

# Declaración de Prácticas de Certificación Certificados Notariales

Versión: 3.5

Vigencia: 08/04/2021



## Información general

### Control documental

|                       |  |
|-----------------------|--|
| Proyecto:             | <b>Declaración de Prácticas de Certificación clase Certificados Notariales</b> |
| Entidad de destino:   | <b>Agencia Notarial de Certificación, S.L.U.</b>                               |
| Código de referencia: |  |
| Versión:              | <b>3.5</b>   |
| Fecha de la edición:  | <b>24/12/2020</b>  |
| Archivo:              | <b>DPC_NOT_V2_20210408_REV.docx</b>  |
| Formato:              | <b>Word 2019</b>   |

### Control de versiones

| Versión | Partes que cambian  | Descripción del cambio  | Fecha cambio | Fecha publicación |
|---------|---|---|--------------|-------------------|
| 2.1     | Original  | Creación del documento  | 27/03/2010   |                   |
| 2.2     |   | Revisión del documento  | 05/05/2010   |                   |
| 2.3     | Certificado Notarial de Servidor Seguro                     | Eliminación de la referencia a las cláusulas EV en los certificados de servidor seguro  | 10/05/2010   |                   |
| 2.4     | 1.3.1   | Incorporación de las huellas digitales de los certificados de las CA  | 02/06/2010   |                   |
| 2.5     | Logo ANCERT   | Nuevo logo ANCERT   | 30/11/2010   |                   |
| 2.6     |   | Revisión de aspectos legales y formato  | 21/12/2010   | 01/01/2011        |
| 2.7     | Secciones 1.4.2.2, 4.9.2, 4.9.3, 5.5.2<br><br>Sección 4.9.6 | Adaptación a los nuevos requisitos para la aceptación de los certificados de firma de código en los programas de Root CA. CRL con 60 días de información histórica. | 30/01/2011   | 01/03/2011        |
| 2.8     | Secciones 4.1, 6.3.1, 6.9.3, 6.9.6, 6.9.9, 7.7.5 y 11.2     | Adecuación controles AICPA/CICA WebTrust Program for CA v 2   | 01/06/2012   | 01/10/2012        |
| 2.9     | Sección 8.2   | Adecuación de algunos puntos de los controles de protección de la clave privada a los requisitos AICPA/CICA WebTrust Program for CA v 2                             | 29/09/2014   | 03/11/2014        |
| 3.0     | Secciones 3.1.2 y 5.1.6                                     | Adecuación a los requisitos del CA/Browser Forum  | 24/11/2015   | 30/11/2015        |

|     |                   |   |            |            |
|-----|-------------------|---|------------|------------|
| 3.1 | Todo el documento | Adecuación de referencias al Reglamento (UE) 910/2014.<br>Nuevos certificados de las EC renovados.<br>Revisión de la sección 7.8 "Terminación del servicio".<br>Estipulación del tiempo máximo para resolver solicitudes de revocación.<br>Añadida descripción de los algoritmos de firma y parámetros utilizados.  | 04/05/2017 | 15/05/2017 |
| 3.2 | Todo el documento | Adecuación al Reglamento (UE) 2016/679 de tratamiento de datos personales.<br>Aclaración en la sección 5.1.2 sobre la identificación de certificados de pruebas.<br>Actualización a los requisitos del CA/Browser Forum versión 1.5.1.  | 15/05/2018 | 25/05/2018 |
| 3.3 | Todo el documento | Certificado Notarial de Sello Electrónico.<br>LOPDP 3/2018  | 01/04/2019 | 03/05/2019 |
| 3.4 | Todo el documento | Adecuación de la estructura al RFC 3647.<br>Definición del periodo de actualización de las DPCs y actualización del procedimiento de revisión de la DPC. (secciones 1.1.5 y 9.12)<br>El histórico de la información de estado de los certificados pasa a proporcionarse por OCSP (sección 4.9.10) en lugar de en la CRL en el que solo se mantienen 60 días.<br>Provisión de información de estado en caso de compromiso o terminación de la entidad (secciones 5.7.3.2 y 5.8.) | 12/02/2020 | 06/04/2020 |
| 3.5 | Todo el documento | Adaptación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza<br>Se traslada a la sección 3.4.2 el requisitos de validación de los registros DNS de tipo CAA para la emisión de certificados SSL.  | 24/12/2020 | 08/04/2021 |

## Índice

|  |    |
|--|----|
| Información general.....   | 2  |
| Control documental.....  | 2  |
| Control de versiones .....   | 2  |
| Índice .....   | 4  |
| 1. Introducción.....   | 13 |
| 1.1. Presentación .....  | 13 |
| 1.1.1. Certificados Notariales .....   | 13 |
| 1.1.2. Certificados que se emiten.....   | 13 |
| 1.2. Nombre del documento e identificación.....  | 17 |
| 1.3. Participantes en los servicios de certificación.....                                | 18 |
| 1.3.1. Autoridades de certificación.....   | 19 |
| 1.3.2. Entidades de registro .....   | 20 |
| 1.3.3. Entidades finales.....  | 21 |
| 1.4. Uso de los certificados.....  | 23 |
| 1.4.1. Usos permitidos para los certificados.....  | 23 |
| 1.5. Administración del documento .....  | 25 |
| 1.5.1. Organización que administra el documento.....                                     | 25 |
| 1.5.2. Datos de contacto de la organización.....   | 25 |
| 1.5.3. Responsable de adecuación de la Declaración de Prácticas de Certificación.....    | 25 |
| 1.5.4. Procedimiento de aprobación de la Declaración de Prácticas de Certificación ..... | 26 |
| 1.5.5. Frecuencia de revisión .....  | 26 |
| 1.6. Definiciones y acrónimos.....   | 26 |
| 1.6.1. Definiciones .....  | 26 |
| 1.6.2. Acrónimos .....   | 27 |
| 2. Publicación de información y depósito de certificados.....                            | 29 |
| 2.1. Depósito(s) de certificados.....  | 29 |
| 2.2. Publicación de información del prestador de servicios de certificación .....        | 29 |
| 2.3. Frecuencia de publicación.....  | 29 |
| 2.4. Control de acceso .....   | 29 |
| 3. Identificación y autenticación.....   | 31 |

|  |    |
|--|----|
| 3.1. Gestión de nombres .....  | 31 |
| 3.1.1. Tipos de nombres.....   | 31 |
| 3.1.2. Significado de los nombres.....   | 31 |
| 3.1.3. Empleo de anónimos y seudónimos .....   | 31 |
| 3.1.4. Interpretación de formatos de nombres .....   | 31 |
| 3.1.5. Unicidad de los nombres .....   | 40 |
| 3.1.6. Resolución de conflictos relativos a nombres y tratamiento de marcas registradas... | 40 |
| 3.2. Validación inicial de la identidad.....   | 41 |
| 3.2.1. Prueba de posesión de clave privada .....   | 41 |
| 3.2.2. Autenticación de la identidad de la organización .....                              | 41 |
| 3.2.3. Autenticación de la identidad de la persona física .....                            | 42 |
| 3.2.4. Autenticación de la identidad de sistemas de información .....                      | 43 |
| 3.2.5. Información de suscriptor no verificada.....  | 43 |
| 3.3. Identificación y autenticación de solicitudes de renovación con cambio de claves..... | 43 |
| 3.3.1. Validación para la renovación rutinaria de certificados .....                       | 43 |
| 3.3.2. Validación para la renovación de certificados tras la revocación .....              | 44 |
| 3.4. Identificación y autenticación de las solicitudes de cambio de estado.....            | 44 |
| 3.4.1. Identificación y autenticación de la solicitud de suspensión.....                   | 44 |
| 3.4.2. Identificación y autenticación de la solicitud de revocación .....                  | 44 |
| 4. Requisitos de operación del ciclo de vida de los certificados .....                     | 45 |
| 4.1. Solicitud de emisión de certificado.....  | 45 |
| 4.1.1. Legitimación para solicitar la emisión.....   | 45 |
| 4.1.2. Procedimiento de alta: Responsabilidades.....                                       | 46 |
| 4.2. Procesamiento de la solicitud de certificación .....                                  | 46 |
| 4.2.1. Ejecución de las funciones de identificación y autenticación .....                  | 46 |
| 4.2.2. Aprobación o rechazo de la solicitud .....  | 47 |
| 4.2.3. Plazo para resolver la solicitud .....  | 47 |
| 4.3. Emisión del certificado.....  | 47 |
| 4.3.1. Acciones durante el proceso de emisión .....  | 47 |
| 4.3.2. Notificación de la emisión al suscriptor.....                                       | 49 |
| 4.4. Entrega y aceptación del certificado.....   | 49 |
| 4.4.1. Conducta que constituye aceptación del certificado.....                             | 50 |

|  |    |
|--|----|
| 4.4.2. Publicación del certificado.....  | 50 |
| 4.4.3. Notificación de la emisión a terceros .....                                 | 50 |
| 4.5. Uso del par de claves y del certificado .....                                 | 51 |
| 4.5.1. Uso por el suscriptor y, en su caso, poseedor de claves .....               | 51 |
| 4.5.2. Uso por el tercero que confía en certificados.....                          | 52 |
| 4.6. Renovación de certificados .....  | 53 |
| 4.7. Renovación de certificados con cambio de claves .....                         | 53 |
| 4.7.1. Causas de renovación de claves y certificados .....                         | 53 |
| 4.7.2. Legitimación para solicitar la renovación .....                             | 54 |
| 4.7.3. Procesamiento de la solicitud de renovación .....                           | 54 |
| 4.7.4. Notificación de la emisión del certificado renovado .....                   | 54 |
| 4.7.5. Conducta que constituye aceptación del certificado.....                     | 54 |
| 4.7.6. Publicación del certificado.....  | 54 |
| 4.7.7. Notificación de la emisión a terceros .....                                 | 54 |
| 4.8. Modificación de certificados .....  | 54 |
| 4.9. Revocación y suspensión de certificados .....                                 | 54 |
| 4.9.1. Causas de revocación de certificados.....                                   | 54 |
| 4.9.2. Legitimación para solicitar la revocación .....                             | 56 |
| 4.9.3. Procedimientos de solicitud de revocación .....                             | 57 |
| 4.9.4. Plazo temporal de solicitud de revocación.....                              | 58 |
| 4.9.5. Plazo temporal para procesar las solicitudes de revocación.....             | 58 |
| 4.9.6. Obligación de consulta de información de revocación de certificados.....    | 58 |
| 4.9.7. Frecuencia de emisión de listas de revocación de certificados (CRLs) .....  | 58 |
| 4.9.8. Tiempo transcurrido entre la generación y la publicación de las CRLs .....  | 58 |
| 4.9.9. Disponibilidad de servicios de comprobación de estado de certificados ..... | 58 |
| 4.9.10. Requisitos de comprobación de revocación online .....                      | 59 |
| 4.9.11. Otras formas de información de revocación de certificados.....             | 59 |
| 4.9.12. Requisitos especiales en caso de compromiso de la clave privada .....      | 59 |
| 4.9.13. Causas de suspensión de certificados .....                                 | 59 |
| 4.9.14. Legitimación para solicitar la suspensión.....                             | 60 |
| 4.9.15. Procedimientos de petición de suspensión.....                              | 60 |
| 4.9.16. Plazo máximo de suspensión.....  | 60 |

|   |    |
|---|----|
| 4.9.17. Levantamiento de la suspensión .....  | 60 |
| 4.9.18. Notificación de la revocación o suspensión .....                            | 61 |
| 4.10. Servicios de comprobación de estado de certificados .....                     | 61 |
| 4.10.1. Características operativas de los servicios.....                            | 61 |
| 4.10.2. Disponibilidad de los servicios .....                                       | 61 |
| 4.10.3. Características opcionales.....   | 61 |
| 4.11. Finalización de la suscripción.....   | 61 |
| 4.12. Depósito y recuperación de claves.....  | 62 |
| 4.12.1. Política y prácticas de depósito y recuperación de claves .....             | 62 |
| 4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión..... | 62 |
| 5. Controles de seguridad física, de gestión y de operaciones .....                 | 63 |
| 5.1. Controles de seguridad física.....   | 63 |
| 5.1.1. Localización y construcción de las instalaciones .....                       | 64 |
| 5.1.2. Acceso físico .....  | 65 |
| 5.1.3. Electricidad y aire acondicionado.....                                       | 65 |
| 5.1.4. Exposición al agua.....  | 66 |
| 5.1.5. Prevención y protección de incendios.....                                    | 66 |
| 5.1.6. Almacenamiento de soportes.....  | 66 |
| 5.1.7. Tratamiento de residuos .....  | 66 |
| 5.1.8. Copia de respaldo fuera de las instalaciones .....                           | 66 |
| 5.2. Controles de procedimientos.....   | 67 |
| 5.2.1. Funciones fiables .....  | 67 |
| 5.2.2. Número de personas por tarea.....  | 68 |
| 5.2.3. Identificación y autenticación para cada función .....                       | 68 |
| 5.2.4. Roles que requieren separación de tareas .....                               | 68 |
| 5.3. Controles de personal.....   | 69 |
| 5.3.1. Requisitos de historial, calificaciones, experiencia y autorización.....     | 69 |
| 5.3.2. Procedimientos de investigación de historial.....                            | 70 |
| 5.3.3. Requisitos de formación .....  | 70 |
| 5.3.4. Requisitos y frecuencia de actualización formativa .....                     | 70 |
| 5.3.5. Secuencia y frecuencia de rotación laboral.....                              | 71 |
| 5.3.6. Sanciones para acciones no autorizadas .....                                 | 71 |

|  |    |
|--|----|
| 5.3.7. Requisitos de contratación de profesionales .....                                 | 73 |
| 5.3.8. Suministro de documentación al personal .....                                     | 74 |
| 5.4. Registros de auditoría .....  | 74 |
| 5.4.1. Tipos de eventos registrados .....  | 74 |
| 5.4.2. Frecuencia de tratamiento de registros de auditoría .....                         | 75 |
| 5.4.3. Periodo de conservación de registros de auditoría .....                           | 75 |
| 5.4.4. Protección de los registros de auditoría.....                                     | 75 |
| 5.4.5. Procedimientos de copia de respaldo de los registros de auditoría .....           | 76 |
| 5.4.6. Recolección de registros de auditoría.....  | 76 |
| 5.4.7. Notificación del evento de auditoría al causante del evento .....                 | 76 |
| 5.4.8. Análisis de vulnerabilidades .....  | 76 |
| 5.5. Archivo de registros .....  | 76 |
| 5.5.1. Tipos de registros archivados.....  | 76 |
| 5.5.2. Periodo de conservación de registros .....  | 77 |
| 5.5.3. Protección del archivo .....  | 77 |
| 5.5.4. Procedimientos de copia de respaldo.....  | 77 |
| 5.5.5. Requisitos de fecha y hora de los registros.....                                  | 78 |
| 5.5.6. Sistema de archivo .....  | 78 |
| 5.5.7. Procedimientos de obtención y verificación de información de archivo .....        | 78 |
| 5.6. Renovación de claves .....  | 78 |
| 5.7. Compromiso de claves y recuperación de desastre .....                               | 79 |
| 5.7.1. Procedimientos de gestión de incidencias .....                                    | 79 |
| 5.7.2. Corrupción de recursos, aplicaciones o datos .....                                | 79 |
| 5.7.3. Procedimiento ante compromiso de la clave privada .....                           | 79 |
| 5.7.4. Continuidad de negocio después de un desastre .....                               | 80 |
| 5.8. Terminación del servicio.....   | 81 |
| 6. Controles de seguridad técnica .....  | 82 |
| 6.1. Generación e instalación del par de claves .....                                    | 82 |
| 6.1.1. Generación del par de claves .....  | 82 |
| 6.1.2. Envío de la clave privada al suscriptor.....                                      | 82 |
| 6.1.3. Envío de la clave pública al emisor del certificado .....                         | 82 |
| 6.1.4. Distribución de la clave pública del prestador de servicios de certificación..... | 83 |



|  |    |
|--|----|
| 6.1.5. Tamaños de claves .....   | 83 |
| 6.1.6. Generación de parámetros de clave pública y verificación de calidad ..... | 83 |
| 6.1.7. Propósitos de uso de claves .....   | 83 |
| 6.2. Protección de la clave privada .....  | 83 |
| 6.2.1. Estándares de módulos criptográficos .....                                | 83 |
| 6.2.2. Control por más de una persona (n de m) sobre la clave privada .....      | 84 |
| 6.2.3. Custodia de la clave privada .....  | 84 |
| 6.2.4. Copia de respaldo de la clave privada.....                                | 84 |
| 6.2.5. Archivo de la clave privada .....   | 84 |
| 6.2.6. Tránsito de la clave privada a o desde el módulo criptográfico.....       | 84 |
| 6.2.7. Almacenamiento de la clave privada en el módulo criptográfico .....       | 85 |
| 6.2.8. Método de activación de la clave privada .....                            | 85 |
| 6.2.9. Método de desactivación de la clave privada.....                          | 85 |
| 6.2.10. Método de destrucción de la clave privada.....                           | 85 |
| 6.2.11. Clasificación de los módulos criptográficos.....                         | 85 |
| 6.3. Otros aspectos de gestión del par de claves.....                            | 86 |
| 6.3.1. Archivo de la clave pública .....   | 86 |
| 6.3.2. Periodos de utilización de las claves pública y privada.....              | 86 |
| 6.4. Datos de activación .....   | 86 |
| 6.4.1. Generación e instalación de datos de activación.....                      | 86 |
| 6.4.2. Protección de datos de activación .....                                   | 86 |
| 6.4.3. Otros aspectos de los datos de activación .....                           | 86 |
| 6.5. Controles de seguridad informática.....                                     | 87 |
| 6.5.1. Requisitos técnicos específicos de seguridad informática.....             | 87 |
| 6.5.2. Evaluación del nivel de seguridad informática.....                        | 87 |
| 6.6. Controles técnicos del ciclo de vida.....                                   | 88 |
| 6.6.1. Controles de desarrollo de sistemas.....                                  | 88 |
| 6.6.2. Controles de gestión de seguridad .....                                   | 88 |
| 6.6.3. Controles de seguridad del ciclo de vida .....                            | 88 |
| 6.7. Controles de seguridad de red .....   | 88 |
| 6.8. Fuente de tiempo .....  | 88 |
| 7. Perfiles de certificados y listas de certificados revocados.....              | 89 |

|  |    |
|--|----|
| 7.1. Perfil de certificado.....  | 89 |
| 7.1.1. Número de versión .....   | 89 |
| 7.1.2. Extensiones de certificado.....   | 89 |
| 7.1.3. Identificadores de objeto de algoritmos.....                                    | 89 |
| 7.1.4. Formatos de nombres .....   | 90 |
| 7.1.5. Restricciones de nombres.....   | 90 |
| 7.1.6. Identificador de objeto de política de certificado.....                         | 90 |
| 7.1.7. Empleo de la extensión restricciones de política.....                           | 90 |
| 7.1.8. Sintaxis y semántica de los calificadores de política.....                      | 90 |
| 7.1.9. Semántica del proceso de la extensión de la política de certificado .....       | 90 |
| 7.2. Perfil de la lista de revocación de certificados.....                             | 90 |
| 7.2.1. Número de versión .....   | 90 |
| 7.2.2. Lista de revocación de certificados y extensiones de elementos de la lista..... | 90 |
| 7.3. Perfil OCSP.....  | 91 |
| 7.3.1. Número de versión .....   | 91 |
| 7.3.2. Extensiones del OCSP .....  | 91 |
| 8. Auditoría de conformidad.....   | 92 |
| 8.1. Frecuencia de la auditoría.....   | 92 |
| 8.2. Identificación y calificación del auditor .....                                   | 92 |
| 8.3. Relación del auditor con la entidad auditada.....                                 | 92 |
| 8.4. Listado de elementos objeto de auditoría.....                                     | 92 |
| 8.5. Acciones a emprender como resultado de una falta de conformidad .....             | 92 |
| 8.6. Comunicación de los resultados.....   | 93 |
| 9. Otros asuntos legales y de actividad .....  | 94 |
| 9.1. Tarifas .....   | 94 |
| 9.1.1. Tarifa de emisión o renovación de certificados.....                             | 94 |
| 9.1.2. Tarifa de acceso a certificados.....  | 94 |
| 9.1.3. Tarifa de acceso a información de estado de certificado.....                    | 94 |
| 9.1.4. Tarifas de otros servicios .....  | 94 |
| 9.1.5. Política de reintegro.....  | 94 |
| 9.2. Responsabilidad financiera .....  | 94 |
| 9.2.1. Cobertura de seguro.....  | 94 |

|  |     |
|--|-----|
| 9.2.2. Otros activos .....   | 95  |
| 9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados .....      | 95  |
| 9.3. Confidencialidad.....   | 95  |
| 9.3.1. Alcance de la información confidencial .....  | 95  |
| 9.3.2. Informaciones no confidenciales.....  | 95  |
| 9.3.3. Responsabilidad para proteger la información confidencial.....                          | 96  |
| 9.4. Protección de datos personales.....   | 96  |
| 9.5. Derechos de propiedad intelectual.....  | 99  |
| 9.5.1. Propiedad de los certificados e información de revocación .....                         | 99  |
| 9.5.2. Propiedad de la política de certificado y Declaración de Prácticas de Certificación.... | 99  |
| 9.5.3. Propiedad de la información relativa a nombres .....                                    | 99  |
| 9.5.4. Propiedad de claves .....   | 99  |
| 9.6. Obligaciones y garantías.....   | 100 |
| 9.6.1. Modelo de obligaciones del prestador de servicios.....                                  | 100 |
| 9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados .....         | 101 |
| 9.7. Rechazo de otras garantías .....  | 102 |
| 9.8. Limitación de responsabilidades .....   | 102 |
| 9.8.1. Limitación de responsabilidad de la Autoridad de Certificación.....                     | 102 |
| 9.8.2. Caso fortuito y fuerza mayor .....  | 103 |
| 9.9. Cláusulas de indemnidad.....  | 103 |
| 9.9.1. Cláusula de indemnidad de suscriptor .....  | 103 |
| 9.9.2. Cláusula de indemnidad de tercero que confía en el certificado .....                    | 103 |
| 9.10. Periodo de validez .....   | 103 |
| 9.10.1. Entrada en vigor.....  | 103 |
| 9.10.2. Finalización.....  | 104 |
| 9.10.3. Efecto de la finalización y supervivencia.....   | 104 |
| 9.11. Notificaciones.....  | 104 |
| 9.12. Modificaciones.....  | 104 |
| 9.12.1. Procedimiento para las modificaciones .....  | 104 |
| 9.12.2. Periodo y mecanismos de notificación .....   | 104 |
| 9.12.3. Circunstancias por las que un OID debe cambiarse.....                                  | 105 |
| 9.13. Reclamaciones y resolución de disputas .....   | 105 |

|   |     |
|---|-----|
| 9.14. Ley aplicable .....                       | 105 |
| 9.15. Cláusula de jurisdicción competente ..... | 105 |
| 9.16. Cláusulas diversas.....                   | 105 |
| 9.16.1. Acuerdo íntegro.....                    | 105 |
| 9.16.2. Subrogación .....                       | 105 |
| 9.16.3. Divisibilidad.....                      | 106 |
| 9.16.4. Aplicaciones.....                       | 106 |
| 9.16.5. Causa mayor .....                       | 106 |
| 9.17. Otras provisiones .....                   | 106 |

## 1. Introducción

Este documento contiene la Declaración de prácticas de certificación que regula la clase de certificados "Certificados Notariales", emitidos por la Agencia Notarial de Certificación.

### 1.1. Presentación

#### 1.1.1. Certificados Notariales

La "Clase Notariales" de certificados agrupa todos los certificados expedidos por la Agencia Notarial de Certificación al público actuando un Notario como Entidad de Registro, aportando los máximos niveles de seguridad jurídica.

#### 1.1.2. Certificados que se emiten

Dentro de la "Clase Notariales", se emiten los siguientes certificados:

##### 1.1.2.1. Certificados Notariales Personales

Los Certificados Notariales Personales son certificados cualificados, en los términos del artículo 28 del Reglamento (UE) 910/2014; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicho Reglamento 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 prestan.

Existen dos modalidades de Certificados Notariales Personales:

- **Certificado Notarial Personal**, que se emite a personas físicas, que actúan en su nombre propio.
- **Certificado Notarial Personal de Representación Personal**, que se emite a personas físicas en representación de otra persona física.

Los Certificados Notariales Personales permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

- La creación de la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia. El certificado de autenticación también puede utilizarse para la creación de firma electrónica avanzada de documentos electrónicos conforme a las condiciones acordadas por las partes para relacionarse entre sí, o cuando la normativa administrativa aplicable lo admita expresamente.
- El cifrado y el descifrado de documentos electrónicos.

Se utiliza una tarjeta criptográfica como único soporte para los tres certificados, con la garantía de dispositivo cualificado de creación de firma, en los términos del artículo 29 del Reglamento (UE) 910/2014.

Los certificados pueden contener informaciones personales adicionales (por ejemplo, la pertenencia a un Colegio profesional, cargo honorífico, etc.), siempre que no se trate de datos especiales de acuerdo con el artículo 9 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 y por el que se deroga la Directiva 95/46/CE.

Los Certificados Notariales Personales se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”.

### **1.1.2.2. Certificados Notariales Corporativos**

Los Certificados Notariales Corporativos de firma electrónica son certificados cualificados, en los términos del artículo 28 del Reglamento (UE) 910/2014; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicho Reglamento 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 prestan.

Los Certificados Notariales Corporativos de sello electrónico son certificados cualificados de sello electrónico, en los términos del artículo 38 del Reglamento (UE) 910/2014; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicho Reglamento 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 prestan.

Existen cuatro modalidades de Certificados Notariales Corporativos:

- **Certificado Notarial Corporativo**, que se emiten a personas jurídicas o entidades sin personalidad jurídica, con identificación de una persona física que actúa como custodio del certificado, de acuerdo con lo establecido en el artículo 7 y la disposición adicional tercera de la Ley 59/2003, de Firma Electrónica, ya derogada.
- **Certificado Notarial Corporativo de Representación**, que se emite a personas jurídicas, con identificación de una persona física que actúa como representante de la persona jurídica. El Certificado Notarial Corporativo de Representación AGE es un certificado dentro de la modalidad Certificado Notarial Corporativo de Representación cuyo perfil de certificado sigue las especificaciones del Anexo 1 del documento “Perfiles de Certificados Electrónicos”, de abril de 2016, publicado por el Ministerio de Hacienda y Administraciones Públicas del Gobierno de España.
- **Certificado Notarial Corporativo de Facturación Electrónica**, que se emite a personas físicas o jurídicas, para la realización de facturación electrónica o bien para la prestación de servicios de facturación electrónica a terceros.

- **Certificado Notarial de Sello Electrónico**, que se emiten a personas jurídicas para la creación de sellos electrónicos avanzados o cualificados.

Los Certificados Notariales Corporativos y Corporativos de Representación de firma electrónica permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

- La creación de la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia. El certificado de autenticación también puede utilizarse para la creación de firma electrónica avanzada de documentos electrónicos conforme a las condiciones acordadas por las partes para relacionarse entre sí, o cuando la normativa administrativa aplicable lo admita expresamente.
- El cifrado y el descifrado de documentos electrónicos.

Los Certificados Corporativos Notariales de Facturación Electrónica permiten un único uso del certificado, la firma de facturas.

Los Certificados Corporativos de Sello Electrónico permiten la creación de sellos electrónicos cualificados o avanzados en función de si es utilizado un dispositivo cualificado de creación de sellos electrónicos o no.

El Certificado Notarial Corporativo sólo podían emplearse, por mandato del artículo 7 de la Ley 59/2003, de Firma Electrónica, en el ámbito de las Administraciones Públicas y en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario, entendiéndose por tal, las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de la actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares.

Los Certificados Notariales Corporativos emitidos a entidades sin entidad jurídica, se expedían a los solos efectos de utilizarse en las comunicaciones y transmisiones de datos por medios electrónicos, informáticos y telemáticos en el ámbito tributario de acuerdo con la Disposición Adicional Tercera de la Ley 59/2003, de 19 de diciembre y la Orden EHA/3256/2004, de 30 de septiembre dictada por el Ministerio de Economía y Hacienda, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 35.4 de la Ley General Tributaria.

Con la entrada en vigor del Reglamento (UE) 910/2014 el 1 de Julio de 2016, a partir de esa fecha, no se emitirán nuevos certificados de la modalidad Certificado Notarial Corporativo.

Se utilizan dispositivos cualificados de creación de firma como soporte para los tres certificados para los certificados de firma electrónica con garantía de dispositivo seguro, en los términos del artículo 29 del Reglamento (UE) 910/2014.

Se utilizan dispositivos cualificados de creación de sello electrónico como soporte de los certificados de sello electrónico con garantía de dispositivo seguro, en los términos del artículo 39 del Reglamento (UE) 910/2014.

Los certificados pueden contener informaciones personales adicionales (por ejemplo, la pertenencia a un Colegio profesional, cargos honoríficos, etc.), siempre que no se trate de datos especiales de acuerdo con el artículo 9 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 y por el que se deroga la Directiva 95/46/CE.

Los Certificados Notariales Corporativos se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”.

### **1.1.2.3. Certificados Notariales de Sistemas**

Los Certificados Notariales de Sistemas son certificados para el aseguramiento informático de las operaciones de sistemas de información. Dichos certificados no tienen la consideración de certificados cualificados, de acuerdo con el Reglamento (UE) 910/2014.

Existen cinco modalidades de Certificados Notariales de Sistemas:

- **Certificado Notarial de Servidor Seguro**, que se emite a personas físicas o jurídicas, en calidad de titulares del nombre de dominio de servidores SSL/TLS, para el establecimiento de comunicaciones seguras y autenticadas entre servidor y cliente SSL/TLS.
- **Certificado Notarial de Sellado de Fecha y Hora**, que se emite a personas físicas o jurídicas, en calidad de titulares de servidores de fecha y hora.
- **Certificado Notarial de Firma de Código**, que se emite a personas físicas o jurídicas, en calidad de editores de código de programa ejecutable, para su distribución pública.
- **Certificado Notarial de Aplicación Segura**, que se emite a personas físicas o jurídicas, en calidad de titulares de aplicaciones informáticas de funcionamiento automatizado, que precisan las funciones de autenticación, firma digital o cifrado/descifrado.
- **Certificado Notarial de OCSP Trusted Responder**, que se emite a personas físicas o jurídicas, en calidad de titulares de servidores de OCSP.

Todas las funcionalidades de cada Certificado Notarial de Sistemas se contienen en un único certificado, pudiendo utilizarse diversos tipos de módulos de seguridad, incluyendo bienes de equipo criptográfico.

Los Certificados Notariales de Sistemas se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”.



## 1.2. Nombre del documento e identificación

Este documento es la Declaración de prácticas de certificación de los Certificados de "Clase Notariales" de la Agencia Notarial de Certificación, y se le ha asignado el siguiente OID: ANCERT.0.1.0.2

El OID de ANCERT es: 1.3.6.1.4.1.18920.

La Agencia Notarial de Certificación ha asignado los siguientes identificadores de objeto (OID) a los certificados, para su identificación por las aplicaciones:

| <u>Certificado</u>  | <u>Identificador</u> |
|---|----------------------|
| Certificado notarial personal (firma)   | ANCERT.1.1.1.2.1     |
| Certificado notarial personal (autenticación)                                   | ANCERT.1.1.1.2.2     |
| Certificado notarial personal (cifrado)   | ANCERT.1.1.1.2.3     |
| Certificado notarial personal de representación personal (firma)                | ANCERT.1.1.2.2.1     |
| Certificado notarial personal de representación personal (autenticación)        | ANCERT.1.1.2.2.2     |
| Certificado notarial personal de representación personal (cifrado)              | ANCERT.1.1.2.2.3     |
| Certificado notarial de servidor seguro (con dispositivo seguro)                | ANCERT.1.2.1.2.1     |
| Certificado notarial de servidor seguro (sin dispositivo seguro)                | ANCERT.1.2.1.2.2     |
| Certificado notarial de autoridad de sellado de tiempo (con dispositivo seguro) | ANCERT.1.2.3.2.1     |
| Certificado notarial de autoridad de sellado de tiempo (sin dispositivo seguro) | ANCERT.1.2.3.2.2     |
| Certificado notarial de firma de código (con dispositivo seguro)                | ANCERT.1.2.5.2.1     |
| Certificado notarial de firma de código (sin dispositivo seguro)                | ANCERT.1.2.5.2.2     |
| Certificado notarial de aplicación segura (con dispositivo seguro)              | ANCERT.1.2.6.1.1     |

|  |                  |
|--|------------------|
| Certificado notarial de aplicación segura (sin dispositivo seguro)                         | ANCERT.1.2.6.1.2 |
| Certificado notarial de OCSP trusted responder (sin dispositivo seguro)                    | ANCERT.1.2.7.1.2 |
| Certificado notarial corporativo (firma)   | ANCERT.1.3.1.2.1 |
| Certificado notarial corporativo (autenticación)   | ANCERT.1.3.1.2.2 |
| Certificado notarial corporativo (cifrado)   | ANCERT.1.3.1.2.3 |
| Certificado notarial corporativo de representación (firma)                                 | ANCERT.1.3.2.2.1 |
| Certificado notarial corporativo de representación (autenticación)                         | ANCERT.1.3.2.2.2 |
| Certificado notarial corporativo de representación (cifrado)                               | ANCERT.1.3.2.2.3 |
| Certificado notarial corporativo de representación AGE (firma)                             | ANCERT.1.3.2.3.1 |
| Certificado notarial corporativo de representación AGE (autenticación)                     | ANCERT.1.3.2.3.2 |
| Certificado notarial corporativo de facturación electrónica (sin dispositivo seguro)       | ANCERT.1.3.3.1.2 |
| Certificado notarial corporativo de sello electrónico (con garantía de dispositivo seguro) | ANCERT.1.3.4.1.1 |
| Certificado notarial corporativo de sello electrónico (sin garantía de dispositivo seguro) | ANCERT.1.3.4.1.2 |

La Agencia Notarial de Certificación publica en su web un documento descriptivo con el detalle técnico de todos estos perfiles.

La Agencia Notarial de Certificación publica en su Depósito un documento con los OIDs correspondientes a las prácticas de certificación y a los certificados vigentes en cada momento.

### **1.3. Participantes en los servicios de certificación**

Esta Declaración de prácticas de certificación regula la prestación de servicios de certificación al público por parte de la Agencia Notarial de Certificación con intervención notarial.

Los participantes en los servicios de certificación son los siguientes:

### **1.3.1. Autoridades de certificación**

La Agencia Notarial de Certificación actúa como prestadora de servicios de certificación, por encargo del Consejo General del Notariado de España.

Para esta clase “Certificados Notariales”, La Agencia Notarial de Certificación dispone de las siguientes Entidades de Certificación.

#### **1.3.1.1. ANCERT Certificados Notariales V2**

ANCERT Certificados Notariales es la entidad de Certificación Raíz, basada en un certificado raíz auto firmado, cuya huella digital basada en el algoritmo SHA-256 es:

CN=ANCERT Certificados Notariales V2

Periodo de validez: 25/05/2010 al 25/05/2030

Resumen: 4BE8B5A1C76C6AEAD0611918FCCF9DBD398B67FB12294758BDF994D0F9682F60

ANCERT Certificados Notariales expide certificados raíz para las siguientes Entidades de Certificación subordinadas:

- ANCERT Certificados Notariales Personales V2.
- ANCERT Certificados Notariales Corporativos V2.
- ANCERT Certificados Notariales de Sistemas V2.

#### **1.3.1.2. ANCERT Certificados Notariales Personales V2**

Esta Entidad de Certificación subordinada emite los certificados electrónicos denominados Certificados Notariales Personales y los Certificados Notariales de Representación

La huella digital de esta Entidad de Certificación subordinada basada en el algoritmo SHA-256 es:

CN=ANCERT Certificados Notariales Personales V2

Periodo de validez: 27/05/2010 al 27/05/2020

Resumen: A6A176268AE84BAC15DE7289AB6F5C7BDAB75B2EB864C33908074034C9B5DABA

CN=ANCERT Certificados Notariales Personales V2

Periodo de validez: 21/06/2016 al 25/10/2030

Resumen: C4472508C3BC689FC59E8BF77A6DDEDFBB29A43316BD0946D544E54DFC001535

#### **1.3.1.3. ANCERT Certificados Notariales Corporativos V2**

Esta Entidad de Certificación subordinada emite los certificados electrónicos denominados Certificados Notariales Corporativos, los Certificados Notariales Corporativos de Representación, los Certificados Notariales Corporativos de Sello Electrónico y los Certificados Notariales Corporativos de Facturación Electrónica.

La huella digital de esta Entidad de Certificación subordinada basada en el algoritmo SHA-256 es:

CN=ANCERT Certificados Notariales Corporativos V2

Periodo de validez: 27/05/2010 al 27/05/2020

Resumen: 88C2BF64188E40B821A5990F29D822F219706EA6790500F376CE8E4DF2EA3E07

CN=ANCERT Certificados Notariales Corporativos V2

Periodo de validez: 21/06/2016 al 25/10/2030

Resumen: 0CA8B7A01506CAFAA1879E7491C662F8264EB3A2F1F0E0657DA3D6A912FF1487

#### **1.3.1.4. ANCERT Certificados Notariales de Sistemas V2**

Esta Entidad de Certificación subordinada emite los certificados electrónicos denominados Certificados Notariales de Sistemas, siendo estos los siguientes:

- Certificado Notarial de Servidor Seguro
- Certificado Notarial de Sello de Fecha y Hora
- Certificado Notarial de Firma de Código
- Certificado Notarial de Aplicación Segura
- Certificado Notarial de OCSP Trusted Responder

La huella digital de esta Entidad de Certificación subordinada basada en el algoritmo SHA-256 es:

CN=ANCERT Certificados Notariales de Sistemas V2

Periodo de validez: 27/05/2010 al 27/05/2020

Resumen: B89EE1F6E629A5ADF95E317F7ECC485A424BEF06BCD4055E6251BC61BD8A5CF4

CN=ANCERT Certificados Notariales de Sistemas V2

Periodo de validez: 21/06/2016 al 25/10/2030

Resumen: 186B5083F6CBE72E94172B57424B0DB7F0F58B2BAE8D7A9C946A4BBB5B4FD7F0

#### **1.3.2. Entidades de registro**

Las entidades de registro son las personas físicas o jurídicas que asisten a la Agencia Notarial en las tareas de emisión y gestión de los certificados, y en concreto, en las tareas de:

- Contratación del servicio de certificación a entidades finales.
- Identificación y autenticación de la identidad y circunstancias personales de las personas que reciben los certificados.
- Generación de certificados y entrega de dispositivos seguros de creación de firma a los suscriptores.
- Almacenamiento de documentos en relación con los servicios de certificación.

Para los certificados de clase “Certificados Notariales” siempre actúa como Entidad de Registro un Notario español.

### 1.3.3. Entidades finales

Las entidades finales son las personas y las organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para firma, autenticación y cifrado, y entre ellas, las siguientes:

- 1) Solicitantes de certificados, que los solicitan para ellos o para terceras personas.
- 2) Suscriptores de certificados, que ostentan la titularidad de los certificados.
- 3) Poseedores de claves, que las emplean para las finalidades y aplicaciones previstas en los certificados.
- 4) Representados.
- 5) Terceros que confían en certificados.

#### 1.3.3.1. Solicitantes de certificados

Para los certificados que se emiten, de clase “Certificados Notariales”, los solicitantes son los siguientes:

- **Certificados Notariales Personales:** una persona física, que actúa en nombre propio.
- **Certificados Notariales Personales de Representación Personal:** una persona física que actúa como representante legal o voluntario de otra persona física.
- **Certificados Notariales Corporativos:** una persona física, que actúa como representante legal o voluntario de una persona jurídica o entidad sin personalidad jurídica, o bien todas las personas que componen un órgano colegiado de la misma.
- **Certificados Notariales Corporativos de Representación:** una persona física, que actúa como representante legal o voluntario de una persona jurídica. Podrá solicitar un certificado a su nombre o bien, en el ámbito de su representación, solicitar un certificado para otras personas físicas a las que previamente se les haya delegado por documento público todas o algunas de las facultades del solicitante.
- **Certificados Notariales de Facturación Electrónica:** una persona física, que actúa en nombre propio o como representante legal o voluntario de una persona jurídica o entidad sin personalidad jurídica.
- **Certificado Notarial de Sello Electrónico:** una persona física, que actúa como representante legal o voluntario de una persona jurídica, o bien todas las personas que componen un órgano colegiado de la misma.
- **Certificados Notariales de Servidor seguro:** una persona física, que actúa en nombre propio, o bien una persona física, que actúa como representante legal o voluntario de una persona jurídica.
- **Certificados Notariales de Sellado de fecha y hora:** una persona física, que actúa en nombre propio, o bien una persona física, que actúa como representante legal o voluntario de una persona jurídica.

- **Certificados Notariales de Firma de código:** una persona física, que actúa en nombre propio, o bien una persona física, que actúa como representante legal o voluntario de una persona jurídica.
- **Certificados Notariales de Aplicación Segura:** una persona física, que actúa en nombre propio, o bien una persona física, que actúa como representante legal o voluntario de una persona jurídica.
- **Certificados Notariales de OCSP Trusted Responder:** una persona física, que actúa en nombre propio o como representante legal o voluntario de una persona jurídica.

### 1.3.3.2. Suscriptores de certificados

Los suscriptores son las personas y las organizaciones titulares del certificado.

Para los certificados que se emiten, de clase “Certificados Notariales”, los suscriptores son:

- **Certificados Notariales Personales:** la persona física identificada en el certificado.
- **Certificados Notariales Personales de Representación Personal:** la persona física identificada en el certificado, con la consideración de representante.
- **Certificados Notariales Corporativos:** la persona jurídica identificada en el certificado.
- **Certificados Notariales Corporativos de Representación:** la persona jurídica identificada en el certificado.
- **Certificados Notariales Corporativo de Facturación Electrónica:** la persona física o jurídica identificada en el certificado.
- **Certificado Notarial de Sello Electrónico:** la persona jurídica identificada en el certificado.
- **Certificados Notariales de Servidor seguro:** la persona física o jurídica identificada en el certificado.
- **Certificados Notariales de Sellado de fecha y hora:** la persona física o jurídica identificada en el certificado.
- **Certificados Notariales de Firma de código:** la persona física o jurídica identificada en el certificado.
- **Certificados Notariales de Aplicación Segura:** la persona física o jurídica identificada en el certificado.
- **Certificados Notariales de OCSP Trusted Responder:** la persona física o jurídica identificada en el certificado.

### 1.3.3.3. Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves criptográficas, cuando no son suscriptores del certificado. El poseedor de claves coincide con el concepto de firmante empleado en la legislación de firma electrónica, pero se denomina de esta forma genérica, dado que también puede emplear el certificado para otras funciones, como la autenticación o el descifrado.

Los poseedores de claves se encuentran debidamente identificados en el certificado, mediante su nombre y apellidos.

Sólo los Certificados Notariales Corporativos emplean la noción de poseedor de claves, que son:

- **Certificados Notariales Corporativos:** la persona física que actúa como custodio.
- **Certificados Notariales Corporativos de Representación:** la persona física que actúa como representante.
- **Certificados Notariales Corporativos de Facturación Electrónica:** la persona física que actúa como custodio.
- **Certificados Notariales de Sello Electrónico:** la persona física que actúa como custodio.

#### **1.3.3.4. Representados**

Tienen la consideración de representados las personas físicas o jurídicas en cuyo nombre los solicitantes solicitan Certificados Notariales Personales de Representación o Certificados Notariales Corporativos de Representación.

La identificación de la persona física o jurídica representada se incluye dentro del certificado, de acuerdo con lo que se establece en la sección 3 de esta Declaración de Prácticas de Certificación.

#### **1.3.3.5. Terceros que confían en certificados**

Los terceros que confían en certificados son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, los terceros deben verificarlos, tal como se establece en esta Declaración de prácticas de certificación y en los documentos jurídicos correspondientes.

### **1.4. Uso de los certificados**

Esta sección lista las aplicaciones para las que puede emplearse cada certificado de los emitidos para la clase “Certificados Notariales”, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

#### **1.4.1. Usos permitidos para los certificados**

Los certificados de Clase Notariales pueden emplearse para los usos descritos en la sección 1.1.2 de esta Declaración de Prácticas de Certificación.

En relación con el uso de los certificados, debe entenderse lo siguiente:

- **Autenticidad de origen:** Asegura que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona o entidad de quien dice provenir. Esta característica se obtiene mediante la firma electrónica. El receptor de un mensaje firmado electrónicamente puede verificar esa firma empleando el certificado.

- **Autenticidad de servidor:** Asegura que la comunicación electrónica proviene del servidor del que dice provenir. El usuario puede verificar la autenticidad del servidor a través del certificado.
- **Aceptación de contenido por el emisor<sup>1</sup>:** Evita que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo. Para ello se utiliza la firma electrónica. El receptor de un mensaje firmado digitalmente puede verificar esa firma empleando el certificado. De esta forma puede demostrar la identidad del emisor del mensaje y la aceptación de su contenido, sin que éste pueda refutarlos falsamente.
- **Integridad:** Permite comprobar que un documento electrónico para el que se ha generado una firma electrónica no ha sido modificado por ningún agente externo. Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (funciones de *hash*), utilizadas en combinación con la firma electrónica. El procedimiento se centra en firmar electrónicamente un resumen único del documento electrónico con la clave privada del suscriptor de forma que cualquier alteración del documento revierte en una alteración de su resumen.
- **Confidencialidad:** Asegura que los datos que se transmiten no pueden ser leídos por terceras personas sin autorización, ya que los datos que se envían están cifrados.

#### **1.4.1.1. Límites de uso**

Todos los certificados deben emplearse para su función propia y finalidad establecida en la descripción del certificado de la sección 1.1.2 de esta Declaración de Prácticas de Certificación, sin que puedan emplearse en otras funciones y con otras finalidades.

Asimismo, los certificados deberán emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados pueden contener límites adicionales de uso en forma de atributos dentro del campo *Subject Directory Attributes*, tal y como se indica en la sección 3.1.4 de esta Declaración de Prácticas de Certificación, así como en las condiciones generales de uso de los certificados. Los terceros deben considerar estas limitaciones antes de confiar en los certificados.

Aunque los certificados de entidad final se pueden emplear, con algunas excepciones, para el cifrado o descifrado de documentos electrónicos, se advierte que dichos usos se realizan bajo la exclusiva responsabilidad del suscriptor.

#### **1.4.1.2. Prohibiciones de usos**

Los Certificados Notariales no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (CRL) o informaciones de estado de certificados (mediante servidores OCSP o similares), excepto cuando se autorice expresamente.

---

<sup>1</sup> También llamado frecuentemente "no repudio" o irrefutabilidad.



Los Certificados Notariales de Firma de Código no pueden emplearse para firmar cualquier tipo de código que pueda ser considerado hostil, incluyendo en este término “spyware” y “malware” que pueda ser descargado por un usuario en su equipo sin su consentimiento.

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.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrá el suscriptor, el poseedor de claves o los terceros perjudicados reclamar a la Agencia Notarial de Certificación, o al Consejo General del Notariado, compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para los usos limitados y/o prohibidos.

## **1.5. Administración del documento**

### **1.5.1. Organización que administra el documento**

AGENCIA NOTARIAL DE CERTIFICACIÓN, S.L. UNIPERSONAL

Avenida de Martínez Campos, número 46.- 6º, Edificio Elcano

28010 Madrid (España)

NIF nº B-83395988

### **1.5.2. Datos de contacto de la organización**

Cualquier contacto con la Agencia Notarial de Certificación, referente a esta Declaración de Prácticas de Certificación puede realizarse por los siguientes medios:

- Vía e-mail a la dirección de correo electrónico [ancert@ancert.com](mailto:ancert@ancert.com).
- Por teléfono al número 912187676.
- Directamente en la sede central de la Agencia Notarial de Certificación: Agencia Notarial de Certificación, S.L. Unipersonal Avenida de Martínez Campos, número 46.- 6º, Edificio Elcano 28010 Madrid (España)

Las alteraciones que se produzcan sobre los anteriores datos como Web, correo, dirección o teléfono constarán debidamente reflejadas en la página web [www.ancert.com](http://www.ancert.com) que la Agencia Notarial de Certificación mantiene en vigor en Internet.

### **1.5.3. Responsable de adecuación de la Declaración de Prácticas de Certificación**

Quien determina la conformidad de esta Declaración de Prácticas de Certificación es el responsable del Servicio de Certificación de la Agencia Notarial de Certificación.

#### **1.5.4. Procedimiento de aprobación de la Declaración de Prácticas de Certificación**

Existe un procedimiento de creación, revisión y aprobación formal que garantiza el correcto mantenimiento de este documento. El Comité de Seguridad de la Agencia Notarial de Certificación es el órgano responsable de la aprobación.

La presente Declaración de Prácticas de Certificación podrá ser modificada en cualquier momento por la Agencia Notarial de Certificación. De no aceptar cualquiera de los suscriptores con certificado en vigor alguna de las modificaciones acordadas podrá instar la revocación de su certificado.

La revocación así solicitada no dará derecho a reclamar indemnización alguna, ni aun la devolución parcial del precio del certificado, salvo que la rectificación o modificación de la Declaración de Prácticas de Certificación implique una limitación de los derechos de uso o una restricción sobre el ámbito de aplicación sobre el certificado emitido, en cuyo caso se podrá exigir el reembolso del precio del mismo.

#### **1.5.5. Frecuencia de revisión**

La Declaración de Prácticas de Certificación y los textos divulgativos son revisados y, si procede, actualizados, con una periodicidad anual.

### **1.6. Definiciones y acrónimos**

#### **1.6.1. Definiciones**

**Autoridad de Certificación (o Entidad de Certificación):** entidad de confianza, responsable de emitir y revocar los certificados.

**Autoridad de Registro (o Entidad de Registro):** entidad que identifica de forma inequívoca al solicitante de un certificado. La Autoridad de Registro suministra a la Autoridad de Certificación los datos verificados del solicitante a fin de que la Autoridad de Certificación emita el correspondiente certificado.

**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, y que contiene los Datos de Verificación de firma de dicha Autoridad firmado con los datos de creación de Firma de la misma.

**Certificado cualificado:** un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el Anexo I del eIDAS.

**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 (calve 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 cifrar y verificar firmas digitales

**Declaración de Prácticas de Certificación:** documento elaborado por una Autoridad de Certificación que recoge o regula la prestación de los servicios de certificación por parte de dicha Autoridad de Certificación en su condición de Prestador de Servicios de Confianza.

**Dispositivo de creación de firma:** un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

**Dispositivo de creación de firma cualificado:** dispositivo de creación de firma que cumple con los requisitos del Anexo II del 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 avanzada:** firma electrónica que cumple los requisitos del artículo 26 de eIDAS.

**Firma 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.

**HSM (Módulo de seguridad criptográfico):** dispositivo de seguridad que genera y protege claves criptográficas

**Lista de Certificados Revocados (CRL):** lista firmada donde figura la relación de certificados revocados de una Autoridad de Certificación.

**OCSP (Online Certificate Status Protocol):** protocolo informático que permite la comprobación del estado de un certificado electrónico

**OID (Object Identifier):** identificador utilizado para nombrar un objeto. Estructuralmente, un OID consiste en un nodo en un espacio de nombres asignados jerárquicamente, formalmente definido utilizando el estándar ASN.1.

**Prestador de Servicios de Confianza (TSP):** una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas.

### 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

**GN:** nombre propio del poseedor en un certificado

**HSM:** Hardware Security Module (Módulo de Seguridad Criptográfico)

**LFE:** Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

**OID:** Object Identifier (Identificador de objeto único)

**PSC:** Prestador de Servicios de Certificación

**TSP:** Prestador de Servicios de Confianza

**RA:** Autoridad de Registro

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

## **2. Publicación de información y depósito de certificados**

### **2.1. Depósito(s) de certificados**

La Agencia Notarial de Certificación dispone de un Depósito de certificados. Los certificados se conservarán en el depósito hasta al menos un año después de su expiración.

El servicio de Depósito se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la Agencia Notarial de Certificación, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación.

### **2.2. Publicación de información del prestador de servicios de certificación**

La Agencia Notarial Certificación publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, incluidos los certificados de Entidades de Certificación que emiten certificados para esta clase de certificados.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La política general de certificación del Consejo General del Notariado, así como cualesquiera políticas específicas de certificados dictadas por la Agencia Notarial de Certificación para desarrollar ulteriores requisitos, dentro del marco de dicha política.
- Las diversas versiones de la Declaración de Prácticas de Certificación.
- Los textos de divulgación (Policy Disclosure Statements - PDS),
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en certificados.

### **2.3. Frecuencia de publicación**

La información anteriormente indicada, incluyendo políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en los documentos de política específica y en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 del documento de política o Declaración de Prácticas de Certificación.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.9 de esta Declaración de Prácticas de Certificación.

### **2.4. Control de acceso**

La Agencia Notarial de Certificación no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información de estado de revocación.

La Agencia Notarial de Certificación emplea sistemas fiables para el Depósito, de modo tal que:

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

## 3. Identificación y autenticación

### 3.1. Gestión de nombres

#### 3.1.1. Tipos de nombres

Todos los certificados contienen un nombre diferenciado de la persona y/o organización, identificados en el certificado, definido de acuerdo con lo previsto en la Recomendación ITU-T X.501 y contenido en el campo *Subject Name*.

Los certificados contienen nombres alternativos de las personas y organizaciones identificadas en los certificados, principalmente en el campo *SubjectAlternativeName*.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados se incluyen en atributos predefinidos en normas y especificaciones técnicas ampliamente utilizadas en el sector o sectores de actividad donde deban emplearse los certificados, así como en atributos definidos de forma específica por la Agencia Notarial de Certificación, principalmente en el campo *Subject Directory Attributes*.

#### 3.1.2. Significado de los nombres

Los nombres de los certificados son comprensibles e interpretados de acuerdo con la legislación aplicable a los nombres de las personas físicas y jurídicas titulares de los certificados, según se indica en el componente *Country* del nombre.

Los nombres incluidos en los certificados son tratados de acuerdo con las siguientes normas:

- Se codifica el nombre tal y como aparece en la documentación acreditativa.
- Se pueden eliminar los acentos, para garantizar la mayor compatibilidad técnica posible.
- Los nombres pueden ser adaptados y reducidos, al objeto de garantizar el cumplimiento de los límites de longitud aplicables a cada campo del certificado.

En el caso de que los datos consignados en el nombre (*CommonName*, *GeneralName* y/o *Surname*) sean ficticios o se indique expresamente su invalidez (e.g. con los literales "PRUEBAS" o "FICTICIO"), se considera al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad.

#### 3.1.3. Empleo de anónimos y seudónimos

En esta clase de certificados no se emiten certificados anónimos. El uso de seudónimos únicamente está permitido en los Certificados Notariales de Facturación Electrónica.

#### 3.1.4. Interpretación de formatos de nombres

La Agencia Notarial de Certificación emplea los siguientes esquemas de nombres. La longitud máxima de los componentes de los nombres sigue preferentemente las especificaciones definidas en la recomendación ITU-T X.509.

### 3.1.4.1. Certificado Notarial Personal

| <b>SUBJECT NAME</b>                 |  |
|-------------------------------------|--|
| <b>CAMPO</b>                        | <b>CONTENIDO</b>   |
| Country (C)                         | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)                         |
| Organizational Unit (OU)            | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit (OU)            | "Certificado Notarial Personal (" + "Firma" o "Autentica" o "Cifrado" + ")"  |
| Surname (SU)                        | Apellidos de la persona física identificada.   |
| Given Name (GN)                     | Nombre de la persona física identificada.  |
| Serial Number (SN)                  | NIF (de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas) |
| Common Name (CN)                    | Nombre y apellidos de la persona física identificada.  |
| <b>SUBJECT ALTERNATIVE NAME</b>     |  |
| rfc822Name                          | Correo electrónico de la persona física identificada.  |
| <b>SUBJECT DIRECTORY ATTRIBUTES</b> |  |
| dateOfBirth                         | Fecha de nacimiento.   |
| CountryOfCitizenship                | Nacionalidad del suscriptor.   |
| ANCERT.10.1.4                       | Circunstancias adicionales de la persona física  |

### 3.1.4.2. Certificado Notarial Personal de Representación personal

| <b>SUBJECT NAME</b>             |  |
|---------------------------------|--|
| <b>CAMPO</b>                    | <b>CONTENIDO</b>   |
| Country (C)                     | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)                         |
| Organizational Unit(OU)         | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit(OU)         | "Certificado Notarial de Representación Personal (" + "Firma" o "Autentica" o "Cifrado" + ")"  |
| Title                           | Rol o función en conexión con la representación.   |
| Surname (SU)                    | Apellidos de la persona física identificada.   |
| Given Name (GN)                 | Nombre de la persona física identificada.  |
| Serial Number(SN)               | NIF (de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas) |
| Common Name (CN)                | Nombre y apellidos de la persona física identificada.  |
| <b>SUBJECT ALTERNATIVE NAME</b> |  |
| rfc822Name                      | Correo electrónico de la persona física identificada.  |



| <b>SUBJECT DIRECTORY ATTRIBUTES</b> |   |
|-------------------------------------|---|
| DateOfBirth                         | Fecha de nacimiento.                        |
| CountryOfCitizenship                | Nacionalidad del suscriptor.                |
| ANCERT.10.1.1                       | Nivel de apoderamiento.                     |
| ANCERT.10.1.3                       | Documento de representación.                |
| ANCERT.10.1.4                       | Atributos adicionales de la persona física. |
| ANCERT.10.1.5                       | Límite de uso.                              |
| ANCERT.10.1.6                       | Datos registrales de la representación.     |
| ANCERT.10.1.7                       | Persona representada (física)               |

### 3.1.4.3. Certificado Notarial Corporativo

| <b>SUBJECT NAME</b>                 |   |
|-------------------------------------|---|
| <b>CAMPO</b>                        | <b>CONTENIDO</b>  |
| Country (C)                         | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)  |
| Organization (O)                    | Nombre de la entidad suscriptora.   |
| Organizational Unit(OU)             | "Autorizado ante Notario " + identificación de Notario  |
| Organizational Unit(OU)             | "Certificado Notarial Corporativo (" + "Firma" o "Autentica" o "Cifrado" + ")"  |
| Title                               | Rol o función del custodio.   |
| Surname (SU)                        | Apellidos del custodio.   |
| Given Name (GN)                     | Nombre del custodio.  |
| OID "1.3.6.1.4.1.18838.1.1"         | NIF del custodio (NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas) |
| Serial Number                       | NIF de la entidad suscriptora.  |
| Common Name (CN)                    | Nombre de la entidad suscriptora.   |
| <b>SUBJECT ALTERNATIVE NAME</b>     |   |
| Rfc822Name                          | Correo electrónico.   |
| <b>SUBJECT DIRECTORY ATTRIBUTES</b> |   |
| dateOfBirth                         | Fecha de nacimiento.  |
| CountryOfCitizenship                | Nacionalidad del suscriptor.  |
| ANCERT.10.1.1                       | Nivel de apoderamiento.   |
| ANCERT.10.1.3                       | Documento de representación.  |
| ANCERT.10.1.5                       | Límite de uso.  |
| ANCERT.10.1.6                       | Datos registrales de la representación.   |

### 3.1.4.4. Certificado Notarial Corporativo de Representación

| <b>SUBJECT NAME</b>                 |  |
|-------------------------------------|--|
| <b>CAMPO</b>                        | <b>CONTENIDO</b>   |
| Country (C)                         | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)   |
| Organization (O)                    | Nombre de la entidad suscriptora.  |
| Organizational Unit (OU)            | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit (OU)            | "Certificado Notarial Corporativo de Representación (" + "Firma" o "Auténtica" o "Cifrado" + ")"   |
| Title                               | Rol o función del custodio.  |
| Surname (SU)                        | Apellidos de la persona física representante.  |
| Given Name (GN)                     | Nombre de la persona física representante.   |
| Serial Number (SN)                  | NIF del representante (de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas) |
| Common Name (CN)                    | Nombre y apellidos de la persona física representante.   |
| <b>SUBJECT ALTERNATIVE NAME</b>     |  |
| Rfc822Name                          | Correo electrónico.  |
| <b>SUBJECT DIRECTORY ATTRIBUTES</b> |  |
| ANCERT.10.1.1                       | Clase de apoderamiento.  |
| ANCERT.10.1.3                       | Documento de representación.   |
| ANCERT.10.1.4                       | Circunstancias adicionales de la persona física.   |
| ANCERT.10.1.5                       | Límite de uso.   |
| ANCERT.10.1.6                       | Datos registrales de la representación.  |
| ANCERT.10.1.7                       | Persona representada (jurídica)  |

### 3.1.4.5. Certificado Notarial Corporativo de Representación AGE

| <b>SUBJECT NAME</b>    |   |
|------------------------|---|
| <b>CAMPO</b>           | <b>CONTENIDO</b>  |
| Description (2.5.4.13) | <p>Documento público que acredita las facultades del representante o los datos registrales.</p> <p>En el Registro Mercantil: Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX</p> <p>Poder Notarial: Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa</p> |

|                                    |  |
|------------------------------------|--|
|                                    | En el caso de que las facultades vengan indicadas en Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX |
| Country (C)                        | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)       |
| Organization (O)                   | Razón Social, tal como figura en los registros oficiales.  |
| Organization Identifier (2.5.4.97) | NIF del representado (utilizando la semántica propuesta por la norma ETSI EN319 412-1)   |
| Organizational Unit (OU)           | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit (OU)           | "Certificado Notarial Corporativo de Representación (" + "Firma" o "Autentica" o "Cifrado" + ")"                                   |
| Surname (SU)                       | Apellidos de la persona física representante (como consta en el DNI/NIE).  |
| Given Name (GN)                    | Nombre de la persona física representante (como consta en el DNI/NIE).   |
| Serial Number (SN)                 | DNI/NIE del representante (utilizando la semántica propuesta por la norma ETSI EN319 412-1)  |
| Common Name (CN)                   | DNI/NIE Nombre Apellido1 (R: NIF) AUTENTIC / FIRMA   |
| <b>SUBJECT ALTERNATIVE NAME</b>    |  |
| Rfc822Name                         | Correo electrónico.  |

### 3.1.4.6. Certificado Notarial de Servidor Seguro (con / sin dispositivo seguro)

| <b>SUBJECT NAME<sup>2</sup></b> |  |
|---------------------------------|--|
| <b>CAMPO</b>                    | <b>CONTENIDO</b>   |
| Country (C)                     | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166) |
| Organization (O)                | Nombre de la entidad, cuando sea suscriptora del certificado.  |
| Organizational Unit (OU)        | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit (OU)        | "Certificado Notarial de Servidor Seguro"  |
| Surname (SU)                    | Apellidos de la persona física, cuando sea suscriptora del certificado.  |
| Given Name (GN)                 | Nombre de la persona física, cuando sea suscriptora del certificado.   |
| Serial Number (SN)              | CIF o NIF de la persona física o entidad suscriptora del certificado.  |
| Common Name (CN)                | Nombre del servidor y dominio. (opcional)  |
| <b>SUBJECT ALTERNATIVE NAME</b> |  |

<sup>2</sup> La longitud máxima de los campos será la definida por el RFC 5280

|            |                                 |
|------------|---------------------------------|
| Rfc822Name | Correo electrónico.             |
| DnsName    | Nombre del servidor y dominios. |

### 3.1.4.7. Certificado Notarial de Sellado de Tiempo (con / sin dispositivo seguro)

| <b>SUBJECT NAME<sup>3</sup></b> |  |
|---------------------------------|--|
| <b>CAMPO</b>                    | <b>CONTENIDO</b>   |
| Country (C)                     | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166) |
| Organization (O)                | Nombre de la entidad, cuando sea suscriptora del certificado.  |
| Organizational Unit (OU)        | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit (OU)        | "Certificado Notarial de Sellado de Tiempo"  |
| Surname (SU)                    | Apellidos de la persona física, cuando sea suscriptora del certificado.  |
| Given Name (GN)                 | Nombre de la persona física, cuando sea suscriptora del certificado.   |
| Serial Number (SN)              | CIF o NIF de la persona física o entidad suscriptora del certificado.  |
| Common Name (CN)                | Nombre de la autoridad de sellado de tiempo.   |
| <b>SUBJECT ALTERNATIVE NAME</b> |  |
| rfc822Name                      | Correo electrónico de la persona física identificada.  |

### 3.1.4.8. Certificado Notarial de Firma de Código (con / sin dispositivo seguro)

| <b>SUBJECT NAME<sup>4</sup></b> |  |
|---------------------------------|--|
| <b>CAMPO</b>                    | <b>CONTENIDO</b>   |
| Country (C)                     | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166) |
| Organization (O)                | Nombre de la entidad, cuando sea suscriptora del certificado.  |
| Organizational Unit(OU)         | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit(OU)         | "Certificado Notarial de Firma de Código"  |
| Surname (SU)                    | Apellidos de la persona física, cuando sea suscriptora del certificado.  |
| Given Name (GN)                 | Nombre de la persona física, cuando sea suscriptora del certificado.   |
| Serial Number (SN)              | CIF o NIF de la persona física o entidad suscriptora del certificado.  |
| Common Name (CN)                | Nombre del editor de código.   |

<sup>3</sup> La longitud máxima de los campos será la definida por el RFC 5280

<sup>4</sup> La longitud máxima de los campos será la definida por el RFC 5280

| <b>SUBJECT ALTERNATIVE NAME</b> |   |
|---------------------------------|---|
| rfc822Name                      | Correo electrónico de la persona física identificada. |

### 3.1.4.9. Certificado Notarial de Aplicación Segura (con / sin dispositivo seguro)

| <b>SUBJECT NAME</b>             |  |
|---------------------------------|--|
| <b>CAMPO</b>                    | <b>CONTENIDO</b>   |
| Country ©                       | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166) |
| Organization (O)                | Nombre de la entidad, cuando sea suscriptora del certificado   |
| Organizational Unit(OU)         | “Autorizado ante Notario ” + identificación de Notario   |
| Organizational Unit(OU)         | “Certificado Notarial de Aplicación Segura”  |
| Surname (SU)                    | Apellidos de la persona física, cuando sea suscriptora del certificado.  |
| Given Name (GN)                 | Nombre de la persona física, cuando sea suscriptora del certificado  |
| Serial Number (SN)              | CIF o NIF de la persona física o entidad suscriptora del certificado.  |
| Common Name (CN)                | Identificación de la aplicación segura.  |
| <b>SUBJECT ALTERNATIVE NAME</b> |  |
| rfc822Name                      | Correo electrónico de la persona física identificada.  |

### 3.1.4.10. Certificado Corporativo Notarial de facturación electrónica (sin dispositivo seguro)

| <b>SUBJECT NAME</b>             |  |
|---------------------------------|--|
| <b>CAMPO</b>                    | <b>CONTENIDO</b>   |
| Country (C)                     | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166) |
| Organization (O)                | Nombre de la entidad o persona física suscriptora del certificado.   |
| Organizational Unit (OU)        | “Autorizado ante Notario ” + identificación de Notario   |
| Organizational Unit (OU)        | "Certificado Notarial de facturación electrónica"  |
| Pseudonym                       | Seudónimo: Custodio de certificado de facturación  |
| Serial Number (SN)              | CIF o NIF de la persona física o entidad suscriptora del certificado.  |
| Common Name (CN)                | Nombre de la entidad suscriptora del certificado.  |
| <b>SUBJECT ALTERNATIVE NAME</b> |  |
| Rfc822Name                      | Correo electrónico.  |

### 3.1.4.11. Certificado Notarial de Sello Electrónico (con / sin dispositivo seguro)

| <b>SUBJECT NAME</b> |
|---------------------|
|---------------------|

| <b>CAMPO</b>                       | <b>CONTENIDO</b>   |
|------------------------------------|--|
| Country (C)                        | País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166) |
| Organization (O)                   | Razón Social, tal como figura en los registros oficiales.  |
| Organization Identifier (2.5.4.97) | CIF de la entidad subscriptora (utilizando la semántica propuesta por la norma ETSI EN319 412-1)                             |
| Organizational Unit (OU)           | "Autorizado ante Notario " + identificación de Notario   |
| Organizational Unit (OU)           | "Certificado Notarial Corporativo de Sello Electrónico"  |
| Common Name (CN)                   | Nombre utilizado para referirse a la entidad subscriptora (puede no coincidir exactamente con la razón social)               |
| <b>SUBJECT ALTERNATIVE NAME</b>    |  |
| Rfc822Name                         | Correo electrónico.  |

### **3.1.4.12. Indicación de límites de uso**

#### **3.1.4.12.1. Indicación de la clase de apoderamiento**

Este límite de uso se contiene en el atributo ANCERT.10.1.1, dentro del campo *Subject Directory Attributes* de los siguientes certificados:

- Certificados Notariales Personales de Representación.
- Certificados Notariales Corporativos.
- Certificados Notariales Corporativos de Representación.

El límite de uso corresponde al nivel de garantía en relación con el apoderamiento, indicando también la ausencia de garantía con respecto a los poderes de una persona física, con las siguientes posibilidades:

- "Sin garantía de poderes", que se emplea para indicar que el certificado se emite sin haber comprobado si la persona tiene algún poder de actuación.
- "Poderes limitados", que se emplea para indicar que el certificado se emite habiendo comprobado que la persona tiene algún poder de actuación. En este caso, debe acudir al atributo ANCERT.10.1.5 sobre límite de uso, que incorpora por referencia los poderes.
- "Poderes generales", que se emplea para indicar que el certificado se emite habiendo comprobado que la persona tiene todos los poderes generales de actuación, bien por ser un representante legal u orgánico, o por ser un representante voluntario con poderes generales de actuación.

#### **3.1.4.12.2. Indicación de límite de uso por razón de la cuantía**

Este límite de uso se contiene en el atributo QcEuLimitValue de la extensión *Qualified Certificate Statements* de los siguientes certificados:

- Certificados Notariales Personales de Representación.
- Certificados Notariales Corporativos.

- Certificados Notariales Corporativos de Representación.
- Certificados Notariales Corporativos de Facturación Electrónica.

El límite de cuantía se codifica de acuerdo con la definición contenida en la especificación ETSI TS 101 862, incluyendo los siguientes campos:

- Moneda, de acuerdo con la Norma ISO 4217.
- Cantidad.
- Exponente.

El valor límite se calcula mediante la siguiente fórmula:  $\text{Valor} = \text{Cantidad} \times 10^{\text{Exponente}}$

#### **3.1.4.12.3. Indicación de límite de uso por razón de la materia**

Este límite de uso se contiene en el atributo ANCERT.10.1.5, dentro del campo *Subject Directory Attributes* de los siguientes certificados:

- Certificados Notariales Personales de Representación.
- Certificados Notariales Corporativos.
- Certificados Notariales Corporativos de Representación.
- Certificados Notariales de Facturación Electrónica.
- Certificados Notariales de Aplicación Segura.
- Certificados Notariales de Sellado de Tiempo.

Este atributo siempre se emplea cuando en el atributo ANCERT.10.1.1 se contiene la clase de apoderamiento "Poderes limitados".

Corresponde a cualquier límite de uso del certificado por razón de la materia (se entiende que diferente del límite de cuantía), expresado como una URL que contiene la lista de los poderes / facultades de que dispone el representante.

#### **3.1.4.13. Indicación de atributos adicionales de la persona física**

Los certificados Notariales pueden incorporar atributos adicionales de la persona física solicitante, como por ejemplo: pertenencia a un Colegio profesional, cargos honoríficos, etc...), dentro del atributo ANCERT.10.1.4 del campo *Subject Directory Attributes*.

#### **3.1.4.14. Informaciones adicionales en relación con la representación**

Los certificados donde se indica una representación contienen las siguientes informaciones específicas, que se contienen en atributos dentro de campo *Subject Directory Attributes*:

En el atributo ANCERT.10.1.3 se contiene el documento de representación.

Dicho atributo incluye el nombre y apellidos del Notario autorizante del documento de representación, así como número y año del protocolo correspondiente, en caso de poder notarial; o a la Entidad u Órgano otorgante, en caso de que la representación no derive de un poder notarial.

En el atributo ANCERT.10.1.6 se contienen los datos registrales de la representación.

Dicho atributo incluye los datos referentes a la inscripción de la escritura pública o actuación judicial del nombramiento del representante, inscrito en el registro jurídico o administrativo correspondiente a la persona física o jurídica, cuando la misma sea obligatoria.

En el atributo ANCERT.10.1.7 se contiene la identificación de la persona representada.

Dicho atributo incluye un nombre diferenciado, formado por una combinación de los siguientes componentes.

- Cuando el representado es una persona física:
  - Country.
  - Surname.
  - Given Name.
  - Serial Number.
- Cuando el representado es una persona jurídica:
  - Country.
  - Organization.
  - Serial Number.

La Agencia Notarial de Certificación publica en el Depósito la información sobre la sintaxis y la semántica necesaria para el tratamiento de dichas extensiones y atributos privados, por parte de los terceros.

### **3.1.5. Unicidad de los nombres**

Los nombres de los suscriptores de certificados son únicos para cada Entidad de Certificación operada por la Agencia Notarial de Certificación. Una persona sólo puede tener más de un certificado con el mismo nombre a la vez, durante el período de renovación de certificados, para garantizar la continuidad de sus operaciones.

En ningún caso se asigna un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente.

### **3.1.6. Resolución de conflictos relativos a nombres y tratamiento de marcas registradas**

Los conflictos de nombres se solucionan mediante la inclusión, en el nombre diferenciado del certificado, del número del Documento Nacional de Identidad, o equivalente, del poseedor de la clave, así como del número del Código de Identificación Fiscal de la persona jurídica, según proceda.

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



La Agencia Notarial de Certificación establece controles razonables para asegurar que los solicitantes de un certificado tienen derecho sobre una marca incluida en una solicitud de certificado mediante consultas a la base de datos de la Oficina Española de Patentes y Marcas.

Sin perjuicio de lo anterior, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación española, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, la Agencia Notarial de Certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

## **3.2. Validación inicial de la identidad**

En esta sección se declaran los procedimientos de identificación y autenticación que deben emplearse durante el registro de suscriptores, incluyendo entidades y personas físicas, que debe realizarse con anterioridad a la emisión y entrega de certificados.

### **3.2.1. Prueba de posesión de clave privada**

Esta sección describe los métodos a emplear para demostrar que se posee la clave privada correspondiente a la clave pública objeto de certificación.

El método de demostración de posesión de la clave privada será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método fiable aprobado por la Agencia Notarial de Certificación.

Este requisito no se aplica cuando el par de claves es generado por la entidad de registro, por delegación del suscriptor, durante el proceso de personalización o de entrega del dispositivo cualificado de creación de firma al suscriptor o poseedor de claves.

En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del dispositivo cualificado y del correspondiente certificado y par de claves almacenados en su interior.

### **3.2.2. Autenticación de la identidad de la organización**

En general, debe aportarse por el solicitante documentación justificativa acerca de los siguientes extremos:

- Nombre legal completo de la organización.
- Estado legal de la organización.
- Número de identificación fiscal.
- Datos de identificación registral.

#### **3.2.2.1. Elementos de identificación requeridos**

El documento necesario para acreditar al Notario la identidad de la persona jurídica es la escritura de constitución de la misma o, en los casos de organizaciones cuya constitución no requiere escritura, cualquier documento público que dé fe de la identidad de la organización.

### **3.2.2.2. Validación de los elementos de identificación**

La Agencia Notarial de Certificación emplea un Notario español como entidad de registro para esta tarea, encargadas de la comprobación de la documentación justificativa aportada por el solicitante.

### **3.2.3. Autenticación de la identidad de la persona física**

El proceso de identificación y autenticación de una persona física se realiza exclusivamente mediante la personación ante un Notario español, que actúa como entidad de registro.

#### **3.2.3.1. Elementos de identificación requeridos**

Los tipos de documentos que son necesarios para acreditar la identidad de una persona física son exclusivamente el documento nacional de identidad, la tarjeta de residencia, el pasaporte, o cualquier otro medio admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos.
- Fecha de nacimiento.
- Número de identidad fiscal (NIF o, en su caso, NIE)

Cuando se trate de Certificados Notariales Personales de Representación Personal, además, es necesario para acreditar al solicitante su condición de representante de otra persona física, escritura, documento público o en su caso resolución judicial o administrativa de donde derive la representación.

Cuando en el certificado se quieran hacer constar otros atributos de la persona física (pertenencia a un Colegio profesional, cargos honoríficos, etc.), el Notario recabará los documentos de los que puedan derivarse dichas circunstancias, pudiendo incluso, tramitar la correspondiente acta de notoriedad de donde se puedan concluir los atributos a incorporar en el certificado.

El solicitante puede aportar certificación original emitida dentro de los diez días anteriores a la solicitud del certificado, por el organismo o empresa que acredite algún atributo adicional. Es responsabilidad del suscriptor la comunicación a la Agencia Notarial de Certificación de posibles cambios de atributos personales.

#### **3.2.3.2. Validación de los elementos de identificación**

La validación de los elementos de identificación requeridos la hace personalmente un Notario español, comprobando la vigencia, originalidad, autenticidad y suficiencia de la documentación aportada.

#### **3.2.3.3. Necesidad de presencia personal**

Para los certificados en los que tenga que identificarse una persona física, es necesaria la presencia de la persona identificada en el certificado.

Para los certificados notariales corporativos puede prescindirse de la personación ante el Notario de la persona física que actúe como custodio del certificado (y que conste en la escritura como tal)

si se aporta una solicitud de expedición del Certificado Notarial Corporativo con la firma legitimada en presencia notarial.

#### **3.2.3.4. Vinculación de la persona física con una entidad**

Para los Certificados Notariales sólo existe vinculación entre una persona física y una entidad en los certificados Corporativos y Corporativos de Representación.

En los Certificados Notariales Corporativos, la persona física vinculada la llamamos Custodio. En los Certificados Notariales Corporativos de Representación, la persona física vinculada a la entidad es el Representante.

El documento para acreditar a una persona física la condición de representante de una entidad es la escritura o documento público de donde derive la representación.

Cuando una persona física actúe como representante de una entidad, el Notario calificará la suficiencia de las facultades comprobando los datos aportados, bien mediante consulta en el Registro en el que estén inscritos los documentos de apoderamiento y de constitución de la entidad representada, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquellos no sean de inscripción obligatoria.

En el caso de realizar la consulta en el Registro Mercantil, aún en el supuesto de no constar debidamente inscritas las facultades, el Notario puede autorizar el proceso de solicitud aplicando la legislación mercantil para los representantes legales de sociedades (se incluye el caso en que la acreditación de las facultades se documente en una escritura autorizada por el Notario que actúe como entidad de registro). La consulta registral se efectuará comunicándose con el Registro Mercantil Central para que le trasmita la información mercantil suministrada por los Registros Mercantiles Provinciales de las sociedades mercantiles inscritas.

Para los Certificados Notariales Corporativos, el Notario califica la suficiencia de las facultades comprobando los datos aportados por el solicitante de conformidad con lo dispuesto en la Ley de Firma Electrónica.

#### **3.2.4. Autenticación de la identidad de sistemas de información**

##### **3.2.4.1. Validación de los elementos de identificación**

Se comprueban los siguientes datos del propietario (*owner*): contacto, organización, nombre completo y datos de contacto.

##### **3.2.5. Información de suscriptor no verificada**

No se incluye información de suscriptor no verificada en los certificados.

### **3.3. Identificación y autenticación de solicitudes de renovación con cambio de claves**

#### **3.3.1. Validación para la renovación rutinaria de certificados**

Se podrán renovar certificados durante su periodo de vigencia.

Antes de renovar un certificado, la Agencia Notarial de Certificación, mediante la actuación de las entidades de registro, comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.

Se puede emplear la firma electrónica basada en un certificado para solicitar la renovación del mismo, siempre antes de su expiración.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registra adecuadamente la nueva información, de acuerdo con lo establecido en la sección 3.2 de esta Declaración de Prácticas de Certificación.

### **3.3.2. Validación para la renovación de certificados tras la revocación**

No resulta aplicable, debido a que la Agencia Notarial de Certificación no renueva en ningún caso certificados que han sido revocados.

## **3.4. Identificación y autenticación de las solicitudes de cambio de estado**

### **3.4.1. Identificación y autenticación de la solicitud de suspensión**

El legítimo solicitante deberá telefonar al número 912187676 del Centro de Atención a Usuarios de la Agencia Notarial de Certificación.

A los efectos probatorios oportunos, la conversación entre el operador y el solicitante de la suspensión es sometida a grabación.

### **3.4.2. Identificación y autenticación de la solicitud de revocación**

La Agencia Notarial de Certificación autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada, mediante los siguientes métodos:

- Presencialmente ante Notario, cumpliendo los mismos requisitos que para la solicitud de emisión de certificado, en cuanto a la identificación y la titularidad del certificado a revocar.
- Mediante la firma electrónica válida de la solicitud de revocación realizada con el certificado a revocar.

## **4. Requisitos de operación del ciclo de vida de los certificados**

### **4.1. Solicitud de emisión de certificado**

Antes de la emisión y entrega de un certificado, existe una solicitud de certificado, a instancia de parte interesada.

Existen los siguientes tipos de solicitudes:

- 1) Presolicitud, que consiste en una solicitud, electrónica o presencial, de un certificado (no contiene clave pública, ni se encuentra firmada digitalmente).
- 2) Solicitud, que se realiza presencialmente, y que en todo caso produce una petición técnica y electrónica de certificado por la entidad de registro, con generación de claves o sobre una clave pública aportada por el solicitante (PKCS#10 o mecanismo compatible, con la clave pública del usuario y su firma digital, al objeto de demostrar la posesión de la clave privada, de acuerdo con la sección 3.2.1 de la presente Declaración de Prácticas de Certificación).

#### **4.1.1. Legitimación para solicitar la emisión**

Están legitimados para solicitar la emisión de un certificado:

- 1) El futuro suscriptor que sea persona física.
- 2) El representante de una persona física o jurídica, incluyendo un órgano colegiado de una entidad, mediante la actuación de todos los miembros del mismo.
- 3) El custodio de certificados notariales corporativos.

Para que los terceros puedan confiar en los términos del certificado expedido a una persona física representante de otra persona, es necesaria la concurrencia de dos elementos, uno de carácter subjetivo y otro de carácter objetivo, que son respectivamente los siguientes:

- 1) Que el Notario califique la suficiencia de las facultades de la persona física que actúa en nombre y representación de la persona y solicita el certificado para sí.
- 2) Que el certificado recoja en términos genéricos o específicos el alcance de las facultades que van a poder ser objeto de contratación y representación con su uso, de acuerdo con lo establecido en la sección 3.1.4.11 de esta Declaración de Prácticas de Certificación.

Adicionalmente, cuando el solicitante sea un representante de la persona jurídica que solicita certificados para otras personas físicas, comparece ante el Notario que actúa como entidad de registro, identificando a las personas físicas que vayan a resultar identificadas en los certificados y que ostentarán la condición de poseedores de claves.

Los certificados se solicitarán para éstos, en función del ámbito de representación que tengan previamente concedido en los documentos públicos de los que resulte su representación, y dentro de las facultades de delegación de facultades que ostente la persona que actúe como solicitante.

Las facultades de representación que recojan directa o indirectamente los certificados tienen que corresponderse, como máximo, con las que ostenten los solicitantes en los documentos públicos de los que traigan causa.

En la concesión, el Notario comprueba, igualmente, que el Solicitante actuó como representante de la persona jurídica poderdante en el momento de otorgarse el apoderamiento en virtud del cual se concede el certificado. La recepción del certificado tiene que realizarse, necesariamente, por el poseedor de claves, y debe constar por diligencia en la póliza que documente el registro de la emisión.

#### **4.1.2. Procedimiento de alta: Responsabilidades.**

La fase de solicitud del certificado comprende con carácter general la personación ante un Notario Español, para la comprobación y confirmación de la identidad personal del solicitante, así como la aportación de la documentación que corresponda, la cumplimentación de formularios, y suscripción de los contratos que se establezcan.

Durante esta fase, el Notario asegura que las solicitudes de certificado son completas, precisas y están debidamente autorizadas, e informa al suscriptor o al poseedor de claves, según proceda, de los términos y condiciones aplicables al certificado.

La citada información se comunica en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible.

A la solicitud se acompaña la documentación justificativa de la identidad y otras circunstancias del solicitante, del futuro suscriptor y del poseedor de claves, según proceda, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3 de esta Declaración de Prácticas de Certificación.

También se acompaña una dirección física, u otros datos, que permiten contactar al solicitante, al futuro suscriptor y al poseedor de claves, según proceda.

### **4.2. Procesamiento de la solicitud de certificación**

#### **4.2.1. Ejecución de las funciones de identificación y autenticación**

Una vez recibida una petición de certificado, el Notario verifica la información proporcionada, conforme a la sección 3.2 de esta Declaración de Prácticas de Certificación.

Dicha comprobación se realiza, en general, en el mismo acto y en presencia del solicitante, con las siguientes excepciones:

- Las solicitudes realizadas por solicitantes de Certificados Notariales Corporativos de Representación, para terceras personas requerirán la ulterior personación de dichas personas, procediéndose a la comprobación de los extremos pertinentes.
- Las solicitudes de Certificados Notariales Corporativos que se hayan practicado con legitimación de firma ante Notario no exigirán la nueva personación del custodio.

Para los Certificados Notariales de Sistemas donde constan nombres de dominio, es necesario establecer una conexión en línea a cualquier registrador de dominios de Internet para obtener el documento acreditativo de la posesión del nombre de dominio.

Además de esta verificación se comprobará y procesará para cada dominio incluido en el certificado la entrada DNS de tipo Certification Authority Authorization (CAA) de acuerdo con lo establecido en el RFC 6844 y en la sección 3.2.2.8 del documento “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates” del CA/Browser Forum.

#### **4.2.2. Aprobación o rechazo de la solicitud**

En general, cuando la documentación aportada por el compareciente sea insuficiente, el Notario no autorizará documento alguno ni solicitará la emisión del certificado, debiendo comparecer de nuevo una vez subsanado el/los defecto/s.

En caso de que los datos se verifiquen correctamente, el Notario aprueba la solicitud del certificado, aprobación que notifica al solicitante en ese mismo acto.

#### **4.2.3. Plazo para resolver la solicitud**

Sin estipulación.

### **4.3. Emisión del certificado**

La emisión de Certificados Notariales de firma electrónica se realiza generalmente en un dispositivo cualificado de creación de firma, excepto para los Certificados Notariales de Sistemas que también se podrán emitir en software.

La emisión de Certificados Notariales de sello electrónico con garantía de dispositivo seguro se realiza mediante un dispositivo cualificado de creación de sello electrónico.

Entendemos por dispositivo cualificado, una tarjeta criptográfica, un dispositivo USB o cualquier otro tipo de dispositivo, en especial maquinaria criptográfica (HSM), que cumpla con los requisitos establecidos por el Anexo II del Reglamento (UE) 910/2014 y que aparezca en la lista de dispositivos cualificados de creación de firma a la que hace referencia el artículo 31 de dicho reglamento.

#### **4.3.1. Acciones durante el proceso de emisión**

Para la emisión de un certificado el Notario, actuando como entidad de registro, debe acceder a la aplicación de emisión de certificados. El acceso a la aplicación está protegido, identificando al Notario mediante su certificado digital. La aplicación comprueba que el Notario, una vez autenticado, está autorizado para emitir certificados notariales. De esta forma se asegura que la comunicación entre la RA y la CA se lleva a cabo de forma segura.

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado. Las acciones a seguir para la emisión de las claves y el certificado son distintas, según si el soporte para su almacenamiento es una tarjeta criptográfica o bien un módulo de maquinaria de seguridad o una aplicación informática.

En todos los casos, la Agencia Notarial de Certificación:

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados electrónicamente con el solicitante, durante la presolicitud.
- Incluye en el certificado las informaciones establecidas en el Anexo I del Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 3.1 y 7.1 de esta Declaración de Prácticas de Certificación.
- Indica la fecha y la hora en que se expide el certificado.
- En los casos en que la Agencia Notarial de Certificación aporta el dispositivo cualificado de creación de firma, como la tarjeta criptográfica, emplea un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al solicitante o al poseedor de claves, según proceda.
- Utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Asegura que el certificado es emitido por sistemas que utilizan protección contra falsificación y, cuando genera claves privadas, que garantizan la confidencialidad de las claves durante el proceso de generación de dichas claves.

#### **4.3.1.1. Emisión en tarjeta criptográfica**

Las acciones a seguir son las siguientes:

1. El Notario introduce en el lector de tarjetas su tarjeta criptográfica con el certificado que le autentica como entidad de registro y accede a la aplicación de registro.
2. Una vez autenticado, el Notario introduce en el lector de tarjetas la tarjeta criptográfica del poseedor de claves, que previamente le ha sido entregada por el citado Notario junto a los códigos PIN y PUK correspondientes en sobre cerrado.
3. El Notario completa el formulario de registro con los datos que le debe aportar el solicitante y solicita la emisión del certificado.
4. En este momento, la aplicación de registro solicita el PIN correspondiente a la tarjeta criptográfica del solicitante, para activar el procedimiento de generación de claves.
5. En ese momento se genera el par de claves en la tarjeta criptográfica del suscriptor, enviando la petición a la Agencia Notarial de Certificación, la cual genera el certificado y lo remite al ordenador del Notario vía TSL, quedando almacenado automáticamente en la tarjeta criptográfica del suscriptor.

#### **4.3.1.2. Emisión en módulo de maquinaria de seguridad o en aplicación informática**

Las acciones a seguir para la emisión en este soporte son las siguientes:

1. El solicitante debe presentar al Notario el archivo en formato PKCS#10 que contiene la petición de certificado.



2. El Notario procede a introducir en el lector de tarjetas su tarjeta criptográfica con el certificado que le autentica como Notario autorizado a emitir Certificados Notariales y accede a la aplicación de registro.

3. El Notario comprueba, mediante las herramientas que le proporciona la Agencia Notarial de Certificación, que el archivo facilitado por el solicitante corresponde con la información aportada y el perfil del certificado.

4. Si los datos son correctos completa el formulario de petición de certificado y envía la petición a la Agencia Notarial de Certificación.

5. En un plazo máximo de 48 horas, el solicitante puede obtener su Certificado Notarial descargándolo de la dirección [www.ancert.com](http://www.ancert.com).

#### **4.3.2. Notificación de la emisión al suscriptor**

La Agencia Notarial de Certificación notifica, en el acto de emisión o posteriormente, la emisión del certificado al suscriptor o, en su caso, al poseedor de claves.

En certificados de sistemas o certificados de otros tipos emitidos a claves generadas en dispositivos seguros que estuvieran previamente en poder del solicitante, se notifica que el certificado se encuentra disponible en un plazo máximo de 48 horas, y que el solicitante puede obtener su Certificado Notarial descargándolo de la dirección [www.ancert.com](http://www.ancert.com).

#### **4.4. Entrega y aceptación del certificado**

La Agencia Notarial de Certificación:

- Proporciona al suscriptor o al poseedor de claves, acceso al certificado, entregando, en su caso, el dispositivo cualificado.
- Mediante el notario como entidad de registro se autoriza en una póliza en presencia del solicitante o, en su caso, del poseedor de claves, la aceptación de las condiciones generales de emisión de certificados, con los siguientes contenidos mínimos:
  - a) Información básica acerca de la política y uso del certificado, incluyendo especialmente información acerca de la Agencia Notarial de Certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades
  - b) Información acerca del certificado y del dispositivo cualificado, según proceda.
  - c) Reconocimiento por parte de suscriptor o poseedor de claves, según proceda, de recibir el certificado y, en su caso, el dispositivo cualificado, y aceptación de los citados elementos.
  - d) Obligaciones del suscriptor y, en su caso, del poseedor de claves.
  - e) Responsabilidad del suscriptor y, en su caso, del poseedor de claves.
  - f) Método de imputación exclusiva al suscriptor y, en su caso, al poseedor, de su clave privada y de sus datos de activación del certificado y, cuando proceda, del dispositivo cualificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4 de esta Declaración de Prácticas de Certificación.

g) La fecha del acto de entrega y aceptación.

#### **4.4.1. Conducta que constituye aceptación del certificado**

La aceptación del certificado por parte del suscriptor se entiende producida desde el momento de su emisión y entrega al mismo por la Agencia Notarial de Certificación y firma ante Notario de la correspondiente póliza.

Al aceptar el certificado el suscriptor también acepta además las normas de uso y las condiciones contenidas en la presente Declaración de Prácticas de Certificación.

En todo caso, al aceptar un Certificado emitido por la Agencia Notarial de Certificación, el suscriptor del mismo declara:

- a) Que toda la información entregada durante el procedimiento de solicitud del Certificado es verdadera.
- b) Que el Certificado será usado exclusivamente para fines legales y autorizados por la Agencia Notarial de Certificación, de acuerdo a la presente Declaración de Prácticas de Certificación y siempre dentro del ámbito determinado en cada Política de Certificación.
- c) Que asegura su exclusivo control sobre los Datos de creación de Firma que se correspondan con los Datos de verificación de Firma incluidos en su certificado emitido por la Agencia Notarial de Certificación y vinculados a su identidad personal, lo que, en todo caso y a título meramente enunciativo, incluirá las acciones y medidas necesarias para prevenir su pérdida, revelación, modificación, o uso por tercero distinto del suscriptor.

La Agencia Notarial de Certificación considera válido todo certificado aceptado por el suscriptor y publicado en su Depósito de Certificados correspondiente, siempre que no haya caducado y que no conozca ninguna causa de revocación que le afecte.

#### **4.4.2. Publicación del certificado**

Una vez emitido el certificado, la Agencia Notarial de Certificación publica automáticamente una copia del mismo en el Depósito de Certificados correspondiente, cumpliendo con lo establecido en la sección 2.1 de esta Declaración de Prácticas de Certificación y con los controles de acceso pertinentes.

#### **4.4.3. Notificación de la emisión a terceros**

La Agencia Notarial de Certificación no notifica la emisión de certificados a terceros.

## **4.5. Uso del par de claves y del certificado**

### **4.5.1. Uso por el suscriptor y, en su caso, poseedor de claves**

#### **4.5.1.1. Obligaciones del suscriptor y en su caso, poseedor de claves**

La Agencia Notarial de Certificación obliga al suscriptor, mediante las condiciones generales de emisión, a:

- En caso que el suscriptor genere sus propias claves, a:
  - a) Generar sus claves de suscriptor empleando un algoritmo reconocido como aceptable para la firma electrónica cualificada.
  - b) Crear las claves dentro del dispositivo cualificado de creación de firma
  - c) Emplear longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica cualificada.
- Facilitar a la Agencia Notarial de Certificación y a sus entidades de registro información completa y adecuada, en especial en lo relativo al procedimiento de registro.
- Manifiestar su consentimiento previo a la emisión y entrega de un certificado, así como a su publicación en el Depósito y cuando, proceda, a la notificación de la emisión a terceros.
- Cumplir las obligaciones que se establecen para el suscriptor en la presente Declaración de Prácticas de Certificación.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4 de esta Declaración de Prácticas de Certificación.
- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de esta Declaración de Prácticas de Certificación, no cediendo el uso de la clave privada a ninguna otra persona.
- Comunicar a la Agencia Notarial de Certificación y a cualquier persona que el suscriptor o el poseedor de claves crea que pueda confiar en el certificado, sin retrasos injustificables:
  - a) La pérdida, el robo o el compromiso potencial de su clave privada o del dispositivo cualificado.
  - b) La pérdida de control sobre su clave privada o del dispositivo cualificado, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo cualificado de creación de firma) o por cualquier otra causa.
  - c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor o el poseedor de claves.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2 de esta Declaración de Prácticas de Certificación.
- Transferir a los poseedores de claves las obligaciones específicas de los mismos.

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.

El suscriptor del certificado de firma electrónica que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado reconoce, en el debido documento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, conforme a lo establecido en el artículo 25 del Reglamento (UE) 910/2014.

#### **4.5.1.2. Responsabilidad civil del suscriptor de certificado**

La Agencia Notarial de Certificación obliga al suscriptor y, en su caso, al poseedor de claves, mediante las condiciones generales de emisión, a garantizar:

- En caso de que el suscriptor fuese el solicitante del certificado, que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con esta Declaración de Prácticas de Certificación.
- Que cada firma digital creada empleando la clave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.
- Que el suscriptor 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 a título de prestador de servicios de certificación ni en ningún otro caso.
- Que sólo creará firmas digitales mientras tenga la seguridad que ninguna persona no autorizada ha tenido jamás acceso a su clave privada.
- Que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada y, en su caso, de generar correctamente dicha clave y emplear un dispositivo cualificado de firma.

#### **4.5.2. Uso por el tercero que confía en certificados**

##### **4.5.2.1. Obligaciones del tercero que confía en certificados**

La Agencia Notarial de Certificación obliga al tercero que confía en certificados, mediante las condiciones generales de uso, a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión 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 tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.
- En relación con los certificados que permiten la firma electrónica, reconocer que las firmas electrónicas válidamente verificadas con los certificados son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con el artículo 25 del Reglamento (UE) 910/2014.

#### **4.5.2.2. Responsabilidad civil del tercero que confía en certificados**

La Agencia Notarial de Certificación obliga al tercero que confía en el certificado, mediante las condiciones generales de uso, a reconocer:

- 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 de certificados**

No se permite la renovación de certificados sin cambio de claves.

#### **4.7. Renovación de certificados con cambio de claves**

##### **4.7.1. Causas de renovación de claves y certificados**

Los certificados deben renovarse conjuntamente con las claves cuando se llegue al final del periodo de vida de las mismas, o del periodo de vida del dispositivo cualificado en que se contengan.

#### **4.7.2. Legitimación para solicitar la renovación**

Antes de la emisión y entrega de un certificado renovado, existe una solicitud de renovación de certificado, que se produce a instancia del suscriptor o del poseedor de claves, según proceda.

#### **4.7.3. Procesamiento de la solicitud de renovación**

La solicitud de renovación podrá ser realizada y enviada por el suscriptor o el poseedor de claves, con su certificado vigente, como prueba de posesión de clave privada, siempre que no hayan transcurrido más de cinco años desde la emisión del certificado a renovar.

En caso que la información a incluir en el certificado renovado no haya cambiado, incluyendo la información de contacto, se emite y entrega automáticamente un nuevo certificado.

En caso de renovación de certificados que hayan expirado o hayan sido revocados, no se procede a la renovación automática, y deben realizarse todos los procedimientos de emisión de un certificado nuevo.

Para las renovaciones de certificados presenciales deben realizarse todos los procedimientos de emisión de un certificado nuevo.

#### **4.7.4. Notificación de la emisión del certificado renovado**

La Agencia Notarial de Certificación notifica la emisión del certificado al suscriptor y al poseedor de claves, según proceda, en la dirección de correo electrónico informada en el mismo.

#### **4.7.5. Conducta que constituye aceptación del certificado**

Sin estipulación.

#### **4.7.6. Publicación del certificado**

La Agencia Notarial de Certificación publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

#### **4.7.7. Notificación de la emisión a terceros**

La Agencia Notarial de Certificación no notifica la renovación de certificados a terceros.

### **4.8. Modificación de certificados**

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, se trata como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1 a 4.4 de esta Declaración de Prácticas de Certificación.

### **4.9. Revocación y suspensión de certificados**

#### **4.9.1. Causas de revocación de certificados**

La Agencia Notarial de Certificación revoca un certificado debido, por lo menos, a 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.
  - 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.
- 2) Circunstancias que afectan a la seguridad de la clave o del certificado:
  - a) Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
  - b) Infracción, por la Agencia Notarial de Certificación, 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 del suscriptor o del poseedor de claves.
  - d) Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor o del poseedor de claves.
  - e) El uso irregular del certificado por el suscriptor o del poseedor de claves, o la falta de diligencia en la custodia de la clave privada.
- 3) Circunstancias que afectan a la seguridad del dispositivo criptográfico:
  - a) Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
  - b) Pérdida o inutilización por daños del dispositivo criptográfico.
  - c) Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del poseedor de claves.
- 4) Circunstancias que afectan al suscriptor o al poseedor de claves:
  - a) Finalización de la relación jurídica entre la Agencia Notarial de Certificación y el suscriptor.
  - b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o del poseedor de claves.
  - c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
  - d) Infracción por el suscriptor o del poseedor de claves, de sus obligaciones, responsabilidad y garantías, establecidas en las condiciones generales de emisión correspondientes o en esta Declaración de Prácticas de Certificación<sup>5</sup>.

---

<sup>5</sup> En especial, para los certificados de firma de código, es responsabilidad del suscriptor que no se utilice el certificado para firmar cualquier tipo de código que pueda ser considerado hostil (incluyendo spyware y malware). Si tras recibir

- e) La incapacidad sobrevenida o el fallecimiento del suscriptor o del poseedor de claves.
- f) En caso de certificados de colectivo, 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 poseedor de claves.
- g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.2 de esta Declaración de Prácticas de Certificación.

5) Otras circunstancias:

- a) La suspensión del certificado digital por un período superior al establecido en la sección 4.9.16 de esta Declaración de Prácticas de Certificación.
- b) La modificación de la Declaración de Prácticas de Certificación que no sea aceptada por el suscriptor del certificado.
- c) La terminación del servicio por la Agencia Notarial de Certificación, de acuerdo con lo establecido en la sección 5.8 de esta Declaración de Prácticas de Certificación.

Si la entidad a la que se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión.

En este caso se considera que las actuaciones realizadas durante el período de suspensión no son válidas, siempre y cuando el certificado finalmente sea revocado. Son válidas si se levanta la suspensión y el certificado vuelve a pasar a la situación de válido.

Las condiciones generales de emisión establecen la obligación de solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

#### **4.9.2. Legitimación para solicitar la revocación**

Están legitimados para solicitar la revocación de un certificado:

- En todo caso el suscriptor a nombre del cual el certificado fue emitido, sea persona física o entidad. Cuando se trate de una entidad, ésta deberá actuar a través de una persona física con facultades jurídicas suficientes para revocar el certificado.
- En caso de certificados de representación, también el representado, sea persona física o entidad. Cuando el representado sea una entidad deberá actuar a través de una persona física con facultades jurídicas suficientes para revocar las facultades alegadas por el custodio en el momento de la obtención del certificado, o la relación de representación que consta en el certificado.
- Cualquier Notario actuando como entidad de registro.

---

una queja se verifica que se está produciendo un mal uso del certificado por el motivo anterior, esta será causa inmediata de su revocación.



### **4.9.3. Procedimientos de solicitud de revocación**

La entidad que precise revocar un certificado debe solicitarlo a la Agencia Notarial de Certificación o, en su caso, a cualquier entidad de registro de las autorizadas, comprensiva de la siguiente información:

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

En aquellos casos en que se requiera revocación inmediata del certificado, se puede hacer una llamada, solicitando la suspensión, o enviar un correo electrónico a la Agencia Notarial de Certificación, a la dirección de correo electrónico [revocacion@ancert.com](mailto:revocacion@ancert.com).

La solicitud es autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 3.4.2 de esta Declaración de Prácticas de Certificación, antes de proceder a la revocación.

En caso de que el destinatario de la solicitud sea un Notario actuando como entidad de registro, ésta deberá:

- Identificar al solicitante de acuerdo con los requisitos establecidos en la sección 3.4.2 de esta Declaración de Prácticas de Certificación.
- Verificar que el solicitante está autorizado a solicitar la revocación del certificado.
- Autorizar una póliza de revocación del Certificado.
- Solicitar la revocación accediendo a la aplicación telemática de revocación.

La solicitud de revocación es procesada a su recepción.

Se informa al suscriptor y, en su caso, al poseedor de claves, acerca del cambio de estado del certificado revocado.

La Agencia Notarial de Certificación no puede reactivar el certificado, una vez revocado.

#### **4.9.3.1. Solicitud de revocación de certificados de Firma de Código**

En aquellos casos en que un tercero detecte que se está utilizando un certificado de Firma de Código emitido por la Agencia Notarial de Certificación para firmar código hostil puede denunciarlo a la dirección [revocacion@ancert.com](mailto:revocacion@ancert.com). En el correo se deberá proveer de la información del certificado y de un método de contacto para que la Agencia Notarial de Certificación se pueda comunicar con el denunciante para el estudio del caso. Tan pronto como la Agencia Notarial de Certificación pueda resolver si se está incurriendo en un uso prohibido o no del certificado, procederá a la ejecución de solicitud de revocación o a su denegación.

#### **4.9.4. Plazo temporal de solicitud de revocación**

Las solicitudes de revocación se remitirán de forma razonablemente inmediata en cuanto se tenga conocimiento de la causa de revocación.

Fuera del horario de atención de las Autoridades de Registro, el suscriptor puede solicitar la suspensión cautelar del certificado a través del Servicio de Atención al usuario según el procedimiento establecido en la sección **¡Error! No se encuentra el origen de la referencia..**

#### **4.9.5. Plazo temporal para procesar las solicitudes de revocación**

El tiempo transcurrido entre la recepción de una solicitud de revocación y la ejecución del cambio de estado del certificado correspondiente no superará en ningún caso las 24 horas, incluyendo en éste el tiempo de diseminación de la información de la información de revocación.

#### **4.9.6. Obligación de consulta de información de revocación de certificados**

Los terceros que confían en certificados deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación Certificados Notariales.

La Agencia Notarial de Certificación suministra información a los terceros que confían en certificados acerca de cómo y dónde encontrar la Lista de Revocación de Certificados correspondiente; entre otros métodos, mediante la inclusión de la dirección web de publicación de las listas dentro de los propios certificados emitidos.

#### **4.9.7. Frecuencia de emisión de listas de revocación de certificados (CRLs)**

La Agencia Notarial de Certificación emite una nueva CRL al menos cada 24 horas. Adicionalmente, se emitirá una nueva CRL después de la suspensión o revocación de un certificado.

Se indica en la CRL el momento programado de emisión de una nueva CRL, si bien se puede emitir una CRL antes del plazo indicado en la CRL anterior.

Los certificados son retirados de la CRL pasados 60 días de su fecha de caducidad.

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

Una vez generadas las CRLs son publicadas en los puntos de distribución indicados en la extensión del certificado con un tiempo de propagación inferior a quince minutos.

#### **4.9.9. Disponibilidad de servicios de comprobación de estado de certificados**

La Agencia Notarial de Certificación dispone de un servicio OCSP público para suministrar información de estado sobre los certificados, accesible en la dirección web indicada en los propios certificados emitidos.

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

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Agencia Notarial de Certificación, ésta realizará sus mejores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible.

#### **4.9.10. Requisitos de comprobación de revocación online**

La petición OCSP para la consulta del estado de un certificado debe incluir el número de serie del certificado y los datos identificativos de la autoridad de certificación emisora del mismo.

El servicio OCSP sigue ofreciendo información de estado de los certificados más allá del periodo de validez de los mismos.

La respuesta generada por el servicio OCSP contiene la información de estado del certificado en el momento de la consulta. Si la petición no se puede satisfacer, el servidor generará una respuesta de error. El validador del certificado debe asegurarse que el certificado firmante de la respuesta OCSP es un certificado con el uso de clave extendido de firma de respuestas OCSP y que ha sido emitido por la misma entidad de certificación que el certificado que está consultando.

#### **4.9.11. Otras formas de información de revocación de certificados**

De forma alternativa, los terceros que confían en certificados pueden consultar su estado en el Depósito de certificados de la Agencia Notarial de Certificación, que se encuentra disponible las 24 horas de los 7 días de la semana, en la dirección web <https://www.ancert.com>.

#### **4.9.12. Requisitos especiales en caso de compromiso de la clave privada**

El compromiso de la clave privada de una Entidad de Certificación de la Clase Notariales se notifica, en la medida de lo posible, a todos los participantes en los servicios de certificación del Consejo General del Notariado y la Agencia Notarial de Certificación.

Dicha notificación se produce, al menos, mediante la publicación de la información en el Depósito de la Agencia Notarial de Certificación.

#### **4.9.13. Causas de suspensión de certificados**

La Agencia Notarial de Certificación puede suspender certificados en los siguientes casos:

- La simple solicitud.
- Resolución judicial o administrativa que lo ordene, o la existencia de una investigación o procedimiento judicial o administrativo que pudiera determinar que el certificado está afectado por una causa de revocación.
- La existencia de dudas fundadas acerca de la concurrencia de las causas de revocación de los certificados.

Debe asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar las causas anteriores.

#### **4.9.14. Legitimación para solicitar la suspensión**

Pueden solicitar la suspensión de un certificado el suscriptor, la persona física o jurídica representada por éste o un tercero autorizado.

También puede solicitar la suspensión la Agencia Notarial de Certificación, cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de suspensión.

#### **4.9.15. Procedimientos de petición de suspensión**

Para proceder a una solicitud electrónica de suspensión, el suscriptor o, en su caso el poseedor de claves, debe telefonar al teléfono 912187676 del Centro de Atención a Usuarios de la Agencia Notarial de Certificación. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante de la suspensión podrá ser sometida a grabación y almacenada en un dispositivo cualificado.

En ningún caso cabe solicitar la suspensión de un certificado mediante envío de correo electrónico.

#### **4.9.16. Plazo máximo de suspensión**

El plazo máximo de suspensión es de sesenta (60) días naturales desde la fecha en que la Agencia Notarial de Certificación tenga conocimiento efectivo de cualquiera de las causas de suspensión, y así lo haga constar en el Depósito de Certificados y en la Lista de Revocación de Certificados.

#### **4.9.17. Levantamiento de la suspensión**

Los suscriptores podrán solicitar el levantamiento de la suspensión durante los sesenta (60) días siguientes a su suspensión debiendo telefonar al teléfono 912187676 del Centro de Atención a Usuarios de la Agencia Notarial de Certificación. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante será sometida a grabación.

El solicitante del levantamiento de la suspensión deberá responder con la contraseña que hubiera hecho constar a estos efectos en el proceso de solicitud del certificado. En caso de que la respuesta coincida con dicha contraseña el operador procederá a levantar la suspensión del certificado.

En todos los casos, una vez levantada la suspensión del Certificado, la misma será publicada en el acto en el Depósito de Certificados de la Agencia Notarial de Certificación, produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la Lista de Certificados Revocados (CRL) en el plazo máximo previsto de veinticuatro (24) horas.

En el caso de que la suspensión haya provenido de la Agencia Notarial de Certificación éste únicamente podrá proceder a levantar la suspensión del certificado cuando por medio fehaciente haya tenido conocimiento cierto de la desaparición de la causa que motivó la suspensión. En este caso, inmediatamente después procederá a eliminar el Certificado de la Lista de Revocación.

#### **4.9.18. Notificación de la revocación o suspensión**

El suscriptor cuyo certificado haya sido suspendido o revocado debe ser informado de dicho hecho, así como, en su caso, del levantamiento de la suspensión, por lo que la Agencia Notarial de Certificación notificará dicha información por correo electrónico o postal o incluso por teléfono cuando no haya sido posible la notificación en alguna de las dos formas anteriores.

No obstante lo dispuesto en el párrafo anterior, la notificación se entenderá debidamente cumplimentada cuando haya sido realizada por correo electrónico a la dirección que aparezca en el certificado y que, por tanto, habrá sido admitida previamente por el usuario del certificado.

Si no obstante el sistema produjera un mensaje de error o rechazara la comunicación, se entenderá que la Agencia Notarial de Certificación ha cumplido suficientemente la notificación cuando ésta haya sido sellada. A fin de justificar ulteriormente el cumplimiento de la debida diligencia, la Agencia Notarial de Certificación conservará durante quince años el comprobante electrónico de haber realizado la comunicación de la revocación o suspensión.

La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el directorio de Listas de Revocación de Certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

#### **4.10. Servicios de comprobación de estado de certificados**

##### **4.10.1. Características operativas de los servicios**

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, a través del Depósito de los certificados, y a través del servicio OCSP.

##### **4.10.2. Disponibilidad de los servicios**

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

##### **4.10.3. Características opcionales**

Sin estipulación.

#### **4.11. Finalización de la suscripción**

Transcurrido el periodo de vigencia del certificado, finaliza la suscripción al servicio, expirando el certificado.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, en los casos y con la antelación que determina esta Declaración de Prácticas de Certificación.

## **4.12. Depósito y recuperación de claves**

### **4.12.1. Política y prácticas de depósito y recuperación de claves**

La Agencia Notarial de Certificación no deposita ni puede recuperar claves de suscriptores o poseedores de claves, con excepción de las claves de los certificados de cifrado, que se encuentran depositadas en la Agencia Notarial de Certificación, con controles de seguridad apropiados que impiden su acceso no autorizado por terceras personas.

Las claves de cifrado sólo se pueden recuperar a solicitud de la persona física identificada en el certificado, y en caso de mandamiento judicial, mediante el correspondiente procedimiento implantado por la Agencia Notarial de Certificación.

### **4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión**

Sin estipulación.

## 5. Controles de seguridad física, de gestión y de operaciones

Diferenciamos en este apartado diversos dominios de actuación en la Agencia Notarial de Certificación, que son:

- Dominio de creación de certificados.

Los controles de seguridad física, de gestión y de operaciones en el dominio de creación de los certificados son operados directamente por la Agencia Notarial de Certificación y se realizan de acuerdo con su política de certificación y esta declaración de prácticas de certificación.

- Dominio de registro de usuario y gestión de tarjetas en Notaría

Los controles de seguridad física, de gestión y de operaciones en el dominio de registro y la gestión de tarjetas criptográficas son operados por un Notario.

### 5.1. Controles de seguridad física

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación dispone de instalaciones que protegen físicamente la prestación de, al menos, los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones se encuentra fuera de estos perímetros.

La Agencia Notarial de Certificación ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación establece prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Allanamiento y entrada no autorizada.
- Recuperación del desastre.

- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación, por medio de una Notaría, ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes de certificados, así como de la gestión de las tarjetas criptográficas.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de registro y aprobación de las solicitudes de certificados, así como de la gestión de las tarjetas criptográficas, ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección antirrobo.
- Allanamiento y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios de la Agencia Notarial de Certificación.

Estas medidas resultan aplicables a las instalaciones de la Notaría donde se realiza la aprobación de las solicitudes de certificados y la gestión de las tarjetas criptográficas bajo la plena responsabilidad de la Agencia Notarial de Certificación.

La Agencia Notarial de Certificación, en las instalaciones de la Notaría, ha establecido medidas de seguridad y de protección de datos personales suficientes en relación con los servicios de aprobación, de generación técnica y de manipulado de tarjetas.

### **5.1.1. Localización y construcción de las instalaciones**

#### **En todos los dominios**

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación dispone de instalaciones que protegen físicamente la prestación de los servicios de generación de certificados, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

La localización de las instalaciones permite la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos.

La Agencia Notarial de Certificación mantiene instalaciones de recuperación ante desastre para sus operaciones de generación de certificados, con perímetros de seguridad comparables a los de las instalaciones principales.



### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación, en las instalaciones de la Notaría, dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados, de gestión de tarjetas y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

#### **5.1.2. Acceso físico**

##### **Dominio de creación de certificados**

La Agencia Notarial de Certificación ha establecido al menos cuatro (4) niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias donde se llevan a cabo procesos relacionados con el ciclo de vida del certificado, es necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Esta identificación, ante el sistema de control de accesos, se realiza mediante técnicas de doble factor de autenticación, incluyendo una tarjeta de proximidad de empleado y códigos PIN, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de las Entidades de Certificación, así como su almacenamiento, se realiza en dependencias específicas para estos fines, y requieren de acceso y permanencia duales.

Los accesos a materiales de claves se encuentran sujetos a una estricta política de segregación de funciones, y la apertura y cierre de dichas cabinas y cajas fuertes se registra para su auditoría posterior.

### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación, en las instalaciones de las Notarías, dispone de la adecuada y suficiente seguridad física para la protección del servicio de aprobación de las solicitudes de certificados y de gestión de las tarjetas criptográficas.

#### **5.1.3. Electricidad y aire acondicionado**

##### **En todos los dominios**

Los equipos informáticos de la Agencia Notarial de Certificación están convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos están ubicados en un entorno donde se garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

#### **5.1.4. Exposición al agua**

##### **En todos los dominios**

La Agencia Notarial de Certificación dispone de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad.

#### **5.1.5. Prevención y protección de incendios**

##### **Dominio de creación de certificados**

Todas las instalaciones y activos de la Agencia Notarial de Certificación cuentan con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos, y soportes que almacenan claves de las Entidades de Certificación, cuentan con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

##### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

Todas las instalaciones y activos de la Agencia Notarial de Certificación, en las instalaciones de las Notarías, cuentan con sistemas de extinción de incendios, de acuerdo con las normativas locales de prevención de incendios.

#### **5.1.6. Almacenamiento de soportes**

##### **En todos los dominios**

El almacenamiento de soportes de información garantiza tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se ha establecido.

Se cuenta para ellos con dependencias o armarios ignífugos.

El acceso a estos soportes, incluso para su eliminación, está restringido a personas específicamente autorizadas.

#### **5.1.7. Tratamiento de residuos**

##### **En todos los dominios**

La eliminación de soportes, tanto papel como magnéticos, se realiza mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

#### **5.1.8. Copia de respaldo fuera de las instalaciones**

##### **En todos los dominios**

Periódicamente, la Agencia Notarial de Certificación almacena copia de respaldo de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

## **5.2. Controles de procedimientos**

### **En todos los dominios**

La Agencia Notarial de Certificación garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de la Agencia Notarial de Certificación realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad establecida.

### **5.2.1. Funciones fiables**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación ha identificado, en su política de seguridad, funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos son formalmente nombradas por la alta dirección de la Agencia Notarial de Certificación.

Las funciones fiables incluyen:

- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Auditores del sistema.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de control específicos.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación, para las instalaciones de las Notarías, ha identificado, en su política de seguridad, funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos son formalmente nombradas por el Notario.

Las funciones fiables incluyen:

- Personal responsable de la seguridad.
- Personal de atención al cliente.
- Personal de operación criptográfica

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de control específicos.

## **5.2.2. Número de personas por tarea**

### **Dominio de creación de certificados**

Las funciones fiables identificadas en la sección anterior y en la política de seguridad, y sus responsabilidades asociadas, han sido documentadas en descripciones de puestos de trabajo.

Dichas descripciones se han realizado teniendo en cuenta que existe una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se han tenido en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

Las tareas más sensibles, como el acceso y la gestión del hardware criptográfico de la Entidad de Certificación y las claves asociadas, requiere múltiples personas fiables. En concreto, los procedimientos de control interno han sido diseñados para garantizar que, como mínimo, se requieren dos personas fiables para acceder física o lógicamente al dispositivo.

El acceso al hardware criptográfico de la Entidad de Certificación por parte de múltiples personas fiables se controla de forma estricta a lo largo de todo el ciclo de vida, desde su recepción e inspección hasta su destrucción final, sea ésta física o lógica.

### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

Las funciones fiables identificadas en la política de seguridad del prestador de servicios de certificación, y sus responsabilidades asociadas, se encuentran documentadas en descripciones de puestos de trabajo.

La Agencia Notarial de Certificación, por medio de la Notaría, establece, mantiene y ejecuta procedimientos de control rigurosos que garantizan la segregación de funciones basada en las funciones anteriormente indicadas y que se requieren personas fiables para la realización de tareas sensibles.

## **5.2.3. Identificación y autenticación para cada función**

### **En todos los dominios**

La Agencia Notarial de Certificación identifica y autentica al personal antes de acceder a la correspondiente función fiable.

## **5.2.4. Roles que requieren separación de tareas**

### **Dominio de creación de certificados**

Las siguientes tareas son realizadas, al menos, por dos personas:

- Gestión del acceso físico.
- Gestión de aplicaciones informáticas del prestador.
- Gestión de configuración y control de cambios.
- Gestión del archivo.
- Gestión de bienes de equipo criptográfico.
- Generación, emisión y destrucción de certificados de entidad de certificación.
- Emisión y revocación de certificados, y el acceso al depósito

### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La solicitud de certificados es realizada por el cliente y la aprobación de dicha solicitud va a cargo del Notario.

El Notario realiza la impresión segura y el manipulado de la tarjeta.

## **5.3. Controles de personal**

### **5.3.1. Requisitos de historial, calificaciones, experiencia y autorización**

#### **En todos los dominios**

La Agencia Notarial de Certificación emplea personal cualificado y con la experiencia necesaria, para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

Este requisito se aplica al personal de gestión, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia pueden suplirse mediante una formación y entrenamiento apropiados.

El personal en puestos fiables se encuentra libre de intereses personales que entre en conflicto con el desarrollo de la función que tiene encomendada.

No se asigna a un puesto fiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se realiza una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación de que realmente se hizo el trabajo alegado.
- Morosidad.
- Hasta donde lo permite la legislación vigente, antecedentes penales.

### **5.3.2. Procedimientos de investigación de historial**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación realiza la investigación antes de que la persona sea contratada y/o acceda al puesto de trabajo.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa.

Se advierte de que la negativa a someterse a la investigación implica el rechazo de la solicitud.

Se obtiene consentimiento inequívoco del afectado para la investigación previa y se procesan y protegen todos sus datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Se realizan las siguientes comprobaciones:

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

La investigación se repite cada tres años.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación comprobará la existencia de la plaza de Notario.

### **5.3.3. Requisitos de formación**

#### **En todos los dominios**

La Agencia Notarial de Certificación formar al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, de acuerdo con lo establecido en la sección 5.3.1 de esta Declaración de Prácticas de Certificación.

La formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Versiones de maquinaria y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.

### **5.3.4. Requisitos y frecuencia de actualización formativa**

#### **En todos los dominios**

La Agencia Notarial de Certificación realiza una actualización en la formación del personal al menos cada dos años.

### **5.3.5. Secuencia y frecuencia de rotación laboral**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación puede establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

No aplicable

### **5.3.6. Sanciones para acciones no autorizadas**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que se encuentra adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

No aplicable

#### **5.3.6.1. Procedimiento disciplinario**

El personal de Agencia Notarial de Certificación está obligado a cumplir lo siguiente:

- Utilizar los medios materiales de la Agencia Notarial de Certificación sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la entidad o de terceros, o que puedan atentar contra la moral o las normas deontológicas y de etiqueta de las redes telemáticas.
- No enviar información confidencial al exterior, mediante soportes físicos, o mediante cualquier medio de comunicación, incluyendo la simple visualización o acceso, excepto autorización de Agencia Notarial de Certificación.
- Guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directa o indirectamente ni mediante terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y otra información a la que tengan acceso durante su relación laboral con la Agencia Notarial de Certificación o con instituciones relacionadas o de las que sea miembro la misma, tanto en soporte físico como informático. Esta obligación restará vigente aunque se hubiera extinguido la relación laboral.
- No poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de la Agencia Notarial de Certificación, tanto ahora como en el futuro.
- En el caso que, por motivos directamente relacionados con el puesto de trabajo, entre en posesión de información confidencial bajo cualquier tipo de soporte, dicha posesión deberá entenderse como estrictamente temporal, con la obligación de secreto y sin que tal hecho le

otorgue ningún derecho de posesión, o titularidad o copia sobre la referida información. Asimismo, deberá devolver los materiales antes comentados a la Agencia Notarial de Certificación inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral.

- Ceder exclusivamente a la Agencia Notarial de Certificación los derechos de patentes, reproducción e inventos u otra propiedad intelectual que ellos originen y/o desarrollen. Todos los programas y documentación generada por los empleados en su tiempo de trabajo y/o con los medios y/o materiales de la Agencia Notarial de Certificación se consideran propiedad de ésta, la cual asume todos los derechos legales de propiedad de los contenidos de todos los sistemas informáticos bajo su control.

Con el fin de asegurar el cumplimiento de la normativa interna de la Agencia Notarial de Certificación, ésta se reserva el derecho a revisar, sin previo aviso, los sistemas informáticos (archivos de correo electrónico, archivos del disco duro de ordenadores personales, archivos de buzón de voz, colas de impresión, etc.). Las inspecciones se efectúan previa aprobación por el Departamento de Seguridad, de acuerdo con el procedimiento establecido en la normativa aplicable.

La Agencia Notarial de Certificación puede eliminar de su sistema informático cualquier material que considere ofensivo o potencialmente ilegal.

### **5.3.6.2. Actividades no autorizadas**

En materia de seguridad, son actividades no autorizadas para los empleados de la Agencia Notarial de Certificación:

- Compartir o facilitar los identificadores de usuario y/o la clave de acceso facilitados por la Agencia Notarial de Certificación con otra tercera persona, incluido el personal de la misma. En caso de incumplimiento de esta prohibición, el empleado será el único responsable de los actos realizados por la tercera persona que utilice de forma no autorizada el identificador del usuario.
- Intentar distorsionar o falsear los registros de auditoría del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Agencia Notarial de Certificación.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Agencia Notarial de Certificación o de terceros.
- Obstaculizar voluntariamente el acceso de otros empleados a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la Agencia Notarial de Certificación, así como realizar acciones que dañen, interrumpan o generen fallos en el sistema.
- Enviar mensajes de correo electrónico de forma masiva o con finalidades comerciales o publicitarias sin el consentimiento del destinatario (Spam).
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros empleados.



- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Agencia Notarial de Certificación o de terceros.
- Intentar aumentar el nivel de privilegios de un empleado en el sistema.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que provoquen o sean susceptibles de causar cualquier tipo de alteración en el sistema informático de la Agencia Notarial de Certificación o de terceros. El empleado tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la Agencia Notarial de Certificación.
- Instalar copias ilegales de cualquier programa, incluidas las estandarizadas.
- Borrar cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos de la Agencia Notarial de Certificación incluida la red Internet, para actividades que no estén relacionadas con el lugar de trabajo del empleado.
- Introducir en la red corporativa de la Agencia Notarial de Certificación contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la misma.
- Acceder y/o utilizar la información sobre personas físicas o jurídicas identificadas o identificables en la red sin la necesaria legitimación para su uso.
- Crear archivos de datos personales sin la autorización de la Agencia Notarial de Certificación.
- Cruzar información relativa a datos personales de diferentes archivos o servicios con la finalidad de establecer perfiles de personalidad, hábitos de consumo o cualquier tipo de preferencias, sin la autorización expresa de la Agencia Notarial de Certificación.
- Cualquier otra actividad expresamente prohibida en la política de Seguridad de la Agencia Notarial de Certificación y en la legislación vigente en materia de protección de datos de carácter personal.
- Tratar datos de carácter personal dentro y fuera del ámbito de tratamiento de la Agencia Notarial de Certificación, en forma escrita o en forma oral, sin contar con la debida legitimación.
- El uso de sistemas de bypass, cuyo objetivo es evitar las medidas de protección, y otros archivos que puedan comprometer los sistemas de protección o los recursos.

### **5.3.7. Requisitos de contratación de profesionales**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación puede contratar profesionales para cualquier función, incluso para un puesto fiable, en cuyo caso se someten a los mismos controles que los restantes empleados.

En el caso de que el profesional no deba someterse a tales controles, está constantemente acompañado por un empleado fiable, cuando se encuentra en las instalaciones de la Agencia Notarial de Certificación.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

No aplicable

### **5.3.8. Suministro de documentación al personal**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación suministra la documentación que estrictamente precisa su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido en la sección 5.3.1 de esta Declaración de Prácticas de Certificación.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

No aplicable

## **5.4. Registros de auditoría**

### **5.4.1. Tipos de eventos registrados**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas.
- Inicio y terminación de la aplicación de entidad de certificación o de entidad de registro central.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves de la entidad de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red de la entidad de certificación.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el depósito de certificados.
- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

La Agencia Notarial de Certificación también guarda, ya sea manual o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Los 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 o del poseedor de claves.
- Posesión de datos de activación, para operaciones con la clave privada de la entidad de certificación.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación por medio de la Notaría guarda la siguiente información:

- Encendido y apagado del sistema donde se aloja la entidad de registro.
- Inicio y terminación de la aplicación de entidad de registro.
- Procesamiento correcto e incorrecto de solicitudes.
- Solicitudes de emisión, renovación y revocación de certificados.

#### **5.4.2. Frecuencia de tratamiento de registros de auditoría**

##### **En todos los dominios**

Los registros de auditoría se examinan por lo menos una vez al mes en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consiste en una revisión de los registros la cual incluye la verificación de que los registros 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 llevadas a cabo a partir de la revisión de auditoría también deben ser documentadas.

#### **5.4.3. Periodo de conservación de registros de auditoría**

##### **En todos los dominios**

Los registros de auditoría se retienen en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivan de acuerdo con la sección 5.5.2 de esta Declaración de Prácticas de Certificación.

#### **5.4.4. Protección de los registros de auditoría**

##### **En todos los dominios**

Los ficheros de registros, tanto manuales como electrónicos, son protegidos de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

#### **5.4.5. Procedimientos de copia de respaldo de los registros de auditoría**

##### **En todos los dominios**

Se generan, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

#### **5.4.6. Recolección de registros de auditoría**

##### **En todos los dominios**

El sistema de acumulación de registros de auditoría es un sistema interno de la Agencia Notarial de Certificación, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que son almacenados por el personal debidamente autorizado.

#### **5.4.7. Notificación del evento de auditoría al causante del evento**

##### **En todos los dominios**

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

Se puede comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

#### **5.4.8. Análisis de vulnerabilidades**

##### **Dominio de creación de certificados**

Los eventos en el proceso de auditoría son guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Se realizan análisis de vulnerabilidades internos y externos de los sistemas con una periodicidad al menos trimestral. Anualmente se realiza un test de penetración conducido por una empresa externa.

### **5.5. Archivo de registros**

##### **En todos los dominios**

La Agencia Notarial de Certificación garantiza que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta Declaración de Prácticas de Certificación.

#### **5.5.1. Tipos de registros archivados**

##### **Dominio de creación de certificados**

La Agencia Notarial de Certificación guarda todos los eventos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación del mismo.

Se guarda un registro de lo siguiente:

- Información del ciclo de vida del certificado
- Identidad de la Notaría que procesa la solicitud de certificado.
- Los datos de auditoría identificados en la sección **¡Error! No se encuentra el origen de la referencia.**

### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

La Agencia Notarial de Certificación, por medio de la Notaría, guarda la siguiente información:

- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- La ubicación de las solicitudes de certificados y del documento firmado por el suscriptor o por el poseedor de las claves, según proceda, que se integra en el protocolo del Notario.

### **5.5.2. Periodo de conservación de registros**

#### **En todos los dominios**

La Agencia Notarial de Certificación guarda los registros especificados en la sección anterior de forma permanente, con un mínimo de quince (15) años contados desde el momento de la expedición del certificado.

Para el caso especial de los certificados de Firma de Código todos los registros relacionados con su ciclo de vida son guardados durante un mínimo de veinte (20) años contados desde el momento de la expedición del certificado.

La Agencia Notarial de Certificación guarda los registros de auditoría de todos los componentes de los sistemas relacionados directa o indirectamente con la emisión de certificados electrónicos durante un mínimo de siete (7) años contados desde el momento de la expedición del certificado.

### **5.5.3. Protección del archivo**

#### **En todos los dominios**

La Agencia Notarial de Certificación:

- Mantiene la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archiva los datos anteriormente citados de forma completa y confidencial.
- Mantiene la privacidad de los datos de registro del suscriptor o del poseedor de las claves, según proceda.

### **5.5.4. Procedimientos de copia de respaldo**

#### **En todos los dominios**

La Agencia Notarial de Certificación realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección 5.5.1 de esta Declaración de Prácticas de Certificación. Además, realiza copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta Declaración de Prácticas de Certificación.

#### **Dominio de creación de certificados**

Además, guarda los documentos en papel, según la sección 5.5.1, en un lugar fuera de las instalaciones de la propia Agencia Notarial de Certificación para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta Declaración de Prácticas de Certificación.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

En este dominio se utilizarán las mismas medidas que las usadas en el Protocolo de la Notaría.

### **5.5.5. Requisitos de fecha y hora de los registros**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación emite los certificados y las CRLs con información fiable de fecha y hora, sin que esta información se encuentre firmada digitalmente. Todos los sistemas de información empleados garantizan el registro de los instantes de tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente precisa de fecha y hora. Todos los sistemas sincronizan su instante de tiempo con esta fuente.

#### **Dominio de registro de usuario y gestión de tarjetas en Notaría**

Las bases de datos de la Entidad de Registro emplean registros fiables de fecha y hora.

No es necesario que esta información se encuentre firmada digitalmente.

### **5.5.6. Sistema de archivo**

#### **En todos los dominios**

La Agencia Notarial de Certificación dispone de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, tal y como se especifica en la sección 5.5.4 de esta Declaración de Prácticas de Certificación.

### **5.5.7. Procedimientos de obtención y verificación de información de archivo**

#### **En todos los dominios**

Sólo personas autorizadas por la Agencia Notarial de Certificación tienen acceso a los datos de archivo, ya sea en las mismas instalaciones de la Agencia Notarial de Certificación o en su ubicación externa.

## **5.6. Renovación de claves**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación ha establecido un plan de renovación programada de las claves de los certificados de infraestructura, que garantiza la continuidad de los servicios.

## **Dominio de registro de usuario y gestión de tarjetas en Notaría**

No aplica

## **5.7. Compromiso de claves y recuperación de desastre**

### **5.7.1. Procedimientos de gestión de incidencias**

#### **Dominio de creación de certificados**

La Agencia Notarial de Certificación ha establecido los procedimientos que aplican a la gestión de incidencias y, muy especialmente, a aquellas incidencias que afectan a la seguridad de sus claves.

#### **Dominio de registro de usuarios y gestión de tarjetas por Notario.**

Se utilizan las mismas medidas que para la gestión de incidencias del Protocolo.

### **5.7.2. Corrupción de recursos, aplicaciones o datos**

#### **Dominio de creación de certificados**

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, la Agencia Notarial de Certificación iniciará las gestiones necesarias, de acuerdo con el plan de seguridad, el plan de continuidad de negocio y recuperación de desastres, o documentos que los sustituyan, para hacer que el sistema vuelva a su estado normal de funcionamiento.

#### **Dominio de registro de usuarios y gestión de tarjetas por Notario.**

Se comunica la incidencia al Responsable de Seguridad de la Notaría y se inician los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente.

### **5.7.3. Procedimiento ante compromiso de la clave privada**

#### **5.7.3.1. Revocación de la clave pública de la entidad**

#### **Dominio de creación de certificados**

En el caso de que la Agencia Notarial de Certificación deba revocar la clave pública de una Entidad de Certificación de su jerarquía, realizará las siguientes acciones:

- Notificar este hecho, cuando se produzca, al Consejo General del Notariado y a la administración competente de la supervisión de los Prestadores de Servicios de Confianza.
- Informar del hecho publicando una CRL, según lo establecido en la sección 4.9.7 de esta Declaración de Prácticas de Certificación.
- Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales la Agencia Notarial de Certificación haya emitido certificados, así como a los terceros que confían en certificados que deseen confiar en esos certificados.
- Realizar una renovación de claves, en caso de que la revocación no haya sido debida a la terminación del servicio por parte de la Agencia Notarial de Certificación acreditado, según lo establecido en la sección 5.6 de esta Declaración de Prácticas de Certificación.

### **Dominio de registro de usuarios y gestión de tarjetas por Notario.**

No aplicable para este dominio

#### **5.7.3.2. Compromiso de la clave privada de la entidad**

##### **Dominio de creación de certificados**

El plan de continuidad de negocio de la Agencia Notarial de Certificación (o plan de recuperación de desastres) considera el compromiso o la sospecha de compromiso de la clave privada de las Entidades de Certificación como un desastre.

En caso de compromiso, la Agencia Notarial de Certificación realizará como mínimo las siguientes acciones:

- Revocar el certificado de la Entidad de Certificación afectada.
- Informar a todos los suscriptores y terceros del compromiso.
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de esta Entidad de Certificación ya no son válidos.

Para el restablecimiento del servicio, la Agencia Notarial de Certificación generará un nuevo par de claves y certificado para la Entidad de Certificación. A partir de ese momento, las nuevas CRL y el certificado del OCSP Responder se firmarán con la nueva clave de la Entidad para dar continuidad al servicio de provisión de estado de revocación de certificados.

### **Dominio de registro de usuarios y gestión de tarjetas por Notario.**

No aplicable para este dominio

#### **5.7.4. Continuidad de negocio después de un desastre**

##### **Dominio de creación de certificados**

La Agencia Notarial de Certificación ha desarrollado, mantiene, prueba y, si es necesario, ejecutará un plan de continuidad de negocio para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indica cómo restaurar los servicios de los sistemas de información en el menor plazo que resulte posible a tenor de las circunstancias.

La Agencia Notarial de Certificación es capaz de restaurar los servicios críticos dentro de las 24 horas siguientes al desastre. Estos servicios son los siguientes:

- Revocación de certificados.
- Publicación de información de revocación de los certificados.

La ubicación de los sistemas de recuperación de desastres debe disponer de las protecciones físicas de seguridad detalladas en el plan de seguridad.

La base de datos de recuperación de desastres utilizada por la Agencia Notarial de Certificación está sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad.



Los equipos de recuperación de desastres tienen las medidas de seguridad físicas especificadas en el plan de seguridad, equivalentes a las de las instalaciones principales.

**Dominio de registro de usuarios y gestión de tarjetas por Notario.**

No aplicable para este dominio

**5.8. Terminación del servicio**

Antes del cese de su actividad la Agencia Notarial de Certificación realizará las siguientes actuaciones:

- Proveerá los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación hasta el cese definitivo de su actividad.
- Informará a todos los subscriptores y entidades con las que tenga acuerdos, así como a todas las terceras partes, otros prestadores de servicios de confianza y autoridades relevantes, incluyendo al organismo de supervisión competente, del cese con una anticipación mínima de dos meses.
- Revocará la autorización para procesar nuevas peticiones a todas las entidades de registro que actúan en nombre de la Entidad de Certificación en el proceso de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información de registro, los de la información de estado de los certificados y los registros de eventos de auditoría al Consejo General del Notariado durante el periodo indicado a los firmantes y usuarios.
- En el momento del cese, generará una CRL con todos los certificados revocados durante toda la historia de la Entidad de Certificación y con el valor de fecha de caducidad (nextUpdate) "99991231235959Z". Esta CRL quedará publicada en la dirección especificada como punto de distribución de listas de revocación en los certificados.
- Las claves privadas de la Autoridad de Certificación, incluyendo las copias de seguridad de éstas, serán destruidas o deshabilitadas para uso.

## **6. Controles de seguridad técnica**

La Agencia Notarial de Certificación emplea sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

### **6.1. Generación e instalación del par de claves**

#### **6.1.1. Generación del par de claves**

La Agencia Notarial de Certificación, cuando actúa como Entidad de Certificación raíz, genera y firma su propio par de claves y procede a la generación de las claves de cada Entidad de Certificación subordinada, todo ello de acuerdo con la ceremonia de claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

Todas las claves criptográficas deben ser generadas siguiendo las recomendaciones de algoritmo y longitud de clave mínimas definidas en ETSI TS 119 312.

Las claves de las entidades finales con garantía de dispositivo seguro son generadas por la Agencia Notarial de Certificación o por las entidades finales en dispositivos seguros, que pueden ser tarjetas o tokens USB criptográficos, o módulos de maquinaria de seguridad (HSM):

- Tarjeta criptográfica o token USB. La creación de las claves pública y privada (2048 bits RSA) la realiza la propia tarjeta o token internamente, de tal forma que se garantiza tanto la robustez de las claves como la imposibilidad de un compromiso de las mismas en el proceso de generación.
- Módulos de maquinaria de seguridad (HSM). La creación de las claves Pública y Privada (2048 bits RSA) la realiza el propio Módulo de Seguridad internamente, de tal forma que se garantiza tanto la robustez de las claves como la imposibilidad de un compromiso de las mismas en el proceso de generación.

Para los certificados de las entidades finales sin garantía de dispositivo seguro las claves son generadas por software en los sistemas operativos o aplicaciones informáticas de los usuarios finales.

#### **6.1.2. Envío de la clave privada al suscriptor**

La clave privada del suscriptor o del poseedor de claves le es entregada debidamente protegida mediante uno de los dispositivos criptográficos mencionados en la sección anterior, excepto cuando la clave es generada por la entidad final, en cuyo caso esta sección no resulta aplicable.

#### **6.1.3. Envío de la clave pública al emisor del certificado**

El método de remisión de la clave pública a la Entidad de Certificación es PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por la Agencia Notarial de Certificación.

#### **6.1.4. Distribución de la clave pública del prestador de servicios de certificación**

Las claves de las Entidades de Certificación son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen.

La clave pública de cada Entidad de Certificación se publica en el Depósito, en forma de certificado autofirmado o firmado por otra Entidad de Certificación, junto a una declaración referente a que la clave autentica a la Entidad de Certificación.

Se establecen medidas adicionales para confiar en los certificados autofirmados, como la comprobación de la huella digital del certificado.

Los usuarios pueden acceder al Depósito para obtener las claves públicas de las Entidades de Certificación.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

#### **6.1.5. Tamaños de claves**

La longitud de las claves RSA de las Entidades de Certificación es al menos de 4096 bits, mientras que la de los restantes tipos de certificados es de al menos 2048 bits.

#### **6.1.6. Generación de parámetros de clave pública y verificación de calidad**

La Agencia Notarial de Certificación puede establecer métodos de comprobación de la calidad de los parámetros de las claves públicas.

Tamaño de clave: 4096 (Entidades de Certificación) / 2048 (Entidades Finales)

Algoritmo de generación de claves: rsagen1

Algoritmo de *padding*: emsa-pkcs1-v1\_5

Algoritmo de resumen: SHA-256

#### **6.1.7. Propósitos de uso de claves**

La Agencia Notarial de Certificación incluye la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas, siempre que resulta posible.

### **6.2. Protección de la clave privada**

#### **6.2.1. Estándares de módulos criptográficos**

Para los módulos que gestionan claves de las Entidades de Certificación y de los suscriptores de certificados de firma electrónica cualificada, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

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

El acceso a las claves privadas de las Entidades de Certificación requiere necesariamente del concurso simultáneo de dos (2) dispositivos criptográficos protegidos por una clave de acceso, de entre cuatro (4) dispositivos.

La clave de acceso es conocida únicamente por una persona responsable de ese dispositivo. Ninguna de ellas conoce más que una de las claves de acceso.

Los dispositivos criptográficos quedan almacenados en las dependencias de la Agencia Notarial de Certificación, y para su acceso es necesaria una persona adicional.

### **6.2.3. Custodia de la clave privada**

Únicamente se custodian copias de respaldo de las claves privadas de los certificados de entidad final cuyo uso exclusivo es el cifrado. La recuperación de una clave privada de cifrado requiere del control multipersona detallado en la sección 6.2.2.

No se custodian otras claves privadas del suscriptor.

### **6.2.4. Copia de respaldo de la clave privada**

La clave privada de las Entidades de Certificación cuenta con una copia de respaldo realizada, almacenada en dependencia independiente de aquélla donde se almacena habitualmente, y recuperada en su caso, por personal sujeto a la política de confianza del personal. Este personal está expresamente autorizado a estos fines, y se limita a aquel que necesite hacerlo.

Los controles de seguridad que se aplican a las copias de respaldo de las Entidades de Certificación son de igual o superior nivel a los que se aplican a las claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

### **6.2.5. Archivo de la clave privada**

Las claves privadas de las Entidades de Certificación son archivadas al final de su periodo de operación, de forma permanente.

No se archivan claves privadas de firma electrónica de usuarios finales.

### **6.2.6. Tránsito de la clave privada a o desde el módulo criptográfico**

Las claves privadas se pueden generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.

Las claves privadas de las Entidades de Certificación quedan almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no pueden ser extraídas)

Dichos dispositivos son empleados para introducir la clave privada en el módulo criptográfico.

### **6.2.7. Almacenamiento de la clave privada en el módulo criptográfico**

Las claves privadas de las Entidades de Certificación se generan directamente en los módulos criptográficos.

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

### **6.2.8. Método de activación de la clave privada**

La clave privada de cada Entidad de certificación se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

La clave privada del suscriptor se activa mediante la introducción del PIN en el dispositivo criptográfico o aplicación de firma.

### **6.2.9. Método de desactivación de la clave privada**

Las claves privadas de la Entidad de certificación raíz se desactivan automáticamente cuando se retira el último de los dispositivos utilizados para su activación descrita en la sección 6.2.2.

Las claves privadas de las Entidades de certificación subordinadas se desactivan automáticamente cuando se detiene el software de soporte de la Entidad de Certificación.

Para certificados de firma electrónica cualificada, cuando se retira el dispositivo criptográfico del lector o se desconecta del ordenador, o la aplicación que lo utilice finaliza la sesión, es necesaria nuevamente la introducción del PIN.

### **6.2.10. Método de destrucción de la clave privada**

Para la destrucción de las claves privadas de la Entidad de certificación y de sus datos de activación se procederá a la destrucción física o al borrado a bajo nivel de los dispositivos que las contengan siguiendo los procedimientos especificados por el fabricante de los mismos. Posteriormente se destruirán de forma segura cualquier copia de seguridad existente.

Para la destrucción de las claves privadas de las entidades finales en hardware se pone a disposición de los suscriptores un servicio de recogida de dispositivos para su destrucción física segura y un software para el borrado seguro de los dispositivos a través de las Entidades de registro y en la Entidad de certificación.

### **6.2.11. Clasificación de los módulos criptográficos**

Los módulos de la Entidad de Certificación tienen que encontrarse certificados con el nivel y los aumentos previstos en un perfil de protección, de acuerdo con Common Criteria EAL 4+, o FIPS 140-2 Nivel 3.

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

Los dispositivos cualificados de firma electrónica del suscriptor admisibles son todos aquellos que se encuentran en la lista de dispositivos cualificados de firma notificados según la normativa eIDAS.

### **6.3. Otros aspectos de gestión del par de claves**

#### **6.3.1. Archivo de la clave pública**

Las Entidades de Certificación archivan sus claves públicas de forma permanente, de acuerdo con lo establecido en la sección 5.5 de esta Declaración de Prácticas de Certificación.

#### **6.3.2. Periodos de utilización de las claves pública y privada**

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

Como excepción, la clave privada puede continuar empleándose para el descifrado de documentos, incluso tras la expiración del certificado.

### **6.4. Datos de activación**

#### **6.4.1. Generación e instalación de datos de activación**

En los casos en que la Agencia Notarial de Certificación facilita al suscriptor un dispositivo cualificado de creación de firma de tipo tarjeta o token USB, entonces los datos de activación del dispositivo, son generados de forma segura por la Agencia Notarial de Certificación.

Para realizar una firma o activar la tarjeta es necesario introducir el código secreto de activación (PIN) que solamente debe conocer el suscriptor de la tarjeta. Tres intentos consecutivos erróneos en la introducción del PIN provocan un bloqueo de la tarjeta. Para desbloquear la tarjeta, el suscriptor deberá introducir el código PUK y del mismo modo tres intentos consecutivos erróneos en la introducción del PUK provocan el bloqueo irreversible de la tarjeta.

En caso de empleo de un dispositivo cualificado HSM, el suscriptor debe configurar adecuadamente el sistema de datos de activación de firma, garantizando, cuando resulte procedente, que el firmante dispone del control exclusivo del uso de la clave de firma electrónica.

#### **6.4.2. Protección de datos de activación**

La Agencia Notarial de Certificación puede generar y facilitar al suscriptor los datos de activación del dispositivo cualificado de creación de firma empleando procedimientos seguros, como la entrega presencial o a distancia, en cuyo caso los datos de activación serán distribuidos separadamente del propio dispositivo de creación de firma (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes).

#### **6.4.3. Otros aspectos de los datos de activación**

Sin estipulación.

## **6.5. Controles de seguridad informática**

### **6.5.1. Requisitos técnicos específicos de seguridad informática**

Se garantiza que el acceso los sistemas está limitado a individuos debidamente autorizados. En particular:

- Se garantiza una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.
- Se garantiza que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema está restringido y estrechamente controlado.
- El personal es identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal es responsable y puede justificar sus actividades, por ejemplo, mediante un archivo de eventos.
- Se evita la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo, ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización permiten una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma).
- El acceso a los depósitos públicos de la información (por ejemplo, certificados o información de estado de revocación) cuenta con un control de accesos para modificaciones o borrado de datos.

### **6.5.2. Evaluación del nivel de seguridad informática**

Las aplicaciones de entidad de certificación y de registro empleadas por la Agencia Notarial de Certificación son fiables, habiéndose acreditado dicha condición, mediante una certificación de producto contra un perfil de protección adecuado, conforme a la norma ISO 15408, con nivel EAL4+.

## **6.6. Controles técnicos del ciclo de vida**

### **6.6.1. Controles de desarrollo de sistemas**

Se ha realizado un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de entidad de certificación y de registro, para garantizar que los sistemas son seguros.

Se emplean procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

### **6.6.2. Controles de gestión de seguridad**

La Agencia Notarial de Certificación mantiene un inventario de todos los activos informativos, debidamente clasificados, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección 8.1 de esta Declaración de Prácticas de Certificación.

Se realiza un seguimiento de las necesidades de capacidad, y se planifican procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

### **6.6.3. Controles de seguridad del ciclo de vida**

Sin estipulaciones adicionales.

## **6.7. Controles de seguridad de red**

Se debe garantizar que el acceso a las diferentes redes de la Agencia Notarial de Certificación está limitado a individuos debidamente autorizados. En particular:

- Se han implementado controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se han configurado de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Certificación.
- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
- Se garantiza que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

## **6.8. Fuente de tiempo**

La Agencia Notarial de Certificación obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada (ROA) siguiendo el protocolo NTP a través de Internet. Todos los sistemas mantienen la sincronización con esta fuente de tiempo mediante el protocolo NTP.

Los algoritmos de generación de claves están aceptados para el uso de la clave a que están destinados.



## 7. Perfiles de certificados y listas de certificados revocados

### 7.1. Perfil de certificado

Los certificados tienen el contenido y campos descritos en esta sección, incluyendo, como mínimo, los siguientes:

- Número de serie, que es un código único con respecto al nombre distinguido del emisor.
- Algoritmo de firma.
- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 5280
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 5280
- Nombre distinguido del sujeto.
- Clave pública del sujeto, codificada de acuerdo con RFC 5280
- Firma, generada y codificada de acuerdo con RFC 5280

Los certificados son conformes con las siguientes normas:

- ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997, con sus actualizaciones y correcciones posteriores.
- RFC 5280: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, Mayo 2008

Adicionalmente, los certificados de firma electrónica serán conformes con las siguientes normas:

- EN 319 412: Certificate Profiles
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (siempre que no entre en conflicto con EN 319 412)

#### 7.1.1. Número de versión

Todos los certificados contienen un campo con el número de versión. El valor del campo es el valor entero “2” utilizando el estándar X.509 versión 3.

#### 7.1.2. Extensiones de certificado

La Agencia Notarial de Certificación publica un documento con el detalle de todos los perfiles de certificados en el Depósito indicado en la sección 2.

#### 7.1.3. Identificadores de objeto de algoritmos

La Agencia Notarial de Certificación utiliza el algoritmo sha256WithRSAEncrypton, con OID 1.2.840.113549.1.1.11, para la firma de todos sus certificados.

#### **7.1.4. Formatos de nombres**

Los formatos de nombres están especificados en el documento con el detalle de todos los perfiles de certificados publicado en el Depósito indicado en la sección 2.

#### **7.1.5. Restricciones de nombres**

Sin estipulación adicional.

#### **7.1.6. Identificador de objeto de política de certificado**

La Agencia Notarial de Certificación incluirá en la extensión Certificate Policy (OID 2.5.29.32) de los certificados el identificador de objeto asociado a la política de cada certificado de acuerdo con la sección **¡Error! No se encuentra el origen de la referencia..**

#### **7.1.7. Empleo de la extensión restricciones de política**

Sin estipulación adicional.

#### **7.1.8. Sintaxis y semántica de los calificadores de política**

La Agencia Notarial de Certificación incluirá en la extensión Certificate Policy (OID 2.5.29.32) de los certificados un calificador con los siguientes elementos:

- CPS Pointer: contiene una dirección electrónica a través de la cual se puede acceder a la Declaración de Prácticas y el resto de documentación relevante del certificado.
- User Notice: contiene una descripción textual concisa relativa al certificado.

#### **7.1.9. Semántica del proceso de la extensión de la política de certificado**

La extensión Certificate Policy (OID 2.5.29.32) de los certificados permite identificar la política asociada al certificado y la dirección electrónica en el que se puede encontrar la información de dicha política.

### **7.2. Perfil de la lista de revocación de certificados**

Las listas de revocación son conformes con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile April 2002.

#### **7.2.1. Número de versión**

Las CRL generadas tienen el número de versión 2.

#### **7.2.2. Lista de revocación de certificados y extensiones de elementos de la lista**

Las CRL generadas contienen las siguientes extensiones:

- Authority key Identifier (OID 2.5.29.35)

- CRL Number (OID 2.5.29.20)

### **7.3. Perfil OCSP**

Las respuestas OCSP de la Agencia Notarial de Certificación son conformes a la norma RFC 6960 y son firmadas por el OCSP Responder cuyo certificado ha sido firmado por la misma Entidad de Certificación con la que se emitió el certificado por el que se está consultando.

#### **7.3.1. Número de versión**

Todos los certificados de OCSP Responder contienen un campo con el número de versión. El valor del campo es el valor entero "2" utilizando el estándar X.509 versión 3.

#### **7.3.2. Extensiones del OCSP**

El detalle del perfil de certificado de OCSP Responder se encuentra en el documento con todos los perfiles de certificados publicado en el Depósito indicado en la sección 2.

Las respuestas OCSP incluirán la extensión ExtendedRevoke (OID 1.3.6.1.5.5.7.48.1.9).

## **8. Auditoría de conformidad**

La Agencia Notarial de Certificación realiza periódicamente una auditoría de cumplimiento para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios para cumplir la política de los servicios de certificación del Consejo General del Notariado.

### **8.1. Frecuencia de la auditoría**

Se realiza una auditoría de conformidad anualmente, además de las auditorías internas que pueda llevar a cabo bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

### **8.2. Identificación y calificación del auditor**

La Agencia Notarial de Certificación deberá acudir a auditores independientes externos para la realización de las auditorías anuales de conformidad. Estos tienen que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Prestadores de Servicios de Confianza y de los elementos relacionados. Los auditores deberán estar acreditados según EN 319 403.

### **8.3. Relación del auditor con la entidad auditada**

Las auditorías de conformidad ejecutadas por terceros son practicadas por una entidad independiente de la Agencia Notarial de Certificación, no debiendo tener ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

### **8.4. Listado de elementos objeto de auditoría**

Los elementos objeto de auditoría son los siguientes:

- Procesos de certificación de clave pública.
- Sistemas de información.
- Protección del centro de proceso
- Documentación del servicio.

Los detalles de cómo llevar a cabo la auditoría de cada uno de estos elementos se detallan en el plan de auditoría de la Agencia Notarial de Certificación.

### **8.5. Acciones a emprender como resultado de una falta de conformidad**

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, la Agencia Notarial de Certificación discute, con la entidad que ha ejecutado la auditoría las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solventa dichas deficiencias.

Si la Agencia Notarial de Certificación no es capaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá realizarse una de las siguientes acciones:

- Revocar la clave de las Entidades de Certificación, tal y como se describe en la sección 5.7.3 de esta Declaración de Prácticas de Certificación.
- Terminar los servicios de certificación, tal y como se describe en la sección 5.8 de esta Declaración de Prácticas de Certificación.

## **8.6. Comunicación de los resultados**

Los informes de auditoría serán entregados al Comité de Seguridad, para su análisis, en un plazo máximo de 15 días después de la ejecución de la auditoría, para su evaluación y gestión diligente.

## **9. Otros asuntos legales y de actividad**

### **9.1. Tarifas**

#### **9.1.1. Tarifa de emisión o renovación de certificados**

La Agencia Notarial de Certificación establece una tarifa por la emisión o por la renovación de los certificados, que es previamente aprobada por el Consejo General del Notariado.

#### **9.1.2. Tarifa de acceso a certificados**

La Agencia Notarial de Certificación no establece ninguna tarifa por el acceso a los certificados.

#### **9.1.3. Tarifa de acceso a información de estado de certificado**

La Agencia Notarial de Certificación no establece ninguna tarifa por el acceso a la información de estado de los certificados.

#### **9.1.4. Tarifas de otros servicios**

Sin estipulación.

#### **9.1.5. Política de reintegro**

La Agencia Notarial de Certificación dispone de la siguiente política de reintegro de la tarifa:

Cuando una rectificación o modificación de la Declaración de Prácticas de Certificación implique una limitación de los derechos de uso o una restricción sobre el ámbito de aplicación de un certificado en vigor, el suscriptor del mismo puede instar la revocación del mismo y reclamar como máximo el reembolso del precio del certificado.

En los demás casos, el suscriptor no tendrá derecho alguno al reintegro del coste del certificado.

### **9.2. Responsabilidad financiera**

La Agencia Notarial de Certificación 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.

La Agencia Notarial de Certificación no actúa como agente fiduciario ni representante en forma alguna de los usuarios ni de los terceros de confianza en los certificados que emite.

#### **9.2.1. Cobertura de seguro**

La Agencia Notarial de Certificación dispone de una garantía de cobertura de su responsabilidad civil suficiente, bien mediante un seguro de responsabilidad civil profesional por errores y omisiones, bien mediante una fianza o aval.

La cuantía garantizada es de al menos 3.000.000 euros.

### **9.2.2. Otros activos**

Sin estipulación.

### **9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados**

Sin estipulación.

## **9.3. Confidencialidad**

### **9.3.1. Alcance de la información confidencial**

Las siguientes informaciones, como mínimo, son mantenidas confidenciales por la Agencia Notarial de Certificación:

- 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 la Agencia Notarial 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 Agencia Notarial de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

### **9.3.2. Informaciones no confidenciales**

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por una Entidad de Certificación.
- El nombre y los apellidos del suscriptor del certificado o del poseedor de claves, según proceda, así como cualesquiera 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 del suscriptor del certificado o del poseedor de claves, según proceda, o la dirección de correo electrónico que corresponda.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.

- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.
- La información contenida en el Depósito.
- Toda otra información que no esté indicada en la sección anterior de esta Declaración de Prácticas de Certificación.

### **9.3.3. Responsabilidad para proteger la información confidencial**

#### **9.3.3.1. Divulgación de información de suspensión y revocación**

Véase la sección anterior.

#### **9.3.3.2. Divulgación legal de información**

La Agencia Notarial de Certificación divulga la información confidencial en los casos legalmente previstos para ello.

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

Se indican estas circunstancias en la política de intimidad prevista en la sección 9.4 de esta Declaración de Prácticas de Certificación.

#### **9.3.3.3. Divulgación de información por petición de su titular**

La Agencia Notarial de Certificación incluye, en la política de intimidad prevista en la sección 9.4 de esta Declaración de Prácticas de Certificación, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del poseedor de claves, directamente a los mismos o a terceros.

#### **9.3.3.4. Otras circunstancias de divulgación de información**

Sin estipulación.

### **9.4. Protección de datos personales**

Para la prestación del servicio, la Agencia Notarial de Certificación precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales.

La Agencia Notarial de Certificación ha desarrollado una política de intimidad, de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (GDPR) y Ley



Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La Agencia Notarial de Certificación ha llevado el correspondiente análisis del riesgos que pudieran generar los tratamientos de los datos de carácter personal y adoptado las medidas adecuadas de seguridad y control para garantizar los derechos y libertades de las personas y para mitigar los riesgos porque supongan un daño o perjuicio material directo, porque vulneren principios o derechos y libertades, o porque incumplan alguna obligación establecida en la normativa de protección de datos.

Para realizar su actividad de certificación las Entidades de Registro accederán a dichos tratamientos. La Agencia Notarial de Certificación tendrá la condición de Responsable del Tratamiento en tanto que decidirá sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal y las entidades de registro se considerarán Encargadas del Tratamiento, las cuales deberán utilizar los datos contenidos en dichos ficheros, única y exclusivamente para los fines que figuran en la Declaración de Prácticas de Certificación.

Las Entidades de Registro, en cumplimiento con lo establecido en el artículo 28 del GDPR se comprometen a:

1. Tratar los datos personales según las instrucciones del Responsable del Tratamiento, recibidas en virtud de la relación contractual que les vincula.
2. A garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y, especialmente, su honor e intimidad personal y familiar.
3. A guardar el secreto profesional respecto de los datos de carácter personal, no divulgando a terceros dicha información obtenida como consecuencia de esta relación contractual, obligación que subsistirá aun después de finalizar sus relaciones con el Responsable del Tratamiento.
4. A cumplir con todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los tratamientos, centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal referidos.
5. A implementar las medidas técnicas y organizativas necesarias que garanticen la seguridad e integridad de los datos de carácter personal incluidos en los ficheros propiedad del Responsable del Tratamiento y que eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural. Las medidas de seguridad que deberán aplicar serán, en todo caso, las adecuadas para mitigar los riesgos que se deriven de los análisis de riesgos que deberán llevar a cabo conforme al GDPR.
6. A remitir a la Agencia Notarial de Certificación los datos personales de los solicitantes y/o suscriptores de certificados mediante comunicaciones seguras.
7. A tratar los datos conforme a lo estipulado en el contrato con la Agencia Notarial de Certificación, y no los aplicarán o utilizarán con fin distinto, ni los comunicarán, ni siquiera para su conservación, a otras personas.

8. A acceder únicamente a los ficheros o tratamientos de la Agencia Notarial de Certificación cuando sea necesario para realizar los servicios contratados.
9. A destruir o devolver todos los datos de carácter personal objeto de tratamiento una vez finalice por cualquier causa la relación con la Agencia Notarial de Certificación, salvo aquellos datos que la legislación obliga a conservarlos por un mínimo de 15 años.

Las entidades de registro verifican que el suscriptor y/o solicitante son informados y prestan su consentimiento para el tratamiento de sus datos, con las finalidades previstas en los documentos de consentimiento correspondiente.

La Agencia Notarial de Certificación queda exonerada de cualquier responsabilidad que se pudiera generar por el incumplimiento por parte de las personas Encargadas del Tratamiento de sus obligaciones descritas. En dichos supuestos de incumplimiento, éstas serán consideradas como responsables del tratamiento y responderán de las infracciones en que hubiese incurrido personalmente.

De conformidad con lo establecido en el artículo 13 del GDPR, se informa al solicitante/suscriptor que los datos de carácter personal que se incluyan en los formularios, contratos o documentos que cumplimente durante el proceso de solicitud de la emisión de un Certificado se registrarán en un fichero creado al efecto. La Agencia Notarial de Certificación únicamente prestará los servicios de certificación si se cumplimentan los formularios íntegramente con información verdadera.

La licitud del tratamiento de datos personales está amparada por la ejecución contractual de los servicios de confianza, comunicando para ello el solicitante/suscriptor a la Agencia Notarial de Certificación sus datos que serán tratados para los usos y finalidades de prestar los servicios de confianza en los términos establecidos en la Ley y esta Declaración de Prácticas de Certificación.

De conformidad con lo establecido en el referido artículo del GDPR el solicitante/suscriptor, o cualquier usuario de certificados consiente la comunicación a los terceros que confían en certificados electrónicos de sus datos de carácter personal que constan en el certificado a través del Depósito de Certificados que consta en la página Web [www.ancert.com](http://www.ancert.com) exclusivamente para la finalidad de permitir la consulta de los certificados emitidos por la Agencia Notarial de Certificación y la vigencia de los mismos, así en el Depósito de Certificados y las Listas de Certificados Revocados para consultar los certificados revocados por la Agencia Notarial de Certificación.

Los terceros que confían en certificados únicamente podrán utilizar la información de acuerdo con las finalidades descritas. No obstante, y con carácter general, cualquier tratamiento, registro o utilización para otros fines distintos de los anteriores requiere obligatoriamente del consentimiento previo de los titulares de los datos. Se advierte que el RGPD sanciona con multas que pueden alcanzar hasta el 4% del volumen de facturación anual con un máximo de 20 millones de euros por cada una de las infracciones o incumplimientos de dicha norma, sin perjuicio de la incoación de acciones penales de acuerdo con el Código Penal, así como de reclamaciones civiles de los perjudicados.

El solicitante/suscriptor podrá ejercitar los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición al tratamiento previstos en el GDPR mediante envío de la solicitud a la dirección que aparece en la sección **¡Error! No se encuentra el origen de la**

**referencia.** de esta Declaración de Prácticas de Certificación, y asimismo tiene el derecho a presentar una reclamación ante una autoridad de control.

## **9.5. Derechos de propiedad intelectual**

### **9.5.1. Propiedad de los certificados e información de revocación**

La Agencia Notarial de Certificación es la única entidad que goza de los derechos de propiedad intelectual sobre los certificados que emite, concediendo 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 usos autorizado y legítimos de acuerdo con esta Declaración de Prácticas de Certificación, según se define en la sección 1.4, y de acuerdo con las correspondientes condiciones generales de uso.

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

Los OID propiedad de la Agencia Notarial de Certificación han sido registrados en la IANA (Internet Assigned Number Authority) bajo la rama 1.3.6.1.4.1., habiéndose asignado el número 18920 (ANCERT), siendo dicha información pública en:

<http://www.iana.org/assignments/enterprise-numbers>

Igualmente queda prohibido el uso total o parcial de cualquiera de los OID asignados a la Agencia Notarial de Certificación salvo para los usos previstos en los Certificados o en el Depósito de Certificados.

Queda prohibida cualquier extracción y/o reutilización de la totalidad o de una parte sustancial de los contenidos o de las bases de datos que la Agencia Notarial de Certificación pone a disposición de los suscriptores de certificados.

### **9.5.2. Propiedad de la política de certificado y Declaración de Prácticas de Certificación**

El Consejo General del Notariado es la única entidad que gozará de los derechos de propiedad intelectual sobre las políticas de certificados.

La Agencia Notarial de Certificación es propietaria de esta Declaración de Prácticas de Certificación.

### **9.5.3. Propiedad de la información relativa a nombres**

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

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 de esta Declaración de Prácticas de Certificación.

### **9.5.4. Propiedad de claves**

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. Modelo de obligaciones del prestador de servicios**

La Agencia Notarial de Certificación garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política de certificado para la que emite certificados.

Es la única entidad responsable del cumplimiento de los procedimientos descritos en esta Declaración de Prácticas de Certificación, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

La Agencia Notarial de Certificación presta sus servicios de certificación conforme con esta Declaración de Prácticas de Certificación vigente, en la que se detallan sus funciones, procedimientos de operación y medidas de seguridad.

Antes de la emisión y entrega del certificado al suscriptor, se le informa de los términos y condiciones relativos al uso del certificado, de su precio – cuando se establece – y de sus limitaciones de uso.

Este requisito se cumple, entre otros medios, mediante un “Texto divulgativo de la política de certificado” aplicable, publicado y transmisible electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Se vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante condiciones generales de emisión y uso de certificados, que se encuentran en lenguaje escrito y comprensible, y que tienen los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.2, 9.2, 9.10, 9.13, 9.15 y 9.16 de la presente Declaración de Prácticas de Certificación.
- Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de empleo de dispositivo cualificado.
- 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, para la provisión del dispositivo cualificado de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.1.1 de esta Declaración de Prácticas de Certificación.
- 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 Agencia Notarial de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Agencia Notarial 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 Entidad de Certificación de certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

La Agencia Notarial de Certificación debe asumir otras obligaciones incorporadas directamente en el certificado o incorporadas por referencia.

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

La Agencia Notarial de Certificación, en las condiciones generales de emisión y uso de certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La Agencia Notarial de Certificación, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Agencia Notarial de Certificación y, en su caso, por la entidad de registro.
- 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 de 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.

La Agencia Notarial de Certificación, como mínimo, garantiza 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 de la presente Declaración de Prácticas de Certificación.

- 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, cuando emita un certificado de firma electrónica, 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 con el Anexo I del Reglamento (UE) 910/2014.
- La responsabilidad de la Agencia Notarial de Certificación, con los límites legales que se establezcan.

## **9.7. Rechazo de otras garantías**

La Agencia Notarial de Certificación rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

Específicamente, la Agencia Notarial de Certificación no garantiza los algoritmos criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que haya aplicado la diligencia debida según el estado de la técnica en cada momento, y haya actuado conforme a lo dispuesto en la presente Declaración de Prácticas de Certificación y en la Ley 6/2020 y su normativa de aplicación.

## **9.8. Limitación de responsabilidades**

### **9.8.1. Limitación de responsabilidad de la Autoridad de Certificación**

La Agencia Notarial de Certificación limita su responsabilidad a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por la Agencia Notarial de Certificación.

La Agencia Notarial de Certificación limita su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede emplearse el certificado, de acuerdo con lo establecido en la sección 1.4.1.1 de esta Declaración de Prácticas de Certificación.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de tales usos quedan a cargo del suscriptor. En ningún caso podrá el suscriptor ni los terceros perjudicados reclamar a la Agencia Notarial de Certificación compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para fines de cifrado.

## **9.8.2. Caso fortuito y fuerza mayor**

La Agencia Notarial de Certificación incluye cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en las condiciones generales de uso de certificados.

## **9.9. Cláusulas de indemnidad**

### **9.9.1. Cláusula de indemnidad de suscriptor**

La Agencia Notarial de Certificación incluye, en las condiciones generales de emisión de certificados, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Agencia Notarial 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 concorra 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 Agencia Notarial de Certificación, la entidad de registro o 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.

### **9.9.2. Cláusula de indemnidad de tercero que confía en el certificado**

La Agencia Notarial de Certificación incluye, en las condiciones generales de uso de certificados, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Agencia Notarial 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 concorra 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.

## **9.10. Periodo de validez**

### **9.10.1. Entrada en vigor**

La Declaración de Prácticas de Certificación entra en vigor en el momento de su publicación.

### **9.10.2. Finalización**

La Declaración de Prácticas de Certificación vigente será derogada en el momento que una nueva versión del documento sea publicada.

La nueva versión sustituirá íntegramente el documento anterior.

### **9.10.3. Efecto de la finalización y supervivencia**

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

## **9.11. Notificaciones**

La Agencia Notarial de Certificación establece, en sus instrumentos jurídicos vinculantes con suscriptores y verificadores, cláusulas de notificación, en las cuales se establece el procedimiento por el cual las partes se notifican hechos mutuamente.

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

## **9.12. Modificaciones**

### **9.12.1. Procedimiento para las modificaciones**

La Agencia Notarial de Certificación podrá modificar, de forma unilateral, la Declaración de Prácticas de Certificación y el resto de documentación jurídica siempre y cuando proceda según el siguiente procedimiento:

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

Las modificaciones de este documento serán aprobadas por el Comité de Seguridad y la dirección de la Agencia Notarial de Certificación.

### **9.12.2. Periodo y mecanismos de notificación**

Se realizará una revisión de la Declaración de Prácticas de Certificación con la periodicidad definida en la sección 1.5.5 en cualquier caso cuando haya que realizar cualquier modificación de la misma.



Las versiones actualizadas de la Declaración de Prácticas de Certificación junto con la relación de modificaciones realizadas pueden ser consultadas en el Depósito indicado en la sección 2.

### **9.12.3. Circunstancias por las que un OID debe cambiarse**

Se procederá al cambio de OID en aquellas circunstancias que se altere alguno de los procedimientos descritos en la sección 9.12.1.

### **9.13. Reclamaciones y resolución de disputas**

La Agencia Notarial de Certificación establece, en las condiciones generales de uso de certificados, los procedimientos de mediación y resolución de conflictos aplicables.

Las situaciones de discrepancia que se deriven de la utilización del empleo de los certificados emitidos, se resolverán aplicando los mismos criterios de competencia que en los casos de los documentos firmados manuscritamente.

### **9.14. Ley aplicable**

La Agencia Notarial de Certificación establece, en las condiciones generales de emisión y uso de certificados, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

### **9.15. Cláusula de jurisdicción competente**

La Agencia Notarial de Certificación establece, en las condiciones generales de uso de certificados, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

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

### **9.16. Cláusulas diversas**

La Agencia Notarial de Certificación establece, en las condiciones generales de uso de certificados, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación.

#### **9.16.1. Acuerdo íntegro**

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.

#### **9.16.2. Subrogación**

Los derechos y los deberes asociados a la condición de Entidad de Certificación no pueden ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad se puede subrogar en la posición jurídica de una Entidad de Certificación.

En caso de que se produzca una cesión o subrogación, se procede a la finalización de la mencionada Entidad de Certificación.

### **9.16.3. Divisibilidad**

En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.

### **9.16.4. Aplicaciones**

Sin estipulación adicional.

### **9.16.5. Causa mayor**

Según lo especificado en la sección 9.8.2.

### **9.17. Otras provisiones**

Sin estipulación adicional.