Política de Sellado de Fecha y Hora

Agencia Notarial de Certificación

ancert
Agencia Notarial de Certificación

1. Información general

1.1. Control documental

Proyecto:	**Política de sellado de fecha y hora**
Entidad de destino:	**Consejo General del Notariado de España**
Código de referencia:	
Versión:	**2.3**
Fecha de la edición:	**06/09/2011**
Archivo:	**Politica-sellado-fecha-y-hora-CGN-v2r3.docx**
Formato:	**Word 2007**

1.2. Control de versiones

Versión	**Partes que cambian**	**Descripción del cambio**	**Fecha cambio**	**Fecha publicación**
2.0	Original	Creación del documento	28/03/2010	
2.2	Logo ANCERT	Nuevo logo ANCERT	30/11/2010	01/01/2011
2.3	Todo	Actualización de requisitos algoritmos claves y certificados. Corrección de errores.	06/09/2011	01/10/2011

2. Índice

3. Introducción

Este documento contiene la política de sellado de fecha y hora de la Agencia Notarial de Certificación.

3.1. Presentación

La Agencia Notarial de Certificación podrá emitir diferentes tipos de sellos de fecha y hora, y con determinadas opciones, que se presentan a continuación.

3.1.1. Tipos de sellado de fecha y hora

A los efectos de esta política, se establecen los siguientes tipos de sellado de fecha y hora:

- Sellado de fecha y hora inicial. Los sellos de fecha y hora podrán ser generados inicialmente para un documento electrónico.
- Resellado de fecha y hora. Los sellos de fecha y hora podrán ser generados posteriormente para el mantenimiento de un documento o sello previamente existentes.

3.1.2. Opciones del servicio

Los sellos de fecha y hora podrán ofrecer opciones, entre las que se pueden mencionar las siguientes:

- Precisión del sello de fecha y hora, que por defecto será de un (1) segundo.
- Custodia del sello producido por la Agencia Notarial de Certificación.

3.2. Nombre del documento e identificación

Este documento es la "Política de sellado de fecha y hora de la Agencia Notarial de Certificación".

La Agencia Notarial de Certificación debe asignar a cada política de sellado de fecha y hora un identificador de objeto (OID), para su identificación por las aplicaciones, que constará en la correspondiente Declaración de Prácticas de Sellado de Tiempo.

Existirán al menos dos políticas diferenciadas de sellado de fecha y hora:

- Política de sellado de fecha y hora sin custodia de sellos.
- Política de sellado de fecha y hora con custodia de sellos.

Adicionalmente, la Agencia Notarial de Certificación publicará en su Depósito un documento con los OIDs correspondientes a las políticas de sellado de fecha y hora vigentes en cada momento.

3.3. Participantes en los servicios de sellado de fecha y hora

Esta política de sellado de fecha y hora regula la prestación de servicios de emisión de sellos de fecha y hora a comunidades cerradas de usuarios y al público.

Las comunidades cerradas de usuarios podrán ser:

- El Notariado español.
- Las Corporaciones de Derecho Público.

En segundo lugar, esta política regula la prestación por la Agencia Notarial de Certificación, de servicios de sellado de fecha y hora al público.

Los participantes en los servicios de sellado de fecha y hora serán los siguientes:

- Prestador de Servicios de Sellado de Fecha y Hora.
- Entidades finales, incluyendo suscriptores y terceros que confían en sellos.

3.3.1. Prestador de Servicios de Sellado de Fecha y Hora

La Agencia Notarial de Certificación actuará como única y exclusiva entidad prestadora de servicios de sellado de fecha y hora para el Notariado español, por encargo del Consejo General del Notariado de España.

La Agencia Notarial de Certificación podrá emitir certificados de prestador de servicios de sellado de fecha y hora, habilitando a terceros la prestación del servicio a las Corporaciones de Derecho Público y, en general, al público.

La Agencia Notarial de Certificación podrá disponer de una o más Entidades de Sellado de Fecha y Hora para la prestación de los servicios, para ofrecer garantías de calidad de servicio, alta disponibilidad, continuidad de negocio, u otros criterios de negocio que lo justifiquen.

3.3.2. Entidades finales

Las entidades finales serán las personas y organizaciones destinatarias de los servicios de sellado de fecha y hora, incluyendo su emisión, gestión y uso, y entre ellas, las siguientes:

1) Suscriptores de sellos de fecha y hora.
2) Terceros que confían en sellos.

3.3.2.1. Suscriptores

Los suscriptores son las personas y las organizaciones que se suscriben a servicios de sellado de fecha y hora y que podrán solicitar sellos durante el periodo de suscripción.

3.3.2.2. Terceros que confían en sellos

Los terceros que confían en sellos son las personas y las organizaciones que reciben sellos de fecha y hora.

Como paso previo a confiar en los sellos, los terceros deben verificarlos, tal como se establece en este documento de política y en las correspondientes condiciones generales de uso.

3.4. Uso de los sellos

Esta sección lista las aplicaciones para las que pueden emplearse los sellos, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los sellos.

La Declaración de Prácticas de Sellado de Tiempo correspondiente determinará los usos concretos de cada tipo de sello soportado, de acuerdo con las normas establecidas en esta sección.

3.4.1. Usos permitidos

Los sellos iniciales se podrán solicitar para cualquier tipo de documento, firmado o no electrónicamente, y para cualquier tipo de objeto digital, incluso código ejecutable, garantizándose la existencia de dichos contenidos a la fecha indicada dentro del sello.

También podrán solicitarse sellos sobre sellos anteriormente expedidos (resellado).

3.4.2. Límites y prohibiciones de uso

3.4.2.1. Límites de uso

Los sellos se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Los sellos pueden incorporar límites de uso por razón de la materia y de la cuantía, que se establecen en las extensiones del certificado de Entidad de Sellado de Fecha y Hora emitido por la Agencia Notarial de Certificación, así como en la correspondiente política de sellado de fecha y hora, que se indicarán en las correspondientes condiciones generales de emisión y uso de sellos de fecha y hora.

3.4.2.2. Prohibiciones de usos

Los sellos no se han diseñado, no se pueden destinar y no se autoriza su uso en 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 podrán el suscriptor 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 los sellos para los usos limitados y/o prohibidos.

3.5. Administración de la política

3.5.1. Organización que administra el documento

Agencia Notarial de Certificación S.L.U.

3.5.2. Datos de contacto de la organización

Agencia Notarial de Certificación S.L.U.

Paseo del General Martínez Campos 46, 6ª planta

28010 Madrid

Teléfono: 902 104 045

ancert@ancert.com

3.5.3. Procedimientos de gestión del documento

La Agencia Notarial de Certificación debe disponer de un comité de aprobación de procedimientos y prácticas de la Entidad de Sellado de Fecha y Hora[1], formado por miembros de la alta dirección, que vele porque esta política se implante adecuadamente[2].

Se deben practicar análisis de riesgos periódicamente, para evaluar los activos de la Entidad de Sellado de Fecha y Hora, las vulnerabilidades y amenazas a dichos activos que puedan producir un impacto en el negocio, con la finalidad de determinar la idoneidad de los controles y procedimientos establecidos por esta política, o la necesidad de cambios en dichos controles y procedimientos[3].

La Agencia Notarial de Certificación debe disponer de una Declaración de Prácticas de Sellado de Tiempo específica para declarar sus controles y procedimientos de acuerdo con esta política de sellado de fecha y hora[4], así como los controles y procedimientos de cualquier entidad subcontratada para colaborar en la prestación del servicio[5].

[1] ETSI TS 102023, sección 7.1.1.f)

[2] ETSI TS 102023, sección 7.1.1.g)

[3] ETSI TS 102023, sección 7.1.1.a)

[4] ETSI TS 102023, sección 7.1.1.b)

[5] ETSI TS 102023, sección 7.1.1.c)

El comité de aprobación de procedimientos y prácticas debe velar por la existencia de un procedimiento de revisión periódica de la Declaración de Prácticas de Sellado de Tiempo[6].

[6] ETSI TS 102023, sección 7.1.1.h)

4. Publicación de información y depósito de sellos

4.1. Depósito(s) de sellos

La Agencia Notarial de Certificación deberá disponer de un Depósito.

El servicio de Depósito estará 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 6.7.4 y la Declaración de Prácticas de Certificación aplicable.

4.2. Publicación de información

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

- Los sellos emitidos, en el caso de la política de sellado de fecha u hora con custodia de sellos.
- Los certificados de Entidades de Sellado de Fecha y Hora propias.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados, correspondientes a las Entidades de Sellado de Fecha y Hora propias.
- La política de sellado de fecha y hora
- La Declaración de Prácticas de Sellado de Tiempo aplicable a los servicios de sellado[7].
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en sellos de fecha y hora[8].

El Depósito debe contener las versiones vigentes en cada momento, así como el histórico de versiones anteriores.

4.3. Frecuencia de publicación

La información anteriormente indicada, incluyendo políticas y la Declaración de Prácticas de Certificación, se publicará inmediatamente tras su aprobación.

Los cambios en los documentos de política y en la Declaración de Prácticas de Sellado de Tiempo se regirán por lo establecido en la sección 3.5 del documento de política o Declaración de Prácticas de Sellado de Tiempo.

La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en la política de certificación correspondiente a la Entidad de Sellado de Fecha y Hora.

[7] ETSI TS 102023, sección 7.1.1.d)

[8] ETSI TS 102023, sección 7.1.1.e)

4.4. Control de acceso

La Agencia Notarial de Certificación no limitará el acceso de lectura a las informaciones establecidas en la sección 4.2, pero establecerá controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información publicada.

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

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

5. Requisitos de operación del ciclo de vida de los sellos de fecha y hora

5.1. Solicitud de sello de fecha y hora

5.1.1. Legitimación para solicitar la emisión

Antes de la emisión de sellos de fecha y hora, debe existir un procedimiento de alta de suscriptor al servicio de sellado, en el que se determinarán las personas y sistemas que podrán solicitar sellos de fecha y hora, y de acuerdo con qué calidades y opciones.

5.1.2. Procedimiento de alta; Responsabilidades

Antes del alta como suscriptor, la Agencia Notarial de Certificación debe informar al suscriptor de los términos y condiciones aplicables al servicio[9].

La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible, y tendrá los siguientes contenidos mínimos[10]:

- La información de contacto de la Entidad de Sellado de Fecha y Hora.
- La política de sellado de fecha y hora aplicable.
- Al menos un algoritmo de resumen criptográfico que se pueda emplear para representar los datos para los que se solicita el sello de fecha y hora.
- El periodo previsto de vida de la firma electrónica empleada para firmar el sello de fecha y hora[11].
- La precisión de la fecha y hora del sello, con respecto al Tiempo Universal Coordinado.
- La disponibilidad del servicio, incluyendo los tiempos previstos de recuperación y de parada programados.
- Cualesquiera limitaciones en el uso del servicio de sellado de fecha y hora.
- Las obligaciones del suscriptor del servicio de sellado de fecha y hora.
- Las obligaciones del tercero que confía en sellos de fecha y hora.
- Información sobre cómo verificar el sello de fecha y hora, de forma que el tercero pueda decidir de forma razonable confiar o no en el mismo, así como cualesquiera limitaciones en el periodo de validez del sello.

[9] ETSI TS 102023, sección 7.1.1.e)

[10] ETSI TS 102023, sección 7.1.2

[11] Esta duración dependerá del algoritmo de resumen, algoritmo de firma y longitud de clave privada empleados por la Entidad de Sellado de Fecha y Hora.

- El periodo durante el cual la Entidad de Sellado de Fecha y Hora retiene registros de auditoría.
- El sistema jurídico que resulte aplicable a la prestación del servicio, incluyendo el cumplimiento de los requisitos establecidos por la legislación aplicable.
- Limitaciones de responsabilidad.
- Procedimientos de reclamaciones y resolución de disputas.
- Si la Entidad de Sellado de Fecha y Hora ha sido declarada conforme con la política de sellado aplicable, y en este caso, por qué organismo independiente.

Tras la adhesión a las condiciones generales del servicio por el suscriptor, la Agencia Notarial de Certificación procederá a su alta en el sistema, habilitando los medios técnicos para recibir solicitudes de sello. En su caso, se expedirán los correspondientes certificados al suscriptor, para la autenticación en el procedimiento de solicitud de sellos de fecha y hora.

La Agencia Notarial de Certificación soportará, al menos, un protocolo de transporte[12] de las solicitudes de sellado de fecha y hora, y entre ellos, al menos dispondrá de la posibilidad de solicitar el servicio empleando servicios web y HTTP[13].

5.2. Procesamiento de la solicitud de sello de fecha y hora

Una vez recibida una solicitud de sello de fecha y hora, la Agencia Notarial de Certificación debe verificar los siguientes aspectos:

- La procedencia y la autenticidad de la solicitud, mediante el protocolo de seguridad apropiado al medio de transporte empleado, incluyendo al menos SSL/TLS para el protocolo HTTP[14]. En caso que resulte necesario, se emitirán certificados para dicha función.
- La corrección técnica[15] de la solicitud, de acuerdo con el protocolo escogido y, en concreto, que la solicitud contiene:
    - El número de versión.
    - Un resumen criptográfico válido conforme a uno de los algoritmos apropiados, según se expone posteriormente.
    - La indicación de la política de sellado de fecha y hora de acuerdo con la que se solicita el sello[16].

[12] RFC 3161, sección 3

[13] ETSI TS 101861, sección 6

[14] RFC 3161 no establece ningún método para autenticar al solicitante de sellos, sino que esta posibilidad debe implantarse mediante la seguridad del protocolo de transporte de las solicitudes, como es HTTPS.

[15] RFC 3161, sección 2.4.1

[16] Aunque en RFC 3161 esta posibilidad se trata como una opción, esta política de sellado de fecha y hora la considera obligatoria para considerar que una solicitud es válida.

  - Opcionalmente, el número de ocurrencia única (*nonce*), generado por el suscriptor.

- Se considerarán válidos los siguientes algoritmos de resumen[17]: SHA-1 o superior, con exclusión expresa de MD5 y otros algoritmos, recomendándose también el abandono a partir de 2011 de SHA-1.
- La solicitud no deberá contener extensiones[18].

En caso de verificación incorrecta de la solicitud, se devolverán los mensajes de error apropiados[19].

5.3. Emisión del sello de fecha y hora

Tras la verificación de la solicitud se procederá a la emisión del sello de fecha y hora, de forma segura.

La Agencia Notarial de Certificación deberá[20]:

- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de sellado de fecha y hora a los que sirven de soporte.
- Emplear fuentes de fecha y hora fiables, de acuerdo con los requisitos establecidos en la sección de esta política.
- Generar sellos de fecha y hora conteniendo las informaciones incluidas en la sección 8 de esta política.
- Emplear una clave específica para la firma de los sellos generados, de acuerdo con los requisitos de gestión de claves especificados en la sección 7 de esta política.

5.4. Entrega del sello de fecha y hora

5.4.1. Entrega del sello de fecha y hora

La Agencia Notarial de Certificación deberá entregar el sello al solicitante, mediante el protocolo de transporte empleado para la solicitud.

La respuesta protocolaria deberá contener el resultado de la solicitud y, en su caso, el sello emitido[21].

---

[17] ETSI TS 101861, sección 4.2.2, con exclusión de MD5 por su pérdida de robustez desde el momento de aprobación de la especificación técnica.

[18] ETSI TS 101861, sección 4.2.1

[19] RFC 3161, sección 2.4.2

[20] ETSI TS 102023, sección 7.3.1

[21] RFC 3161, sección 2.4.2

5.4.2. Publicación del sello de fecha y hora

En los casos de sellos de fecha y hora con custodia, la Agencia Notarial de Certificación publicará el sello en el Depósito a que se refiere la sección 4.1 de esta política, con los controles de acceso pertinentes.

5.4.3. Notificación de la emisión a terceros

La Agencia Notarial de Certificación podrá establecer casos y métodos en que se notifique la emisión a terceros, de acuerdo con las necesidades de los suscriptores.

5.5. Finalización de la suscripción

Transcurrido el plazo contractualmente establecido, finalizará la suscripción al servicio, y no se podrán seguir solicitando sellos de fecha y hora.

6. Controles de seguridad física, de gestión y de operaciones

La Agencia de Notarial de Certificación deberá implantar los siguientes controles:

- Seguridad física[22].
- Gestión de la seguridad[23].
- Personal[24]
- Auditoría de seguridad[25].
- Archivo de operaciones[26].
- Renovación de claves[27].
- Compromiso de claves y recuperación de desastre[28].
- Terminación del servicio[29].

6.1. Controles de seguridad física

La Agencia Notarial de Certificación debe disponer de instalaciones que protejan físicamente la prestación del servicio de sellado de fecha y hora del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se logrará mediante la creación de perímetros de seguridad claramente definidos en torno al servicio, pudiendo compartirse estos espacios con los restantes servicios de certificación de la Agencia Notarial de Certificación. La parte de las instalaciones compartida con otras organizaciones debe encontrarse fuera de estos perímetros.

La Agencia Notarial de Certificación establecerá 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 al servicio de sellado de fecha y hora deberá establecer prescripciones para las siguientes contingencias, que se documentarán sucintamente en la Declaración de Prácticas de Certificación:

---

[22] ETSI TS 102023, sección 7.4.4

[23] ETSI TS 102023, secciones 7.4.1, 7.4.2 y 7.4.5

[24] ETSI TS 102023, sección 7.4.3

[25] ETSI TS 102023, sección 7.4.11

[26] ETSI TS 102023, sección 7.4.11

[27] ETSI TS 102023, sección 7.2.4

[28] ETSI TS 102023, sección 7.4.8

[29] ETSI TS 102023, sección 7.4.9

- 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 antirrobos.
- Allanamiento y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para el servicio de sellado de fecha y hora.

6.1.1. Localización y construcción de las instalaciones

La localización de las instalaciones debe permitir la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos (en el caso de no contar con presencia física permanente de personal de seguridad del prestador de servicios de certificación)

La calidad y solidez de los materiales de construcción de las instalaciones deberá garantizar unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

6.1.2. Acceso físico

La Agencia Notarial de Certificación deberá establecer 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 lleven a cabo procesos relacionados con el ciclo de vida del sello de fecha y hora, será 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, deberá realizarse mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de las Entidades de Sellado de Fecha y Hora, así como su almacenamiento, deberá realizarse en dependencias específicas para estos fines, y requerirán de acceso y permanencia duales.

6.1.3. Electricidad y aire acondicionado

Los equipos informáticos deberán estar convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones contarán 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 deberán estar ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

6.1.4. Exposición al agua

La Agencia Notarial de Certificación deberá disponer de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso de que las condiciones de ubicación de las instalaciones lo hagan necesario.

6.1.5. Prevención y protección de incendios

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

En concreto, los dispositivos criptográficos y los soportes que almacenen claves, deberán contar con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

6.1.6. Almacenamiento de soportes

El almacenamiento de soportes de información debe realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Deberá contarse para ellos con dependencias o armarios ignífugos.

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

6.1.7. Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se deberá realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

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

En el caso de documentación en papel, éste deberá someterse a un tratamiento físico de destrucción.

6.1.8. Copia de respaldo fuera de las instalaciones

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

6.2. Controles de gestión

La Agencia Notarial de Certificación debe garantizar que sus sistemas se operan de forma segura, para lo cual deberá establecer e implantar procedimientos para las funciones que afecten a la provisión de sus servicios.

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

6.2.1. Funciones fiables

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

Las personas que deban ocupar tales puestos deberán ser formalmente nombrados por la alta dirección del prestador de servicios de certificación.

Las funciones fiables deberán incluir:

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

6.2.2. Número de personas por tarea

Las funciones fiables identificadas en la política de seguridad, y sus responsabilidades asociadas, serán documentadas en descripciones de puestos de trabajo, y descritas de forma sucinta en la Declaración de Prácticas de Certificación correspondiente.

Dichas descripciones deberán realizarse teniendo en cuenta que debe existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

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

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

6.2.3. Identificación y autenticación para cada función

La Agencia Notarial de Certificación deberá identificar y autenticar al personal antes de acceder a la correspondiente función fiable.

6.2.4. Roles que requieren separación de tareas

Las siguientes tareas deberán ser realizadas, al menos, por dos personas:

- Gestión del acceso físico.
- Gestión de aplicaciones informáticas de la Entidad de Sellado de Fecha y Hora.
- Gestión de bienes de equipo criptográfico.
- Gestión de claves de la Entidad de Sellado de Fecha y Hora.
- Gestión de configuración y control de cambios.
- Gestión del archivo.

6.3. Controles de personal

6.3.1. Requisitos de historial, calificaciones, experiencia y autorización

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

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

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

El personal en puestos fiables deberá encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

No se podrá asignar a un puesto fiable o de gestión a una persona que no sea idóneo para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se deberá realizar 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.

6.3.2. Procedimientos de investigación de historial

La Agencia Notarial de Certificación deberá realizar 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 informará acerca de la necesidad de someterse a una investigación previa.

Se deberá advertir de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

Se deberá obtener consentimiento inequívoco del afectado por la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la LOPD y su Reglamento de desarrollo.

La investigación se repetirá cada tres años.

6.3.3. Requisitos de formación

La Agencia Notarial de Certificación deberá formar al personal en puestos fiables y de gestión, hasta que alcancen la cualificación necesaria, de acuerdo con lo establecido en la sección 6.3.1 de esta política.

La formación deberá incluir 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.

6.3.4. Requisitos y frecuencia de actualización formativa

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

6.3.5. Secuencia y frecuencia de rotación laboral

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

6.3.6. Sanciones para acciones no autorizadas

La Agencia Notarial de Certificación deberá disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que deberá encontrarse 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 podrán incluir la suspensión y el despido de la persona responsable de la acción dañina.

6.3.7. Requisitos de contratación de profesionales

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

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

6.3.8. Suministro de documentación al personal

La Agencia Notarial de Certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido en la sección 6.3.1 de esta política.

6.4. Procedimientos de auditoría de seguridad

6.4.1. Tipos de eventos registrados

La Agencia Notarial de Certificación debe guardar 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 autoridad de sellado de fecha y hora.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves de la Entidad de Sellado de Fecha y Hora.
- Operaciones que afecten a los relojes.
- Cambios en las políticas de emisión de sellos de fecha y hora.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red de la Entidad de Sellado de Fecha y Hora.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un sello custodiado, y de lectura y escritura en el Depósito.
- Eventos relacionados con el ciclo de vida del sello, como solicitud, emisión o publicación en el Depósito.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

La Agencia Notarial de Certificación debe también guardar, 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 Sellado de Fecha y Hora.

6.4.2. Frecuencia de tratamiento de registros de auditoría

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

El procesamiento de los registros de auditoría consistirá 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.

6.4.3. Periodo de conservación de registros de auditoría

Los registros de auditoría se deben retener en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivarán de acuerdo con la sección 6.5.2 de esta política.

6.4.4. Protección de los registros de auditoría

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

6.4.5. Procedimientos de copia de respaldo

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

6.4.6. Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría deberá ser, al menos, 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 serán almacenados por el personal debidamente autorizado.

6.4.7. Notificación del evento de auditoría al causante del evento

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

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

6.4.8. Análisis de vulnerabilidades

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

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.

Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, de la Agencia Notarial de Certificación.

6.5. Archivo de informaciones

La Agencia Notarial de Certificación debe garantizar que toda la información relativa a los sellos de fecha y hora se guarda durante un período de tiempo apropiado, según lo establecido en la sección 6.5.2 de esta política.

6.5.1. Tipos de eventos registrados

La Agencia Notarial de Certificación debe guardar todos los eventos que tengan lugar durante el ciclo de vida de un sello de fecha y hora, incluyendo la renovación del mismo.

Se debe guardar un registro de lo siguiente:

- Altas y bajas de suscriptores.
- Listados de sellos emitidos.
- Los sellos custodiados, cuando se preste el servicio.

6.5.2. Periodo de conservación de registros

La Agencia Notarial de Certificación debe guardar los registros especificados en la sección anterior de esta política de forma permanente, con un mínimo de quince (15) años.

6.5.3. Protección del archivo

La Agencia Notarial de Certificación debe:

- Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los sellos emitidos.
- Archivar los datos anteriormente citados de forma completa y confidencial.
- Mantener la privacidad de los datos del suscriptor.

6.5.4. Procedimientos de copia de respaldo

La Agencia Notarial de Certificación debe realizar copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección 6.5.1 de esta política.

Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección 6.7 de esta política.

Además, debe guardar los documentos en papel, según la sección 6.5.1, 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 6.7 de esta política.

6.5.5. Localización del sistema de archivo

La Agencia Notarial de Certificación debe disponer de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, tal y como se especifica en la sección 6.5.4 de esta política.

6.5.6. Procedimientos de obtención y verificación de información de archivo

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

6.6. Renovación de claves

La Agencia Notarial de Certificación deberá establecer un plan de renovación programada de las claves de las Entidades de Sellado de Fecha y Hora, que garantice la continuidad de los servicios.

6.7. Compromiso de claves y recuperación de desastre

6.7.1. Corrupción de recursos, aplicaciones o datos

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

6.7.2. Revocación de la clave pública de la entidad

En el caso de que la Agencia Notarial de Certificación deba revocar la clave pública de una Entidad de Sellado de Fecha y Hora, deberá llevar a cabo lo siguiente:

- Desactivar el uso de la clave privada de la Entidad de Sellado de Fecha y Hora.
- Solicitar la revocación y seguir los procedimientos correspondientes descritos en la Declaración de Prácticas de Certificación para los certificados de Entidad de Sellado de Fecha y Hora.
- Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales la Agencia Notarial de Certificación haya emitido sellos, así como a los terceros, mediante la publicación de la revocación en el depósito.
- 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, según lo establecido en la sección 6.6 de esta política.

6.7.3. Compromiso de la clave privada de la entidad

El plan de continuidad de negocio de la Agencia Notarial de Certificación (o plan de recuperación de desastres) debe considerar el compromiso o la sospecha de compromiso de la clave privada de las Entidades de Sellado de Fecha y Hora como un desastre.

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

- Informar a todos los suscriptores y terceros del compromiso.
- Indicar que los sellos que han sido entregados usando la clave de esta Entidad de Sellado de Fecha y Hora ya no son válidos.

6.7.4. Desastre sobre las instalaciones

La Agencia Notarial de Certificación debe desarrollar, mantener, probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indique cómo restaurar los servicios de los sistemas de información.

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

La Agencia Notarial de Certificación debe ser capaz de restaurar la operación normal de los servicios de sellado de fecha y hora, en las 24 horas siguientes al desastre.

La base de datos de recuperación de desastres utilizada por la Agencia Notarial de Certificación debe estar 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 deben tener las medidas de seguridad físicas especificadas en el plan de seguridad, equivalentes a las de las instalaciones principales.

6.8. Terminación del servicio

La Agencia Notarial de Certificación debe asegurar que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios de la Entidad de Sellado de Fecha y Hora y, en particular, asegurar un mantenimiento continuo de los sellos custodiados que sean requeridos para proporcionar evidencia en caso de investigación civil o criminal.

Antes de terminar sus servicios, la Agencia Notarial de Certificación debe ejecutar, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y terceros que confían en sellos.
- Retirar toda autorización de subcontrataciones que actúan en su nombre en el proceso de emisión de sellos.
- Ejecutar las tareas necesarias para transferir las obligaciones de mantenimiento de los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en sellos.
- Destruir las claves privadas de la Entidad de Sellado de Fecha y Hora.

La Agencia Notarial de Certificación debe declarar en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas deben incluir:

- Notificación a las entidades afectadas.
- Transferencia de sus obligaciones a otras personas.

7. Controles de seguridad técnica

La Agencia Notarial de Certificación deberá emplear sistemas y productos fiables[30], que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sellado de fecha y hora a los que sirven de soporte.

Asimismo, debe garantizar el empleo de fuentes de fecha y hora fiables para garantizar la precisión del sello.

7.1. Fiabilidad de la fuente de fecha y hora

Los valores de fecha y hora incluidos en los sellos serán trazables al menos a un valor de tiempo real distribuido por un laboratorio oficial de Tiempo Universal Coordinado, debiéndose consultar en primer lugar al Real Observatorio de la Armada.

La Agencia Notarial de Certificación debe asegurar que el reloj de las Entidades de Sellado de Fecha y Hora se encuentra sincronizado con Tiempo Universal Coordinado con la precisión declarada en el sello[31].

- La calibración de los relojes debe ser mantenida de forma que no resulte previsible un desplazamiento en la fecha y hora de los mismos.
- Los relojes serán protegidos contra amenazas que pudieran resultar en un cambio no detectado que descalibre el reloj.
- Se asegurará que se detectarán los desplazamientos y saltos del reloj, que impidan su sincronización con Tiempo Universal Coordinado.
- Se asegurará que se mantiene la sincronización del reloj cuando se notifica un segundo de salto, notificado por el órgano competente.

7.2. Generación e instalación del par de claves

7.2.1. Generación del par de claves

Los pares de claves de las Entidades de Sellado de Fecha y Hora deben ser generados empleando hardware criptográfico que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 parte 2, según proceda, o de acuerdo con un objetivo de seguridad o perfil de protección equivalente; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.

[30] ETSI TS 102023, sección 7.4.7

[31] ETSI TS 102023, sección 7.3.2

7.2.2. Envío de la clave pública al emisor del certificado

La clave pública de la Entidad de Sellado de Fecha y Hora será certificada por la Agencia Notarial de Certificación, de acuerdo con lo establecido en su Declaración de Prácticas de Certificación.

El algoritmo de firma de los certificados de la Entidad de Sellado de Fecha y Hora debe ser sha256rsa o superior.

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

7.2.3. Distribución de la clave pública de la Entidad de Sellado de Fecha y Hora

Las claves de las Entidades de Sellado de Fecha y Hora deben ser comunicadas a los terceros que confían en sellos, asegurando la integridad de la clave y autenticando su origen.

La clave pública de cada Entidad de Sellado de Fecha y Hora se publicará en el Depósito, en forma de certificado firmado por una Entidad de Certificación de la Agencia Notarial de Certificación, junto a una declaración referente a que la clave autentica a la Entidad de Sellado de Fecha y Hora.

Los usuarios podrán acceder al Depósito para obtener las claves públicas de las Entidades de Sellado de Fecha y Hora.

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

7.2.4. Longitudes de claves

La longitud de las claves de las Entidades de Sellado de Fecha y Hora será al menos de 2048 bits.

7.2.5. Generación de parámetros de clave pública

Sin estipulación.

7.2.6. Comprobación de calidad de parámetros de clave pública

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

7.2.7. Generación de claves en aplicaciones informáticas o en bienes de equipo

Los pares de claves de las Entidades de Sellado de Fecha y Hora deben ser generados empleando hardware criptográfico que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 parte 2, según proceda, o de acuerdo con un objetivo de seguridad o perfil de protección equivalente; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.

7.3. Protección de la clave privada

7.3.1. Estándares de módulos criptográficos

Para los módulos que gestionan claves de las Entidades de Sellado de Fecha y Hora se deberá asegurar el nivel exigido por los estándares indicados en las secciones anteriores.

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

El acceso de operación a las claves privadas de las Entidades de Sellado de Fecha y Hora deberá requerir necesariamente del concurso sucesivo de dos (2) dispositivos criptográficos protegidos por una clave de acceso, de entre cuatro (4) dispositivos.

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

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

7.3.3. Depósito de la clave privada

Las claves privadas de las Entidades de Certificación se almacenarán en espacios ignífugos y protegidos por controles de acceso físico dual.

No se depositarán otras claves privadas.

7.3.4. Copia de respaldo de la clave privada

No se podrán realizar copias de respaldo de las claves privadas de las Entidades de Sellado de Fecha y Hora[32].

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.

7.3.5. Archivo de la clave privada

No se archivarán claves privadas de Entidades de Sellado de Fecha y Hora.

7.3.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se podrán 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.

[32] ETSI TS 102023, sección 7.2.1

En este caso, las claves privadas de las Entidades de Sellado de Fecha y Hora quedarán almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no podrán ser extraídas).

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

7.3.7. Método de activación de la clave privada

La clave privada de cada Entidad de Sellado de Fecha y Hora se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 7.3.2.

7.3.8. Método de desactivación de la clave privada

La desactivación de la clave privada se producirá en los casos de apagado del módulo criptográfico, o mediante los procedimientos soportados por el módulo criptográfico.

7.3.9. Método de destrucción de la clave privada

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

7.4. Otros aspectos de gestión del par de claves

7.4.1. Archivo de la clave pública

Las Entidades de Sellado de Fecha y Hora archivarán sus claves públicas de forma permanente, de acuerdo con lo establecido en la sección 6.5 de esta política.

7.4.2. Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves serán los determinados por la duración del certificado de la Entidad de Sellado de Fecha y Hora, transcurrido el cual no podrán continuar utilizándose.

Dicho periodo no podrá ser superior al periodo previsto de validez criptográfica del algoritmo y longitud de clave empleados para la producción de sellos[33].

La clave privada se podrá emplear sólo durante el primer año de vida del certificado, que será de hasta seis años. A partir del segundo año y hasta el fin del período de validez del certificado de la Entidad de Sellado de Fecha y Hora únicamente se podrá emplear la clave pública para la verificación de los sellos.

[33] ETSI TS 102023, sección 7.2.4

7.5. Datos de activación

7.5.1. Generación e instalación de datos de activación

Los datos de activación se deberán formar a partir del concurso sucesivo de dos (2) dispositivos criptográficos protegidos por una clave de acceso, de entre cuatro (4) dispositivos.

7.5.2. Protección de datos de activación

Los poseedores de los dispositivos criptográficos anteriormente indicados deberán proteger las claves de acceso a los mismos.

7.5.3. Otros aspectos de los datos de activación

Sin estipulación.

7.6. Controles de seguridad informática

7.6.1. Requisitos técnicos específicos de seguridad informática

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados[34]. En particular:

- Se debe garantizar 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 debe garantizar 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 estará restringido y estrechamente controlado.
- El personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del sello de fecha y hora.
- El personal será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- Deberá evitarse 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.

[34] ETSI TS 102023, sección 7.4.6

- Los sistemas de seguridad y monitorización deben permitir 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 deberá contar con un control de accesos para modificaciones o borrado de datos.

7.6.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de sellado de fecha y hora empleadas por la Agencia Notarial de Certificación deberán ser fiables, debiendo acreditarse dicha condición, por ejemplo, mediante una certificación de producto contra un perfil de protección adecuado, conforme a la norma ISO 15408, o equivalente.

7.7. Controles técnicos del ciclo de vida

7.7.1. Controles de desarrollo de sistemas

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de autoridad de certificación y de registro, para garantizar que los sistemas son seguros.

Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

7.7.2. Controles de gestión de seguridad

La Agencia Notarial de Certificación deberá mantener un inventario de todos los activos informativos y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección 9.1.1 de esta política.

Se realizará un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

7.7.3. Evaluación del nivel de seguridad del ciclo de vida

El Consejo General del Notariado podrá exigir que la Agencia Notarial de Certificación se someta a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos que emplea.

7.8. Controles de seguridad de red

Se deberá garantizar que el acceso a las diferentes redes de la Agencia Notarial de Certificación está limitado a individuos debidamente autorizados. En particular:

- Deben implementarse controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos deberán configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Certificación.
- Los datos sensibles deberán protegerse cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
- Se debe garantizar que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

7.9. Controles de ingeniería de módulos criptográficos

Se debe garantizar que las claves de las Entidades de Sellado de Fecha y Hora son generadas en equipamientos criptográficos, que cumplan los estándares criptográficos de seguridad que se han indicado en las secciones anteriores.

8. Perfiles de sellos de fecha y hora

Los sellos tendrán el contenido y campos descritos en esta sección, incluyendo, como mínimo, los siguientes[35]:

- Número de versión del sello.
- Indicador de política de sellado de fecha y hora.
- Resumen criptográfico del objeto sellado.
- Número de serie.
- Fecha y hora del sello.
- Precisión.
- Identificación de la Entidad de Sellado de Fecha y Hora.

No se emplearán ni el campo Ordenación ni extensiones.

La Agencia Notarial de Certificación publicará sus perfiles de sellos en el Depósito indicado en la sección 4.

[35] RFC 3161, sección 2.4.2; ETSI TS 101861, sección 5.2.1

9. Auditoría de conformidad

La Agencia Notarial de Certificación debe realizar 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 sellado de fecha y hora del Consejo General del Notariado.

9.1.1. Frecuencia de la auditoría de conformidad

Se debe llevar a cabo 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.

9.1.2. Identificación y calificación del auditor

Si la Agencia Notarial de Certificación de certificación dispone de un departamento de auditoría interno, éste podrá encargarse de llevar a cabo la auditoría de conformidad.

En el caso de no poseer ese departamento, o de considerarlos oportuno, se deberá acudir a un auditor independiente, el cual debe demostrar experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública y de sellado de fecha y hora.

9.1.3. Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros deben ser llevadas a cabo 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.

9.1.4. Listado de elementos objeto de auditoría

Los elementos objeto de auditoría serán los siguientes:

- Procesos de sellado de fecha y hora.
- 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 detallarán en el plan de auditoría de la Agencia Notarial de Certificación.

9.1.5. 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 debe discutir, con la entidad que ha ejecutado la auditoría y, en su caso, con el

Consejo General del Notariado, las deficiencias encontradas y desarrollar y ejecutar un plan correctivo que solvente 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 Sellado de Fecha y Hora, tal y como se describe en la sección 6.7.2 de esta política.
- Terminar los servicios de sellado de fecha y hora, tal y como se describe en la sección 6.8 de esta política.

9.1.6. Tratamiento de los informes de auditoría

La Agencia Notarial de Certificación debe entregar los informes de resultados de auditoría, al Consejo General del Notariado, en un plazo máximo de 15 días tras la ejecución de la auditoría.

10. Requisitos comerciales y legales

10.1. Tarifas

10.1.1. Tarifa de emisión o renovación de sellos

La Agencia Notarial de Certificación podrá establecer una tarifa por la emisión o por la renovación de los sellos, que deberá ser aprobada por el Consejo General del Notariado.

10.1.2. Tarifa de acceso a sellos

La Agencia Notarial de Certificación no podrá establecer ninguna tarifa por el acceso a los sellos que en su caso se publiquen.

10.1.3. Tarifas de otros servicios

Sin estipulación.

10.1.4. Política de reintegro

La Agencia Notarial de Certificación no podrá reintegrar las tarifas del servicio, excepto por funcionamiento erróneo, debiendo documentar en su Declaración de Prácticas de Certificación los casos en que se reintegrarán dichas tarifas.

10.2. Capacidad financiera

La Agencia Notarial de Certificación deberá disponer 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.

10.2.1. Cobertura de seguro

La Agencia Notarial de Certificación deberá disponer 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.

10.2.2. Otros activos

Sin estipulación.

10.2.3. Cobertura de seguro para suscriptores y terceros que confían en sellos

Sin estipulación.

10.3. Confidencialidad

10.3.1. Informaciones confidenciales

Las siguientes informaciones, como mínimo, serán mantenidas confidenciales 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".

10.3.2. Informaciones no confidenciales

La siguiente información será considerada no confidencial:

- La información contenida en el Depósito.
- Toda otra información que no esté indicada en la sección anterior de esta política.

10.3.3. Divulgación legal de información

La Agencia Notarial de Certificación divulgará la información confidencial en los casos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el sello de fecha y hora serán divulgados en caso de ser requerido para ofrecer evidencia del sellado en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del servicio.

Se indicarán estas circunstancias en la política de intimidad prevista en la sección 10.4 de esta política.

10.3.4. Divulgación de información por petición de su titular

La Agencia Notarial de Certificación incluirá, en la política de intimidad prevista en la sección 10.4 de esta política, prescripciones para permitir la divulgación de la información del suscriptor, directamente a los mismos o a terceros.

10.3.5. Otras circunstancias de divulgación de información

Sin estipulación.

10.4. Protección de datos personales

Para la prestación del servicio, la Agencia Notarial de Certificación precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones serán recabadas directamente de los afectados, con su consentimiento explícito o en los casos es los que la ley permita recabar la información sin consentimiento del afectado.

Se recabarán los datos exclusivamente necesarios para la prestación del servicio de sellado de fecha y hora.

La Agencia Notarial de Certificación deberá desarrollar una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documentar en su Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Reglamento de desarrollo de la Ley. Dicha Declaración de Prácticas de Certificación tendrá la consideración de documento de seguridad.

La Agencia Notarial de Certificación no divulgará ni cederá datos personales, excepto en los casos previstos en las secciones 10.3.2 a 10.3.5 de esta política, y en la sección 6.8, en caso de terminación de la Entidad de Certificación.

La información confidencial de acuerdo con la LOPD será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Reglamento de desarrollo de la LOPD.

10.5. Derechos de propiedad intelectual

El Consejo General del Notariado será la única entidad que gozará de los derechos de propiedad intelectual sobre las políticas de sellado de fecha y hora.

La Agencia Notarial de Certificación será propietaria de las Declaraciones de Prácticas de Certificación.

10.6. Obligaciones y responsabilidad civil

10.6.1. Obligaciones de la Agencia Notarial de Certificación

La Agencia Notarial de Certificación debe garantizar, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política para la que emite sellos de fecha y hora.

Será la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

La Agencia Notarial de Certificación debe prestar sus servicios de certificación conforme con su Declaración de Prácticas de Certificación vigente, en la que se detallarán sus funciones, procedimientos de operación y medidas de seguridad.

Se debe vincular a los suscriptores y a los terceros que confían en sellos mediante condiciones generales de emisión y uso, que deberán estar en lenguaje escrito y comprensible.

10.6.2. Garantías ofrecidas a suscriptores y terceros que confían en sellos

La Agencia Notarial de Certificación, en las condiciones generales de emisión y uso, establecerá y rechazará garantías, y limitaciones de responsabilidad aplicables.

La Agencia Notarial de Certificación, como mínimo, garantizará:

- Que los sellos de fecha y hora cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.
- Que el servicio de Depósito cumple con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

10.6.3. Rechazo de otras garantías

La Agencia Notarial de Certificación podrá rechazar toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 10.6.2.

10.6.4. Limitación de responsabilidades

La Agencia Notarial de Certificación limitará su responsabilidad a la producción de sellos con fecha y hora en las condiciones de esta política, y en ningún caso aceptará responsabilidad alguna por el uso de dicho sello.

10.6.5. Caso fortuito y fuerza mayor

La Agencia Notarial de Certificación incluirá cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en las condiciones generales de emisión y uso.

10.6.6. Ley aplicable

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

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

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, se velará porque, al menos los requisitos contenidos en las secciones 10.6.1 (Obligaciones y

responsabilidad), 9 (Auditoría de conformidad) y 10.3 (Confidencialidad), continúen vigentes tras la terminación de los servicios.

- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

10.6.8. Cláusula de jurisdicción competente

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

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

10.6.9. Resolución de conflictos

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso, los procedimientos de mediación y resolución de conflictos aplicables.