BOLETIN OFICIAL

DEL

PARLAMENTO DE NAVARRA

X Legislatura | Pamplona, 9 de febrero de 2023 | NÚM. 22

S U M A R I O

SERIE H:

Otros Textos Normativos:

—Resolución 2/2023, de 10 de enero, de la Letrada Mayor del Parlamento de Navarra, por la que se aprueba el documento “Política de gestión del documento electrónico en el Parlamento de Navarra” (Pág. 2).

—Política de gestión del documento electrónico en el Parlamento de Navarra (Pág. 2).

—Resolución 3/2023, de 10 de enero, de la Letrada Mayor del Parlamento de Navarra, por la que se aprueba el documento “Política de identidad y firma electrónica en el Parlamento de Navarra” (Pág. 16).

—Política de identidad y firma electrónica en el Parlamento de Navarra (Pág. 16).

Serie H:
OTROS TEXTOS NORMATIVOS

Resolución 2/2023, de 10 de enero, de la Letrada Mayor del Parlamento de Navarra, por la que se aprueba el documento "Política de gestión del documento electrónico en el Parlamento de Navarra"

La Mesa del Parlamento, en sesión de 9 de enero de 2023, se dio por enterada de la propuesta normativa "Política de gestión del documento electrónico en el Parlamento de Navarra", mostrando su conformidad con la misma.

Por lo expuesto, y de conformidad con lo dispuesto en el artículo 37 del Reglamento del Parlamento de Navarra,

RESUELVO:

1º. Aprobar el documento "Política de gestión del documento electrónico en el Parlamento de Navarra", que se adjunta a la presente Resolución y que entrará en vigor cuando la Mesa de la Cámara lo determine, conforme a la implantación de la administración electrónica.

2º. Ordenar la publicación de la presente Resolución en el Boletín Oficial del Parlamento de Navarra.

Pamplona, 10 de enero de 2023

La Letrada Mayor: Silvia Doménech Alegre

Política de gestión del documento electrónico en el Parlamento de Navarra

Se ordena la publicación en el Boletín Oficial del Parlamento de Navarra del documento "Política de gestión del documento electrónico en el Parlamento de Navarra", aprobado por Resolución de la Letrada Mayor n.º 2/2023, de 10 de enero de 2023.

Pamplona, 10 de enero de 2023

El Presidente: Unai Hualde Iglesias

Política de Gestión de Documentos Electrónicos (PGDE) del Parlamento de Navarra

Sumario

1. Introducción

2. Alcance y ámbito de aplicación

3. Datos identificativos del documento

4. Principios de la gestión documental

5. Actores involucrados y responsabilidades

6. Elementos de la gestión del documento electrónico

6.1 Modelo de Gestión de Expedientes y Documentos Electrónicos (MGEDE)

6.2 Firma electrónica

6.3 Descripción y asociación de metadatos

7. Desarrollo de la Política

8. Plan de formación

9. Supervisión y auditoría

10. Gestión de la Política

Anexo I - Conceptos básicos

Anexo II - Referencias

1. Legislación y normativa

2. Normas Técnicas de Interoperabilidad

3. Guías técnicas

4. Otras referencias

5. Abreviaturas

1. INTRODUCCIÓN

El Parlamento de Navarra, en su estrategia de implantación del documento y expediente electrónico como elemento base en su actuación administrativa y parlamentaria, requiere dotarse de una política de gestión de documentos electrónicos, tal y como establece la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas y según se indica en la resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

En dicho contexto, el Parlamento ha optado por establecer un modelo de gestión basado en el uso de la documentación electrónica que proporcione cobertura a los siguientes principios básicos:

• **Transparencia**. El hecho de que la documentación esté disponible en un formato fácil de compartir supone una respuesta adecuada a la obligación de poner a disposición de la ciudadanía la información oportuna para la rendición de cuentas de la actividad realizada por el Parlamento.

• **Eficacia en la gestión**. La incorporación de herramientas de tramitación y de gestión de expedientes electrónicos agiliza el funcionamiento de la organización y da mayores garantías en la consecución de los objetivos trazados previamente.

• **Eficiencia en el aprovechamiento de los recursos**. El uso de la documentación electrónica permite automatizar tareas redundantes, con lo que se reduce el tiempo invertido en la gestión de documentos en soporte papel, evita el espacio físico destinado a su archivo, elimina los desplazamientos y economiza en el consumo de sistemas de instalación y materiales de conservación.

• **Seguridad de la información**. La definición de estrategias de conservación y sistemas de seguridad documental permite aplicar mecanismos automatizados de control de acceso a la documentación, garantizando además su conservación a largo plazo.

La presente Política de Gestión de Documentos Electrónicos (en adelante, la Política) pone las bases estratégicas y organizativas para el establecimiento de unos criterios homogéneos en el uso, la gestión y la conservación de los documentos electrónicos, desarrollados en detalle en el Modelo de Gestión de Expedientes y Documentos Electrónicos (en adelante MGEDE).

2. ALCANCE Y ÁMBITO DE APLICACIÓN

La Política tiene como finalidad establecer las directrices estratégicas para la gestión de la documentación electrónica en el Parlamento de Navarra en el marco de la generación de documentos y expedientes electrónicos.

Establece un conjunto de directrices, procedimientos y prácticas con el fin de garantizar una gestión eficiente de la documentación electrónica durante todo su ciclo de vida, es decir, desde el instante de su generación, captura o incorporación al sistema de gestión durante tanto tiempo como deba conservarse en atención su valor administrativo y, en el caso de la documentación con valor histórico, permanente.

El objetivo principal es asegurar que los documentos y expedientes electrónicos se mantienen auténticos, fiables, íntegros y disponibles como información fehaciente y evidencia de apoyo a las funciones y actividades del Parlamento a lo largo del tiempo.

Las directrices mencionadas se agrupan en tres ámbitos fundamentales:

• El establecimiento de unos principios estratégicos en la gestión del documento electrónico, que respetan cualquier herramienta o proyecto del Parlamento que trabaje con documentación electrónica.

• La identificación y caracterización de los principales procesos relacionados con la gestión de los documentos y expedientes electrónicos.

• La atribución de responsabilidades a los distintos órganos y miembros del Parlamento para la implantación y el desarrollo de la Política.

Establecidas las directrices, la Política identifica los instrumentos y los modelos operativos —desarrollados en profundidad en el MGEDE— para su implementación efectiva, identificando en cada caso el ámbito funcional responsable de su desarrollo y mantenimiento.

3. DATOS IDENTIFICATIVOS DEL DOCUMENTO

A modo de referencia y seguimiento, se identifica formalmente la Política con el siguiente cuadro de características:

Nombre del documento	Política de Gestión de Documentos Electrónicos (PGDE) del Parlamento de Navarra
Versión	1.0
Identificador de la Política	Política_Gestión_Documento_Electrónico_v1.0
URI de referencia	https://sede.parlamentodenavarra.es/normativa
Fecha de aprobación	20 de diciembre de 2022
Ámbito de aplicación	Gestión de la documentación electrónica producida y conservada por el Parlamento de Navarra, afectando a la totalidad de su personal, tanto público como contratado, ya sea en grado de dependencia directa o a través de empresas externas mediante convenios o cualquier otra modalidad contractual.
Responsable de la Política y datos de contacto	Mikel Iriarte Cilveti, Jefe del Servicio de Publicaciones, Archivo, Biblioteca y Documentación. mikeli@nafarroakoparlamentua.eus Teléfono: 948 209 267 Asun Marzal Parras, Jefa del Servicio de Informática, Sistemas Audiovisuales y Tecnología. amarzal@parlamentodenavarra.es Teléfono: 948 209 234 Dirección: c / Navarrería 39, 31001, Pamplona / Iruña

4. PRINCIPIOS DE LA GESTIÓN DOCUMENTAL

La gestión del documento electrónico en el Parlamento de Navarra se rige por los siguientes principios:

• Los documentos y expedientes administrativos y parlamentarios producidos en el entorno del Parlamento se crearán en base a expedientes electrónicos.

• Los documentos recibidos en soporte papel de fuentes externas al Parlamento que se tengan que incorporar en un expediente electrónico se digitalizarán de forma segura para su incorporación en soporte electrónico.

• Todos los documentos de carácter administrativo o parlamentario pertenecerán a un expediente. Los expedientes se organizarán, desde su fase de tramitación, en base a su procedimiento bajo una serie definida en el Cuadro de Clasificación y serán identificados mediante un código único.

• La conservación, transferencia y eliminación de documentos y expedientes se rige por la aplicación sistemática de las Tablas de Valoración Documental establecidas por el órgano competente conforme a la normativa de evaluación documental.

• Desde el punto de vista tecnológico, el Parlamento dispone una plataforma de gestión documental en la que se gestionan tanto los documen-

tos asociados a la actividad administrativa como a la parlamentaria en fase de tramitación, independientemente de las herramientas utilizadas en su tramitación. Una vez cerrados, se mantendrán en el mismo gestor hasta su transferencia a la herramienta de archivo electrónico único, según las necesidades del Parlamento de Navarra.

• Asimismo, el Parlamento dispone de una herramienta de archivo electrónico único en la que se realiza la valoración de los expedientes administrativos y parlamentarios y se conservan a largo plazo según corresponda.

• El acceso a la documentación se rige por los siguientes principios:

✓ La consulta de expedientes por parte del personal al servicio del Parlamento se rige por lo establecido en el MGEDE.

✓ La ciudadanía tiene acceso a los expedientes correspondientes en fase de tramitación según lo que determina la legislación de procedimiento administrativo o de transparencia, según corresponda. Para acceder a ellos se hará uso de la Carpeta Ciudadana.

✓ La consulta de los expedientes electrónicos cerrados se rige por la Ley Foral de Archivos y Documentos.

5. ACTORES INVOLUCRADOS Y RESPONSABILIDADES

La implantación de la administración electrónica en el Parlamento de Navarra se ha venido desarrollando a partir de las decisiones tomadas por un grupo de trabajo pluridisciplinar en el que han estado presentes los distintos ámbitos que requiere un proyecto de esta envergadura: jurídico, organizativo, archivo y tecnológico.

La implicación ha sido tanto a nivel de la alta dirección como de los responsables y sus equipos de cada uno de estos ámbitos.

Para la aplicación sistemática de la Política también se requiere la cooperación de los diferentes ámbitos y niveles de toma de decisión dentro del organigrama del Parlamento.

A continuación, se detallan los actores involucrados y sus responsabilidades:

• **Secretaría General**. Es la encargada de impulsar y dotar de los recursos humanos y materiales necesarios para el cumplimiento de la Política.

• **Comisión de Administración Electrónica**, liderada por la Letrada Mayor y formada por personas con capacidad de decisión y liderazgo dentro de los ámbitos normativo, organizativo, tecnológico y archivístico. Debe encargarse de la adopción de lo establecido en la Política sobre todos los procedimientos del Parlamento y de identificar posibles necesidades de ampliación o de actualización.

• **Archivo**. Es el responsable de ejecutar las decisiones tomadas por la Comisión de Administración Electrónica en el ámbito de la gestión documental y archivo. Concretamente, es el responsable de:

✓ Desarrollar y mantener los procesos e instrumentos de gestión documental definidos en la Política y gestionar la documentación electrónica una vez finalizada su fase de tramitación.

✓ Desarrollar y mantener los capítulos del MGEDE referentes al Ciclo de vida y el Modelo de preservación del documento electrónico.

✓ Verificar que las decisiones adoptadas en el ámbito de la gestión documental se aplican sobre todos los expedientes y documentos electrónicos producidos por el Parlamento.

• **Responsable de Informática y Tecnología**. Es el responsable de garantizar que las infraestructuras tecnológicas del sistema de gestión documental se implementan de acuerdo con la presente Política y los capítulos que conforman el MGEDE. Asimismo, es el responsable de proporcionar el correcto nivel de servicio de las infraestructuras tecnológicas del sistema de gestión documental.

Asimismo, es el responsable de garantizar la seguridad de las infraestructuras tecnológicas del sistema de gestión documental y de la definición y aplicación de los requisitos establecidos por el Esquema Nacional de Seguridad (ENS).

También es responsable de desarrollar y mantener los siguientes capítulos del MGEDE: Modelo de digitalización segura, Modelo de impresión segura, Política de firma electrónica y de certificados digitales, Modelo de seguridad y acceso y Modelo tecnológico.

• **Servicio Jurídico**. Es el responsable de garantizar que la implementación del documento y expediente electrónico se hace de acuerdo con las leyes y normas vigentes en todo momento. Asimismo, es el encargado de dar la información normativa necesaria tanto al ámbito de Archivo como al ámbito Tecnológico para que puedan mantener la Política y el MGEDE actualizados de acuerdo con la normativa vigente.

• **Organización**. Es el responsable de dar cumplimiento al plan de gestión del cambio para la implantación de la documentación electrónica. Asimismo, es el responsable de definir, junto con la Comisión de Administración Electrónica y con Archivo, las actuaciones a realizar para comunicar la implementación de la documentación electrónica como soporte principal de la gestión documental del Parlamento.

• **Responsables de procedimientos**. Participan en las labores de reingeniería para la digitalización de los procedimientos al objeto de una correcta implementación de la Política y del MGEDE, así como en la definición de los criterios para crear, acceder y cerrar los expedientes generados en el marco de estos procedimientos.

• **Todo el personal de cualquier nivel** implicado en tareas de gestión de documentación electrónica. Debe aplicar las directrices establecidas por la Política y por el MGEDE en todas las acciones y trámites cotidianos que realizan y, especialmente, mantener los documentos y los expedientes de forma adecuada y completos para prestar un servicio óptimo a la ciudadanía y dar cumplimiento a la obligación de dar cuentas de la actuación del Parlamento de Navarra.

6. ELEMENTOS DE LA GESTIÓN DEL DOCUMENTO ELECTRÓNICO

6.1 MODELO DE GESTIÓN DE EXPEDIENTES Y DOCUMENTOS ELECTRÓNICOS (MGEDE)

El MGEDE desarrolla en detalle las bases estratégicas y organizativas para el establecimiento de los criterios homogéneos que marca la Política en el uso, la gestión y la conservación de los documentos electrónicos.

Este desarrollo se lleva a cabo a través de la definición del ciclo de vida del documento electrónico, de los procesos que intervienen en la gestión documental y de los instrumentos y controles de gestión documental. Además, determinados aspectos clave de la gestión de la documentación electrónica y el desarrollo de los procesos de gestión documental se delimitan y desarrollan en profundidad a través de sus capítulos, que se detallan en el apartado 7.

6.1.1 Ciclo de vida del documento electrónico

La gestión del documento electrónico en el Parlamento de Navarra contempla el tratamiento de los expedientes de manera homogénea a través de las fases que componen su ciclo de vida, estructuradas de la manera siguiente:

1. Fase de tramitación
2. Fase de vigencia
3. Fase histórica

Fase de tramitación

La fase de tramitación se inicia con la apertura del expediente y abarca toda su vida mientras el procedimiento al que hace referencia se encuentra en fase de tramitación. En esta fase se incorporan de forma progresiva los documentos al expediente almacenado en el gestor documental, de modo que se documenta en el mismo toda la actividad de la que es testimonio.

En la incorporación de documentos al expediente se aplican procesos de registro, de captura, de clasificación y de descripción, que se explican con más detalle en el apartado 6.1.2.

Una vez finalizada la fase de tramitación del procedimiento, la unidad responsable realiza el cierre del expediente tras el foliado del mismo, lo que comporta los correspondientes cambios de responsabilidad en cuanto a su gestión hacia el Archivo del Parlamento.

Fase de vigencia

La fase de vigencia se inicia con el cierre del expediente en el gestor documental y dura tanto tiempo como perviva su vigencia administrativa. A partir de este momento su gestión corresponde a Archivo.

En esta fase prima garantizar la disponibilidad del expediente para su uso y el mantenimiento de la información de contexto a través de los metadatos, para lo que es imprescindible definir y aplicar correctamente unas políticas de acceso y uso.

En función de las necesidades del Parlamento y de las Tablas de Valoración Documental aplicables, los expedientes entrarán en un proceso de transferencia física hacia la herramienta de archivo electrónico único, donde se procederá a la preparación de los documentos que han perdido completamente su valor y utilidad administrativa para su eliminación, siempre que no tengan un valor histórico o informativo a largo plazo que justifique su conservación permanente. La determinación de este valor, así como de los plazos de acceso, es competencia de la Comisión de Evaluación Documental. El proceso de evaluación se detalla en el apartado 6.1.2.

Fase histórica

En la fase histórica del ciclo de vida, la principal prioridad es garantizar la autenticidad, fiabilidad, integridad y disponibilidad de aquellos docu-

mentos y expedientes destinados a su conservación permanente. La responsabilidad en esta etapa recae también en Archivo.

Los procedimientos aplicables para mantener el carácter fehaciente de los documentos y expedientes electrónicos se desarrollan con detalle en el Modelo de preservación del MGEDE, explicado con más detalle en el apartado 7.

6.1.2 Procesos de gestión documental

A lo largo de las fases descritas en el apartado anterior tienen lugar un conjunto de procesos de gestión documental. Estos procesos se concretan en unos instrumentos de gestión documental y en los capítulos que se describen en los apartados 6.1.3 y 7, respectivamente.

• **Captura**. Consiste en incorporar un documento al sistema de gestión documental, de acuerdo con las siguientes reglas:

✓ Los documentos que se generan bajo el control del Parlamento lo hacen en soporte electrónico.

✓ Los documentos que provienen de fuentes externas al Parlamento en soporte papel se digitalizan de manera segura o certificada en el momento en el que sea posible, previamente a su incorporación al expediente.

✓ Los documentos capturados se asignan siempre a un expediente.

• **Registro**. Los documentos que proceden de fuentes externas al Parlamento se registran en un registro único de acuerdo con lo establecido en la legislación.

• **Clasificación**. Los expedientes se clasifican de acuerdo con su función encuadrados en la correspondiente serie documental identificada en el Cuadro de Clasificación, instrumento al que se hace referencia en el apartado 6.1.3. En el contexto de cada serie documental, todos los expedientes se ordenan mediante una referencia única que los identifica de manera unívoca y que se atribuye en el momento de su creación.

• **Descripción**. La descripción de los documentos y expedientes electrónicos se hace de acuerdo con el Vocabulario de Metadatos, instrumento al que se hace referencia en el apartado 6.1.3.

• **Acceso**. Para gestionar los derechos de acceso a la documentación, se realiza un análisis detallado de cada serie documental y se define tanto la valoración de seguridad de la documentación asociada a dicha serie como los grupos y los perfiles de usuarios que deben tener acceso a ella en cada una de las etapas del ciclo de vida de la documentación, según lo establecido en el Modelo de acceso y seguridad del MGEDE, descrito en el apartado 7.

• **Foliado**. Al cierre del expediente se aplica un procedimiento de foliado que genera un documento adicional de índice del expediente con la lista de todos los documentos contenidos en el mismo, incluyendo mecanismos que permiten validar su integridad y garantizar el proceso de conservación posterior. Este documento de índice del expediente se firma de manera automática y sirve como evidencia de la autenticidad e integridad del expediente.

• **Evaluación**. Para cada serie documental de las identificadas en el Cuadro de Clasificación se aplica un proceso de evaluación documental que permite determinar, sobre la base de unos criterios de valoración bien definidos, qué documentación puede ser eliminada o debe ser conservada en los plazos temporales que se establezcan. Este proceso de análisis se fundamenta en las Tablas de Valoración Documental y en el Calendario de Conservación y Acceso, instrumentos identificados en el apartado 6.1.3.

• **Conservación**. En función del resultado de la evaluación documental se aplican al expediente las políticas que se describen en el Modelo de preservación del documento electrónico del MGEDE, al que se remite en el apartado 7.

• **Transferencia**. La transferencia es el procedimiento por el que se traslada tanto la ubicación lógica como la responsabilidad sobre la documentación de la unidad responsable de su tramitación al Archivo.

• **Eliminación**. La eliminación constituye un proceso clave en la gestión de documentos. Su objetivo es impedir la recuperación o restauración y la posterior reutilización de documentos. Para ello, es necesario aplicar un proceso que incluya el borrado de la información y la destrucción física del soporte, en función de las características del formato y de las del propio soporte.

La eliminación de documentos está sujeta a la aplicación de las Tablas de Valoración Documental tras el dictamen y aprobación por parte del órgano competente.

6.1.3 Instrumentos y controles de gestión documental

La aplicación de los procesos de gestión documental tiene como consecuencia la obtención de un conjunto de instrumentos y controles básicos

para la gestión archivística, aplicables en la gestión de la documentación electrónica y, algunos, aplicables también en la documentación física. En el marco del Parlamento se concretan en los siguientes:

• **Cuadro de Clasificación**. Este instrumento muestra la organización en series documentales de los expedientes de acuerdo con su función para el conjunto del Parlamento. Su desarrollo y mantenimiento corresponde al responsable del Archivo en coordinación con los responsables funcionales de cada serie documental o proceso.

• Vocabulario de Metadatos. Este instrumento define la forma de denominar y describir expedientes, documentos y firmas electrónicas, normalizando su descripción mediante un conjunto de metadatos estructurados. El responsable del Archivo es el encargado de su desarrollo y mantenimiento, en coordinación con el responsable de Informática y Tecnología.

• **Tablas de Valoración Documental y Calendario de Conservación y Acceso**. Las Tablas de Valoración Documental señalan para cada serie documental los plazos de accesibilidad y conservación de la documentación, indicando qué documentos se tienen que conservar permanentemente y cuáles se tienen que eliminar, en función de la aplicación de un conjunto de criterios de evaluación de documentos. El Calendario de Conservación y Acceso recoge la decisión en cuanto a los períodos de conservación, la decisión de disposición para todas las series documentales y los plazos de accesibilidad. El responsable del Archivo es el encargado del desarrollo y mantenimiento de ambos instrumentos.

• **Registro de eliminación**. Constituye un instrumento esencial para documentar los procesos de eliminación de expedientes, como consecuencia de la aplicación de las Tablas de Valoración Documental.

• **Catálogo de Tipologías documentales**. Identifica las tipologías de documentos que, desde un punto de vista funcional, constituyen los expedientes del Parlamento mediante un sistema que simplifica su creación, facilita su diferenciación y mantenimiento y permite la automatización de la atribución de valores de metadatos en base a la combinación de tipologías documentales y los procesos que generan los expedientes, así como el control de la completitud documental de los expedientes. El responsable del Archivo es el encargado del desarrollo y mantenimiento de este instrumento.

• **Catálogo de Formatos documentales**. Identifica los formatos electrónicos admitidos por el Parlamento en cumplimiento de la NTI sobre el Catálogo de Estándares. El responsable de Archivo es el encargado de su desarrollo y mantenimiento, en coordinación con el responsable de Informática y Tecnología, teniendo siempre en cuenta la posible obsolescencia futura y las necesidades de migración de formatos.

• **Catálogo de documentos esenciales**. Identifica los documentos que resultan indispensables y vitales para que el Parlamento pueda alcanzar sus objetivos, cumplir con sus obligaciones y servicios y respetar la legalidad vigente y los derechos de las personas. El responsable de Archivo es el encargado de su desarrollo y mantenimiento.

6.2 FIRMA ELECTRÓNICA

El Parlamento de Navarra gestiona documentos producidos y firmados electrónicamente tanto por parte de la ciudadanía como de los empleados públicos, así como los que proceden de la actuación administrativa automatizada.

El marco de referencia para el uso de las herramientas de firma electrónica es la Política de Firma electrónica y de Certificados digitales, que sirve de apoyo a la estrategia del Parlamento de utilizar el documento y el expediente electrónico como elementos base sobre los que proporcionar evidencia de la debida ejecución de sus procesos de gestión.

Las firmas electrónicas procedentes de la ciudadanía que admite el Parlamento serán las generadas a través de los siguientes mecanismos previstos por la Ley 39/2015 de Procedimiento Administrativo Común:

• **Firma electrónica basada en el uso de certificado digital.** La ciudadanía, en su relación telemática con el Parlamento, puede usar certificados digitales para firmar documentos electrónicos. Los certificados digitales aceptados son los que se encuentran incluidos en la Lista de confianza de prestadores de servicios de certificación (TSL), publicada en la sede electrónica del Ministerio de Energía, Turismo y Agenda Digital.

• **Firma electrónica basada en la identificación más las evidencias de la voluntad de firma**. Se pueden usar los sistemas de identificación admitidos por la plataforma @firma, del Ministerio de Asuntos Económicos y Transformación Digital.

• **Firma con CSV**. Se puede usar como sistema de firma por actuación administrativa automa-

tizada y solo para documentos que vayan dirigidos a la ciudadanía, empresas u otras administraciones.

• **Firma biométrica**. Consiste en la captación de las evidencias biométricas del firmante y del contexto de la firma (hash del documento, momento de la firma, lugar, etc.) a través de un dispositivo especializado.

6.3 DESCRIPCIÓN Y ASOCIACIÓN DE METADATOS

El Parlamento dispone de un Vocabulario de Metadatos con diferentes elementos descriptivos basado en el Esquema Nacional de Interoperabilidad, explicado con mayor detalle en el apartado 7.

El Vocabulario de Metadatos se aplica sobre expedientes, documentos y firmas electrónicas, permitiendo al Parlamento su identificación, localización y gestión.

Los sistemas informáticos que participan en la tramitación se ocupan de automatizar en la medida de lo posible la carga del valor de los metadatos. Aquellos valores que no han podido ser automatizados se informan manualmente por parte de los responsables de la tramitación en el momento de la creación del expediente, en la captura del documento o en la realización de la firma electrónica.

Sólo en casos excepcionales se permite informar el valor de determinados metadatos al finalizar la tramitación, y siempre con carácter previo al cierre del expediente.

Una vez cerrado el expediente, sólo se actualiza de forma automatizada el valor de aquellos metadatos que sufren cambios como consecuencia de la aplicación de los procesos de conservación documental.

7. DESARROLLO DE LA POLÍTICA

La Política se implementa mediante el MGEDE definido en el punto 6.1 y los capítulos que lo componen, que establecen directrices concretas. A continuación, se identifica cada uno de estos capítulos, así como el responsable de su desarrollo y actualización:

• **Ciclo de vida**. Define cómo se debe gestionar el ciclo de vida de los documentos y expedientes tanto físicos como electrónicos desde su producción o recepción hasta su disposición o conservación como un continuo. Archivo es el encargado de su desarrollo y mantenimiento.

• **Modelo organizativo**. Identifica a los participantes en la elaboración del MGEDE, así como sus responsabilidades y competencias al respecto. Asimismo, aborda cómo afrontar la gestión del cambio en la organización, cómo realizar la reingeniería y simplificación de procedimientos, cómo ofrecer y recibir servicios relacionados con la interoperabilidad y la posibilidad de hacer uso de la actuación administrativa automatizada. Organización es el encargado de su desarrollo y mantenimiento.

• **Modelo tecnológico**. Describe la estructura y el formato de los objetos electrónicos a los que se refiere la Política (expedientes, documentos y firmas electrónicas) y cómo las plataformas tecnológicas del Parlamento implementan sus directrices. El responsable de Informática y Tecnología es el encargado de su desarrollo y mantenimiento.

• **Modelo de digitalización segura**. Describe el procedimiento y las herramientas a utilizar para la generación de copias electrónicas auténticas de documentos en soporte papel, definiendo el formato del documento resultante, los metadatos a incorporar y los mecanismos de seguridad exigidos. El responsable de Informática y Tecnología es el encargado de su desarrollo y mantenimiento, en colaboración con Archivo.

• **Modelo de impresión segura**. Describe el procedimiento para la generación y emisión y verificación de copias auténticas en papel de documentos originales electrónicos. El responsable de Informática y Tecnología es el encargado de su desarrollo y mantenimiento.

• **Modelo de preservación del documento electrónico**. Describe la estrategia del Parlamento para garantizar la integridad, autenticidad, disponibilidad, trazabilidad e interoperabilidad de los documentos electrónicos a largo plazo, estableciendo mecanismos para superar la obsolescencia tecnológica y criptográfica de los documentos y de las firmas electrónicas. Archivo es el encargado de su desarrollo y mantenimiento.

• **Modelo de seguridad y acceso**. Establece el modelo de roles y permisos a aplicar en el acceso, la consulta, la modificación y la eliminación de la documentación electrónica mediante la asignación de las personas a grupos de usuarios en relación con sus funciones en la organización. Establece también los mecanismos de monitorización y copia de seguridad que garantizan la disponibilidad del sistema de gestión documental. El responsable de Informática y Tecnología es el encargado de su desarrollo y mantenimiento, en colaboración con Archivo, teniendo en cuenta lo

establecido por el estándar ISO 27001 y el Esquema Nacional de Seguridad (ENS).

• **Casos de uso**. Describe algunos casos concretos que pretenden facilitar la comprensión del MGEDE, teniendo en cuenta todo el ciclo de vida documental dentro de los procedimientos establecidos.

• **Política de firma electrónica y de certificados digitales**. Define el uso de la firma electrónica: qué certificados electrónicos u otros mecanismos de identificación y firma electrónica se usan y admiten y qué formatos tecnológicos y procedimientos se aplican en la generación, validación y preservación de las firmas electrónicas. El responsable de Informática y Tecnología es el encargado de su desarrollo y mantenimiento.

La suma de todos estos capítulos completa el MGEDE del Parlamento de Navarra, hallándose implementados en los sistemas de información y procesos de gestión documental disponibles y difundidos internamente para su aplicación efectiva por parte de todo el personal de la organización.

8. PLAN DE FORMACIÓN

El Plan de formación del Parlamento de Navarra incorpora previsiones de formación continuada para el personal que participa en la generación y en la gestión de la documentación electrónica. Todos los responsables identificados en el apartado 5 tienen acceso a formación específica en este ámbito.

9. SUPERVISIÓN Y AUDITORÍA

La correcta aplicación de esta Política está sujeta a procedimientos periódicos de auditoría que verifican su cumplimiento y la correcta implementación de los instrumentos y capítulos a los que se hace referencia en los apartados 6.1.3 y 7.

10. GESTIÓN DE LA POLÍTICA

La aplicación, el mantenimiento y la actualización de la Política corresponde, de acuerdo con las responsabilidades definidas en el apartado 5, a la Comisión de Administración Electrónica.

ANEXO I - CONCEPTOS BÁSICOS

A continuación, se identifican y definen los principales conceptos básicos que se tratan en la Política con el objetivo de consensuar un lenguaje unívoco que permita a todos los implicados en el proyecto trabajar de manera coherente y consensuada.

Estos conceptos se recogen y definen en las diferentes guías de aplicación de la NTI y en las 11 guías de aplicación de la Política de gestión de documentos electrónicos publicadas por los Ministerios de Hacienda y de Política Territorial y Función Pública.

• **@firma**. Plataforma de firma electrónica del Ministerio de Hacienda y Función Pública.

• **Acceso**. Derecho a la consulta de la información pública, de acuerdo con la normativa vigente, así como el procedimiento para llevar a cabo dicha consulta, tanto por parte del interesado en un procedimiento administrativo como por los responsables del sistema, los responsables de la gestión y conservación de los documentos y el conjunto de los ciudadanos.

• **Actuación administrativa automatizada**. Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular.

• **Archivo Electrónico Único**. Sistema que permite almacenar por medios electrónicos todos los documentos utilizados en las actuaciones administrativas de una organización correspondientes a procedimientos finalizados. Permite la conservación de los documentos electrónicos garantizando su autenticidad, integridad y conservación a largo plazo, así como su consulta con independencia del tiempo transcurrido desde su producción.

• **Autenticidad**. Referido a un documento, propiedad que puede atribuírsele como consecuencia de que puede probarse que es lo que afirma ser, que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado, y que ha sido creado o enviado en el momento en que se afirma, sin que haya sufrido ningún tipo de modificación.

• **Captura**. Proceso de gestión de documentos que señala la incorporación de un documento a un sistema de gestión de documentos. En el momento de captura se crea la relación entre el documento, su productor y el contexto en que se originó, que se mantiene a lo largo de su ciclo de vida.

• **Certificado electrónico**. Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, documento 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 de sello electrónico**. Declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona.

• **Ciclo de vida del documento electrónico**. Conjunto de las etapas o fases que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos hasta su selección para conservación permanente de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su eliminación reglamentaria.

• **Clasificación**. Proceso destinado a organizar los documentos y a su codificación de acuerdo con las categorías o clases contempladas en el Cuadro de Clasificación de la organización permitiendo que sean gestionados dentro de un sistema de gestión de documentos.

• **Código seguro de verificación (CSV)**. Código único que vincula un documento electrónico al órgano u organismo responsable y, en su caso, a la persona firmante del documento. Sirve para la comprobación de la integridad del documento mediante un servicio de cotejo que se ofrece desde la sede electrónica correspondiente.

• **Conservación**. Conjunto de procesos y operaciones dedicados a asegurar la permanencia intelectual y técnica de los documentos a lo largo del tiempo.

• **Copia auténtica**. Documento expedido por un órgano con competencias atribuidas para ello, y con un valor probatorio pleno sobre los hechos o actos que documente, equivalente al documento original.

• **Cuadro de clasificación**. Estructura de categorías funcionales organizadas de manera codificada, jerárquica y lógica, comprehensiva de todas las actividades desarrolladas por la organización en el cumplimiento de sus fines.

• **Dato**. Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para su comunicación, interpretación o procesamiento por medios automáticos o humanos.

• **Descripción**. Proceso de gestión de documentos o recursos de información por el que se

recogen datos significativos de los mismos, con el fin de que estos puedan gestionarse y recuperarse de manera ágil, pertinente y exhaustiva. Incluye la elaboración de estructuras de lenguaje controlado, como tesauros, e índices, como auxiliares del proceso de clasificación de los documentos. En el ámbito electrónico, la descripción se asimila a la asignación de metadatos.

• **Digitalización segura/certificada**. Proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

• **Disponibilidad**. Referido a un documento, indica la propiedad o característica de este, que permite que éste pueda ser localizado, recuperado, presentado o interpretado. El documento debe señalar la actividad o actuación donde se generó, proporcionar la información necesaria para la comprensión de las actuaciones que motivaron su creación y utilización, identificar el contexto marco de las actividades y las funciones de la organización y mantener los vínculos existentes con otros documentos como reflejo de una secuencia de actuaciones.

• **Documento**. Información de cualquier naturaleza archivada en un soporte y susceptible de identificación y tratamiento diferenciado.

• **Documento electrónico**. Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. / Todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.

• **Documento esencial**. Documento para el que, en el marco de un proceso de evaluación, se ha determinado un proceso especial de duplicación, como una garantía frente a los riesgos que correría una organización en caso de que dicho documento no estuviera disponible.

• **Vocabulario de metadatos**. Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos o recursos de información reutilizable a lo largo de su ciclo de vida.

• **Expediente**. Se entiende por expediente el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa o parlamentaria, así como las diligencias encaminadas a ejecutarla.

• **Expediente electrónico**. Conjunto de documentos electrónicos correspondientes a un procedimiento administrativo o parlamentario, cualquiera que sea el tipo de información que contengan.

• **Evaluación**. Proceso de gestión de documentos que tiene como finalidad juzgar los valores de los documentos, estableciendo plazos de conservación y determinando su accesibilidad, decisión sobre su destino al final de su ciclo de vida y eventual calificación como documento esencial de una organización.

• **Fiabilidad**. Referido a un documento, propiedad o característica que indica que su contenido puede ser considerado una representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades.

• **Firma electrónica**. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. / Datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

• **Foliado**. Proceso de gestión del expediente electrónico mediante el que se incluye en el índice electrónico del mismo la concatenación ordenada de las referencias a los documentos que lo integran y las huellas digitales de dichos documentos, finalizando el proceso con la firma electrónica del índice.

• **Formato**. Conjunto de reglas que definen la manera correcta de intercambiar o almacenar datos en memoria.

• **Gestión de documentos**. Conjunto de operaciones dirigidas al control eficaz y sistemático de la creación, recepción, uso, valoración y conservación de los documentos, incluidos los procesos para incorporar y mantener pruebas de las actuaciones o actividades de dicha organización, en forma de documentos y sistemas de información.

• **Gestor documental**. Sistema que permite controlar y gestionar de forma sistemática la creación, la recepción y el uso de los documentos y expedientes electrónicos pertenecientes a procedimientos no finalizados.

• **Hash / Huella digital**. Secuencia de valores resultado de la aplicación de una función hash a un documento electrónico.

• **Identidad**. Conjunto de características de un documento que lo identifican de manera única y lo distinguen de cualquier otro documento. Junto con la integridad, es un componente de la autenticidad.

• **Índice electrónico**. Documento electrónico que incluye la relación de documentos electrónicos de un expediente electrónico, firmado por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

• **Integridad**. Referido a un documento, propiedad o característica que indica su carácter de completo, sin alteración de ningún aspecto esencial. La integridad es un componente de la autenticidad junto a la identidad.

• **Interoperabilidad**. Capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

• **Lista de servicios de confianza (TSL)**. Lista, de acceso público, que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones Públicas españolas y europeas.

• **Sello de tiempo**. La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

• **Metadato**. Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

• **Original**. Referido a un documento, que posee las cualidades de genuino y eficaz (que produce efectos), que se remonta directamente a su autor y que no ha sido copiado ni imitado de otro.

• **Política de firma electrónica**. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

• **Política de gestión de documentos electrónicos**. Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

• **Registro**. Proceso de gestión de documentos paralelo al de la captura, establecido como un requisito legal, definido en la legislación de procedimiento administrativo como dotado de fe pública, que marca la incorporación de un documento al sistema de gestión de documentos de una Administración pública, mediante la adjudicación de un identificador único en el momento de su entrada en el sistema.

• **Sede electrónica**. A efectos de interoperabilidad, aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones de la que es titular una Administración Pública, órgano o entidad administrativa.

• **Sello electrónico**. Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

• **Sistema de gestión documental**. Sistema diseñado para almacenar, administrar y controlar el flujo de los documentos dentro de una organización.

• **Soporte**. Objeto sobre el que es posible grabar y recuperar datos.

• **Tipo documental**. Modelo estructurado y reconocido que adopta un documento, en el desarrollo de una competencia concreta, en base a una Regulación y cuyo formato, contenido informativo o soporte son homogéneos.

• **Trazabilidad**. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. En el ámbito de la gestión de documentos, proceso que facilita el seguimiento de la creación, incorporación, movimiento, uso y eventual modificación de los documentos dentro de un sistema de gestión de documentos.

• **Validación**. Proceso de verificar y confirmar la validez de una firma o sello electrónicos.

ANEXO II - REFERENCIAS

1. Legislación y normativa

• Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

• Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

• Ley Foral 11/2019, de 11 de marzo, de la Administración de la Comunidad Foral de Navarra y del Sector Público Institucional Foral.

• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

• Ley 39/2015 de 1 de octubre, de Procedimiento Administrativo Común de las administraciones Públicas.

• Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Publico.

• Decreto Foral 30/2015, de 20 de mayo, por el que se regula la digitalización de documentos la copia y conversión de documentos electrónicos en el ámbito de la Administración de la Comunidad Foral de Navarra y sus Organismos Públicos.

• Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).

• Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

• La Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno.

• Ley Foral 12/2019, de 22 de mayo, de Participación Democrática en Navarra.

• Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

• Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

• Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos.

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

2. Normas Técnicas de Interoperabilidad

• Resolución de 27 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.

• Resolución de 19 de febrero de 2013, por la que se aprueba la Norma Técnica de Interoperabilidad de Reutilización de recursos de información.

• Resolución de 3 de octubre de 2012, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares.

• Resolución de 28 de junio de 2012, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

• Resolución de 28 de junio de 2012, por la que se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos.

• Resolución de 28 de junio de 2012, por la que se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos.

• Resolución de 19 de julio de 2011 por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

• Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos.

• Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.

• Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.

• Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las entidades registrales.

• Resolución de 19 de julio de 2011, por la que se aprueba la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

3. Guías técnicas

• Guías de aplicación de la Política de gestión de documentos electrónicos (2019).

• Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la administración (2ª ed.) (2017).

• Guía de aplicación de la Norma Técnica de Interoperabilidad de Reutilización de recursos de información (2ª ed.) (2016).

• Perfiles de certificados electrónicos (2016).

• Guía de aplicación de la NTI de Política de gestión de documentos electrónicos (2ª ed.) (2016).

• Guía de aplicación de la NTI de documento electrónico (2ª ed.) (2016).

• Guía de aplicación de la NTI de Expediente electrónico (2ª ed.) (2016).

• Guía de aplicación de la NTI de Digitalización de documentos (2ª ed.) (2016).

• Guía de aplicación de la NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos (2ª ed.) (2016).

• Guía de aplicación de la NTI de Relación de modelos de datos (2ª ed.) (2014).

• Guía de aplicación de la NTI de Modelo de datos para el intercambio de asientos entre las entidades registrales: Sicres 3.0 (2ª ed.) (2013).

• Guía de aplicación de la NTI de Catálogo de estándares (2012).

• Guía de aplicación de la NTI de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas (2011).

4. Otras referencias

• MoReq2010 (Modular Requirements for Records Systems): Proporciona a la industria un conjunto de requisitos que debe cumplir un sistema de software para la gestión de documentos de archivo electrónicos aplicable a diferentes sectores.

• ISO 15489-1: Define las características de los documentos electrónicos fehacientes, regula la implementación de los sistemas que garantizan su mantenimiento e identifica los procesos e instrumentos de gestión de documentos.

• ISO 30300, 30301 y 30302: Conjunto de normas que definen los principios y las políticas de un sistema de gestión para documentos y la medición de su conformidad de acuerdo con procesos de auditoría y certificación, basadas en la importancia estratégica de la información en las organizaciones.

• ISO 14721 (OAIS Open Archival Information System): Proporciona un modelo de referencia para un sistema de información archivística abierto en el contexto de sistemas de transferencia de datos e información espacial. Define el funcionamiento y los requisitos de un archivo digital. Aborda una amplia gama de funciones incluyendo la ingesta, almacenamiento de archivos, gestión de datos, acceso y difusión.

• ISO/TR 13028: Directrices para la implementación de la digitalización de documentos.

• ISO 23081-1, ISO 23081-2 y ISO/TR 23081-3: Conjunto de normas pensadas para comprender, implementar y usar metadatos en un contexto de gestión de documentos electrónicos.

• ISO 16175-1, ISO 16175-2 y ISO 16175-3: Incide en los principios y requisitos funcionales para documentos en entornos electrónicos de oficina.

• ISO/TR 26122: Proporciona orientación sobre el análisis de los procesos de trabajo desde la perspectiva de la creación, captura y control de los documentos.

• ISO 13008: Guía para la conversión de formatos de documentos electrónicos y para la migración.

• ISO/TR 15801: Establece recomendaciones para la veracidad y fiabilidad de la información, con el fin de asegurar la autenticidad de los documentos y, en consecuencia, garantizar su admisibilidad legal.

• ISO/TR 18492: Incide en las estrategias de conservación y recuperación de la información de manera fidedigna frente a los riesgos de obsolescencia.

• ISO 14641: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital.

• PREMIS Preservation Metadata Implementation Strategies: estándar de metadatos de preservación.

• ISAD(G): Norma Internacional General de Descripción Archivística basada en la entidad documento.

• ISAAR (CPF): Norma Internacional sobre los registros de autoridad de archivos relativos a instituciones, personas y familias.

• ISDF: Norma archivística internacional para la descripción de funciones.

• EAD: Norma de Descripción Archivística Codificada.

• NEDA: Normas Españolas de Descripción Archivística, realizadas mediante la técnica de modelado de datos entidad-relación, que identifica tanto los tipos de entidad (fijados en documentos de archivo; agente; función y sus divisiones; norma; concepto, objeto o acontecimiento; lugar), las relaciones entre entidades y los atributos.

• AGRKMS Australian Government Recordkeeping Metadata Standard (2008). Directrices de aplicación del AGRKMS (2010)

• UN/CEFACT United Nations Centre for Trade Facilitation and Electronic Business - Business Requirements Specification.

5. Abreviaturas

• CSV (Código Seguro de Verificación).

• ENI (Esquema Nacional de Interoperabilidad).

• ENS (Esquema Nacional de Seguridad).

• MGEDE (Modelo de Gestión de Expedientes y Documentos Electrónicos).

• NTI (Norma Técnica de Interoperabilidad).

Resolución 3/2023, de 10 de enero, de la Letrada Mayor del Parlamento de Navarra, por la que se aprueba el documento "Política de identidad y firma electrónica en el Parlamento de Navarra"

La Mesa del Parlamento, en sesión de 9 de enero de 2023, se dio por enterada de la propuesta normativa "Política de identidad y firma electrónica en el Parlamento de Navarra", mostrando su conformidad con la misma.

Por lo expuesto, y de conformidad con lo dispuesto en el artículo 37 del Reglamento del Parlamento de Navarra,

RESUELVO:

1.º Aprobar el documento "Política de identidad y firma electrónica en el Parlamento de Navarra", que se adjunta a la presente Resolución y que entrará en vigor cuando la Mesa de la Cámara lo determine, conforme a la implantación de la administración electrónica.

2.º Ordenar la publicación de la presente Resolución en el Boletín Oficial del Parlamento de Navarra.

Pamplona, 10 de enero de 2023

La Letrada Mayor: Silvia Doménech Alegre

Política de identidad y firma electrónica en el Parlamento de Navarra

Se ordena la publicación en el Boletín Oficial del Parlamento de Navarra del documento "Política de identidad y firma electrónica en el Parlamento de Navarra", aprobado por Resolución de la Letrada Mayor n.º 3/2023, de 10 de enero de 2023.

Pamplona, 10 de enero de 2023

El Presidente: Unai Hualde Iglesias

Política de identidad y firma electrónicas del Parlamento de Navarra

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

2. NORMATIVA APLICABLE

2.1 Normativa de ámbito europeo

2.2 Normativa de ámbito estatal

2.3 Normativa foral

2.4 Normativa propia del Parlamento

2.5 Estándares internacionales y otras convenciones

3. DATOS DE LA POLÍTICA DE IDENTIDAD Y FIRMA ELECTRÓNICAS DEL PARLAMENTO DE NAVARRA

3.1 Identificación de la política

3.2 Períodos de validez y transición

3.3 Órgano responsable

4. IDENTIDAD ELECTRÓNICA EN EL PARLAMENTO

5. CERTIFICADOS DIGITALES

5.1 Certificados digitales empleados por el Parlamento

5.2 Certificados digitales admitidos por el Parlamento.

5.3 Certificados digitales del personal y miembros del Parlamento.

5.4 Supuestos autorizados para hacer uso de los certificados de vinculación con el Parlamento.

5.5 Procedimientos relacionados con el ciclo de vida de los certificados de vinculación con el Parlamento.

5.5.1 Obtención, renovación y revocación

5.5.2 Almacenamiento de los certificados

5.5.3 Mantenimiento del inventario de certificados en el Parlamento

6. SISTEMAS DE FIRMA ELECTRÓNICA

6.1 Firma electrónica mediante certificado digital personal (de persona física, de vinculación con el Parlamento o de representante)

6.2 Firma electrónica mediante sello electrónico para actuación administrativa automatizada

6.3 Firma electrónica basada en un código seguro de verificación para actuación administrativa automatizada

6.4 Firma electrónica utilizando la plataforma Cl@ve

6.5 Firma electrónica biométrica

6.6 Firma múltiple

6.7 Sello de tiempo

7. CASOS DE USO DE LA FIRMA ELECTRÓNICA

7.1 Firma electrónica de un documento elaborado por el Parlamento

7.2 Firma electrónica de documentos por parte de un tercero

7.3 Firma electrónica de contratos, convenios o acuerdos con otras partes:

7.4 Firma electrónica automatizada:

7.5 Firma electrónica para digitalización segura

7.6 Incorporación de documentos electrónicos firmados de fuentes externas

7.7 Identificación y firma de personas extranjeras

8. ESTRATEGIA DE PRESERVACIÓN DE DOCUMENTOS Y FIRMAS ELECTRÓNICAS

8.1 Resellado y preservación de firmas electrónicas en entornos propios

8.2 Copias electrónicas de documentos firmados digitalmente

9. MANTENIMIENTO DE LA POLÍTICA

9.1 Desarrollo de la Política de Firma Electrónica

Disposición transitoria primera. - Disposición de medios tecnológicos

Disposición transitoria segunda. - Actualización de sistemas

ANEXO I - GLOSARIO Y CONCEPTOS EN FIRMA ELECTRÓNICA

Glosario

Conceptos en firma electrónica

Definición jurídica de la firma electrónica

Fundamentos técnicos de la Firma electrónica

Especificaciones Técnicas de los formatos de firma electrónica

Firma electrónica con política de firma y con sello de tiempo

Firma electrónica de Archivo

Firma PAdES-LTV

Código seguro de verificación (CSV)

ANEXO II - CERTIFICADOS ELECTRÓNICOS PARA EL USO POR PARTE DEL PARLAMENTO Y SUS EMPLEADOS

ANEXO III - PROCEDIMIENTOS DE OBTENCIÓN Y REVOCACIÓN DE CERTIFICADOS

Certificado de vinculación con el Parlamento.

Certificado de representante en software

Certificado de sello electrónico

ANEXO IV - ESTÁNDARES INTERNACIONALES Y OTRAS CONVENCIONES

ANEXO V - COMPROBACIONES A LLEVAR A CABO PARA LA VALIDACIÓN DE FIRMAS DE TERCEROS

1. INTRODUCCIÓN Y OBJETO

El Parlamento de Navarra (en adelante el Parlamento) en su estrategia de implantación de la administración electrónica requiere dotarse de una política de identidad y firma electrónicas que regule, dentro de su ámbito de competencia, las directrices generales en relación a la seguridad, la organización y sus aspectos técnicos y legales, de conformidad con lo previsto en el Real Decreto 4/2010, de 8 de enero, por el que se desarrolla el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y la Resolución de 27 de octubre de 2016 que aprueba la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y certificados de la Administración.

En este contexto, la política de identidad y firma electrónicas (en adelante la Política) tiene por objeto establecer los tipos de certificados digitales y firmas electrónicas que el Parlamento acepta para su relación con terceros y cuáles van a usar sus empleados y miembros del Parlamento, tanto para su gestión como para la relación con el Gobierno de Navarra y resto de administraciones públicas. Se regula sus usos y procedimientos, su obtención, así como su almacenamiento y preservación a largo plazo para poder garantizar la autenticidad, integridad y conservación de los documentos firmados digitalmente en las aplicaciones corporativas del Parlamento.

La implantación de un modelo de firma electrónica requiere definir cuáles serán los certificados digitales admitidos, utilizados y para qué usos, así como su ciclo de vida.

Por otra parte, la evolución de la tecnología, pero sobre todo de la normativa, ha originado la aparición de otros sistemas que permiten la firma electrónica a través de mecanismos como son las claves concertadas y el código seguro de verificación. El Parlamento considera que es importante contemplar y regular su uso. Por ello, la Política regula por una parte la firma electrónica basada en claves concertadas, las cuales se fundamentarán por una parte en el usuario y contraseña del ciudadano y adicionalmente con el sistema que permitirá recoger las evidencias de voluntad de firma. Este sistema se contemplará a partir de la plataforma Cl@ve, con las identidades aceptadas por esta plataforma y sus evidencias de voluntad de firma proporcionadas por esta, como sistema de firma electrónica.

Por su parte, la firma a través de la generación del Código Seguro de Verificación o del sello electrónico se podrán emplear en la actuación administrativa automatizada de firma de determinados documentos.

Asimismo, esta Política también describe la firma digital biométrica, que se podrá utilizar para la firma de documentos electrónicos generados presencialmente ante un tercero.

En la Política se especifica cuáles son los tipos de firma a utilizar a la hora de firmar los documentos electrónicos generados y gestionados por el Parlamento, por lo que se incluye tanto una relación de formatos técnicos utilizados, como los tipos de firma generados o aceptados por el Parlamento.

Finalmente, se establecen las estrategias que el Parlamento implementará para la preservación a largo plazo de las firmas electrónicas.

Cabe señalar que en este documento se utilizan indistintamente los términos firma digital y firma electrónica, ya que corresponden al mismo concepto.

Para la elaboración de este documento se ha tenido en cuenta la normativa aplicable en la materia tanto supranacional como estatal, foral o propia. Especialmente, se destaca lo que el Esquema Nacional de Interoperabilidad establece y, muy concretamente, lo que se define en la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración, así como lo previsto en la del expediente electrónico con respecto a la firma electrónica de los expedientes. Por su parte, se han considerado como marco de elaboración de esta Política los estándares internacionales y otras convenciones en el ámbito de la firma electrónica.

El detalle de la normativa y estándares internacionales de referencia se puede encontrar en el Anexo IV.

2. NORMATIVA APLICABLE

En este apartado se recogerá la normativa de referencia para la aplicación de la Política.

La reciente revolución en el uso del documento electrónico es el resultado de la aparición de cambios normativos que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como en la Unión Europea o internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

El contenido presentado a continuación es la identificación del conjunto de normativas y estándares internacionales que se han tenido en cuenta para la definición de la Política.

La identificación de la normativa es útil para enmarcar la norma y para poder actualizar en función de que haya cambios en este contexto.

2.1 NORMATIVA DE ÁMBITO EUROPEO

• Reglamento Europeo (UE) 910/2014 del Parlamento Europeo y el Consejo, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior.

• Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público conforme a los artículos 27, apartado 5 y 37, apartado 5 del anterior Reglamento.

2.2 NORMATIVA DE ÁMBITO ESTATAL

• Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

• Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

• Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social.

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

• Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad.

• Real Decreto 4/2010, de 8 de enero, del Esquema Nacional de Interoperabilidad.

• Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación o funcionamiento del sector público por medios electrónicos.

• Resolución de 27 de octubre de 2016 de la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónico y de Certificados de la Administración.

• Resolución de 19 de julio de 2011 de la Norma Técnica de Interoperabilidad de Expediente Electrónico.

• Resolución de 19 de julio de 2011 de la Norma Técnica de Interoperabilidad de Documento Electrónico.

• Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, según la cual se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del estado y sus organismos públicos.

2.3 NORMATIVA FORAL

• Ley Foral 11/2019, de 11 de marzo, de la Administración de la Comunidad Foral de Navarra y del Sector Público Institucional Foral.

• Ley Foral 12/2019, de 22 de marzo, de Participación Democrática en Navarra.

• Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos.

2.4 NORMATIVA PROPIA DEL PARLAMENTO

• Reglamento de funcionamiento de la Administración Electrónica del Parlamento.

2.5 ESTÁNDARES INTERNACIONALES Y OTRAS CONVENCIONES

Se incluye en el Anexo IV una relación de todos los estándares internacionales que definen los diferentes formatos, tipos de firma y sello de tiempo y el resto de las tecnologías que se han utilizado para construir esta Política.

3. DATOS DE LA POLÍTICA DE IDENTIDAD Y FIRMA ELECTRÓNICAS DEL PARLAMENTO DE NAVARRA

3.1 IDENTIFICACIÓN DE LA POLÍTICA

Los datos identificativos de la Política son los que se incluyen a continuación:

Nombre del documento	Política de Identidad y Firma Electrónicas del Parlamento de Navarra.
versión	1.0
ID de la Política	Política_Identidad_y_Firma_Electrónica_Parlamento v1.0
URL de referencia de la política	https://sede.parlamentodenavarra.es/normativa
Fecha de expedición	20 de diciembre de 2022
Ámbito de aplicación	Documentos y expedientes producidos y/o custodiados por el Parlamento.
Responsable de la política	Secretaría General

3.2 PERÍODOS DE VALIDEZ Y TRANSICIÓN

Esta Política entra en vigor en la fecha de su aprobación y publicación en la sede electrónica y será válida hasta que no sea sustituida o derogada por otra Política posterior.

3.3 ÓRGANO RESPONSABLE

La Mesa del Parlamento es el órgano responsable de la publicación y el mantenimiento actualizado de la Política que se realizará mediante las correspondientes instrucciones en el caso de actualizaciones técnicas o tecnológicas. La Mesa del Parlamento cuenta con el apoyo del Servicio de Informática, Sistemas Audiovisuales y Tecnología para llevar a cabo la implementación de la Política y velar por su correcta aplicación.

La Mesa del Parlamento será responsable de garantizar que en la sede electrónica del Parlamento consten tanto la versión actualizada de la Política como el acceso a anteriores versiones de la misma, para que se puedan verificar las firmas electrónicas realizadas en el marco de una Política anterior a la vigente.

4. IDENTIDAD ELECTRÓNICA EN EL PARLAMENTO

Las relaciones telemáticas requieren, para su seguridad, de una identificación cierta de todas las partes que participan.

El Parlamento admitirá como medios para acreditar electrónicamente la identidad los que se describen a continuación. Según se desarrolla en el apartado 7 de este documento, en cada caso de uso admitirán unos u otros de los que se listan, en función de los requerimientos de seguridad:

1. Certificados digitales de firma electrónica, emitidos por una autoridad de la lista de prestadores de servicios electrónicos de confianza.

2. Certificados digitales de sello electrónico, emitidos por una autoridad de la lista de prestadores de servicios electrónicos de confianza.

3. Certificados digitales de aplicación, de servidores y de sede electrónica, emitidos por una autoridad de la lista de prestadores.

4. Los sistemas de identificación basada en registro previo administrados por la AGE, tales como el Sistema Cl@ve Permanente y Cl@ve PIN24H.

5. CERTIFICADOS DIGITALES

5.1 CERTIFICADOS DIGITALES EMPLEADOS POR EL PARLAMENTO

El personal y los miembros del Parlamento que tengan que firmar documentos digitalmente o tener acceso a determinados servicios o aplicaciones donde se requiera un alto nivel de autenticación, pueden requerir certificados digitales. Para este propósito la organización utilizará los certificados que se describen a continuación.

• Certificado de persona física: Certificados a título personal sin vinculación con el Parlamento.

• Certificados de vinculación con el Parlamento: Certificados personales que puede tener cualquier trabajador o miembros del Parlamento y que contienen el dato de su vinculación con el Parlamento, emitidos por un prestador incluido en la lista de prestadores de confianza (Certificados de personal adscrito a la administración pública o funcionario según terminología de la Fábrica Nacional de la Moneda y Timbre (en adelante, FNMT)).

• Certificados de representante: Certificados personales que sólo pueden tener personas que pueden representar al Parlamento frente a terceros y que contienen el dato de su vinculación con el Parlamento, emitidos por un prestador incluido en la lista de prestadores de confianza.

• Certificado de sello electrónico: Corresponde al certificado digital que sirve para autorizar la actuación administrativa automatizada, según el artículo 42 de la Ley 40/2015 de régimen jurídico de sector público. Este certificado puede utilizarse para las compulsas y copias electrónicas, foliados de expedientes y emisión de certificados que no requieran el ejercicio de discrecionalidad administrativa o parlamentaria ni valoración técnica, entre otros.

• Certificado de aplicación: Corresponde al certificado digital que sirve para la identificación de aplicaciones y servidores. Este certificado es requerido por una aplicación para firmar documentos o mensajes para asegurar la autenticidad e integridad de los mensajes o ficheros firmados. También puede utilizarse para el intercambio de datos (entre administraciones, administraciones y ciudadanos y entre administraciones y empresas), la identificación y autenticación de un sistema, servicio web, entre otros. (Certificados de sello de entidad terminología de la FNMT):

• Certificado de servidor seguro: Corresponde al certificado que se utiliza para garantizar el acceso seguro a los entornos de tramitación telemática con el Parlamento (páginas web y / o sede electrónica). Con esta finalidad se podrán utilizar los certificados emitidos por cualquiera de las autoridades de certificación que ya tengan un alto nivel de reconocimiento de sus claves públicas, en los navegadores de uso más extendido. Cabe señalar que, si bien estos certificados no generan actos jurídicos, al igual que los de aplicación, se ha considerado oportuno incorporarlos a las políticas.

El personal y los miembros del Parlamento podrán tener dos tipos de certificados digitales de los listados anteriormente, uno de persona física y uno de vinculación con el Parlamento que podrán utilizar cuando la actuación que realicen sea en nombre propio.

Las personas con capacidad de representación podrán tener tres tipos de certificados digitales: uno de persona física, uno de vinculación con el Parlamento y uno de representación. Para identificar qué deben utilizar en cada caso deben tener en consideración lo siguiente:

• Cuando actúen como representantes legales, con competencia estatutaria del Parlamento, y sea una actuación que sólo pueden realizar en virtud de su cargo, utilizarán el certificado de representante.

• Cuando la actuación que realicen sea en nombre propio utilizarán el certificado de vinculación con el Parlamento o el de persona física.

En el Anexo II se identifican las tecnologías y proveedores concretos admitidos por el Parlamento para cada caso. La Comisión de Administración Electrónica podrá proponer a la Mesa del Parlamento la actualización del contenido del Anexo II en función de las evoluciones de la tecnología o de las prácticas de certificación de cada prestador.

5.2 CERTIFICADOS DIGITALES ADMITIDOS POR EL PARLAMENTO.

Los interesados e interesadas que se relacionan con el Parlamento podrán hacer uso de los certificados relacionados en la lista de confianza de prestadores calificados de servicios electrónicos de confianza (TSL) del Ministerio competente que consten publicados en la sede electrónica del Parlamento para identificarse en las diferentes actuaciones en que intervengan, así como para la firma electrónica de documentación en soporte digital.

El Parlamento se apoya, para la validación de los certificados, en los servicios que presta el @firma de la AGE (Ministerio de Industria, Comer-

cio y Turismo). Los prestadores o las tipologías de certificado que, a pesar de estar en la lista del Ministerio, no sean reconocidos por estos sistemas, no podrán ser empleados en los trámites o procedimientos que impliquen una validación automática, en tanto no se hayan actualizado los criterios de reconocimiento de @firma.

5.3 CERTIFICADOS DIGITALES DEL PERSONAL Y MIEMBROS DEL PARLAMENTO.

En aquellos supuestos en que el personal y miembros del Parlamento necesiten disponer de certificado electrónico, podrán usar uno de persona física, de vinculación con el Parlamento o de representante. Estos últimos podrán ser generados cuando su cargo o sus tareas y competencias lo requieran. Para el caso de terceros que participen o colaboren puntualmente con el Parlamento, podrán usar uno de persona física o uno de vinculación con el Parlamento. En particular:

• Todas las personas que por cargo o designación pueden representar al Parlamento deberán tener como mínimo un certificado electrónico de representante, de las tipologías previstas en el Anexo II.

• Todos el personal y miembros del Parlamento que en el ejercicio de sus funciones necesiten firmar documentos electrónicos o realizar alguna de las tareas para las que se requiere certificado, podrán o bien usar los certificados de persona física o bien solicitar un certificado de vinculación con el Parlamento de acuerdo con el procedimiento descrito en el Anexo III. Es responsabilidad del trabajador o miembro del Parlamento asegurarse de la vigencia de su certificado.

• El resto de las personas vinculadas al Parlamento o personas que participen o colaboren puntualmente con el Parlamento, podrán usar un certificado de persona física u obtener un certificado electrónico de vinculación con el Parlamento, acompañando la justificación de su necesidad verificada por su superior jerárquico o por el responsable del servicio con el que colabore.

5.4 SUPUESTOS AUTORIZADOS PARA HACER USO DE LOS CERTIFICADOS DE VINCULACIÓN CON EL PARLAMENTO.

Los certificados emitidos a favor de los trabajadores o miembros del Parlamento, de vinculación con este, se emiten con el fin de ser utilizados en los procedimientos y trámites que se desarrollen dentro del Parlamento. En particular:

• Autenticación, en su caso, en los sistemas de información del Parlamento.

• Autenticación ante los portales del Gobierno de Navarra o de otras administraciones con las que se relacione el Parlamento (Ministerios, Notific@, …)

• Firma electrónica de documentos generados por el Parlamento.

• Firma electrónica de documentos generados por un tercero, que estén asociados a un procedimiento o expediente electrónico en el ámbito del Parlamento.

5.5 PROCEDIMIENTOS RELACIONADOS CON EL CICLO DE VIDA DE LOS CERTIFICADOS DE VINCULACIÓN CON EL PARLAMENTO.

5.5.1 Obtención, renovación y revocación

Corresponde a Secretaría General establecer los procedimientos a seguir para la obtención, renovación y revocación de los diferentes tipos de certificados en uso en el Parlamento.

La renovación de estos procedimientos se hará de oficio, siempre que los cambios en las circunstancias normativas o tecnológicas lo hagan necesario.

Los procedimientos vigentes en cada momento se harán públicos en la Sede Electrónica del Parlamento.

En el momento de aprobar esta Política, los procedimientos que se establecen son los que figuran en el Anexo III.

5.5.2 Almacenamiento de los certificados

Los certificados digitales del Parlamento se pueden encontrar en los siguientes repositorios:

a) En el repositorio de gestión de certificados digitales de los ordenadores de los respectivos puestos de trabajo (para certificados de persona física, de vinculación con el Parlamento o de representante).

b) En el repositorio de gestión de certificados digitales de los servidores del Parlamento (para certificados de sello electrónico para la actuación administrativa automatizada, los de entidad o por certificados de servidor web y de su electrónica).

Los certificados de sello electrónico se podrán instalar también en el servidor de un tercero, prestador de servicios de seguridad, en caso de que sea imprescindible para la ejecución de tareas automáticas por orden del Parlamento. Este tipo de cesiones deberá estar descrita en un contrato

o convenio, acotada a usos concretos y sujeto a las potestades de verificación apropiadas por parte del Parlamento.

5.5.3 Mantenimiento del inventario de certificados en el Parlamento

El mantenimiento del inventario de certificados digitales del Parlamento lo lleva a cabo el Servicio de Informática, Sistemas Audiovisuales y Tecnología. Este inventario es único para todos los certificados digitales, no importa quien sea la autoridad de certificación que los ha emitido.

El inventario de certificados digitales del Parlamento no debe incluir los certificados digitales de persona física, puesto que estos al no ser del Parlamento, no deben formar parte de este inventario.

El inventario incluye la información necesaria para la gestión del certificado, como mínimo: Titular, autoridad emisora, tipo de certificado y fecha de caducidad.

Con una periodicidad mínima semestral se debe realizar una revisión proactiva de la vigencia de los diferentes certificados digitales. A raíz de esta revisión se puede tener que proceder a la revocación de certificados digitales cuya existencia ya no sea conforme con esta Política.

En relación con las políticas de emisión, gestión y vigencia de los certificados, se atenderá a lo que establezcan las autoridades de certificación responsables.

6. SISTEMAS DE FIRMA ELECTRÓNICA

Los sistemas de firma electrónica que se podrán utilizar en el seno de las aplicaciones corporativas del Parlamento, para poder garantizar la autenticidad, integridad, inalterabilidad y conservación de los documentos firmados digitalmente, son los siguientes:

6.1 FIRMA ELECTRÓNICA MEDIANTE CERTIFICADO DIGITAL PERSONAL (DE PERSONA FÍSICA, DE VINCULACIÓN CON EL PARLAMENTO O DE REPRESENTANTE)

Es el sistema de firma electrónica en la que, partiendo de la clave privada de un certificado digital de una persona, se cifra el resumen criptográfico del documento a firmar y se añade a esta firma información del certificado utilizado para realizarla, la fecha de la firma, la política de firma, etc.

El Parlamento utilizará este sistema para la firma de los documentos electrónicos por parte de personal del Parlamento y admitirá documentos firmados con este sistema de firma por parte de terceros que se relacionen con el Parlamento.

Desde el punto de vista del formato tecnológico, la firma a realizar será del tipo PAdES preferiblemente cuando se pueda generar como firma attached a un documento PDF, de lo contrario se utilizará firma detached en formato XAdES. Generalmente se preferirá que incorporen sello de tiempo, a menos que se haya evaluado para el procedimiento en concreto que el tiempo previsto de custodia de los documentos no lo requiere. Por lo tanto:

	Con carácter general, sello de tiempo	Cuando se haya evaluado que no hay sello de tiempo
Cuando sea posible, firma attached sobre PDF	PAdES-LTV	PAdES-BES
En otro caso, firma detached	XAdES-BT	XAdES-BB

6.2 FIRMA ELECTRÓNICA MEDIANTE SELLO ELECTRÓNICO PARA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA

Es el sistema de firma electrónica mediante actuación automatizada, en el que partiendo de la clave privada de un certificado digital de sello electrónico se cifra el resumen criptográfico del documento a firmar y se añade a esta firma información del certificado de sello electrónico utilizado para realizarla, la fecha de la firma, la política de firma, etc.

Este sistema permite la firma de documentación electrónica emitida por el Parlamento, de manera transparente para el personal a su servicio. De este modo, se vincula esta documentación a la actuación administrativa automatizada, la cual tiene su regulación específica en una norma aprobada al efecto, llevada a cabo por ella misma.

Se podrá utilizar este sistema de firma electrónica en las actuaciones administrativas automatizadas que se determine, con carácter previo, mediante Acuerdo de la Mesa, de acuerdo con el artículo 41.2 de la Ley 40/2015 de Régimen Jurídico del Sector Público, que se publicará en la sede electrónica.

Desde el punto de vista del formato tecnológico, la firma a realizar será del tipo PAdES preferiblemente cuando se pueda generar como firma attached a un documento PDF, de lo contrario se utilizará firma detached en formato XAdES. Generalmente se preferirá que incorporen sello de tiempo, a menos que se haya evaluado para el procedimiento en concreto que el tiempo previsto de custodia de los documentos no lo requiere. Por lo tanto:

	Con carácter general, sello de tiempo	Cuando se haya evaluado que no hay sello de tiempo
Cuando sea posible, firma attached sobre PDF	PAdES-LTV	PAdES-BES
En otro caso, firma detached	XAdES-BT	XAdES-BB

6.3 FIRMA ELECTRÓNICA BASADA EN UN CÓDIGO SEGURO DE VERIFICACIÓN PARA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA

El artículo 42.b de la ley 40/2015 de Régimen Jurídico del Sector Público regula el uso del Código Seguro de Verificación (CSV) como medio de firma, vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, permite en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Este sistema, que sólo se puede utilizar en actuación administrativa automatizada, consiste en añadir un código único de verificación en un documento, para que se pueda validar su autenticidad a través del acceso a la sede electrónica.

Se considera firma electrónica en base a lo previsto en el artículo 42, de sistemas de firma para la actuación administrativa automatizada, apartado b de la Ley 40/2015.

Tal como se ha mencionado en el apartado anterior, se podrá utilizar este sistema de firma electrónica en las actuaciones administrativas automatizadas que se determine previamente mediante Acuerdo de la Mesa, de acuerdo con el artículo 41.2 de la Ley 40/2015 de Régimen jurídico del Sector Público, que se publicará en la sede electrónica.

6.4 FIRMA ELECTRÓNICA UTILIZANDO LA PLATAFORMA CL@VE

La plataforma Cl@ve que ofrece la Administración General del Estado, es un intermediario de identidades que simplifica el uso de diversos mecanismos de identificación electrónica, que permite al Parlamento admitir todos los medios reconocidos por esta plataforma sin tener que implementar las integraciones correspondientes cada uno de ellos.

Cl@ve ofrece también la posibilidad de generar una evidencia de firma, en la que el firmante utiliza su identidad para asociarla a un documento o una declaración de voluntad, generando de esta manera una firma electrónica de las que admite el artículo 10.4 de la Ley 39/2015.

Se contemplará este sistema de firma como un caso particular de firma electrónica con claves concertadas más voluntad de firma, pero delegando la generación de las evidencias en el sistema Cl@ve.

Este sistema se basa en el uso de la plataforma Cl@ve y será ésta quien solicitará al firmante que autentique y posteriormente, generará las evidencias tanto de identificación como de voluntad de firmar.

Cl@ve genera un fichero con las evidencias de identificación las que se guardarán como en el caso anterior dentro del mismo documento a firmar. En caso de que por algún motivo técnico no

fuera posible almacenar este archivo de evidencias en el mismo documento y éstas se guardaran en los sistemas corporativos del Parlamento; en estos casos, en el mismo procedimiento administrativo o parlamentario informará del lugar donde se almacenarán las evidencias. Posteriormente se compone o bien un documento (en XML) con el objeto firmado y los datos proporcionados por CI@ve o bien un PDF/A con la evidencia guardada dentro del PDF/A. Este es el documento que el Parlamento firma con su sello electrónico para su custodia.

En caso de conflicto con alguna firma, el Parlamento podrá acreditar que ha aprobado y publicado en la sede electrónica la regulación específica, que ha obtenido las evidencias de esta firma (firma primaria), que esta firma se produjo en un momento determinado (sello de tiempo) y que el contenido del documento no ha cambiado al estar firmado con el segundo sello electrónico (firma secundaria).

6.5 FIRMA ELECTRÓNICA BIOMÉTRICA

Este será un sistema específico, de firma electrónica avanzada para los documentos electrónicos que se generan presencialmente por parte de un tercero y en el que se guardan cifrados, conjuntamente con el resumen criptográfico del documento, la siguiente información:

• Datos biométricos de la persona que firma de forma manuscrita el documento, entre ellos:

✓ Detalle temporal de la realización de la firma (inicio, final y duración en milisegundos).

✓ Detalle de la traza, en relación con la velocidad, aceleración y presión del trazo en toda su figura.

Los datos biométricos se recogen con elementos específicos de captura permitiendo el firmante la visualización del documento a firmar en el mismo acto de firma.

• Otra información que pueda resultar relevante para el proceso de firma o el documento firmado como puede ser la identificación del software y hardware de captura de firma o la localización GPS del elemento hardware de captura de firma.

• En este tipo de firma biométrica estamos contemplando sólo la biometría de la firma manuscrita, y no otras medidas biométricas que podrían considerarse en el futuro, pero actualmente están fuera del alcance de esta Política, como el reconocimiento facial o de la huella dactilar.

El cifrado de información se realiza con la clave pública de un certificado digital específico de firma electrónica biométrica, la clave pública del que se almacena en los servidores del Parlamento. La clave privada es custodiada por un tercero de confianza al que se podrá requerir cuando sea necesario verificar una firma biométrica, en caso de reclamación o litigio.

En este formato de firma puede haber más de una firma biométrica sobre el documento, pero siempre serán en paralelo. En cualquier caso, una vez finalizadas todas las firmas biométricas y cifrada la información mencionada anteriormente se guardará de forma conjunta con el documento y, para garantizar su integridad, se realizará sobre el mismo una firma electrónica automática de sello electrónico a nombre del Parlamento completada con sello de tiempo.

Por lo tanto, la validez jurídica de la firma electrónica biométrica está vinculada al documento y a las evidencias biométricas que se guardan dentro del mismo documento de forma cifrada aportando la firma electrónica y el sellado de tiempo únicamente evidencias de integridad y no de autenticidad.

En caso de conflicto, una vez descifradas los datos por parte del tercero de confianza que custodia la clave privada del certificado de cifrado, deberá solicitar un peritaje de los datos biométricos guardadas en el documento y compararlas con una nueva toma de datos biométricos de la persona a la que supuestamente corresponden los datos biométricos y que debe hacerse bajo condiciones similares, en cuanto a elementos hardware y software, con las que se realizó la firma a verificar.

6.6 FIRMA MÚLTIPLE

La firma múltiple se produce cuando un documento contiene dos o más firmas. Dependiendo de la forma de la firma, se considera que las firmas se han realizado de forma paralela o secuencial:

• Se considera que se han realizado firmas secuenciales cuando la segunda firma se realiza sobre el objeto digital ya firmado anteriormente.

• Se considera que se han realizado firmas en paralelo cuando las firmas se refieren a un mismo objeto digital (un mismo resumen criptográfico), ya sea porque se generan en formato detached o porque el documento ha sido preparado previamente para aceptar firmas attached en paralelo.

En la medida de lo posible, se evitará el uso de la firma secuencial para los circuitos de firma donde los documentos tengan que firmarse a la vez y con el mismo objetivo por parte de varias personas.

La firma múltiple se utilizará en diversas situaciones en el marco de los procedimientos del Parlamento, como en la firma de documentos electrónicos por más de una persona o el resellado de documentos (ver apartado 8.1) ya firmados para actualizar su validez legal a lo largo del tiempo, antes de que se pueda poner en duda la validez criptográfica de la firma electrónica.

La combinación de sistemas de firma será posible en los casos siguientes:

• Firmas electrónicas mediante certificados digitales (paralela o secuencial), para cualquier documento en soporte electrónico que requiera más de una firma.

• Firmas electrónicas mediante sistemas basados en claves concertadas (Cl@ve) (paralela o secuencial), en el caso de documentos en soporte electrónico que requieran más de una firma.

• Firmas electrónicas biométricas (secuencial), para documentos en soporte electrónico que se generen presencialmente ante terceros y requieran dos o más de sus firmas.

• Firma electrónica mediante sistema basado en claves concertadas (Cl@ve) y, posteriormente, firma electrónica mediante certificado digital (paralela o secuencial), para aquellos documentos en soporte electrónico que requieran la firma de una persona (cargos de representación, empleados, los licitadores y proveedores, otras terceras personas) y requiera una firma electrónica posterior para completar su validez, mediante sello electrónico.

• Firma electrónica Biométrica y, posteriormente, firma electrónica mediante certificado digital (secuencial), en el caso de documentos en soporte electrónico que se generen ante un tercero y que, posteriormente a su firma sobre la base de biometría, requiera la firma electrónica posterior para completar su validez, mediante sello electrónico.

• Se procurará que, en todos los casos de firma del documento por varias personas, todos los participantes utilicen tecnologías similares (se evitará generar documentos firmados por una parte con firma basada en certificados, y otra parte con firma biométrica).

6.7 SELLO DE TIEMPO

El sello de tiempo es una firma electrónica generada por un tercero de confianza en base a un certificado digital especialmente destinado al efecto. Sus características principales son:

• Evidencia la fecha y hora en que se ha producido un acto. Se utiliza conjuntamente con un documento en cualquier formato y que puede estar firmado electrónicamente. El sello de tiempo puede hacer referencia a:

✓ Firma del documento: el sello de tiempo está asociado a la firma electrónica.

✓ Creación del documento: el sello de tiempo está asociado al documento.

• Mediante un proveedor de sellado de tiempo, se sellará la fecha y hora del instante en que se ha realizado el acto. El proveedor será la plataforma de TSA de @ firma del Ministerio de Hacienda y Administraciones Públicas.

• Se podrá disponer de un proveedor de sello de tiempo alternativo para garantizar la disponibilidad de los procedimientos de sellado de tiempo. Este proveedor debe estar sincronizado con fuentes fiables de tiempo como la Real Armada Española, reconocida como tal por el Esquema Nacional de Interoperabilidad. Hay varias fuentes de sellado de tiempo en el mercado, y habrá que elegir la que más convenga dependiendo de: disponibilidad del servicio, calidad de proveedor, costo del servicio, posibilidad de firma de acuerdos de nivel de servicio y autoridad certificada para este servicio.

• El proceso consiste en crear una evidencia electrónica sobre una firma electrónica: se calcula el resumen criptográfico del documento y / o las firmas electrónicas (en el caso del resellado), es decir, una operación matemática que se aplica al conjunto de información sobre el que emitió el sello de tiempo y obtiene una cadena de bits llamada "hash" la que se cifra con la clave privada del certificado de sello de tiempo utilizado para realizar la operación. Se devuelve esta firma conjuntamente con la fecha y hora de la operación, así como información sobre el certificado de sello de tiempo utilizado para hacer la firma.

7. CASOS DE USO DE LA FIRMA ELECTRÓNICA

Para cada uno de los casos que se presentan, se comenta su caracterización jurídica, y se recomienda los sistemas de firma a emplear, de entre

los que se han descrito en el apartado 6, y los niveles de seguridad aplicables.

7.1 FIRMA ELECTRÓNICA DE UN DOCUMENTO ELABORADO POR EL PARLAMENTO

Este caso de uso aplica a documentos producidos internamente en el Parlamento, que deben ser firmados por un trabajador o miembro de este en el ejercicio de sus funciones o terceros que participen o colaboren puntualmente con el Parlamento.

Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida.

Las principales características son:

• Se realiza la firma sobre un documento original en soporte electrónico.

• El documento original y las firmas deben incorporarse al sistema.

• Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla, utilizando un servicio o autoridad de validación.

• El documento electrónico estará en cualquier formato de los aceptados por el Parlamento, preferiblemente PDF / A y XML, siempre que sea necesario garantizar su preservación a lo largo del tiempo.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

• Clase de firma:

✓ Avanzada o cualificada, Según descrita en 6.1.

✓ Firma basada en claves concertadas, según descrita en 6.4

• Tipo de certificado: Certificado de persona jurídica, de vinculación con el Parlamento o Certificado de representante. En el caso de firmas basadas en claves concertadas, se complementan con un Certificado de Sello Electrónico en los términos descritos en el apartado 6.4 de esta Política.

• Formatos: PAdES-LTV con sello de tiempo o XAdES-BT.

• Sello de tiempo: Sí

• Nivel de firma: Simple, Múltiple (imbricada o paralelo)

Tipo de firma: Attached o detached según el caso.

7.2 FIRMA ELECTRÓNICA DE DOCUMENTOS POR PARTE DE UN TERCERO

Este caso de uso aplica a documentos, producidos por el Parlamento o por terceros, que son firmados por el tercero en un entorno controlado por el Parlamento. Los casos en que el documento lo firma el tercero y lo aporta firmado, se contemplan en la sección 7.6.

En particular, aplica a la firma de documentos en el momento de su presentación en un registro electrónico, o al caso en que el tercero ha de firmar electrónicamente documentos en pasos posteriores de su participación en un proceso administrativo del Parlamento. Las principales características son:

• Se realiza la firma sobre un documento original en soporte electrónico.

• El documento original y las firmas deben incorporarse al sistema.

• Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla, utilizando un servicio o autoridad de validación.

• El documento electrónico estará en cualquier formato de los aceptados por el Parlamento, preferiblemente PDF / A y XML, siempre que sea necesario garantizar su preservación a lo largo del tiempo.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

• Clase de firma:

✓ Avanzada o cualificada, Según descrita en 6.1.

✓ Firma basada en claves concertadas (Cl@ve), según descrita en 6.4.

✓ Firma electrónica biométrica, según descrita en 6.5.

• Tipo de certificado:

✓ Para las firmas generadas por terceros con certificado electrónico: Cualquier certificado definido en el punto 5 de este documento.

✓ Para los otros mecanismos de firma, certificado de sello electrónico.

• Formatos: PAdES-LTV con sello de tiempo o XAdES-BT.

• Sello de tiempo: Sí

• Nivel de firma: Simple

• Tipo de firma: Attached o detached según el caso

7.3 FIRMA ELECTRÓNICA DE CONTRATOS, CONVENIOS O ACUERDOS CON OTRAS PARTES:

Este caso de uso aplica a documentos contractuales multilaterales en los que participa el Parlamento conjuntamente con una o más partes. En este caso, las partes firman los documentos en un entorno controlado por el Parlamento.

Los casos en que el documento lo firma el tercero y lo aporta firmado para su firma posterior por parte del Parlamento, quedan englobados dentro de las previsiones que se contemplan en la sección 7.7

Las principales características son:

• Se realiza la firma sobre un documento original en soporte electrónico.

• El documento original y las firmas deben incorporarse al sistema.

• Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla, utilizando un servicio o autoridad de validación.

• El documento electrónico estará en cualquier formato de los aceptados por el Parlamento, preferiblemente PDF / A y XML, para garantizar su preservación a lo largo del tiempo.

• El documento se podrá firmar varias veces y por diferentes usuarios.

• Se podrá firmar en paralelo y / o de forma secuencial.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

• Clase de firma: Cualificada y/o Avanzada, según descrito en 6.1.

• Tipo de certificado:

✓ Para las firmas generadas por parte del Parlamento: Certificado de representante o de vinculación con el Parlamento.

✓ Para las firmas géneros por terceros. Cualquier certificado definido en el punto 5.2 de este documento.

• Formatos: PAdES-LTV con sello de tiempo o XAdES-BT.

• Sello de tiempo: Sí

• Nivel de firma: Múltiple (imbricada o paralelo)

• Tipo de firma: Attached o detached en función del procedimiento.

7.4 FIRMA ELECTRÓNICA AUTOMATIZADA:

Permite la firma de varios documentos de forma automática con plenas garantías jurídicas, mediante certificados de sello electrónico sin la intervención de un firmante en el proceso de firma.

Las principales características de este escenario son:

• Firma de varios documentos de forma automática.

• El documento electrónico puede estar en cualquier formato de los aceptados (PDF, PDF / A y XML), pero se preferirá el formato PDF para documentos que deban compartir con los interesados.

• Los certificados digitales, así como las correspondientes claves privadas que deben permitir generar procesos de firma automatizada se guardarán en un repositorio seguro en el servidor del Parlamento, o el de un tercero prestador de servicios, siempre que la cesión esté limitada y controlada de acuerdo con lo dispuesto en el apartado 5.5.2 de esta Política.

Una vez descritas las características concretas de este escenario, se enumeran los criterios de aplicación y actuación:

• Este escenario está pensado para aquellas tareas en las que se tienen que firmar varios documentos de forma automatizada con garantías jurídicas.

• Se utilizará un certificado de sello electrónico, que firmará los documentos en nombre de la aplicación y del Parlamento.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

• Tipo de firma:

✓ Avanzada, según descrita en 6.2.

✓ CSV, según descrita en 6.3

• Tipo de certificado: Certificado de Sello Electrónico.

• Para documentos PDF o PDF / A: PAdES-LTV con sello de tiempo.

• Nivel de firma: simple

Tipo de firma: Attached.

7.5 FIRMA ELECTRÓNICA PARA DIGITALIZACIÓN SEGURA

Consiste en la firma electrónica de un documento digitalizado, en formato PDF o PDF / A, para crear una copia auténtica electrónica. La Firma es importante para garantizar la integridad y la autenticidad del documento digitalizado., Así como la fecha de digitalización. Firmará electrónicamente:

• El empleado público habilitado que digitalice el documento, en caso de control manual y cotejo del original.

• Un sello electrónico del sistema en caso de actuación administrativa automatizada (un caso específico de los que se prevén en el apartado anterior).

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

• Tipo de firma: Avanzada según descrito en los puntos 6.1 y 6.2

• Tipo de certificado: Certificado de empleado o público o de Sello Electrónico.

• Formatos: PAdES-LTV.

• Sello de tiempo: Sí

• Nivel de firma: Simple

• Tipo de firma: Attached.

7.6 INCORPORACIÓN DE DOCUMENTOS ELECTRÓNICOS FIRMADOS DE FUENTES EXTERNAS

En el caso de firmas que provienen de plataformas externas (otras administraciones, herramientas de cliente, etc.) se procederá a validarlas, y se incorporarán al expediente, si es posible, las evidencias de validación.

Para poder realizar la validación de un documento firmado electrónicamente en el Anexo V se indican las comprobaciones a llevar a cabo para la validación de firmas de terceros.

7.7 IDENTIFICACIÓN Y FIRMA DE PERSONAS EXTRANJERAS

El Parlamento tiene relación puntual con personas extranjeras, físicas o jurídicas, tanto en temas de contratación pública, en proyectos internacionales de investigación o de docencia.

En general, admitimos todos los certificados electrónicos reconocidos por las autoridades homologadas al Ministerio de Industria, Comercio y Turismo, según el Reglamento eIDAS. Este reconocimiento cruzado puede estar limitado por las capacidades de las herramientas de parsing e interpretación (@firma) que utilice el Parlamento.

En el caso de que una persona extranjera no disponga de un certificado:

• Si es una persona jurídica, ésta no podrá relacionarse con el Parlamento por los medios descritos.

• Si es una persona física y su relación con el Parlamento implica la realización de tareas de representación del Parlamento o de empleado público, también necesitará obtener un certificado electrónico apropiado, de los tipos que se prevén en el Anexo II.

• Si es una persona física y su relación con el Parlamento no implica la realización de tareas de representación y de empleado público, las cuales exigen firmar con certificado (ver casos de uso en el Anexo III de la presente Política), se le permitirá identificarse alegando sus datos, con las que se generará una identidad, mediante el sistema de clave concertada (que se encuentra explicado en detalle en el apartado 6.4 de la presente Política).

8. ESTRATEGIA DE PRESERVACIÓN DE DOCUMENTOS Y FIRMAS ELECTRÓNICAS

La firma electrónica permite acreditar la autenticidad de la expresión de voluntad y consentimiento a los documentos electrónicos. Sin embargo, esta validez está sujeta a ciertos riesgos que deben gestionarse debidamente para garantizar una validez jurídica indefinida del documento en soporte electrónico. Estos riesgos pueden ser:

• Caducidad del certificado digital o del sello electrónico con el que se firma un documento electrónico.

• Validez del certificado digital o del sello electrónico en el momento de generarse la firma electrónica.

• Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certifica-

do digital y con las que se generan las firmas electrónicas.

Para contrarrestar los riesgos descritos, el Parlamento se dota de dos mecanismos diferenciados: el resellado de las firmas y las copias electrónicas de documentos firmados digitalmente.

8.1 RESELLADO Y PRESERVACIÓN DE FIRMAS ELECTRÓNICAS EN ENTORNOS PROPIOS

El objetivo principal de esta función es garantizar la firma electrónica a lo largo del tiempo.

El proceso de resellado consiste en renovar el sello de fecha y hora, añadiendo un nuevo eslabón en la cadena de evidencias electrónicas a la firma electrónica que ya está en el documento.

Para poder aplicar este proceso es necesario que las firmas estén en un formato que permita añadir estas evidencias de tiempo. Estas son las firmas del tipo XAdES-A o PAdES-LTV. En el caso de que una firma no esté en estos formatos, previo al resellado tendremos que completar la firma en uno de los formatos anteriormente definidos.

Este será un proceso que se llevará a cabo para aquellos documentos que no se hayan transferido a la solución de Archivo definitivo del Parlamento:

• En el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar.

• Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves que firman el documento.

Partiremos, tal como se ha comentado en el punto anterior, del supuesto de que los documentos tendrán ya una firma del tipo longevo: XAdES-A o PAdES-LTV. Sobre estas firmas se incorporará un nuevo sello de tiempo, ya que su estructura permite esta posibilidad. Este nuevo sello de tiempo estará ya generado con un certificado reciente, con un período de validez superior a la actual en la firma a resellado, con una longitud de clave que no estará comprometida y con un algoritmo que no esté sujeto a la obsolescencia criptográfica del algoritmo en el momento de su emisión.

En el caso de las firmas realizadas a través de acreditación de la identidad y de evidencias de la voluntad de firma, se realizará el resellado de la firma secundaria.

En definitiva, el resellado consiste pues en mantener la validez de la firma incorporando nuevo material criptográfico, concretamente sellos de fecha y hora, en la misma estructura de la firma electrónica.

El proceso de revisión de la validez de las firmas electrónicas en el Parlamento será el siguiente:

1. En el caso de firmas generadas dentro del entorno de esta (aquellas firmas generadas con las herramientas de firma internas) se procederá, en fase de tramitación, a la generación de las firmas electrónicas en formato preservable, es decir en formato de firma de archivo.

Así, por documentos XML las firmas se transformarán en XAdES - A, como podría ser el caso del foliado del expediente y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.

2. En el caso de firmas que provienen de plataformas externas (otras administraciones, los licitadores y proveedores, terceras personas, etc.) se procederá en su caso a completarlas. Este proceso de compleción se realizará previo cierre y foliación del expediente. Para documentos XML las firmas se pasarán a XAdES-A, como las facturas, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.

3. Para las firmas electrónicas basadas en identidad más voluntad de firma, se generará la firma mediante el sello electrónico ya con un formato preservable (PAdES-LTV).

4. Para las firmas electrónicas basada en CSV, se mantendrá en el repositorio de consulta, una versión del documento con firmas electrónicas preservadas.

5. Para las firmas biométricas, se generará firma mediante sello electrónico ya con formato preservable (PAdES-LTV).

8.2 COPIAS ELECTRÓNICAS DE DOCUMENTOS FIRMADOS DIGITALMENTE

En el caso de que algún documento, por el motivo que sea, tenga caducada la firma electrónica, el Parlamento podrá generar una copia auténtica de dicho documento mediante la firma electrónica basada en un certificado de sello electrónico y actuación administrativa automatizada, o a la copia de este mediante la firma electrónica de un funcionario habilitado siempre que:

1. Existan evidencias suficientes de que el documento cuando entro en el Parlamento, su firma era válida.

2. Que el documento no se ha modificado ni se ha sustituido por otro durante todo el tiempo que ha estado en el Parlamento.

Solo en estos casos se podrá proceder a la generación de la copia electrónica. Dicha copia se hará previa resolución de Secretaría General del Parlamento, que una vez analizados los antecedentes del o de los documentos que tengan la firma caducada se pueda asegurar los dos puntos anteriores.

A continuación, se procederá a la generación de un nuevo documento, con el mismo contenido y formato que el original y se podrá proceder a su firma con un sello electrónico o con un certificado digital de un funcionario habilitado. Dicha firma deberá cumplir con los requerimientos de esta Política en cuanto a formato y completitud. Así mismo deberá indicarse, en sus correspondientes metadatos de que el documento es una copia autentica de un documento original electrónico o de una copia electrónica auténtica.

Finalmente se sustituirá el documento original con la firma caducada por el nuevo documento dentro del sistema de gestión documental del Parlamento.

9. MANTENIMIENTO DE LA POLÍTICA

9.1 DESARROLLO DE LA POLÍTICA DE FIRMA ELECTRÓNICA

La correcta aplicación de esta Política requiere la adecuación de las diferentes aplicaciones, herramientas informáticas y procesos que se utilizan dentro del Parlamento.

Los servicios y sistemas que se desarrollen tras la aprobación de la Política estarán sujetos a ella desde el momento de su puesta en funcionamiento.

Con una periodicidad bienal, los Servicios Jurídicos realizaran auditorías internas para comprobar el estado de cumplimiento de la Política, su adecuación a las necesidades reales del Parlamento y su alineamiento con las tecnologías disponibles e informará a la Mesa del Parlamento.

Disposición transitoria primera. Disposición de medios tecnológicos

Se podrá hacer uso de todos los tipos de identificación y firma electrónica previstos en la presente Política de forma progresiva a medida que se disponga de las aplicaciones, las herramientas técnicas y los procesos necesarios para su uso.

Disposición transitoria segunda. Actualización de sistemas

En el plazo de seis meses desde la aprobación de esta Política, se actualizarán los sistemas en uso afectados, con el objetivo que se adecuen a lo establecido.

ANEXO I GLOSARIO Y CONCEPTOS EN FIRMA ELECTRÓNICA

GLOSARIO

Se ha considerado importante incorporar un capítulo de definición de términos, aplicados en este documento, para hacer más comprensible la Política.

Casos de uso de la firma electrónica. En este documento nos referimos a los casos de uso de la firma electrónica, entendidos como los escenarios posibles de generación de documentos electrónicos firmados. Para cada caso de uso se identificarán los formatos de firma electrónica, los posibles niveles de firma, etc.

Clases de firma electrónica. En este documento nos referiremos a las clases y a la validez jurídica de la firma electrónica, según se define en el Reglamento 910/2014, relativo a identificación electrónica y servicios de confianza para las transacciones electrónicas (eIDAS): Firma simple, avanzada y cualificada.

Formato de firma electrónica. Forma en que se codifican las firmas electrónicas. Los formatos más utilizados son los formatos S / MIME, CMS, XAdES, CAdES y PAdES.

Nivel de firma: Con este nombre nos referiremos a si el documento tiene una única firma o múltiples firmas y en este caso si se generan en paralelo o secuenciales.

Sellado de tiempo: Acreditación, a cargo de un tercero de confianza, de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Sistema de firma: Con este nombre nos referimos a la forma en que se firma un documento electrónico, ya sea mediante un certificado digital del firmante, con un sistema de identificación más evidencia electrónica del acto de la firma, firma biométrica o mediante código seguro de verificación (CSV)

Tipo de firma: Forma como se relaciona la firma electrónica con el documento firmado: dentro del mismo documento, como un documento aparte, dentro de estructuras XML, ...

Los actores involucrados en el proceso de creación y validación de una firma electrónica son los siguientes:

a) **Firmante**: persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica.

b) **Creador de un sello**: Persona jurídica que crea un sello electrónico

c) **Verificador**: Entidad, tanto si se trata de una persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política por la que se rige la plataforma de relación electrónica, o el servicio concreto a que se 'está invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.

d) **Prestador de servicios de firma electrónica**: Una persona física o jurídica que expide certificados electrónicos o presta otros servicios relacionados con la firma electrónica.

e) **Emisor y gestor de la Política de Firma Electrónica y de Certificados**: Entidad que se encarga de generar y gestionar el documento de la política, que regirá las actuaciones del firmante, el verificador y los prestadores de servicios, en los procesos de generación y validación de firma electrónica.

En este documento se utilizará el término "firmante" tanto para referirse a la persona que firma como el creador de un sello. En el segundo de los casos, se puede tratar de un proceso de actuación administrativa automatizada.

CONCEPTOS EN FIRMA ELECTRÓNICA

DEFINICIÓN JURÍDICA DE LA FIRMA ELECTRÓNICA

Hay que tomar en consideración la definición de las clases de firma desde un punto de vista jurídico:

• **Ordinaria**: Es el conjunto de datos en forma electrónica, consignados junto a otros o que están asociados, que pueden ser utilizados como medio de identificación de la persona que firma (donde identificación debe entenderse como autenticación de entidades).

• **Firma electrónica avanzada**: Es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única ya los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su control exclusivo.

• **Firma electrónica cualificada**: Es la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada mediante un dispositivo seguro de creación de firma.

Para las definiciones anteriores, se utiliza un concepto clave que habría que concretar y no es otro que el de certificado reconocido, que son aquellos certificados electrónicos emitidos por un prestador de servicios de certificación, que cumplen con los requisitos establecidos en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y la fiabilidad y las garantías de los servicios de certificación que presten.

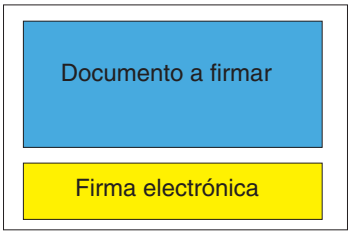
FUNDAMENTOS TÉCNICOS DE LA FIRMA ELECTRÓNICA

Se definen los tipos de firma desde un punto de vista técnico:

• **Firma attached:** Los datos de firma residen en el documento firmado. Por lo tanto, el mismo documento dispone de toda la información para comprobar la autenticidad e integridad del documento, así como la información necesaria para la validación de la firma. Hay que diferenciar entre dos tipos diferentes de firma attached:

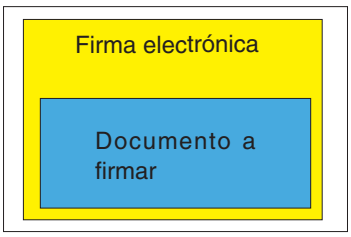
✔ Enveloped (incrustada), en este caso el documento firmado está compuesto por el contenido del documento a firmar más la firma de este contenido.

documento firmado

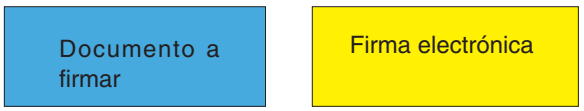


✔ Enveloping (envolvente), en este caso el documento firmado es la firma electrónica del documento a firmar y dentro de esta firma está el mismo documento a firmar.

documento firmado



• **Firma detached**: Los datos de firma residen fuera del documento a firmar, pero asociados a este. Los datos de la firma se mantendrán por separado durante todo el ciclo de vida del documento. Para validar la firma hay que crear un documento de evidencia electrónica que contenga de forma conjunta el documento y sus datos completos de la firma.



A continuación, definiremos el nivel de firmas.

• **Firma simple**: el documento contiene una única firma.

• **Firma múltiple**: el documento contiene dos o más firmas. Esta firma múltiple consiste en que varios firmantes firmen el documento consecutivamente. Esta firma se puede aplicar sobre el documento original cada vez, lo que se identifica como firma **paralela**, o sobre el documento firmado, que se identifica como firma **secuencial**.

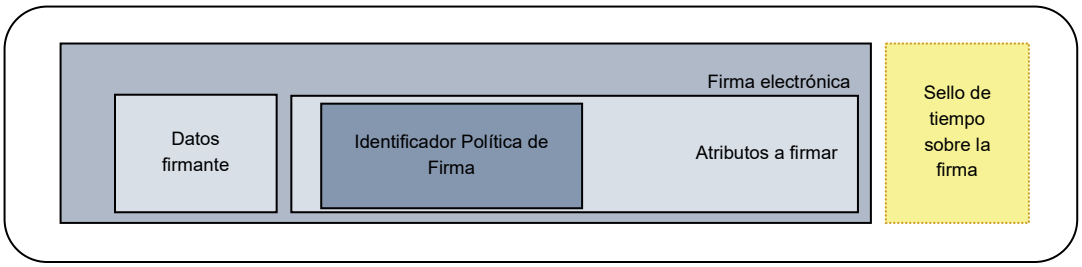
La firma múltiple se utilizará en diversas situaciones en el marco de los procedimientos del Parlamento, como en la firma de documentos electrónicos por más de una persona o el resellado de documentos ya firmados para actualizar la validez legal del documento a lo largo del tiempo, antes de que pueda quedar en entredicho la validez criptográfica de la firma electrónica.

ESPECIFICACIONES TÉCNICAS DE LOS FORMATOS DE FIRMA ELECTRÓNICA

Firma electrónica con política de firma y con sello de tiempo

Formato de firma derivado de la firma electrónica avanzada con identificador de política (en nuestra nomenclatura normativa de firma electrónica), también conocida EPES, con la incorporación de un sello de tiempo que sitúa la firma electrónica en un momento determinado del tiempo.

La representación gráfica de este formato de firma, identificado como ADES-T es la siguiente:



La firma electrónica con política explícita (XAdES-T), debe contener todos los elementos que se listan a continuación de los que todos, excepto el último, corresponden a el formato XAdES-EPES (firma electrónica avanzada con identificador de política):

• Los datos firmados por el usuario, como por ejemplo un documento electrónico

• El tipo de contenido firmado: contentType

• El resumen criptográfico del mensaje: MessageDigest

• El certificado utilizado para firmar: ESSSigningCertificate o OtherSigningCertificate

• La fecha y hora alegada de la firma: signingTime (Opcional)

• Las pistas sobre el contenido firmado: ContentHints (Opcional)

• La identificación del contenido: ContentIdentifier (Opcional)

• La referencia a los contenidos: ContentReference (Opcional)

• La indicación del tipo de compromiso: CommitmentTypeIndication (Opcional)

• La localización del firmante: SignerLocation (Opcional)

• Los atributos del firmante: SignerAttributes (Opcional)

• El sello de fecha y hora sobre el contenido: ContentTimestamp (Opcional)

• Contrafirma: Countersignature (Opcional)

• Identificación de la política de firma: SignaturePolicyIdentifier (en nuestra nomenclatura normativa de firma electrónica)

• Sello de fecha y hora de la firma: SignatureTimeStamp

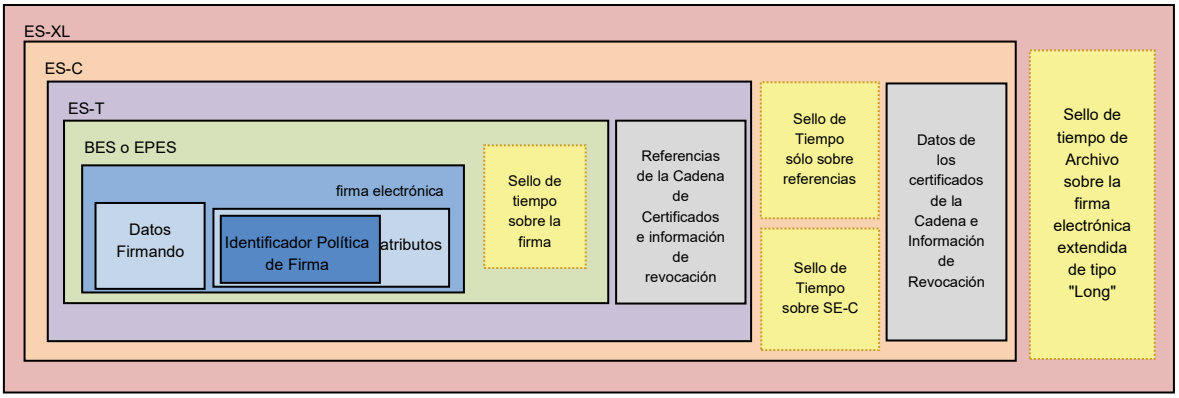
Firma electrónica de Archivo

La firma electrónica de archivo acepta dos formatos:

Firma AdES

La firma electrónica de archivo (AdES-A) parte del formato de firma electrónica extensa (XL), que incluye todos los elementos de verificación de la vigencia del certificado para poder repetir la validación de manera autónoma. Sobre este formato extenso de firma, añade un sello de tiempo, previendo el resellado sucesivo de manera periódica. Este es el formato de firma más completo y está pensado expresamente para los documentos que se quiere garantizar la disponibilidad a lo largo del tiempo.

Firma electrónica de Archivo (ES-A)



• La firma electrónica XML: Signature

• El certificado utilizado para firmar: SigningCertificate o KeyInfo: X509Data

• La fecha y hora alegada de la firma: signingTime (Opcional)

• El formato del objeto de datos firmado: DataObjectFormat (Opcional)

• La indicación del tipo de compromiso: CommitmentTypeIndication (Opcional)

• El lugar de producción de la firma: SignatureProductionPlace (Opcional)

• El papel de la persona que firma: SignerRole (Opcional)

• El sello de fecha y hora sobre el contenido: AllDataObjectsTimeStamp o IndividualDataObjectsTimeStamp (Opcional)

• La contrafirma: Reference o CounterSignature (Opcional)

• Identificación de la política de firma: SignaturePolicyIdentifier (en nuestra nomenclatura normativa de firma electrónica)

• Sello de fecha y hora de la firma: SignatureTimeStamp

• Referencias completas de certificados: CompleteCertificateRefs

• Referencias completas de revocación: CompleteRevocationRefs

• Referencias completas de certificados de atributos: AttributeCertificateRefs

• Referencias completas de revocación de atributos: AttributeRevocationRefs

• Sello de fecha y hora sobre la firma completa: SigAndRefsTimeStamp

• Sello de fecha y hora sobre las referencias de certificados y revocaciones: RefsOnlyTimeStamp

• Valores de certificados: CertificateValues

• Valores de revocación: RevocationValues

• Valores de certificados de atributo: AttrAuthoritiesCertsValues

• Valores de revocación de certificados de atributo: AttributeRevocationValues

• Sello de fecha y hora de archivo: ArchiveTimeStamp Obligatorio

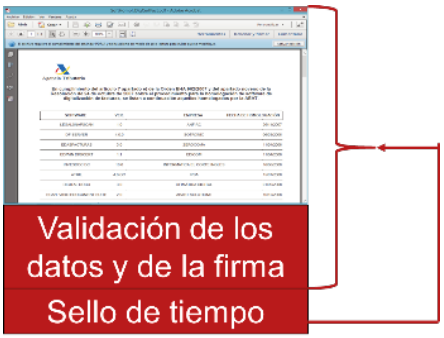
Firma PAdES-LTV

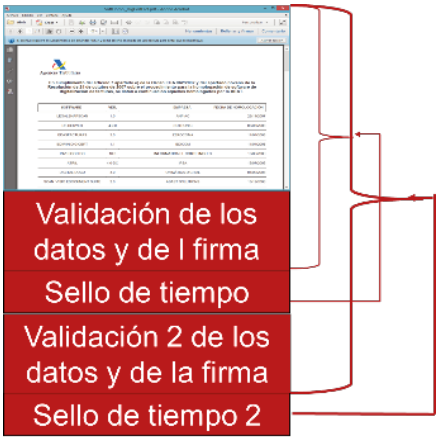
La firma electrónica de larga duración (Long Term Validation) es un formato específico de la familia PAdES. La firma más básica, la PAdES Basic está especificada en la ISO 32000 - 1. La firma PAdES EPES incluye la firma electrónica del documento (en formato CAdES - BES), con sello de tiempo (recomendado). Puede incluir, además, motivos de firma, el lugar de la firma y datos de contacto del firmante. Incluye, además, la política de firma.

Sobre estas firmas se puede construir una firma PAdES – LTV, la cual incluye además información sobre la validación de la firma electrónica. Dicha validación podrá ser a través de la consulta de la lista de certificados revocados (CRL's) o bien la respuesta del servicio de validación OCSP. Finalmente se añade un sello de tiempo sobre esta información de verificación de firmas.

A la firma se puede añadir, a posteriori, un nuevo comprobante de verificación que garantiza que la verificación que se hizo en su momento sigue siendo válida y, además, se añade un nuevo sello de tiempo que protege las firmas y sus validaciones.

Ejemplos:





Este tipo de firma se usa para cualquier tipo de documento, que deba conservarse más que el tiempo de validez del sello de tiempo correspondiente.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV)

Generación del Código seguro de verificación

El código seguro de verificación consiste en una secuencia de letras y números generada de manera aleatoria y no deducible del contenido del documento y asociada unívocamente al documento. Su creación se realiza en base a un sistema de generación de una URI (Uniform Resource Identifier) única para cada uno de los documentos electrónicos a imprimir de forma segura.

El Parlamento utiliza el siguiente procedimiento para generar los CSV:

1. Se generará una cadena de caracteres uniendo la dirección MAC del servidor, el tiempo actual en milisegundos, un número aleatorio y la petición recibida como cadena de caracteres.

2. Sobre esta cadena de caracteres resultante, se aplicará un algoritmo SHA-2 para trinchar, el cual será truncado a 15 bytes.

3. Una vez obtenido este código, se codificará en base64 para obtener 20 caracteres alfanuméricos.

Procedimiento de validación de los documentos firmados con CSV

Para la confrontación de los documentos, los interesados e interesadas deben dirigirse a la Sede Electrónica del Parlamento, donde se podrá acceder al servicio de Validación de documentos electrónicos con código seguro de verificación. En este servicio se debe introducir íntegramente el CSV que consta en el documento que se compara y si el CSV coincide con un documento disponible para la consulta, el sistema devolverá:

• En el caso de documentos generados de origen con CSV, el documento original desde la ubicación correspondiente en el sistema de gestión documental.

• En el caso de copias auténticas de documentos no previstos para su impresión segura desde su creación, el documento copia auténtica con cambio de formato desde la ubicación específica del sistema de gestión documental de impresión segura.

ANEXO II - CERTIFICADOS ELECTRÓNICOS PARA EL USO POR PARTE DEL PARLAMENTO Y SUS EMPLEADOS

A continuación, se listan los prestadores y tecnologías concretas admitidas en el Parlamento para cada una de las necesidades de certificación identificadas en el apartado 5.1.

Esta lista puede ser actualizada por la Mesa del Parlamento a propuesta de la Secretaría General, en función de posibles modificaciones en la tecnología o en las prácticas de certificador de las autoridades, siempre que los certificados que se emplean sean certificados cualificados emitidos por autoridades de la lista de prestadores de servicios electrónicos de confianza.

El personal o miembros del Parlamento que tengan que firmar documentos digitalmente o tener acceso a determinados servicios o aplicaciones donde se requiera un alto nivel de autenticación, pueden requerir certificados digitales. Para este propósito el Parlamento utilizará los siguientes certificados:

• **Certificado de persona física**: el personal y miembros del Parlamento podrán usar cualquier certificado de persona física de la TSL del Ministerio de Ministerio de Asuntos Económicos y Transformación Digital.

• **Certificados de vinculación con el Parlamento**:

✓ *Certificado de firma electrónica del personal al servicio del Sector Público (Certificado de empleado público, según terminología de la FNMT).* Corresponde al certificado de identificación y firma avanzada, que va dirigido a personas físicas y dispone de información referente al titular que permite identificarlo y vincularlo al Parlamento. Se suministra en software. Para este tipo de certificados, el Parlamento utilizará los de la FNMT y se solicitarán por el procedimiento establecido en el Anexo III.

• **Certificados de representante**:

✓ *Certificados de representante.* Corresponde al certificado electrónico de representante. Es un certificado de identificación y firma avanzada o también reconocida o cualificada. Se suministra tanto en software como en tarjeta criptográfica. Este certificado acredita que el titular del certificado puede representar al Parlamento en general o ante otras administraciones públicas. Para este tipo de certificados, el Parlamento utilizará los de la FNMT y se solicitarán por el procedimiento establecido en el Anexo III. La Secretaría General del Parlamento centralizará la solicitud de este tipo de certificados, dado que su obtención está condicionada a la acreditación del nombramiento como representante. Tal acreditación debe constar documentalmente en una publicación en el diario o boletín oficial, inscripción en un registro público o un documento notarial, según establece el artículo 7 de la Ley 6/2020, de 11 de noviembre, reguladora de los servicios electrónicos de confianza.

• **Certificados técnicos:**

✓ *Certificado de Sello electrónico en el ámbito de la Administración para actuaciones administrativas automatizadas*: Corresponden a los certificados digitales que sirven para autorizar la actuación administrativa automatizada, según el artículo 42 de la Ley 40/2015 de régimen jurídico de sector público. Este certificado puede utilizarse para las compulsas y copias electrónicas, foliados de expedientes, emisión de certificados que no requieran discrecionalidad administrativa ni valoración técnica, entre otros. Para este tipo de certificados, el Parlamento utilizará los de la FNMT. Se podrá obtener un único sello electrónico para todos los usos, o especializarse en función de las competencias de cada uno de los custodios. En este último caso, podrán ser custodios de los correspondientes sellos:

– El Parlamento

– La Mesa del Parlamento

– La Secretaría General del Parlamento

En las resoluciones de creación de sellos electrónicos se deberá indicar expresamente las actuaciones administrativas automatizadas para las que se utiliza cada uno de ellos.

✓ *Certificados de sello de entidad*: Corresponden a los certificados digitales que sirven para la identificación de aplicaciones y servidores. Estos certificados pueden utilizarse para el intercambio de datos (entre administraciones, administraciones y ciudadanos y entre administraciones y empresas), la identificación y autenticación de un sistema, servicio web, entre otros. Para este tipo de certificados, el Parlamento utilizará los de la FNMT.

✓ *Certificados de servidor o de sede electrónica*. Estos certificados se utilizan para garantizar el acceso seguro a los entornos de tramitación telemática con el Parlamento (páginas web o sede electrónica en su caso). Con esta finalidad se podrán utilizar los certificados emitidos por cualquiera de las autoridades de certificación que ya tengan un alto nivel de reconocimiento de sus claves públicas, en los navegadores de uso más

extendido. Cabe señalar que, si bien estos certificados no generan actos jurídicos, al igual que los de aplicación, se ha considerado oportuno mencionarlos en esta Política para gobernar su uso y la responsabilidad de su custodia.

ANEXO III - PROCEDIMIENTOS DE OBTENCIÓN Y REVOCACIÓN DE CERTIFICADOS

CERTIFICADO DE VINCULACIÓN CON EL PARLAMENTO.

Solicitud

En el caso de que la persona sea personal del Parlamento, esta debe hacer llegar una solicitud de que necesita un certificado digital de vinculación con el Parlamento, indicando el motivo a su inmediato superior. Este verificará la necesidad y trasladará la solicitud a Secretaría General y si lo autoriza, emitirá la acreditación de la vinculación con el Parlamento.

En el caso de que sea Parlamentario, este lo solicitará a Secretaría General y si lo autoriza, esta emitirá la acreditación de vinculación con el Parlamento.

Con esta acreditación, la persona solicitará el certificado a través del formulario disponible en la web de la FNMT y posteriormente deberá contactar con la Entidad de Registro para concretar fecha y hora para realizar la acreditación de la identidad para la obtención del certificado digital.

Validación de la Identidad

• Una vez confirmada la cita, debe personarse en la Entidad de Registro, identificarse con el documento oficial de identidad ante el operador y llevar el documento de acreditación emitido por el Parlamento.

• El operador de la Entidad de Registro verificará que los datos personales que constan en la solicitud del certificado son exactamente los mismos que figuran en el documento oficial que lo identifica y por tanto, con las que se emitirá el certificado.

• También comprobará la vinculación de la persona con el Parlamento.

Emisión y entrega del certificado

• El operador procederá a la generación del certificado digital.

• El operador entregará la hoja de entrega al titular para que lo firme.

• El titular debe firmar la Hoja de Entrega, documento que acredita la posesión del certificado.

• El solicitante recibirá un e-mail, en el que haya informado en la solicitud, un enlace de descarga del certificado digital y accederá a través de la palabra clave que le haya suministrado el operador.

En el caso que el solicitante necesite soporte, el Servicio de Informática, Sistemas Audiovisuales y Tecnología prestará este servicio, tanto para la solicitud como para su descarga.

Procedimiento de revocación

• La revocación se hará a petición del propio titular del certificado digital o de Secretaría General, cuando la persona física deje de pertenecer al Parlamento.

CERTIFICADO DE REPRESENTANTE EN SOFTWARE

Este certificado se expide a las personas físicas como representantes de las personas jurídicas.

Solicitud

La persona debe contactar con Secretaría General o bien Secretaría General informará a la persona del inicio del proceso de solicitud. Secretaría General emitirá la acreditación de la representación del Parlamento y la entregará a la persona.

Con esta acreditación, la persona solicitar el certificado a través del formulario disponible en la web de la FNMT y posteriormente deberá contactar con la Entidad de Registro para concretar fecha y hora para realizar la acreditación de la identidad para la obtención del certificado digital.

Validación de la Identidad

• Una vez confirmada la cita, debe personarse en la Entidad de Registro, identificarse con el documento oficial de identidad y llevar el documento de acreditación de la representación más una copia del BOPN (Boletín Oficial del Parlamento de Navarra) donde aparezca el nombramiento del o de la Secretaría General.

• El operador de la Entidad de Registro verificará que los datos personales que constan en la solicitud del certificado son exactamente los mismos que figuran en el documento oficial que lo identifica y, por tanto, con las que se emitirá el certificado.

• También comprobará la representación de la persona en relación con el Parlamento.

Emisión y entrega del certificado

• El operador procederá a la generación del certificado digital.

• El operador entregará la hoja de entrega al titular para que lo firme.

• El titular debe firmar la Hoja de Entrega, documento que acredita la posesión del certificado.

• El solicitante recibirá un e-mail, en el que haya informado en la solicitud, un enlace de descarga del certificado digital y accederá a través de la palabra clave que le haya suministrado el operador.

En el caso que el solicitante necesite soporte, el Servicio de Informática, Sistemas Audiovisuales y Tecnología prestará este servicio, tanto para la solicitud como para su descarga.

Procedimiento de revocación

• La revocación se hará a petición del propio titular del certificado digital o de Secretaría General, cuando la persona física deje de tener la capacidad de representación en relación con el Parlamento.

CERTIFICADO DE SELLO ELECTRÓNICO

Solicitud

La unidad que necesita un certificado de sello debe hacer llegar una solicitud de dicha necesidad, indicando el motivo, a Secretaría General que será quien deberá dar su autorización.

Validación de la necesidad del certificado

En caso de que alguno de los certificados existentes pueda hacer la función requerida:

• Secretaría General aprobará este nuevo uso.

• El Servicio de Informática, Sistemas Audiovisuales y Tecnología procederá a habilitar el sello para el nuevo uso.

En caso de que no se pueda utilizar ninguno de los existentes y se tenga que crear un nuevo sello:

• Secretaría General aprobará la solicitud de este nuevo sello electrónico.

• Una vez aprobado, el Servicio de Informática, Sistemas Audiovisuales y Tecnología, solicitará a la Entidad Certificadora (FNMT), un nuevo sello electrónico.

• El Servicio de Informática, Sistemas Audiovisuales y Tecnología descargará e instalará el certificado en el servidor correspondiente

El Parlamento podrá ceder sellos electrónicos a terceros. En este caso siempre se firmará un documento de cesión del certificado de sello con el organismo al que se le cede el certificado y siempre será un certificado de sello específico, para poder tener un control de los usos que se puedan hacer con estos certificados.

ANEXO IV - ESTÁNDARES INTERNACIONALES Y OTRAS CONVENCIONES

• ETSI RFC 2315 (1998), ETSI RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: Cryptographic Message Syntax (CMS).

• ETSI TS 101 733. v.1.6.3, v1.7.4 y v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

• ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures: Part 3: incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES.

• ETSI TR 119124-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.

• ETSI TS 119124-2: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures.

• ETSI TS 119124-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures.

• ETSI TS 119124-4: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CAdES baseline signatures.

• ETSI TS 119124-5: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CAdES signatures.

• ETSI TR 119134-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.

• ETSI TS 119134-2: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures.

• ETSI TS 119134-3: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures.

• ETSI TS 119134-4: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures.

• ETSI TS 119134-5: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures.

• ETSI TS 119142-3: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS).

• ETSI TR 119144-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.

• ETSI SR 019 020: The framework for Standardization of signatures; Standards for Ades digital signatures in mobile and distributed environments.

• IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

• IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP.

• IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.

• ISO 19005 (2008): Formato de archivo / A-1.

• ISO/TR 18492: 2005 - Long-term preservation of electronic document-based Information.

• UNE - ISO/TR 13008: 2010 - Información y documentación. Conversión de documentos digitales y procesos de migración.

• ETSI TS 102176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

• ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

• ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

• ETSI TS 101 861 V1.3.1 Time stamping profile.

• ETSE TR 102.038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

• ETSE TR 102.041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

• ETSE TR 102.045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

• ETSE TR 102.272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

• IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.

• IETF RFC 3125, Electronic Signature Policies.

• IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

• IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate revocation List (CRL) Profile.

• IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).

• ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic Notation".

ANEXO V - COMPROBACIONES A LLEVAR A CABO PARA LA VALIDACIÓN DE FIRMAS DE TERCEROS

Para verificar las firmas de terceros y su correcto cumplimiento se han de seguir todos los pasos siguientes:

Identificación del certificado y la cadena de confianza

Con el fin de generar una firma electrónica será necesaria la utilización de un certificado electrónico reconocido. Quienes emiten este tipo de certificados son los prestadores de servicios electrónicos de confianza cualificados para emitir certificados electrónicos reconocidos. Para acreditar que la firma es segura y que la persona que aparece es realmente el firmante, verificar que el certificado ha sido emitido por un prestador de confianza. Tal como se ha indicado en 5.2, el Parlamento delega su confianza en la plataforma @firma.

Si la validación del emisor de los certificados falla, el emisor no se considerará de confianza y el Parlamento no depositará confianza en la firma del documento y éste será devuelto al emisor para que lo firme un emisor de confianza.

Identidad del titular del certificado

Un certificado electrónico nos ofrece información que sirve para identificar a la persona o entidad que se ha comprometido con el contenido del documento. Por lo tanto, verificar la identidad del titular del certificado es importante para poder establecer que el documento ha sido firmado por la persona correcta.

En caso de que el firmante sea una persona física en representación de una persona jurídica, en el campo que corresponda deberá constar los datos identificativos de ambos.

Si el titular del certificado coincide con la persona que consta como firmante en el texto del documento, la verificación puede entenderse como finalizada, pero en caso de que el titular del certificado no coincida con la identidad de la persona que debería firmar el documento, no se podrá admitir la firma y se rechazará el documento.

Validar las facultades del firmante

Habitualmente, puede ocurrir que el firmante del documento no firme en nombre propio, sino que lo haga en representación de un tercero. El Parlamento deberá comprobar que el representante está capacitado para ejercer la representación, en caso de que estas facultades no consten en el propio certificado. Puede ser necesario requerir la presentación de documentación adicional para acreditar la representación, o la verificación de registros externos.

En caso de que no se pueda verificar o validar la suficiencia de los poderes de representación del firmante, el documento se devolverá al emisor.

Verificar la vigencia del certificado

Los certificados electrónicos constan de una fecha de caducidad fijada en el momento de su emisión.

Los certificados, se pueden suspender o revocar incluso antes de su caducidad por motivos como: pérdida de la vigencia de datos de los certificados, pérdida de la tarjeta criptográfica, etc.

La importancia de realizar esta validación radica en que sólo es válida la firma electrónica realizada con un certificado que sea vigente y por tanto, no puede estar caducado, revocado o suspendido. La información para realizar la validación de la caducidad se extrae directamente del certificado o la autoridad de certificación. Se pueden seguir los siguientes procedimientos:

• Verificación de listas de revocación de certificados (CRLs). Esta validación se implementa automáticamente por la mayoría de las aplicaciones que permiten ver los documentos firmados, pero no generan pruebas concretas.

• Solicitud de un informe de verificación (OCSP). Se trata de un protocolo que se puede solicitar desde el prestador del servicio de certificación, pero que tiene que solicitar un sistema informático desde el Parlamento.

• Validación a través de una plataforma centralizada, como @firma.

Puede suceder, que el certificado caduque después de haber firmado un documento, por este motivo es importante que el Parlamento pueda acreditar, que el certificado se encontraba vigente en la fecha de verificación, por este motivo es necesario que el documento conste de un sello de tiempo emitido por una Autoridad (TSA).

Verificar la vinculación criptográfica del documento con la firma

La verificación de la vinculación criptográfica del documento con la firma se lleva a cabo para validar que la firma electrónica hace referencia al documento en cuestión.

El documento puede haber sufrido modificaciones posteriores al momento de la firma, la herramienta de firma no ha realizado correctamente el proceso de firma, etc. y, por tanto, puede suceder

que la vinculación entre el documento y la firma no correspondan.

Esta verificación se puede llevar a cabo mediante alguna aplicación ofimática que permita la visualización de documentos PDF, pero en los procesos de incorporación del documento al sistema se podrá hacer a través de una aplicación que ejecute la incorporación.

En caso de que falle esta comprobación, el documento se considerará mal firmado y el Parlamento realizará la devolución del documento a su emisor informando de lo sucedido.

Verificar el contenido del documento

La verificación del contenido de un documento electrónico es tan necesaria como la verificación de cualquier documento en formato papel.

En este caso las comprobaciones se centrarán en analizar si el contenido del documento es adecuado y se ajusta a las necesidades jurídicas oportunas. Por lo tanto, hablamos de validación jurídica del contenido del documento.

En caso de que el documento haya sido originalmente producido por el Parlamento, la recomendación es ofrecerlo a firmar al tercero previa firma de un sello de órgano del Parlamento, con el fin de automatizar la verificación del retorno.

En caso de que la verificación no se pueda realizar automáticamente habrá que analizar el documento para asegurarse de que no se ha realizado ningún cambio entre la versión enviada al firmante y la versión que se devuelve firmada. En caso de que esta comprobación falle y, por tanto, el documento haya sido modificado, el documento firmado por el tercero será devolver al emisor.

Verificar la fecha de la firma

La verificación de la fecha de la firma es relevante por dos motivos que se citan a continuación:

• El documento puede tener en su contenido una fecha de firma, pero puede ocurrir que ésta no coincida con la fecha de firma electrónica.

• La fecha de firma es relevante para gestionar la vigencia del certificado del firmante.

Hay que validar la fecha en la que se ha producido la firma y diferenciar si la fecha de firma se ha establecido mediante un sello de tiempo o la hora del ordenador del firmante.

Estas comprobaciones se deben realizar de manera manual a pesar de que existe la posibilidad de realizar de manera automática mediante la aplicación de captura del documento.

Depósito Legal: NA – 180-1980 ISSN 2254 – 1969