificación a otras entidades	34
4.7.	Renovación con regeneración de las claves del certificado	34
4.8.	Modificación del certificado	34
4.9.	Revocación de certificados	34
4.9.1.	Circunstancias para la revocación	34
4.9.2.	Quién puede solicitar la revocación	36
4.9.3.	Tratamiento de las peticiones de revocación	36
4.9.4.	Periodo de gracia de la solicitud de revocación	36
4.9.5.	Tiempo de plazo de la CA para procesar la revocación	37
4.9.6.	Obligación de verificación de las revocaciones por terceros de confianza	37
4.9.7.	Frecuencia de generación de CRLs	38
4.9.8.	Tiempo transcurrido entre la generación y la publicación de las CRLs	38
4.9.9.	Disponibilidad del sistema de verificación online del estado de los certificados	38
4.9.10.	Obligación de consulta de servicios de comprobación de estado de certificados	39

Civitana: Declaración de Prácticas de Certificación

4.9.11.	Requisitos especiales en caso de compromiso de la clave privada	39
En el supuesto de compromiso de la clave privada de cualquiera de las Autoridades de Certificación de la jerarquía de CIVITANA, se procederá a notificar a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de CIVITANA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.		
4.10.	Finalización de la suscripción	39
4.11.	Custodia y recuperación de claves	39
4.11.1.	4.12.1 Prácticas y políticas de custodia y recuperación de claves	39
4.11.2.	Prácticas y políticas de protección y recuperación de la clave de sesión	39
5.	CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTO Y DEL PERSONAL	40
5.1.	Controles de seguridad física	40
5.1.1.	Localización y construcción de las instalaciones	40
5.1.2.	Acceso físico:	40
5.1.3.	Electricidad y aire acondicionado	40
5.1.4.	Exposición al agua	41
5.1.5.	Prevención y protección de incendios	41
5.1.6.	Almacenamiento de soportes	41
5.1.7.	Tratamiento de residuos	41
5.1.8.	Copia de respaldo fuera de las instalaciones	41
5.2.	Controles de procedimientos	41
5.2.1.	Roles de confianza	41
5.2.2.	Número de personas por tarea	42
5.2.3.	Identificación y autenticación para cada rol	42
5.2.4.	Separación de tareas en los diferentes roles	42
5.3.	5.3 Controles de personal	43
5.3.1.	Requisitos de historial, calificaciones, experiencia y autenticación	43
5.3.2.	Procedimientos de investigación de historial	43
5.3.3.	Requisitos de formación	44
5.3.4.	Requisitos y frecuencia de actualización formativa	44
5.3.5.	Secuencia y frecuencia de rotación laboral	44
5.3.6.	Sanciones para acciones no autorizadas	44
5.3.7.	Requisitos de contratación de personal	45
5.3.8.	Suministro de documentación al personal	45
5.4.	Procedimientos de auditoría de seguridad	45

Civitana: Declaración de Prácticas de Certificación

5.4.1.	Tipo de eventos registrados	45
5.4.2.	Frecuencia de procesamiento de logs	46
5.4.3.	Periodo de retención de registros de auditoría	47
5.4.4.	Protección de los registros de auditoría	47
5.4.5.	Procedimiento de copia de respaldo	47
5.4.6.	Localización del sistema de acumulación de registros de auditoría	47
5.4.7.	Notificación del evento de auditoría al causante del evento	48
5.4.8.	Análisis de vulnerabilidades	48
5.5.	Archivado de registros	48
5.5.1.	Tipo de registros archivados	48
5.5.2.	Periodo de retención del archivo	49
5.5.3.	Protección del archivo	49
5.5.4.	Procedimientos de copias de seguridad del archivo	49
5.5.5.	Requisitos para el sellado de tiempo de los registros	49
5.5.6.	Localización del sistema de archivo	49
5.5.7.	Procedimientos para obtener y verificar la información del archivo	49
5.6.	Cambio de claves de la CA	50
5.7.	Compromiso de claves y recuperación ante desastres	50
5.7.1.	Procedimientos de gestión de incidentes y compromisos de seguridad	50
5.7.2.	Corrupción de recursos, aplicaciones o datos	50
5.7.3.	Compromiso de la clave privada de la entidad	50
5.7.4.	Continuidad del negocio después de un desastre	50
5.7.5.	Notificación de incidentes al Organismo Supervisor Nacional en materia de servicios de confianza	51
5.7.6.	Notificación a la Autoridad Nacional de Protección de Datos	51
5.8.	Terminación de la CA	52
6.	Controles de seguridad técnica	53
6.1.	Generación e instalación del par de claves	53
6.1.1.	Generación del par de claves	53
6.1.2.	Generación del par de claves del firmante	53
6.1.3.	Envío de la clave privada al firmante	54
6.1.4.	Envío de la clave pública al emisor del certificado.	54
6.1.5.	Distribución de la clave pública del prestador de servicios de confianza	54
6.1.6.	Tamaños de claves	54
6.1.7.	Parámetros de generación de la clave pública	54

Civitana: Declaración de Prácticas de Certificación

6.1.8.	Comprobación de calidad de parámetros de clave pública	55
6.1.9.	Propósitos de uso de claves	55
6.2.	Protección de la clave privada	55
6.2.1.	Estándares de módulos criptográficos	55
6.2.2.	Control por más de una persona (m de n) sobre la clave privada	55
6.2.3.	Depósito de la clave privada	55
6.2.4.	Copia de respaldo de la clave privada	56
6.2.5.	Archivado de la clave privada	56
6.2.6.	Introducción de la clave privada en el módulo criptográfico	56
6.2.7.	Método de activación de la clave privada	56
6.2.8.	Método de desactivación de la clave privada	56
6.2.9.	Método de destrucción de la clave privada	56
6.2.10.	Clasificación del módulo criptográfico	57
6.3.	Otros aspectos de gestión del par de claves	57
6.3.1.	Archivo de la clave pública	57
6.3.2.	Periodos de operación del certificado y periodos de uso del par de claves	57
6.4.	Datos de activación	57
6.4.1.	Generación e instalación de datos de activación	57
6.4.2.	Protección de datos de activación	57
6.5.	Controles de seguridad informática	58
6.5.1.	Requisitos técnicos específicos de seguridad informática	58
6.5.2.	Evaluación de nivel de seguridad informática	58
6.6.	Controles técnicos del ciclo de vida	59
6.6.1.	Controles de desarrollo de sistemas	59
6.6.2.	Controles de gestión de la seguridad	59
6.7.	Controles de seguridad de red	61
6.8.	Controles de ingeniería de módulos criptográficos	62
6.9.	Fuente de tiempo	62
6.10.	Cambio de estado de un Dispositivo Seguro de Creación de Firma (QSCD)	62
7.	Perfiles de certificados y listas de certificados revocados	63
7.1.	Perfil de certificado	63
7.1.1.	Número de versión	63
7.1.2.	Extensiones de certificado	63
7.1.3.	Identificadores de objeto de algoritmos	63

Civitana: Declaración de Prácticas de Certificación

7.1.4.	Formatos de nombres	63
7.1.5.	Restricciones de nombres	63
7.1.6.	Identificador de objeto de política de certificado	63
7.1.7.	Empleo de la extensión restricciones de política	64
7.1.8.	Sintaxis y semántica de los calificadores de política	64
7.1.9.	Tratamiento semántico para la extensión "certificate policy"	64
7.2.	Perfil de la lista de revocación de certificados	64
7.3.	Perfil OCSP	64
8.	Auditorías de cumplimiento	65
8.1.	Frecuencia de auditoría	65
8.2.	Cualificación del auditor	65
8.3.	Relación del auditor con la empresa auditada	65
8.4.	Elementos objeto de auditoría	65
8.5.	Toma de decisiones como resultado de una falta de conformidad	66
8.6.	Tratamiento de los informes de auditoría	66
9.	Otros asuntos legales y de actividad	67
9.1.	Tarifas	67
9.1.1.	Tarifas de emisión o renovación de certificados	67
9.1.2.	Tarifas de acceso a los certificados	67
9.1.3.	Tarifas de acceso a la información de estado de los certificados	67
9.1.4.	Tarifas para otros servicios	67
9.1.5.	Política de reintegro	67
9.2.	Responsabilidad financiera	67
9.2.1.	Seguro de responsabilidad civil	67
9.2.2.	Otros activos	67
9.2.3.	Seguros y garantías para entidades finales	68
9.3.	Confidencialidad de la información	68
9.3.1.	Alcance de la información confidencial	68
9.3.2.	Información que no está dentro del alcance	68
9.3.3.	Divulgación de información de suspensión y revocación	69
9.3.4.	Divulgación legal de información	69
9.3.5.	Divulgación de información por petición de su titular	69
9.3.6.	Otras circunstancias de divulgación de información	69
9.4.	Protección de datos de carácter personal	69

Civitana: Declaración de Prácticas de Certificación

9.4.1.	Responsable del tratamiento	70
9.4.2.	Finalidad del tratamiento	70
9.4.3.	Legitimación del tratamiento	70
9.4.4.	Datos tratados y conservación	70
9.4.5.	Transferencia de datos	71
9.4.6.	Derechos de los usuarios	71
9.5.	Derechos de propiedad intelectual	72
9.5.1.	Propiedad de los certificados e información de revocación	72
9.5.2.	Propiedad de la Declaración de Prácticas de Certificación	72
9.5.3.	Propiedad de la información relativa a nombres	72
9.5.4.	Propiedad de claves y material relacionado	72
9.6.	Obligaciones y garantías	73
9.6.1.	Obligaciones de CIVITANA	73
9.6.2.	Garantías ofrecidas a suscriptores y terceros que confían en los certificados	74
9.6.3.	Rechazo de otras garantías	74
9.6.4.	Limitación de responsabilidades	75
9.6.5.	Cláusulas de indemnidad	75
9.6.6.	Caso fortuito y fuerza mayor	75

1. INTRODUCCIÓN

1.1. Presentación

Civitana es una fundación inscrita en el Registro Nacional de Fundaciones, con domicilio en la Calle Lanzada número 33, 28008 de Madrid, España y con número de identificación fiscal G72932239, que tiene como objeto fundacional [x], en lo sucesivo “CIVITANA”. Para ello ha decidido constituirse como Prestador de Servicios de Confianza Cualificado y proveer de una infraestructura de clave pública (PKI).

El presente documento contiene la Declaración de Prácticas de Certificación de CIVITANA para la prestación de servicios de confianza cualificados de expedición de certificados cualificados de firma electrónica.

Los perfiles de certificados electrónicos cualificados que se emiten son los siguientes:

- Certificado electrónico cualificado de persona física en QSCD remoto.
- Certificado electrónico cualificado de persona física en HSM remoto.

1.2. Nombre del documento e identificación

1.2.1. Identificador del documento

Este documento contiene la Declaración de Prácticas de Certificación (DPC) como Prestador de Servicios de Confianza Cualificado y establece los términos y condiciones generales para la prestación de servicios de confianza de CIVITANA. Asimismo, esta DPC cumple las funciones de Política de Certificación (PC) para el servicio de expedición de certificados cualificados de CIVITANA.

OID del documento: 1.3.6.1.4.1.63167.1.0.

1.2.2. Identificadores de certificados

CIVITANA ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Tipo de certificados
1.3.6.1.4.1.63167.1.1.1.1	Certificado cualificado de Persona Física en QSCD remoto
1.3.6.1.4.1.63167.1.1.1.2	Certificado cualificado de Persona Física en HSM remoto

1.3. Participantes en los servicios de certificación

1.3.1. Prestador de servicios de certificación

El **prestador de servicios electrónicos de certificación** es la persona, física o jurídica, que expide y gestiona certificados electrónicos para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

CIVITANA es un prestador de servicios electrónicos de confianza, que actúa de acuerdo con lo dispuesto en el Reglamento (UE) 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, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados cualificados, principalmente EN 319 401, 319 411-1 y EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, CIVITANA ha establecido una jerarquía de Autoridades de Certificación:

1.3.1.1. Civitana Root CA

Se trata de la Autoridad de Certificación raíz de la jerarquía que emite certificados a otras Autoridades de certificación, y cuyo certificado de clave pública ha sido auto firmado.

Datos de identificación:

CN:	Civitana Root CA
Huella digital:	☒
Válido desde:	☒
Válido hasta:	☒
Longitud de clave ECD:	☒

1.3.1.2. Civitana Subordinate CA 01

Se trata de la Autoridad de Certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por Civitana Root CA

Datos de identificación:

CN:	Civitana Subordinate CA 01
Huella digital:	☒
Válido desde:	☒
Válido hasta:	☒

Civitana: Declaración de Prácticas de Certificación

Longitud de clave ECD: ☒

1.3.1.3. Civitana Subordinate CA 02

Se trata de la Autoridad de Certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por Civitana Root CA

Datos de identificación:

CN: Civitana Subordinate CA 02

Huella digital: ☒

Válido desde: ☒

Válido hasta: ☒

Longitud de clave ECD: ☒

1.3.2. Autoridades de Registro

1.3.2.1. Qué es una autoridad de registro

Una Autoridad de Registro puede ser una persona física o jurídica que actúa conforme esta Declaración de Prácticas de Certificación y, en su caso, mediante el oportuno acuerdo que debe suscribir con CIVITANA y que ejerce funciones de gestión de las solicitudes, identificación y registro de los solicitantes del certificado y aquellas otras que puedan disponerse en las concretas Políticas y/o Prácticas de certificación, en atención a los certificados concretos que puedan emitirse conforme las Políticas de Certificación.

La entidad que actúe como Autoridad de Registro de CIVITANA podrá autorizar a una o varias personas como Operadores de la Autoridad de Registro (RAO) para operar con el sistema de emisión de certificados de CIVITANA. Estos Operadores de Registro siempre estarán sometidos al control y a la supervisión de la Autoridad de Registro.

La Autoridad de Registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones. CIVITANA deberá autorizar de manera expresa dicho acuerdo de colaboración y será la responsable de todo el proceso de emisión de los certificados.

1.3.2.2. Funciones de la autoridad de registro

Con carácter general las Autoridades de Registros podrán tener entre sus atribuciones:

- Tramitar las solicitudes de certificados
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado.

Civitana: Declaración de Prácticas de Certificación

- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

1.3.3. Suscriptores

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a CIVITANA (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas físicas que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de confianza es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados.

1.3.4. Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica avanzada o cualificada.

Los firmantes se encuentran debidamente autorizados por el suscriptor, según corresponda, y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el prestador de servicios electrónicos de confianza, por lo que las personas físicas identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de “persona física identificada en el certificado”, siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.5. Partes que confían

Las partes que confían son aquellas personas físicas o jurídicas, diferentes del Firmante / Suscriptor, que reciben y / o usan Certificados expedidos por CIVITANA y, como tales, les son aplicables la Presente Declaración de Prácticas de Certificación, cuando deciden confiar efectivamente en los certificados.

Civitana: Declaración de Prácticas de Certificación

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación.

1.3.6. Proveedor de herramientas de identificación remota

CIVITANA ha suscrito un contrato de prestación de servicios con Signicat, S.L.U., donde este último provee una solución para la identificación remota de suscriptores y firmantes conforme lo establecido en las Órdenes Ministeriales ETD/465/2021 y ETD/743/2022.

La herramienta de identificación remota de Signicat, S.L.U., se encuentra incluida dentro del Catálogo de Productos del Centro Criptológico Nacional (CCN) en la Guía de Seguridad de las TIC CCN-STIC 105 cumpliendo con el Esquema Nacional de Seguridad (ENS).

En este marco, Signicat se obliga a proporcionar una plataforma de video identificación que permita la verificación de identidad de los solicitantes de certificados, incluyendo validación documental, comprobaciones biométricas y, en su caso, intervención como Operadores de la Autoridad de Registro.

Asimismo, Signicat garantiza la disponibilidad, mantenimiento y soporte del servicio conforme a los niveles de servicio acordados, así como la aplicación de medidas de seguridad adecuadas para la protección de la información y la conservación de las evidencias generadas durante los procesos de identificación.

Igualmente, el proveedor se compromete a cumplir con la normativa aplicable y a asegurar la correcta integración e interoperabilidad de sus servicios con los sistemas de CIVITANA.

1.4. Uso de los certificados

1.4.1. Usos permitidos de los certificados

A continuación se detallan los usos permitidos de los certificados electrónicos expedidos por CIVITANA. Se deben tener en cuenta los usos permitidos identificados en los campos que conforman los perfiles de certificados y que se definen en el presente documento. Asimismo, se establecen limitaciones y prohibiciones a ciertas aplicaciones de los certificados electrónicos de CIVITANA.

1.4.1.1. Certificado cualificado de Persona Física en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.63167.1.1.1.1. Es un certificado electrónico cualificado que se emite para la firma electrónica cualificada y autenticación, de acuerdo con la política de certificación QCP-N-QSCD con el OID 0.4.0.194112.1.2. Este certificado se emite en un Dispositivo Cualificado de Creación de Firma (QSCD), es un certificado cualificado de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014 eIDAS.

Funciona con dispositivos cualificados de creación de firma (QSCD), de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de confianza, y permite la generación de la “firma electrónica cualificada”, es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo

Civitana: Declaración de Prácticas de Certificación

cualificado, por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a) Firma digital (Digital Signature, para realizar la función de autenticación)
- b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c) Key Encipherment

1.4.1.2. Certificado cualificado de Persona Física en HSM centralizado

Este certificado dispone del OID 1.3.6.1.4.1.63167.1.1.1.2. Es un certificado electrónico cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-N- con el OID 0.4.0.194112.1.0. Este certificado es considerado cualificado de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014 eIDAS.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de confianza, y permite la generación de la “firma electrónica avanzada”, basada en un certificado cualificado.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a) Firma digital (Digital Signature, para realizar la función de autenticación)
- b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c) Key Encipherment

1.4.2. Ámbito de uso de los certificados

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

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

Civitana: Declaración de Prácticas de Certificación

Consultar las especificidades en cuanto al ámbito de uso de cada certificado en la Prácticas y/o Políticas de Certificación aplicables a cada certificado.

- Los certificados emitidos por CIVITANA 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 poseedores de claves podrán utilizar estos certificados para otros usos siempre que se respeten los límites de uso señalados en el apartado anterior.

Consultar las especificidades en cuanto al ámbito de uso de cada certificado en la Prácticas y/o Políticas de Certificación aplicables a cada certificado.

1.4.3. Límites y prohibiciones de uso de los certificados

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

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la legislación aplicable.

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

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de CIVITANA.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las Autoridades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a CIVITANA, en función de la legislación vigente, de responsabilidades que provengan del uso indebido de los certificados ya sea realizado el uso por el firmante o por tercero.

CIVITANA no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, y por ello no es posible emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las Autoridades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5. Administración de la política

1.5.1. Entidad Responsable

Fundación Civitana

NIF: G72932239

Dirección: Calle Lanzada número 33, 28008 de Madrid, España

1.5.2. Datos de contacto

Dirección:

Mail:

Teléfono:

Para informar problemas de seguridad relacionados con un certificado, tales como sospecha de compromiso clave, uso indebido o fraude, envíenos un informe de incidencia sobre certificado a la cuenta de correo electrónico: _____

1.5.3. Responsables de adecuación de la Declaración de Prácticas de Certificación

El Comité de Seguridad de CIVITANA es el órgano responsable de la aprobación de la presente Declaración de Prácticas de Certificación, así como de las modificaciones que se produzcan sobre la misma.

1.5.4. Procedimientos de gestión del documento

El sistema documental y de organización de CIVITANA garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones del servicio relacionado con el mismo.

En el caso de modificación y/o actualización de la DPC, cuando dichas modificaciones no supongan cambios significativos, de tal manera que no puedan verse afectados los derechos y obligaciones de SUSCRITORES y/o FIRMANTES de los certificados, CIVITANA no procederá a informar respecto de los cambios, limitándose a publicar la nueva versión del documento correspondiente en su página web inmediatamente tras la aprobación.

Si las modificaciones producen cambios relevantes que puedan afectar a los derechos y obligaciones de SUSCRITORES y/o FIRMANTES de los certificados, CIVITANA procederá a comunicar mediante un medio que resulte idóneo para cada caso en concreto, indicando los cambios propuestos y, en su caso, para recoger las opiniones de las partes afectadas.

No obstante lo anterior, cualquier tipo de cambio, se reflejará en el apartado de control de versiones del documento y se dará el trámite correspondiente de notificación y publicidad especificado en la propia DPC.

1.6. Definiciones y acrónimos

1.6.1. Definiciones

- **Agencia de Española de Protección de Datos (APD):** es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena

Civitana: Declaración de Prácticas de Certificación

independencia de las Administraciones Públicas en el ejercicio de sus funciones y cuya principal finalidad es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.

- **Autoridad de Certificación (CA):** Sistema de confianza, gestionado por un Prestador de Servicios de Confianza, responsable de emitir y revocar los Certificados, utilizados en la Firma electrónica.
- **Autoridad de Registro (RA):** la autoridad de registro es la entidad encargada de realizar las tareas de identificación de los solicitantes, suscriptores y poseedores de claves de los certificados, comprobar la documentación acreditativa de las circunstancias que constan en los certificados, así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los certificados. El usuario se debe dirigir a la autoridad de registro para solicitar un certificado con la garantía de la autoridad certificadora asociada a la autoridad de registro.
- **Autoridad de Sellado de Tiempo (TSA):** autoridad que emite sellos de tiempo
- **Certificado:** es un documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- **Certificado Raíz:** certificado cuyo suscriptor es una Autoridad de Certificación perteneciente a la jerarquía de CIVITANA, y que contiene los Datos de Verificación de firma de dicha Autoridad firmado con los datos de creación de Firma de la misma como Prestador de Servicios de Certificación. Las entidades emisoras de CIVITANA forman una jerarquía, de forma que hay una entidad raíz común para cualquier tipo de certificado y varias entidades subordinadas, para los diferentes tipos de certificados.
- **Certificado cualificado:** son los certificados electrónicos expedidos por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en eIDAS1 y eIDAS2, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.
- **Certificados no cualificados:** son certificados ordinarios, sin la consideración legal de certificado cualificado.
- **Clave:** secuencia de símbolos empleados para controlar las operaciones de cifrado y descifrado.
- **Confidencialidad:** la confidencialidad es la capacidad de mantener un documento electrónico inaccesible a todos los usuarios, salvo a una determinada lista de personas. De este modo, podemos conseguir que las comunicaciones no sean escuchadas por otros y enviar documentos que solo puedan ser leídos por el destinatario indicado.
- **Criptografía:** la criptografía es una rama de las Matemáticas que estudia la transformación de información legible en información que no se puede leer directamente, es decir, que tiene que ser descifrada para ser leída.
- **Datos de creación de firma (Clave Privada):** una clave privada es un número único y secreto que pertenece a una única persona de manera que se puede identificar a la persona por medio de su clave privada. Esta clave es asimétrica a su clave pública. Una clave puede verificar y descifrar lo que la otra ha firmado o cifrado.
- **Datos de Verificación de firma (Clave Pública):** una clave pública es un número único que pertenece a una única persona pero que, a diferencia de la clave privada, puede ser conocida por todos. A través de procedimientos matemáticos se relaciona con la clave privada y sirve para encriptar y verificar firmas digitales.
- **Declaración de Prácticas de Certificación (DPC):** declaración que CIVITANA pone a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita. Tendrá la consideración de documento de seguridad en el que se detallarán, en el marco de eIDAS, las obligaciones que los Prestadores de Servicios de Certificación se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre

Civitana: Declaración de Prácticas de Certificación

- 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, CIVITANA mantiene un directorio actualizado de certificados en el que se indicarán los certificados expedidos.
- **Dispositivo cualificado de creación de firma:** dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II de eIDAS.
- **Firma electrónica:** los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- **Firma electrónica avanzada:** firma electrónica que cumple los requisitos contemplados en el artículo 26 de eIDAS1 y eIDAS2.
- **Firma electrónica cualificada:** firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- **Firmante:** es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
- **Hash o huella digital:** resultado de tamaño fijo que se obtiene tras aplicar una Función hash a un mensaje y que se encuentra asociado unívocamente a los datos iniciales.
- **HSM (Módulo de seguridad criptográfico):** es un dispositivo de seguridad que genera y protege claves criptográficas.
- **Infraestructura de Claves Públicas (PKI, Public Key Infrastructure):** una PKI determina qué entidades entran a formar parte del sistema de certificación, qué papel juegan dichas entidades, qué normas y protocolos se deben seguir para poder operar dentro del sistema, cómo se codifica y se transmite la información digital, y qué información contendrán los objetos y documentos gestionados por la infraestructura. Todo esto basado en la tecnología de Clave Pública (dos claves).
- **RGPD o 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, 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 CIVITANA 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 CIVITANA. En cuanto a la publicación de las Listas de Certificados Revocados, se garantiza un acceso a los usuarios y suscriptores de los certificados de forma segura y rápida.
- **Número de serie del Certificado:** es un valor entero y único asociado inequívocamente con un certificado expedido por cualquier Prestador de Servicios de Certificación.
- **OCSP (Online Certificate Status Protocol):** es un protocolo informático que permite la comprobación del estado de un certificado electrónico.
- **OID (Object Identifier):** valor que comprende una secuencia de componentes variables constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que poseen la propiedad de ser únicos entre el resto de OID.
- **PIN (Personal Identification Number):** Secuencia de caracteres que únicamente puede ser conocido por el sujeto que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- **Política de Certificación:** es un documento anexo a la Declaración de Prácticas de Certificación que recoge el ámbito de aplicación, los caracteres técnicos de los diferentes

tipos de certificados, el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación, así como sus condiciones de uso.

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

Civitana: Declaración de Prácticas de Certificación

- **Dispositivo cualificado de creación de sello electrónico:** dispositivo de creación de sellos electrónicos que cumple mutatis mutandis los requisitos enumerados en el anexo II de eIDAS
- **Sello de tiempo electrónico:** datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante
- **Sello cualificado de tiempo electrónico:** sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 de eIDAS

1.6.2. Acrónimos

- **ARL:** Lista de Revocación de Autoridades de Certificación
- **CA:** Autoridad de Certificación
- **CN:** Common Name (Nombre común)
- **CRL:** Certificate Revocation List (Lista de Certificados Revocados)
- **DN:** Distinguished Name (Nombre distintivo)
- **DPC:** Declaración de Prácticas de Certificación
- **QSCD:** Dispositivo Cualificado de Creación de Firma
- **ETSI:** European Telecommunications Standards Institute
- **GN:** nombre propio del poseedor en un certificado
- **HSM:** Hardware Security Module (Módulo de Seguridad Criptográfico)
- **LRA:** Autoridad de Registro Local
- **OCSP:** Online Certificate Status Protocol (Servicio de Publicación de Certificados 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
- **RA:** Autoridad de Registro
- **SSL:** Secure Socket Layer
- **TSA:** Servidor de la Autoridad de Sellado de Tiempo
- **eIDAS1:** Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- **eIDAS2:** Reglamento 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital

2. PUBLICACIÓN Y RESPONSABLES DEL REPOSITORIO DE INFORMACIÓN

2.1. Repositorio de información

CIVITANA dispone de un repositorio de información pública en el que se publican todas las informaciones relativas al servicio de confianza prestado. Este se encuentra en [\[Enlace repositorio\]](#), disponible las 24 horas del día, los 7 días de la semana.

2.2. Publicación de información de certificación

CIVITANA garantiza la disponibilidad de la DPC, PDS, políticas específicas de certificados y términos y condiciones de uso de los certificados en [\[Enlace repositorio\]](#).

CIVITANA 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): CIVITANA 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).

2.3. Política de publicación y notificación

Los cambios en las especificaciones o en las condiciones del servicio serán comunicados por CIVITANA a los usuarios a través de [\[Enlace repositorio\]](#). CIVITANA podrá establecer canales adicionales de comunicación para situaciones específicas.

En el caso de DPC, y Términos y Condiciones de Uso se mantendrán en [\[Enlace repositorio\]](#) de forma indefinida la versión vigente y todas las anteriores.

2.4. Frecuencia de publicación

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

La información sobre el estado de los certificados se publica de acuerdo con lo establecido en esta Declaración de Prácticas de Certificación.

2.5. Control de acceso al repositorio

CIVITANA 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.

CIVITANA 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.

Civitana: Declaración de Prácticas de Certificación

- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación.

La codificación de los Certificados sigue el estándar RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

3.1. Tipos de nombres

Todos los certificados de entidad final contienen un nombre distinguido (Distinguished name) en el campo Subject. Los atributos que componen el nombre diferenciado del campo subject son los recogidos en el apartado correspondiente al perfil del certificado.

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

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

3.1.1. Emisor

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

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

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

3.1.2. Asunto

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

El campo no puede estar en blanco y contiene obligatoriamente un nombre diferenciado (DN).

Un nombre diferenciado se compone de un conjunto de atributos, que consisten en un nombre o etiqueta y un valor asociado.

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

Civitana: Declaración de Prácticas de Certificación

3.1.2.1. Certificado cualificado de Persona Física en QSCD centralizado

Country (C)	Estado ¹
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	DNI/NIE/Pasaporte/ u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

3.1.2.2. Certificado cualificado de Persona Física en HSM centralizado

Country (C)	Estado ²
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	DNI/NIE/Pasaporte/ u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre y apellidos del firmante

3.1.3. Significado de los nombres

Todos los nombres distintivos (DN) del campo Subject Name son significativos. La descripción de los atributos asociados al Suscriptor del Certificado es legible por humanos.

3.1.4. Emisión de certificados de prueba

Como norma general, los certificados de prueba se expedirán con los siguientes datos de identificación, sin perjuicio de las modificaciones que puedan surgir como consecuencia de cambios normativos y/o instrucciones específicas emitidas por el Organismo Nacional de Supervisión.

- Número de Documento Nacional de Identidad (DNI): 00000000T
- Número de Identidad de Extranjero (NIE): X0000000T, Y0000000R, Z0000000W
- Nombre: Nombre
- Primer apellido: Apellido1
- Segundo apellido: Apellido2

El resto de campos que conformen el “DN” o “Subject” del certificado, deberán utilizar palabras que denoten su invalidez (ej. “TEST”, “Prueba” o “Invalido”).

En caso necesario y previo aviso al Órgano Supervisor Nacional, CIVITANA podrá generar certificados de prueba con otros datos, cuya vigencia estará limitada a la duración de las pruebas.

Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al Supervisor Nacional su evaluación. Todos los certificados de pruebas se considerarán sin validez legal y por lo tanto sin responsabilidad alguna sobre CIVITANA.

¹ El campo “Estado” corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

² El campo “Estado” corresponderá al del estado donde se produzca la relación contractual entre el firmante y la entidad a la que está vinculado (por ser empleado, miembro, socio u otra vinculación), con independencia de la nacionalidad del trabajador.

3.1.5. Seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

3.1.6. Reglas para la Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” o “estado” será el del suscriptor del certificado.

En el campo “número de serie” se incluye el DNI, NIE, Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

Sin perjuicio de lo anteriormente expuesto, cualquier tipo de certificado electrónico cualificado, cuando se expida para la identificación de las personas interesadas ante las Administraciones Públicas, debe contener como atributos su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal de manera inequívoca según corresponda.

3.1.7. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la

3.1.8. Resolución de conflictos relativos a nombres y tratamiento de marcas registradas

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

CIVITANA 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.

CIVITANA se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres. En caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

3.2. Validación de la identidad

La identidad de los suscriptores de los certificados resulta fijada en el momento de la firma del contrato entre CIVITANA y el suscriptor, momento en el que queda verificada la existencia del

Civitana: Declaración de Prácticas de Certificación

suscriptor mediante su documento oficial de identidad. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

3.2.1. Métodos para probar la posesión de la clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado y/o sus credenciales por el suscriptor o firmante.

Las claves son generadas por CIVITANA y 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.

3.2.2. Métodos de validación de la identidad

Para lo solicitud de certificados los Operadores de Registro de CIVITANA verificarán la identidad del firmante a la que se le expide el certificado, así como cualquier atributo específico de acuerdo con el perfil del certificado.

Para la verificación se procederá directamente o bien por medio de un tercero de conformidad con el derecho nacional, de acuerdo con los siguientes métodos:

- a) a través de la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con lo establecido en la normativa de aplicación.
- b) por medio del procedimiento de identificación electrónica a través del sistema de vídeo identificación remota de CIVITANA, conforme los métodos de identificación reconocidos a escala nacional mediante 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.
- c) por medio de un certificado de una firma electrónica cualificada expedido de conformidad con la letra a) y c) del presente apartado, así como utilizando otros métodos de identificación que garanticen la identificación de la persona con un nivel alto de confianza, cuya conformidad será confirmada por un organismo de evaluación de la conformidad, según lo establecido en el artículo 24. 1.bis del Reglamento eIDAS.

Sin perjuicio de lo anterior, no se exigirá la validación de la identidad cuando la identidad u otras circunstancias permanentes de los firmantes a los que se les expiden los certificados, ya constasen en CIVITANA en virtud de una relación preexistente, siempre y cuando para identificar al firmante se haya empleado un método de identificación presencial y no hayan pasado más de 5 años.

3.2.3. Validación de la identidad por medios electrónicos

El Proceso de Identificación por Vídeo o Videoconferencia Asíncrona (en adelante, el "Proceso de Identificación por "Vídeo" o el "Proceso") es un método de verificación de identidad por vídeo remota, no supervisada y en tiempo real, que registra todo el proceso de registro de una persona y permite la validación remota de documentos de identidad, mediante una grabación de vídeo que captura y valida el documento de identidad en tiempo real y de forma automatizada (aproximadamente de 10 a 20 segundos), que lleva a cabo SIGNICAT SLU a través de sus operadores de verificación.

El proceso consta de dos partes: un módulo automático en el que se realizan múltiples controles de los elementos de seguridad del documento que se muestra durante la grabación del vídeo, así como una comparación biométrica facial entre el portador del documento, el usuario, y la fotografía del mismo, realizando alternativamente una prueba de vida y una extracción precisa de datos.

Civitana: Declaración de Prácticas de Certificación

Toda esta información sirve como elemento de apoyo a la toma de decisiones para un agente humano de la autoridad de registro (RAO), quien revisará la grabación de vídeo completa posteriormente (de forma asíncrona) y determinará si se puede otorgar o no una identidad sobre la base de las pruebas mostradas.

Esta tecnología verifica la autenticidad de los documentos de identidad, incluyendo controles de seguridad en tiempo real, como la detección de hologramas, insignias, patrones y otras características de seguridad de los documentos.

3.2.3.1. Descripción del proceso de video identificación

El proceso de video identificación se desarrolla sobre la base de los siguientes elementos:

- Guiado por voz y texto durante el proceso de videoidentificación.
- Control automatizado de los elementos del entorno (condiciones de iluminación, red, calidad de la cámara) con el fin de obtener una grabación óptima de la videoidentificación y de las evidencias generadas.
- Comparación de imágenes con documentos originales mediante tecnología de reconocimiento de patrones, con el objetivo de verificar la autenticidad del documento.
- Extracción de datos (OCR) de la MRZ u otras partes del documento, así como la posibilidad de consultar credenciales en tiempo real.
- Verificación de que el anverso y reverso (cuando aplique) pertenecen al mismo documento.
- Registro biométrico de la persona (biometric enrolment) y comparación en tiempo real con la imagen del documento de identidad.
- Herramienta de verificación de la Autoridad de Registro (RA), que permite la revisión del proceso por parte de una persona cualificada, debidamente formada mediante capacitación específica.

En este sentido, una vez que el usuario selecciona el documento que se utilizará para llevar a cabo el proceso, se realiza una grabación de vídeo en streaming, controlada por la aplicación, en la que se inicia el procedimiento y en la que el usuario deberá mostrar el anverso y reverso de su documento para su identificación y validación en tiempo real. Asimismo, se solicitará al usuario que muestre su rostro para la realización de un proceso de reconocimiento facial basado en evaluación biométrica automatizada (biometric scoring), incluyendo mecanismos de detección de vida (*liveness detection*), requiriendo la interacción del usuario mediante movimientos, así como la extracción de datos del documento mediante OCR.

Para la revisión asíncrona por parte de un agente humano, se dispone de un protocolo de seguridad basado en buenas prácticas de la Unión Europea, apoyado en una herramienta puesta a disposición del agente, en la que se muestran tanto las evidencias obtenidas durante el proceso como las alertas o indicadores relativos a aquellas no obtenidas o que requieren verificación adicional. Todo el proceso queda trazado mediante sellos temporales asociados a cada uno de los pasos.

En consecuencia, el sistema garantiza la cadena de custodia de la verificación, desde las evidencias recopiladas durante el proceso automatizado de videoidentificación hasta las trazas que vinculan la identificación con el agente cualificado de la Autoridad de Registro. El resultado es una identidad verificada con un nivel de seguridad técnica equivalente al de un proceso realizado en presencia física del titular.

3.2.3.2. Obligaciones del usuario en relación con el proceso de videoidentificación

El usuario, a lo largo del proceso, se compromete a:

- Utilizar el servicio de conformidad con lo dispuesto en los términos y condiciones del proceso de videoidentificación y de emisión de certificados cualificados, en la Declaración de Prácticas

Civitana: Declaración de Prácticas de Certificación

de Certificación (CPS), en las condiciones particulares que, en su caso, resulten de aplicación, así como en cualquier otra instrucción, manual o procedimiento facilitado por SIGNICAT, S.L.U.

- Garantizar que el documento utilizado en el proceso es un documento auténtico y legalmente válido y, adicionalmente, que:
 - No se trata de una fotocopia ni de una impresión.
 - No se presenta en formato digital (teléfono móvil, tableta u ordenador).
 - No se encuentra dentro de una funda o cubierta.
 - Está completo y en buen estado, sin deterioros que comprometan su integridad, incluyendo todos sus elementos de seguridad.
- Asimismo, durante todo el proceso y mientras se realiza la grabación de vídeo, y con el fin de evitar su rechazo:
 - Las condiciones de iluminación deben permitir una visualización clara tanto del rostro de la persona identificada como del documento.
 - El vídeo debe mantener un flujo continuo, sin interrupciones ni retrasos.
 - La identificación debe ser realizada por una persona viva (*liveness*).
 - En caso de que el proceso sea realizado por una persona distinta del titular objeto de identificación, la identificación será rechazada.
 - En el supuesto de que aparezca otra persona en el vídeo, pero resulte evidente que no actúa de forma concertada con el sujeto a identificar, la identificación podrá considerarse válida, en términos equivalentes a aquellos supuestos en los que una persona presta asistencia a otra con discapacidad para llevar a cabo el proceso de identificación.
 - Todas las áreas del documento capturado deben visualizarse con claridad, tanto en su anverso como en su reverso, así como el rostro de la persona.
 - El usuario no debe encontrarse dormido ni presentar signos que puedan interpretarse como estar bajo los efectos de drogas o alcohol.

3.2.3.3. Periodo de conservación de la información

Toda la información relativa al proceso de videoidentificación y a la emisión de certificados electrónicos cualificados en dicho contexto, incluida la información biométrica, será conservada durante la vigencia de la relación contractual, siempre que no se solicite su supresión, y durante el plazo de prescripción de las posibles acciones legales que pudieran derivarse, así como de las reclamaciones que pudieran formular organismos oficiales.

El periodo máximo de conservación de la información relevante en relación con el proceso de videoidentificación y la emisión de certificados cualificados será de 15 años desde el momento de emisión del certificado, salvo que la normativa aplicable establezca un plazo distinto. Una vez finalizada la relación, los datos serán debidamente bloqueados, de conformidad con lo dispuesto en la normativa vigente.

Asimismo, se informa de que todas las evidencias relativas a procesos de identificación incompletos que no hayan sido finalizados debido a sospechas de intento de fraude serán conservadas durante un periodo de 5 años desde la ejecución del proceso, especificándose el motivo de la no finalización, de acuerdo con la política establecida al efecto.

3.2.4. Autenticación de la identidad de la persona física solicitante

La identidad de las personas físicas firmantes identificados en los certificados, se valida a través de los métodos de identificación especificados en el apartado 3.2.2., de tal manera que:

Civitana: Declaración de Prácticas de Certificación

- (i) Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de CIVITANA, deberá mostrar su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho.
- (ii) Si se identifica electrónicamente a través del sistema de video identificación remota de CIVITANA:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho.
 - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro de CIVITANA comprobará la identidad de la persona física identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión del Documento de identidad aportado.
- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de CIVITANA mediante:
 - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
 - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
 - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
 - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

Durante este trámite se confirma rigurosamente la identidad de la persona física identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita ante un operador de registro la identidad de la persona física firmante.

La Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

3.2.5. Información no verificada del suscriptor

Bajo ningún concepto se incluirá información de suscriptor no verificada en los certificados, a excepción del correo electrónico del suscriptor o firmante.

3.2.6. Validación de la autoridad de registro

Para la constitución de una nueva Autoridad de Registro, CIVITANA realiza las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Civitana: Declaración de Prácticas de Certificación

Igualmente de forma directa o a través de su Autoridad de Registro, se verifica y valida la identidad de los operadores de las Autoridades de Registro, para lo cual estas últimas envían a CIVITANA la documentación referente a la identificación del nuevo operador, juntamente con su autorización para actuar como tal.

En el caso de que el operador de la Autoridad de Registro desee emitirse un certificado de cualquier otro tipo de perfil de certificado, siempre que cumpla las condiciones para poderse emitir, no podrá actuar como operador de registro para la solicitud de dicho certificado, debiendo ser dicho operador de registro una persona distinta a la solicitante del certificado.

CIVITANA se asegura que los operadores de la Autoridad de Registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la Autoridad de Registro previamente autorizada por CIVITANA.

Para la prestación de los servicios debe asegurarse de que los operadores de Autoridad de Registro acceden al sistema mediante autenticación fuerte con certificado digital.

3.3. Identificación y autenticación para peticiones de renovación

3.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos.

El método aceptable para dicha comprobación es el empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2. Identificación y autenticación de la solicitud de renovación

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.4. Identificación y autenticación para peticiones de revocación

CIVITANA o un operador o personal autorizado de la Autoridad de Registro autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación podrá ser realizada por:

- El suscriptor y/o firmante:
 - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de CIVITANA en horario 24 horas al día 7 días a la semana.
 - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de CIVITANA y/o Autoridades de Registro.
- Las autoridades de registro deberán identificar al firmante y/o suscriptor ante una petición de revocación según los propios medios que considere necesarios. Se considerará que se ha identificado correctamente mediante solicitud enviada por el firmante, firmada con el propio certificado

3.5. Suspensión de certificados

CIVITANA no permite la suspensión de certificados.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

El solicitante del certificado, como norma general una persona física, debe firmar un contrato de prestación de servicios de certificación con CIVITANA.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, en un documento específico de hoja de solicitud de certificados o ante la autoridad de registro.

En el caso de solicitudes realizadas por medios electrónicos, se entenderá formalizada la solicitud de certificado cuando el solicitante complete el proceso habilitado a tal efecto a través de la plataforma web de CIVITANA, incluyendo la aceptación expresa de los términos y condiciones aplicables al servicio de certificación.

4.1.2. Comprobación de la solicitud

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

4.1.3. Proceso de inscripción y responsabilidades.

Las tareas de identificación y acreditación de la información que consta en el certificado, así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los mismos serán realizados por Autoridades de Registro propias o con las que CIVITANA suscriba el correspondiente instrumento legal.

CIVITANA recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de datos externas, o a través de una capa de servicios web cuyo destinatario es CIVITANA.

CIVITANA es titular de distintos servicios electrónicos gestionados a través de servicios web por la que se tramitan las solicitudes de certificados:

Toda solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, conforme con la política de certificado correspondiente. Asimismo se deberá acompañar de medios de contacto que permitan contactar a la persona física identificada en el certificado.

4.2. Procesamiento de las solicitudes

4.2.1. Realización de funciones de identificación y autenticación

Es responsabilidad de CIVITANA realizar la identificación del suscriptor de forma adecuada. Este proceso deberá ser realizado previamente a la emisión del certificado y entre ambos procesos no puede transcurrir un periodo temporal superior a un mes.

Civitana: Declaración de Prácticas de Certificación

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

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la extinción del certificado o la finalización del servicio prestado, incluso en caso de pérdida anticipada de vigencia por revocación.

4.2.2. Aprobar o rechazar solicitudes

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

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación y/o servicio de CIVITANA, sus Autoridades de Registro o de los suscriptores, deberá denegarse la petición, o detener su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que observadas las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la solicitud quedará denegada definitivamente.

En cualquier caso, debe realizarse la notificación correspondiente sobre la aprobación o denegación de la solicitud. CIVITANA podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.2.3. Tiempo en procesar la solicitud

Las solicitudes de certificados serán atendidas por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3. Emisión del certificado

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

Si en el plazo de 1 mes desde la solicitud de emisión el solicitante no ha recibido el certificado y/o credenciales para su uso o generación, deberá ponerse en contacto con CIVITANA.

4.3.1. Acciones de la CA durante la emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, CIVITANA:

Civitana: Declaración de Prácticas de Certificación

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza 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.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia CIVITANA o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

4.3.2. Notificación al suscriptor de la emisión

CIVITANA notifica al suscriptor la emisión del certificado, así como y el método de generación y utilización.

4.4. Entrega y Aceptación del certificado

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

4.4.1. Responsabilidad de la CA

Con carácter previo a la entrega del certificado, el operador o personal autorizado de la Autoridad de Registro debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona física identificada en el certificado, de acuerdo con lo establecido en el presente documento.
- Disponer del Contrato de Prestación de Servicios de Confianza debidamente firmado por el Suscriptor o en su defecto, de la aceptación de los términos y condiciones.
- Entregar la hoja de entrega y aceptación del certificado a la persona física identificada en el certificado con los siguientes contenidos mínimos:
 - o Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades.
 - o Información acerca del certificado.
 - o Reconocimiento, por parte del firmante, de recibir el certificado y/o los mecanismos para su generación/descarga y la aceptación de los citados elementos.
 - o Régimen de obligaciones del firmante.
 - o Responsabilidad del firmante.
 - o Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
 - o La fecha del acto de entrega y aceptación.

Civitana: Declaración de Prácticas de Certificación

Toda esta información podrá incluirse en el propio Contrato de Prestación de Servicios de Confianza y/o en los términos y condiciones del servicio. Dicho lo cual, cuando se produzca la firma del Contrato de Prestación de Servicios de Confianza o la aceptación de los términos y condiciones por el Suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado.

- Obtener cuando corresponda la firma de la persona identificada en el certificado.

Las Autoridades de Registro son las encargadas de realizar estos procesos, debiendo registrar documentalmente los anteriores actos y conservar los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a CIVITANA, así como los originales cuando se precise acceso a los mismos.

4.4.2. Proceso de aceptación del certificado

Con la firma del documento de solicitud del certificado se aceptan también los términos y condiciones de uso, disponibles en [\[Enlace repositorio\]](#).

Cuando la generación y entrega del certificado se lleve a cabo a través del procedimiento automatizado definido por CIVITANA, la aceptación del certificado por la persona física identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Confianza utilizando el propio certificado y/o mediante la aceptación de los términos y condiciones del Servicio.

4.4.3. Publicación del certificado por la CA

Una vez que el certificado ha sido aceptado por el suscriptor y generado, el certificado será publicado en repositorios internos de CIVITANA. Cualquiera puede acceder a la información de estado del certificado mediante consulta a la Autoridad de Validación, ya sea a través del servicio OCSP o la CRL.

4.4.4. Notificación de la emisión del certificado por la CA a otras entidades

CIVITANA no notifica la emisión del certificado a otras entidades. Únicamente se informa al Suscriptor del certificado.

4.5. Uso del par de claves y usos del certificado

4.5.1. Clave privada del suscriptor y uso del certificado

El suscriptor que custodia sus claves,

- Facilitará a CIVITANA información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestará su consentimiento previo a la emisión y entrega de un certificado.
- Garantizará el buen uso y la conservación de los soportes de los certificados.
- Empleará adecuadamente el certificado y, en concreto, cumplirá con las limitaciones de uso de los certificados.
- Será diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en esta Declaración de Prácticas de Certificación.

Civitana: Declaración de Prácticas de Certificación

- Notificará a CIVITANA 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.
- No monitorizará, manipulará o realizará actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito.
- No comprometerá intencionadamente la seguridad de los servicios de certificación.
- El suscriptor de certificados cualificados que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado, debe reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se emplee un dispositivo cualificado de creación de firma, conforme a lo preceptuado en eIDAS.

El Suscriptor queda obligado a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado y/o a sus credenciales de activación, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

Las presentes obligaciones serán de aplicación tanto a los suscriptores como firmantes del certificado.

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

El usuario verificador de certificados queda obligado a:

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

Civitana: Declaración de Prácticas de Certificación

- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de CIVITANA
- No comprometer intencionadamente la seguridad de los servicios de certificación.
- Reconocer que tales firmas electrónicas son equivalentes a firmas manuscritas, de acuerdo con eIDAS1 y eIDAS2.

CIVITANA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6. Renovación del certificado

La renovación del certificado consiste en la emisión de un nuevo certificado al suscriptor sin cambiar ninguna información del suscriptor (u otros participantes) o cualquier otra información que aparezca en el certificado.

4.6.1. Circunstancias para la renovación del certificado

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

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

Se consideran al menos dos posibilidades para la renovación de certificados:

- Proceso de renovación, que se efectuará del mismo modo que la emisión de un nuevo certificado.
- Proceso de renovación online (a través de internet), que se detalla a continuación.

Solamente se podrá proceder a la renovación online del certificado si se cumplen las condiciones siguientes:

- La Autoridad de Registro y/o CIVITANA dispone del servicio de renovación online.
- El certificado con el que se firma la renovación esté vigente, es decir, no haya caducado, no esté revocado ni suspendido.
- Que no hayan transcurrido más de 5 años desde la última acreditación de su identidad ante un operador de identificación para la obtención de un certificado.

4.6.2. Quién puede solicitar la renovación

Cualquier suscriptor podrá pedir la renovación online de su certificado si se cumplen las circunstancias descritas en el punto anterior.

El firmante podrá formalizar su solicitud accediendo al servicio de renovación online de certificados en la página web de CIVITANA.

4.6.3. Tratamiento de peticiones de renovación de certificado

La solicitud de una renovación del certificado se realizará de acuerdo con lo siguiente:

- Cuando el certificado digital de un usuario esté próximo a caducar, podrá enviarse una o más notificaciones distribuidas en el tiempo, invitándole a su renovación.
- El firmante se conectará al servicio de renovación de la página web de CIVITANA y procederá a la solicitud de renovación. El Operador de Registro comprobará que la información empleada para verificar la identidad y los restantes datos del usuario identificado en el certificado continúan siendo válidos. Si cualquier información del usuario identificado en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2
- El firmante firmará la renovación de su certificado válido.
- Se procederá a la generación del nuevo par de claves y generación e importación del certificado, respetando los siguientes condicionantes:
 - Protege la confidencialidad e integridad de los datos de registro de que dispone.
 - Utiliza 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.
 - Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
 - Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
 - Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
 - Indica la fecha y la hora en que se expidió un certificado.
 - Garantiza el control exclusivo del usuario sobre sus propias claves, no pudiendo la propia CIVITANA o sus Autoridades de Registro deducirlas o utilizarlas.

4.6.4. Notificación al suscriptor

En caso de que los datos se verifiquen correctamente, CIVITANA aprobará la solicitud de renovación del certificado y proceder a su emisión y entrega, siendo notificada al solicitante la aprobación o denegación de la solicitud.

4.6.5. Procedimiento de aceptación de un certificado renovado

El certificado se considerará aceptado al firmar electrónicamente la renovación, esto es firmando el contrato de emisión de certificados que se genera con la solicitud de renovación.

4.6.6. Publicación del certificado

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

4.6.7. Notificación a otras entidades

CIVITANA no notifica la emisión y/o renovación del certificado a otras entidades. Únicamente se informa al Suscriptor del certificado.

4.7. Renovación con regeneración de las claves del certificado

El proceso de “re-key” consiste en crear un nuevo certificado con una clave pública diferente (y número de serie) mientras se mantiene el contenido del subject del antiguo certificado. CIVITANA no permite la renovación con regeneración de las claves del certificado.

4.8. Modificación del certificado

En caso de necesidad de modificar algún dato del certificado, CIVITANA procederá a la revocación del certificado y a la emisión de uno nuevo conforme los procedimientos definidos en el presente documento.

4.9. Revocación de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

4.9.1. Circunstancias para la revocación

Un certificado será revocado cuando concurra alguna de las siguientes causas:

- 1) Circunstancias que afectan a la información contenida en el certificado:
 - a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
 - b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
 - c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
 - d) Alteración posterior de las circunstancias verificadas para la expedición del certificado, como por ejemplo las relativas al cargo o facultades.
- 2) Circunstancias que afectan a la seguridad de la clave o del certificado:
 - a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de confianza que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
 - b) Infracción, por CIVITANA de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.
 - c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
 - d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
 - e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
 - f) Utilización de dispositivos cualificados de creación de firma que no cumplen con los estándares de seguridad mínimos y necesarios para garantizar la seguridad del certificado o sus claves privadas.
 - g) Que ya no cumple con la Declaración de Prácticas del Certificado o la Política del Certificado bajo la cual fue emitido.
- 3) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:
 - a) Finalización de la relación jurídica de prestación de servicios entre el prestador y el suscriptor.

Civitana: Declaración de Prácticas de Certificación

- b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.
 - c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
 - d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente, así como la presente Declaración de Prácticas de Certificación.
 - e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
 - f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.
 - g) Solicitud formulada por el suscriptor y/o firmante del certificado, la persona física o jurídica representada por este o un tercero autorizado, requiriendo la revocación del certificado.
 - h) Terminación de la representación en los certificados electrónicos con atributo de representante. Corresponde tanto al suscriptor como al firmante, solicitar la revocación del certificado cuando exista una modificación o extinción de la relación de representación.
- 4) Otras circunstancias:
- a) La terminación del servicio de certificación de la Autoridad de Certificación de CIVITANA, salvo que de acuerdo con su plan de cese se opte por transferir la gestión de los certificados a otro Prestador de Servicios de Confianza.
 - b) El incumplimiento de la declaración de prácticas y demás políticas de certificación sobre la que ha sido expedido el certificado.
 - c) Resolución judicial o administrativa que lo ordene.
 - d) El uso del certificado que sea dañino y continuado para CIVITANA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
 - o La naturaleza y el número de quejas recibidas.
 - o La identidad de las entidades que presentan las quejas.
 - o La legislación relevante vigente en cada momento.
 - o La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.9.2. Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La persona identificada en el certificado, véase el firmante.
- El suscriptor del certificado por medio su representante legal o voluntario o tercero autorizado.
- Autoridad judicial o administrativa mediante la resolución correspondiente.
- CIVITANA en los casos de causa técnica contemplados en este documento.

4.9.3. Tratamiento de las peticiones de revocación

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

- Online mediante el servicio disponible en la dirección [\[Enlace repositorio\]](#)

Civitana: Declaración de Prácticas de Certificación

- Por correo electrónico, enviando el formulario de solicitud de revocación a _____@_____.com firmado con un certificado cualificado la solicitud de revocación autenticada, así como la información que justifica la revocación, es registrada y archivada.

La solicitud de revocación que se realice por correo electrónico deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Nombre y apellidos de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por CIVITANA, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

El servicio online de revocación se encuentra en la página web de CIVITANA en la dirección: [\[Enlace repositorio\]](#).

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado.

Tanto el servicio de gestión de revocación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencia y el plan de continuidad de negocio de CIVITANA. Para garantizar la precisión en los procedimientos de revocación, suspensión o reactivación de certificados, los sistemas involucrados en estos procesos se sincronizan con UTC al menos una vez al día.

4.9.4. Periodo de gracia de la solicitud de revocación

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

4.9.5. Tiempo de plazo de la CA para procesar la revocación

Las solicitudes de revocación realizadas a través del servicio online se tramitarán de manera inmediata.

Si la petición se realiza mediante solicitud directa a CIVITANA o a través de un operador de registro, se ejecutará dentro del horario ordinario de operación de CIVITANA o en su caso de la Autoridad de Registro correspondiente. En cualquier caso, las peticiones se tramitarán en un plazo no superior a 24 horas desde la recepción de la misma.

En el caso de que, debido a una incidencia técnica u operativa, no se pudiese cumplir con el plazo de 24 horas, CIVITANA registrará la solicitud en su sistema de ticketing, asignando un número de caso único, registrando la fecha y hora de recepción de la misma, y designando un responsable para su seguimiento. De igual forma, se indicarán los motivos específicos del retraso, así como las acciones concretas que se llevarán a cabo para asegurar la resolución de la solicitud en el menor tiempo posible.

Civitana: Declaración de Prácticas de Certificación

CIVITANA informará al usuario de forma inmediata notificándole:

- Que su solicitud ha sido registrada.
- Información sobre el motivo del retraso.
- Estimación del tiempo para la finalización del proceso.

Asimismo, CIVITANA mantendrá al usuario informado del progreso de su solicitud mediante actualizaciones periódicas hasta su resolución. El solicitante podrá ponerse en contacto con CIVITANA a través de los datos de contacto especificados en el epígrafe 1.5.2. del presente documento. Una vez procesada la solicitud, CIVITANA notificará al usuario, confirmando el resultado de la revocación; y procederá a cerrar el ticket abierto relacionado con la incidencia.

4.9.6. Obligación de verificación de las revocaciones por terceros de confianza

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

Las Listas de Revocación de Certificados se publican en el repositorio de la Autoridad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- <http://crl1.civitana.com/>
- <http://crl2.civitana.com/>

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSF.

- <http://ocsp1.civitana.com/>
- <http://ocsp2.civitana.com/>

4.9.7. Frecuencia de generación de CRLs

CIVITANA emite una Lista de Revocación de Certificados (en adelante CRL) cada 60 minutos, desde el momento en que se produce una revocación y al menos una cada 24 horas.

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

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

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

Para garantizar la precisión en la gestión de revocación de certificados de la Autoridad de Certificación, los sistemas involucrados en la emisión y publicación de Listas de Revocación de Certificados (CRLs) se sincronizan con UTC al menos una vez al día.

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

Las CRL se publican en el Repositorio en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

En caso de diferencia temporales en la actualización del estado de los certificados entre la CRL y el servicio OCSF, el mecanismo de validación que prevalece es el OCSF, ya que proporciona información

Civitana: Declaración de Prácticas de Certificación

en tiempo real sobre la revocación de certificados, mientras que la CRL se actualiza de forma periódica.

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

CIVITANA 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.

- <http://ocsp1.civitana.com/>
- <http://ocsp2.civitana.com/>

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

De forma alternativa, los terceros que confían en certificados podrán consultar el repositorio de certificados de CIVITANA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web: [Enlace repositorio], la siguiente información:

- Lista de Autoridades de Certificación Revocadas (ARL) expedida por la **ROOT**:
<http://arl1.civitana.com/>
<http://arl2.civitana.com/>
- Lista de Certificados Revocados (CRL) expedida por las **Autoridades** Subordinadas.
 - o <http://crl1.civitana.com/>
 - o <http://crl2.civitana.com/>

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de CIVITANA, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día. Se suministrará información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

4.9.10. Obligación de consulta de servicios de comprobación de estado de certificados

Es obligatorio consultar los servicios de comprobación de estado de los certificados electrónicos de CIVITANA con carácter previo a confiar en los mismos.

4.9.11. Requisitos especiales en caso de compromiso de la clave privada

En el supuesto de compromiso de la clave privada de cualquiera de las Autoridades de Certificación de la jerarquía de CIVITANA, se procederá a notificar a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de CIVITANA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.10. Finalización de la suscripción

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

Civitana: Declaración de Prácticas de Certificación

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción del servicio.

4.11. Custodia y recuperación de claves

4.11.1. 4.12.1 Prácticas y políticas de custodia y recuperación de claves

CIVITANA únicamente almacena las claves de los certificados emitidos en los perfiles en la nube. Estas claves no son exportables y permanecen bajo el control exclusivo del titular del certificado.

CIVITANA no ofrece servicios de recuperación de claves.

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

Sin estipulación.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTO Y DEL PERSONAL

5.1. Controles de seguridad física

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

5.1.1. Localización y construcción de las instalaciones

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

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

5.1.2. Acceso físico:

5.1.2.1. Centro de Proceso de Datos

Las instalaciones de CIVITANA 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,
 - o Únicamente está permitido el acceso a personal autorizado.
 - o Los derechos de acceso al área segura son revisados y actualizados periódicamente.
 - o 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.
 - o El personal ajeno a la operación de CIVITANA que se encuentre trabajando en sus instalaciones es supervisado.

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

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

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

5.1.2.2. Autoridades de Registro (RAs)

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

5.1.3. Electricidad y aire acondicionado

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

Así mismo las instalaciones de CIVITANA disponen de una funcionalidad de alimentación ininterrumpida (SAI y grupo electrógeno) que mantiene los equipos en funcionamiento durante el

Civitana: Declaración de Prácticas de Certificación

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

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

5.1.5. Prevención y protección de incendios

El Centro de Procesos de Datos de CIVITANA 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 CIVITANA.
- Cumplir con las misiones de desconexión del sistema de ventilación, cierre de las compuertas contrafuego, corte de la energía eléctrica y el disparo de la instalación automática de extinción.

5.1.6. Almacenamiento de soportes

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

5.1.7. Tratamiento de residuos

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

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

5.1.8. Copia de respaldo fuera de las instalaciones

CIVITANA 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

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

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

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

Civitana: Declaración de Prácticas de Certificación

CIVITANA ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- Responsable de Seguridad: Encargado de administrar e implementar las políticas y prácticas de seguridad de la información. Es el encargado de velar porque las políticas de seguridad de CIVITANA se cumplan.
- Administrador de Sistemas: Responsable de instalar, configurar y mantener los sistemas fiables del prestador para la gestión del servicio. Esto incluye también las tareas de recuperación del sistema.
- Operador de Sistemas: Responsable de la operación diaria de los sistemas. Autorizados a realizar las copias de seguridad del sistema.
- Auditores de interno: Responsable de verificar el cumplimiento de los procedimientos operativos.
- Operador de Registro: Responsable de verificar la identidad del solicitante, la veracidad de los atributos que se incluirán en el certificado, así como de aprobar las peticiones de certificados. Asimismo es el encargado de gestionar las peticiones que afecten al ciclo de vida del certificado.
- Oficial de Revocación: Encargado de procesar las solicitudes de revocación de los certificados.

5.2.2. Número de personas por tarea

Deben garantizarse al menos dos personas para realizar las tareas relativas a la generación, recuperación y copia de seguridad de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz y subordinadas.

5.2.3. Identificación y autenticación para cada rol

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados. El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.2.4. Separación de tareas en los diferentes roles

El rol de confianza de Auditor Interno es incompatible con el resto de roles.

El rol de confianza de Responsable de Seguridad no puede desempeñar las funciones de Auditor Interno, Operador de Sistemas y Administrador de Sistemas.

Los roles de confianza de Administrador y Operador de Sistemas, no podrán desempeñar las funciones de Auditor Interno, Responsable de Seguridad, así como ningún rol de Operador de la Autoridad de Registro.

5.3. 5.3 Controles de personal

5.3.1. Requisitos de historial, calificaciones, experiencia y autenticación

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

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

CIVITANA se asegura que todo el personal de registro es confiable para realizar las tareas de registro. El personal al cargo de la Autoridad de Registro recibe formación específica para el desempeño correcto de sus funciones.

En general, retirará de sus funciones de confianza a un empleado y/o tercero, cuando se tenga conocimiento de la existencia de conflictos de interés, incumplimiento de los procedimientos y/o políticas de seguridad, así como la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

Además de ello, no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos: Estudios, trabajos anteriores así como referencias profesionales.

5.3.2. Procedimientos de investigación de historial

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

CIVITANA antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años.
- Referencias profesionales.
- Estudios, incluyendo titulación alegada.

CIVITANA obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales, reflejada en el Reglamento Europeo nº2016/679 General de Protección de Datos y en general cualquier normativa nacional que resulte de aplicación.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

5.3.3. Requisitos de formación

El personal de CIVITANA, tanto roles fiables como de gestión, recibe la formación requerida para asegurar su competencia en la realización de sus funciones.

Los programas de formación son revisados periódicamente, y son actualizados para su mejor y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

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

5.3.4. Requisitos y frecuencia de actualización formativa

Se actualiza la formación del personal atendiendo a sus necesidades y con la frecuencia temporal suficiente para que los mismos puedan cumplir sus funciones y obligaciones de forma competente y satisfactoria, principalmente cuando se realicen modificaciones sustanciales de las tareas establecidas de certificación.

Los roles de confianza reciben como mínimo una vez al año actualizaciones formativas respecto nuevas amenazas y prácticas de seguridad.

5.3.5. Secuencia y frecuencia de rotación laboral

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

5.3.6. Sanciones para acciones no autorizadas

CIVITANA dispone de un régimen disciplinario, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7. Requisitos de contratación de personal

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por CIVITANA. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de confianza sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de confianza. CIVITANA será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de confianza por tercero distinto a CIVITANA.

5.3.8. Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4. Procedimientos de auditoría de seguridad

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

5.4.1. Tipo de eventos registrados

Se produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la CA a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la CA.
- Encendido y apagado de la aplicación de la CA.
- Cambios en los detalles de la CA y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Civitana: Declaración de Prácticas de Certificación

- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Autoridad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.
- Eventos relacionados con la sincronización, así como pérdida de esta en lo relativo a las fuentes fiables de tiempo usadas para proporcionar la marca de tiempo en los registros relativos a la Infraestructura de Clave Pública para la prestación de los servicios.
- Eventos relacionados con caídas de los servicios proporcionados mediante la Infraestructura de Clave Pública.
- Eventos relacionados con la mal función de los equipos usados en lo relativo a la prestación de servicios de confianza.
- Eventos relacionados con los cortafuegos vinculados a la Infraestructura de Clave Pública.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

5.4.2. Frecuencia de procesamiento de logs

Además de lo anterior, se realiza una revisión de los logs cuando existe una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.

Civitana: Declaración de Prácticas de Certificación

- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una base de datos para su posterior exploración.

5.4.3. Periodo de retención de registros de auditoría

CIVITANA almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

No obstante lo anterior, los registros de auditoría que tengan relación con la gestión del ciclo de vida de los certificados electrónicos se conservarán por el periodo máximo de 15 años desde la extinción del certificado.

5.4.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la CA.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5. Procedimiento de copia de respaldo

Se dispone de un procedimiento adecuado de copia de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de seguridad de los logs.

Sumado a lo anterior, tiene implementado un procedimiento de copia de seguridad seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6. Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de CIVITANA.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5. Archivos de registros

5.5.1. Tipo de registros archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por CIVITANA (o por las Autoridades de registro):

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Autoridad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación.
- Todos los datos de auditoría identificados en la sección 5.4.
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

CIVITANA y/o las Autoridades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

5.5.2. Periodo de retención del archivo

CIVITANA archiva los registros especificados anteriormente durante al menos 15 años, o el período que establezca la legislación vigente.

En particular, los registros de certificados revocados estarán accesibles para su libre consulta durante al menos 15 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3. Protección del archivo

Se protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable, asegurando la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.5.4. Procedimientos de copias de seguridad del archivo

Se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

Respecto de los documentos electrónicos, se realizan copias de respaldo incrementales diarias de todos los documentos y copias de respaldo completas semanalmente para casos de recuperación de datos.

5.5.5. Requisitos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

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

5.5.7. Procedimientos para obtener y verificar la información del archivo

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Además, proporciona la información y medios de verificación al auditor.

5.6. Cambio de claves de la CA

Con anterioridad a que el uso de la clave privada de la Autoridad de Certificación caduque, será realizado un cambio de claves. La antigua CA y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha CA.

Se generará una nueva CA con una clave privada nueva y un nuevo DN. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Alternativamente, en el caso de Autoridades de Certificación subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves, no resultando aplicable el procedimiento antes descrito.

5.7. Compromiso de claves y recuperación ante desastres

5.7.1. Procedimientos de gestión de incidentes y compromisos de seguridad

CIVITANA ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de CIVITANA.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de CIVITANA se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.7.4. Continuidad del negocio después de un desastre

Deberán restablecerse los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

Se dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.7.5. Notificación de incidentes al Organismo Supervisor Nacional en materia de servicios de confianza

De conformidad con el Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS), CIVITANA notificará cualquier vulneración de la seguridad o pérdida de integridad que afecte a la prestación de servicios de confianza en un plazo de 24 horas desde que tenga conocimiento de la misma, a la autoridad de supervisión competente, independientemente de la denominación que ostente en cada momento.

Asimismo, se respetarán los mismos plazos para cualquier vulneración de la seguridad o pérdida de integridad que afecte al servicio de identificación por vídeo, así como el contenido de las notificaciones iniciales y posteriores.

Las notificaciones se realizarán de conformidad con los procedimientos y protocolos internos establecidos para la gestión y comunicación de incidentes de seguridad, garantizando una comunicación oportuna, completa y coherente a la autoridad competente y, en su caso, a los interesados afectados. Asimismo, CIVITANA cumplirá con los protocolos, formatos y canales de comunicación establecidos por la autoridad nacional de control, así como con cualquier requisito adicional que esta pueda emitir en relación con la notificación de incidentes.

5.7.6. Notificación a la Autoridad Nacional de Protección de Datos

En cumplimiento del 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 (Reglamento General de Protección de Datos - RGPD), cuando los datos personales puedan verse comprometidos debido a una brecha de seguridad, CIVITANA, como responsable del tratamiento, notificará a la Agencia Española de Protección de Datos (AEPD) en un plazo de 72 horas desde que tenga conocimiento de la brecha. Además de lo dispuesto en el apartado de Notificación a los Interesados, CIVITANA notificará a los interesados afectados si la brecha supone un alto riesgo para sus derechos y libertades.

Se respetarán los mismos plazos para cualquier brecha de seguridad o pérdida de integridad que afecte al servicio de Videoidentificación, así como para el contenido de la notificación.

Las notificaciones se realizarán de acuerdo con los procedimientos y protocolos internos establecidos para la gestión y comunicación de incidentes de seguridad, garantizando una comunicación oportuna, completa y coherente a la autoridad competente y, en su caso, a los interesados afectados. Asimismo, CIVITANA cumplirá con los protocolos, formatos y canales de comunicación establecidos por la AEPD, así como con cualquier requisito adicional que esta pueda emitir en relación con la notificación de incidentes.

5.8. Terminación de la CA

CIVITANA asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación. En este sentido, CIVITANA garantiza un mantenimiento continuo de los registros definidos en el apartado 5.5.1, por el tiempo establecido en el apartado 5.5.2 de esta Declaración de Prácticas de Certificación.

No obstante lo anterior, si procede CIVITANA ejecutará todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

Antes de terminar sus servicios, se ha realizado el desarrollo de un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras CA con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la CA en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la CA.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos. La información sobre el estado de revocación se mantendrá conforme lo establecido en esta DPC o bien se dará traslado a un tercero.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los periodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Comunicará al Organismo Supervisor Nacional, con una antelación mínima de 3 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también al Organismo Supervisor Nacional, la apertura de cualquier proceso concursal que se siga contra CIVITANA, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6. Controles de seguridad técnica

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

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

El par de claves de las Autoridades de Certificación Subordinadas (**NOMBRE CAS**), es creada por la Autoridad de Certificación Raíz (**NOMBRE RAIZ**) de acuerdo con los procedimientos de ceremonia de CIVITANA, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por CIVITANA.

Para la generación de la clave de las Autoridades de Certificación de la jerarquía de CIVITANA, se han utilizado los siguientes dispositivos.

- Dispositivo Raíz

QSCD SubCA

- SAM SubCA

Raíz	Algoritmo	Años
Sub 1		
Sub 2		
Entidad final		

CIVITANA no emitirá certificados de entidad final cuya duración exceda de la vida útil del certificado de la Autoridad de Certificación Subordinada.

La presente DPC, así como el texto divulgativo (PDS) de todos los perfiles de certificados indicados en el presente documento se encuentran disponible en este enlace: [**Enlace repositorio**]

6.1.2. Generación del par de claves del firmante

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o software autorizado por CIVITANA.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.3. Envío de la clave privada al firmante

La clave privada de los certificados de entidad final se genera y se almacena debidamente protegida en el interior de los dispositivos cualificados de creación de firma (QSCD). La clave privada del firmante se genera en un área privada del firmante en un HSM remoto. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

6.1.4. Envío de la clave pública al emisor del certificado.

El método de remisión de la clave pública al prestador de servicios electrónicos de confianza es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado.

6.1.5. Distribución de la clave pública del prestador de servicios de confianza

Las claves son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las Autoridades de Certificación Raíz y Subordinadas estarán a disposición de los usuarios en la página web de CITIVANA.

6.1.6. Tamaños de claves

La longitud de las claves de la Autoridad de Certificación raíz es de 4096 bits utilizando RSA.

La longitud de las claves de las Autoridad de Certificación subordinadas es de 521 bits utilizando ECDSA.

La longitud de las claves de los Certificados de Entidad final es de 256 bits utilizando ECDSA.

6.1.7. Parámetros de generación de la clave pública

La clave pública de la Autoridades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280. Adicionalmente, CIVITANA sigue las directrices de interoperabilidad definidas en el estándar, incluyendo los límites máximos de caracteres en los campos de los certificados. No se han definido restricciones adicionales o más estrictas que las indicadas en RFC 5280.

6.1.8. Comprobación de calidad de parámetros de clave pública

Longitud del Módulo = 4096 bits

Algoritmo de generación de claves: rsagen1

Funciones criptográficas de Resumen: SHA-512.

6.1.9. Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital, el no repudio y cifrado de la clave.

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de CIVITANA y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

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

Se requiere un control multi-persona para la activación de la clave privada de la CA. En el caso de esta Declaración de Prácticas de Certificación, en concreto existe una política de 3 de 5 personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3. Depósito de la clave privada

No se realiza el almacenamiento de copias utilizables por medios propios de las claves privadas de los firmantes.

6.2.4. Copia de respaldo de la clave privada

Se realiza copia de seguridad o respaldo de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Sólo es posible realizar backups de un bloob cifrado con la clave Security World del HSM utilizado, siendo imposible su descifrado sin el uso de las credenciales que sólo el titular del certificado conoce.

6.2.5. Archivado de la clave privada

Las claves privadas de las CA son archivadas por un periodo de 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las CA en el dispositivo criptográfico inicial.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción.

Las claves privadas de la Autoridad de Certificación se almacenan cifradas en los módulos criptográficos de producción.

6.2.7. Método de activación de la clave privada

La clave privada de CIVITANA se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas autorizadas de acuerdo con esta Declaración de Prácticas de Certificación.

Las claves de la CA se activan por un proceso de m de n (3 de 5). La activación de las claves privadas de la CA Subordinada es gestionada con el mismo proceso de m de n que las claves de la CA.

6.2.8. Método de desactivación de la clave privada

Para la desactivación de la clave privada se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

6.2.9. Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de CIVITANA. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Respecto a las claves privadas de los firmantes se procederá acorde a los establecido en el plan de cese.

6.2.10. Clasificación del módulo criptográfico

Según indicado en el apartado 6.2.1 del presente documento

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

Las claves públicas son archivadas de forma rutinaria, atendiendo a lo establecido en la sección 5.5 del presente documento.

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

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada. Asimismo, se generan de forma segura los datos de activación.

6.4.2. Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de subordinadas, están protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves. Los datos de activación del dispositivo que protege la raíz, se encuentra protegido por una clave maestra resguardada por custodios, tal y como se documenta en la ceremonia de claves.

Los datos de activación de las claves privadas de los certificados de entidad corresponden al firmante del certificado, quien es el responsable de la protección de su clave privada, con una o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

6.5. Controles de seguridad informática

Se emplean sistemas fiables para ofrecer sus servicios de confianza. Para atender a este fin, se han realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Civitana: Declaración de Prácticas de Certificación

Respecto a la seguridad de la información, CIVITANA aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1. Requisitos técnicos específicos de seguridad informática

Cada servidor de incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las Autoridades de Certificación subordinadas y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las Autoridades de Certificación subordinadas.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Evaluación de nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por CIVITANA son fiables.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por CIVITANA de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

Civitana: Declaración de Prácticas de Certificación

CIVITANA realiza la revisión de las configuraciones y del estado de sus sistemas conforme a su control operacional, estableciendo una periodicidad en función de la criticidad del activo y del sistema, que como mínimo será anual. Dichas revisiones quedan documentadas y forman parte del proceso de mejora continua de la seguridad de CIVITANA.

6.6.2. Controles de gestión de la seguridad

CIVITANA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos, son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

CIVITANA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de confianza.

6.6.2.1. Clasificación y gestión de información y bienes

CIVITANA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.6.2.2. Operaciones de gestión

Se dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad se desarrolla en detalle el proceso de gestión de incidencias.

CIVITANA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Civitana: Declaración de Prácticas de Certificación

6.6.2.4. Planificación del sistema

El departamento de Sistemas mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.6.2.5. Reportes de incidencias y respuesta

Se dispone de un procedimiento para realizar el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.6. Procedimientos operacionales y responsabilidades

Se definen las actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.7. Gestión del sistema de acceso

Deben realizarse todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular, la Autoridad de Certificación

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- CIVITANA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- CIVITANA dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal es responsable de sus actos mediante el compromiso de confidencialidad firmado con CIVITANA.

6.6.2.8. Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de CIVITANA.

6.6.2.9. Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador.

6.6.2.10. Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.11. Gestión del ciclo de vida del hardware criptográfico

CIVITANA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

Se registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Además de ello, se realizan test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema, así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7. Controles de seguridad de red

CIVITANA protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8. Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas son realizadas en módulos con las certificaciones FIPS 140-3 nivel 3 o Common Criteria EAL4+ o superior.

6.9. Fuente de tiempo

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

6.10. Cambio de estado de un Dispositivo Seguro de Creación de Firma (QSCD)

En el caso de modificación del estado de la certificación de los dispositivos cualificados de creación de firma (QSCD), se procederá de la siguiente manera:

1. Se dispone de una lista de varios QSCD certificados, así como una estrecha relación con proveedores de dichos dispositivos, con el fin de garantizar alternativas a posibles pérdidas de estado de certificación de dispositivos QSCD.
2. En el supuesto de finalización del periodo de validez o pérdida de la certificación, no se utilizarán dichos QSCD para la emisión de nuevos certificados digitales, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.
3. Procederá de inmediato a cambiar a dispositivos QSCD con certificación válida.
4. En el supuesto caso que un dispositivo QSCD haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, se procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados digitales emitidos en estos dispositivos y reemplazarlos emitiéndolos en QSCD válidos.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 5280 y las siguientes normas: ETSI EN 319 412-2 para los certificados emitidos a personas físicas y ETSI EN 319 412-5 para la definición de los QcStatements de los certificados electrónicos cualificados según el Reglamento eIDAS.

7.1.1. Número de versión

Los certificados emitidos bajo la presente Declaración de Prácticas de Certificación utilizan el estándar X.509 versión 3.

7.1.2. Extensiones de certificado

Las extensiones de los certificados se encuentran desarrolladas en los propios certificados.

7.1.3. Identificadores de objeto de algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Formatos de nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5. Restricciones de nombres

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que son únicos y no ambiguos.

7.1.6. Identificador de objeto de política de certificado

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.2.

7.1.7. Empleo de la extensión restricciones de política

No se emplean restricciones de política.

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión Certificate Policies contiene los siguientes calificadores de política:

- CPS Pointer: contiene la URL a la Declaración de Prácticas de Certificación de CIVITANA.
- User notice: Texto para que el usuario pueda visualizar la información del certificado.
- Policy Identifier: Indica el OID del certificado User Notice común a todos los certificados.

7.1.9. Tratamiento semántico para la extensión “certificate policy”

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

7.2. Perfil de la lista de revocación de certificados

Las CRL emitidas por CIVITANA son conformes a la norma RFC 58280

Las CRL emitidas por CIVITANA son de la versión 2.

7.3. Perfil OCSP

Las respuestas OCSP de CIVITANA 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.

8. Auditorías de cumplimiento

CIVITANA realiza auditorías de conformidad para asegurar el cumplimiento y adecuación con las políticas, normativas, planes y procedimientos de seguridad del sistema de gestión de seguridad de la información. Como resultado de estas se elaboran planes de acciones correctivas como respuesta a las no conformidades y desviaciones detectadas.

CIVITANA realiza auditorías de conformidad del Reglamento eIDAS por medio de evaluaciones de conformidad anuales sobre el servicio de expedición de certificados electrónicos cualificados de firma electrónica.

Los controles para la realización de las auditorías de cumplimiento se basan en las siguientes guías de referencia:

- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates.

8.1. Frecuencia de auditoria

CIVITANA realiza evaluaciones de conformidad eIDAS con carácter bienal, además de revisiones anuales

8.2. Cualificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3. Relación del auditor con la empresa auditada

Los auditores internos o externos responsables de ejecutar las auditorías son independientes funcionalmente del servicio de producción objeto de auditoría.

8.4. Elementos objeto de auditoría

La auditoría verifica respecto a CIVITANA:

- a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
- b) Que la entidad cumple con los requerimientos de la Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados electrónicos.
- c) Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por CIVITANA y con lo establecido en la normativa vigente.

Civitana: Declaración de Prácticas de Certificación

- d) Que la entidad gestiona de forma adecuada sus sistemas de información.

En particular, los elementos objeto de auditoría serán los siguientes:

- a) Procesos de las Autoridades de Certificación, Autoridades de Registro y elementos relacionados.
- b) Sistemas de información.
- c) Protección del centro de proceso de datos.
- d) Documentos.

8.5. Toma de decisiones como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si CIVITANA es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad de CIVITANA que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Autoridad de Certificación y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Certificación.
- Otras acciones complementarias que resulten necesarias.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de CIVITANA en un plazo máximo de 15 días tras la ejecución de la auditoría, para su análisis y tratamiento. Si a causa de la auditoría realizada fuera necesaria la revocación de certificados, este informe servirá como justificante de dicha revocación.

9. Otros asuntos legales y de actividad

9.1. Tarifas

9.1.1. Tarifas de emisión o renovación de certificados

CIVITANA puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2. Tarifas de acceso a los certificados

CIVITANA no ha establecido ninguna tarifa por el acceso a los certificados.

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

CIVITANA no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4. Tarifas para otros servicios

Sin estipulación.

9.1.5. Política de reintegro

Sin estipulación.

9.2. Responsabilidad financiera

CIVITANA dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401 7.12 c), en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1. Seguro de responsabilidad civil

CIVITANA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo con la normativa vigente aplicable.

9.2.2. Otros activos

Sin estipulación.

9.2.3. Seguros y garantías para entidades finales

CIVITANA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, para los servicios electrónicos de confianza, con un mínimo asegurado de 3.000.000 de euros.

9.3. Confidencialidad de la información

9.3.1. Alcance de la información confidencial

Las siguientes informaciones son mantenidas confidenciales por CIVITANA:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- 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 la Autoridad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2. Información que no está dentro del alcance

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

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Autoridad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- 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.

Civitana: Declaración de Prácticas de Certificación

- Las listas de revocación de certificados (CRL), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

CIVITANA divulga la información confidencial únicamente en los casos legalmente previstos.

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 un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

CIVITANA indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5. Divulgación de información por petición de su titular

CIVITANA incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de datos de carácter personal

CIVITANA garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales, reflejada en el Reglamento Europeo nº2016/679 General de Protección de Datos y en general cualquier normativa nacional que resulte de aplicación.

En cumplimiento de esta, CIVITANA ha documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad y organizativos, con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

A continuación, se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por CIVITANA:

9.4.1. Responsable del tratamiento

Civitana

NIF: G72932239

Dirección: Calle Lanzada número 33, 28008 de Madrid, España

Correo electrónico: **TBD**

9.4.2. Finalidad del tratamiento

CIVITANA trata los datos de carácter personal facilitados para llevar a cabo los servicios electrónicos solicitados, concretamente la expedición de certificados electrónicos, todo ello de acuerdo con lo previsto en esta Declaración de Prácticas de Certificación de CIVITANA, la cual se encuentra disponible en el siguiente enlace: **[Enlace repositorio]**.

Las finalidades de tratamiento de datos relativos a los servicios de confianza son las siguientes:

- Identificación de los suscriptores y/o firmantes de los certificados electrónicos.
- Expedición y gestión de certificados electrónicos.
- Gestión del ciclo de vida del certificado (suspensión, renovación, reactivación y revocación).
- Comunicaciones relativas al servicio.
- Custodia y mantenimiento del archivo relativo al certificado electrónico.
- Gestión administrativa, contable y de facturación derivada de la contratación.

9.4.3. Legitimación del tratamiento

La legitimación del tratamiento de datos personales para la Prestación de Servicios de Confianza para la expedición de certificados electrónicos, se basa en la ejecución de un contrato de los servicios solicitados, donde el usuario es parte del mismo.

La legitimación del tratamiento para atender las consultas y solicitudes se basa en el consentimiento del interesado, el cual lo presta expresa e inequívocamente, mediante acción positiva y previa al envío, al aceptar las condiciones y la política de privacidad. Dicho consentimiento puede ser retirado en cualquier momento mediante el envío de un correo electrónico a **TBD**.

9.4.4. Datos tratados y conservación

Las categorías de datos personales tratados por CIVITANA, a título enunciativo pero no limitativo, comprenden:

- Datos identificativos: nombre, apellidos y número oficial de identidad.
- Datos de contacto: dirección postal, correo electrónico y número de teléfono.
- Datos relativos a la identidad o identificación de los usuarios: videos, fotografías y/o cuando corresponda el patrón biométrico facial, con la finalidad de poder llevar a cabo el proceso de vídeo identificación de CIVITANA.

Civitana: Declaración de Prácticas de Certificación

Los datos personales se conservarán hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso. Como norma general, los datos personales relativos al SERVICIO se conservarán durante 15 años desde la revocación del certificado correspondiente.

Asimismo, las pruebas de los procesos de identificación se conservarán 15 años, a excepción de aquellas pruebas incompletas las cuales se conservarán un tiempo mínimo 5 años.

Los datos personales se almacenarán en las instalaciones seguras ubicadas en España.

9.4.5. Transferencia de datos

Los datos pueden ser puestos a disposición de terceros, dentro del territorio de la Unión Europea, con motivo de la prestación de servicios contratados por el usuario (por ejemplo proveedores de alojamiento de datos (CPD), servicios de apoyo en la identificación, etc.), todo ello al amparo del correspondiente contrato de encargo de tratamiento de datos personales, garantizando en todo momento unas medidas de seguridad idóneas que aseguren la debida protección de los datos personales de los usuarios.

Sin perjuicio de lo anterior, como norma general los datos personales únicamente se cederán a terceros bajo obligación legal.

Como norma general, no se realizarán transferencias internacionales.

9.4.6. Derechos de los usuarios

Los usuarios podrán ejercitar sus derechos de confirmación, acceso, rectificación, supresión, cancelación, limitación, oposición y portabilidad.

- Confirmación. Todos los usuarios tienen derecho a obtener confirmación sobre si CIVITANA está tratando datos personales que les conciernan.
- Acceso y rectificación. Los usuarios tienen derecho a acceder a todos sus datos personales, así como solicitar la rectificación de aquellos que sean inexactos o erróneos.
- Supresión y cancelación. Los usuarios podrán solicitar la supresión/cancelación de los datos cuando, entre otros motivos, éstos no sean necesarios para los fines para los que fueron recogidos.
- Limitación y oposición. El usuario podrá solicitar la limitación del tratamiento para que sus datos personales no se apliquen en las operaciones que correspondan. En determinadas circunstancias y por motivos relacionados con su situación particular, el usuario podrá oponerse al tratamiento de datos, estando CIVITANA obligada a dejar de tratarlos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.
- Portabilidad. Los interesados podrán solicitar que sus datos personales les sean enviados o bien se transmitan a otro responsable, en un formato electrónico estructurado y de uso habitual.

Civitana: Declaración de Prácticas de Certificación

Para ejercer sus derechos, los usuarios pueden enviar una petición a la dirección de correo electrónico **TBD** o bien dirigir un escrito a la dirección indicada en el apartado de información del Responsable del tratamiento. En dicha petición, deberán adjuntar copia de su documento de identidad e indicar claramente cuál es el derecho que se desea ejercer.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Únicamente CIVITANA goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por CIVITANA contienen un aviso legal relativo a la propiedad de estos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2. Propiedad de la Declaración de Prácticas de Certificación

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

9.5.3. Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado, conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (DN) del certificado, formado por las informaciones especificadas en la sección 3 de este documento.

9.5.4. Propiedad de claves y material relacionado

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

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y garantías

9.6.1. Obligaciones de CIVITANA

CIVITANA garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

CIVITANA presta los servicios electrónicos de confianza conforme con esta Declaración de Prácticas de Certificación.

CIVITANA informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS, cumple el contenido del anexo A de la ETSI EN 319 411-1, documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

CIVITANA vincula a suscriptores, poseedores de claves y terceros que confían en certificados, mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Autoridad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.3.
- 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, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Autoridad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Autoridad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Autoridad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en los certificados

CIVITANA, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

CIVITANA, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

CIVITANA, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, CIVITANA garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo lo previsto en la Ley 6/2020, de 11 de noviembre.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan.

9.6.3. Rechazo de otras garantías

CIVITANA rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Limitación de responsabilidades

CIVITANA limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Autoridad de Certificación.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

CIVITANA incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Autoridad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Autoridad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de dominio), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

CIVITANA incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Autoridad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6. Caso fortuito y fuerza mayor

CIVITANA no será responsable en ningún caso bajo situaciones que incurran en caso fortuito y en caso de fuerza mayor.

Se entiende por caso fortuito como aquella situación o suceso que sea imposible de prever, o que, previsto, sea inevitable respecto de su mitigación. Adicionalmente, se entiende por fuerza mayor aquellas situación o suceso que es inevitable de hacer efectivas sus circunstancias, imprevisible y extraordinario en su origen, emanante de un ámbito ajeno e irresistible.

Civitana: Declaración de Prácticas de Certificación

Por ello, CIVITANA no será responsable bajo ningún concepto en situación de guerra, desastres naturales, funcionamiento disfuncional de servicios eléctricos, redes o infraestructura informática, por causa no imputable a CIVITANA.

9.6.7. Ley aplicable

CIVITANA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

CIVITANA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Autoridad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9. Cláusula de jurisdicción competente

CIVITANA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

CIVITANA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.