Agencia Estatal
de Seguridad Aérea

Guía de Documentación Electrónica en el entorno de la Aeronavegabilidad

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE
AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

REGISTRO DE EDICIONES		
EDICIÓN	**Fecha de APLICABILIDAD**	**MOTIVO DE LA EDICIÓN DEL DOCUMENTO**
01	Desde publicación	– Edición inicial: – Cambio en la codificación de procedimientos, formatos y guías según ***SIG-GD-P01-ITR01***, por lo que la edición pasa a Ed. 01. – Sustituye a la guía ***G-CA-DEEA-02.*** *Los cambios incorporados respecto a la anterior edición del procedimiento están marcados en azul: – Se añade la referencia a la guía de EASA "Electronic documents, records and signatures".

REFERENCIAS		
CÓDIGO	**TIPO DOCUMENTO**	**TÍTULO**
LEY 6/2020	LEY	LEY 6/2020, DE 11 DE NOVIEMBRE, REGULADORA DE DETERMINADOS ASPECTOS DE LOS SERVICIOS ELECTRÓNICOS DE CONFIANZA.
LEY 39/2015	LEY	LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS.
RD 203/2021	REAL DECRETO	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.
BR	REGLAMENTO (UE)	REGLAMENTO (UE) Nº 2018/1139 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 4 DE JULIO DE 2018, SOBRE NORMAS COMUNES EN EL ÁMBITO DE LA AVIACIÓN CIVIL Y POR EL QUE SE CREA UNA AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD AÉREA Y POR EL QUE SE MODIFICAN LOS REGLAMENTOS (CE) Nº 2111/2005, (CE) Nº 1008/2008, (UE) Nº 996/2010, (CE) Nº 376/2014 Y LAS DIRECTIVAS 2014/30/UE Y 2014/53/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y SE DEROGAN LOS REGLAMENTOS (CE) Nº 552/2004 Y (CE) Nº 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y EL REGLAMENTO (CEE) Nº 3922/91 DEL CONSEJO.
REG. 1321/2014 (IR)	REGLAMENTO (UE)	REGLAMENTO (UE) Nº 1321/2014 DE LA COMISIÓN DE 26 DE NOVIEMBRE DE 2014 SOBRE EL MANTENIMIENTO DE LA AERONAVEGABILIDAD DE LAS AERONAVES Y PRODUCTOS AERONÁUTICOS, COMPONENTES Y EQUIPOS Y SOBRE LA APROBACIÓN DE LAS ORGANIZACIONES Y PERSONAL QUE PARTICIPAN EN DICHAS TAREAS. (REFUNDICIÓN DEL REGLAMENTO (CE Nº 2042/2003).
REG. 910/2014	REGLAMENTO (UE)	REGLAMENTO (UE) Nº 914/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 23 DE JULIO DE 2014, RELATIVO A LA IDENTIFICACIÓN ELECTRÓNICA Y LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS EN EL MERCADO INTERIOR Y POR LA QUE SE DEROGA LA DIRECTIVA 1999/93/CE.
REG. 748/2012	REGLAMENTO (UE)	REGLAMENTO (UE) Nº 748/2012 DE LA COMISIÓN, DE 3 DE AGOSTO DE 2012, POR EL QUE SE ESTABLECEN LAS DISPOSICIONES DE APLICACIÓN SOBRE LA CERTIFICACIÓN DE AERONAVEGABILIDAD Y MEDIOAMBIENTAL DE LAS AERONAVES Y LOS PRODUCTOS, COMPONENTES Y EQUIPOS RELACIONADOS CON ELLAS, ASÍ COMO SOBRE LA CERTIFICACIÓN DE LAS ORGANIZACIONES DE DISEÑO Y DE PRODUCCIÓN.
N/A	GUÍA	EASA GUIDELINES ON THE USE OF ELECTRONIC DOCUMENTS, RECORDS AND SIGNATURES

* Se aplica la Última Edición en vigor.

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
AESA	AGENCIA ESTATAL DE SEGURIDAD AÉREA
ARC	CERTIFICADO DE REVISIÓN DE LA AERONAVEGABILIDAD (AIRWORTHINESS REVIEW CERTIFICATE)
ATA	ASOCIACIÓN DEL TRANSPORTE AÉREO (AIR TRANSPORT ASSOCIATION)
CA	COORDINACIÓN DE AERONAVEGABILIDAD
CAE	MEMORIA DE ORGANIZACIÓN DE AERONAVEGABILIDAD COMBINADA
CAME	MANUAL DE GESTIÓN DEL MANTENIMIENTO DE LA AERONAVEGABILIDAD (CONTINUING AIRWORTHINESS MANAGEMENT EXPOSITION).
CRS	CERTIFICADO DE PUESTA EN SERVICIO (CERTIFICATE OF REALEASE OF SERVICE)
DAEA	DIVISIÓN DE APROBACIONES Y ESTANDARIZACIÓN DE AERONAVEGABILIDAD
DAI	DIVISIÓN DE AERONAVEGABILIDAD INICIAL
DOA	ORGANIZACIÓN DE DISEÑO
DOH	MANUAL ORGANIZACIONES DE DISEÑO
DSA	DIRECCIÓN DE SEGURIDAD DE AERONAVES
EASA	AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD AÉREA
eIDAS	SISTEMA EUROPEO DE RECONOCIMIENTO DE IDENTIDADES ELECTRÓNICAS (ELECTRONIC IDENTIFICATION, AUTHENTICATION AND TRUST SERVICES)
MOE	MANUAL DE ORGANIZACIÓN DE MANTENIMIENTO PARTE 145
MOP	MANUAL DE ORGANIZACIÓN DE PRODUCCIÓN
MTOE	MEMORIA DE LA ORGANIZACIÓN DE FORMACIÓN DE MANTENIMIENTO
NDT	ENSAYOS NO DESTRUCTIVOS
OSV	OFICINA DE SEGURIDAD EN VUELO
PM	PRINCIPAL DE MANTENIMIENTO
POA	ORGANIZACIÓN DE PRODUCCIÓN
POE	MANUAL ORGANIZACIONES DE PRODUCCIÓN
PRA	PERSONAL DE REVISIÓN DE AERONAVEGABILIDAD
SIPA	SISTEMA DE INFORMACIÓN DE PROCESOS AERONÁUTICOS
TLB	CUADERNO DE REGISTRO TÉCNICO DE LA AERONAVE (TECHNICAL LOGBOOK)

ÍNDICE

1. INTRODUCCIÓN

Las normativas aeronáuticas nacieron y se desarrollaron en un entorno en el que la documentación tenía un soporte exclusivamente en papel. Es raro, hoy en día, encontrar documentación técnica que tenga este tipo de soporte. No obstante, la documentación relativa a la gestión de la aeronavegabilidad, puestas en servicio, logbooks, workcards, etc., aún no habían dado el salto. Cada vez parece más claro que ese entorno está dando paso a otro nuevo basado en soportes digitales. El paso de un mundo analógico a uno digital nunca es una translación directa y sencilla. Además, en este entorno se debe considerar de forma especial las implicaciones de responsabilidad, validez de registros y garantías legales de los documentos.

2. OBJETO Y ALCANCE

Se pretende establecer, para aquellas organizaciones relacionadas con la aeronavegabilidad inicial y la aeronavegabilidad continuada cuya responsabilidad como Autoridad Aeronáutica de supervisión recaiga en AESA, los requisitos mínimos que garanticen que las aplicaciones que sustituyan a los registros en papel dentro del entorno de la aeronavegabilidad den soporte al cumplimiento del Reglamento (UE) 748/2012 y el Reglamento (UE) Nº 1321/2014, así como el de las normativas aplicables de firma electrónica (Reglamento (UE) Nº 910/2014) y a otras normativas o referencias técnicas que pudieran ser de interés (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).

La finalidad es estandarizar su aplicación estableciendo una serie de criterios técnicos mínimos que deberán cumplir, tanto los documentos firmados electrónicamente, como las aplicaciones que los soporten, en cuanto a seguridad, interoperabilidad y garantías legales.

A continuación, se listan, a modo de ejemplo, registros que son susceptibles de ser convertidos a un formato digital, y por tanto su tratamiento debería ser sometido a dichos criterios mínimos.

- Certificados de puestas en servicio de aeronaves (CRS, TLB)
- Certificados de aptitud para el servicio (EASA Form 1, EASA Form 52, EASA Form 53 y Permiso de vuelo)
- Firma de tareas de mantenimiento (Task/Job/Work Card, doble inspección, supervisión)
- Documentación interna de las organizaciones (Autorizaciones de certificación, Evaluación de la competencia, Certificados NDT, etc.)
- Certificados de reconocimiento según formatos EASA 148 y 149 emitidos por las organizaciones Parte 147.

Esta guía está alineada con lo establecido en la guía que ha publicado EASA "*Guidelines on the use of electronic documents, records and signatures*".

https://www.easa.europa.eu/en/faq/137907

No es objeto de esta Guía, la documentación emitida o delegada por AESA (ejemplo: un ARC emitido por un PRA independiente en la plataforma SIPA), ya que su desarrollo y garantías legales están sujetas a la normativa y reglamentación desarrollada por la propia Administración. Tampoco es objeto de esta guía la parte del TLB de operaciones sin tareas de mantenimiento.

Cualquier sugerencia de modificación de la guía, por errores o mejoras, deberá comunicarse al Servicio correspondiente dependiendo del tipo de organización, a través de los siguientes correos electrónicos, que archivarán dichas sugerencias para ser evaluadas en la siguiente revisión del procedimiento.

- Organizaciones de mantenimiento: mantenimiento.aesa@seguridadaerea.es
- Organizaciones de Gestión de Mantenimiento de la Aeronavegabilidad: camo.aesa@seguridadaerea.es
- Organizaciones de Aeronavegabilidad Combinada: cao.aesa@seguridadaerea.es
- Organizaciones de Formación Parte 147: aesa.parte147@seguridadaerea.es
- Organizaciones de Producción y Diseño: poa-doa.aesa@seguridadaerea.es

3. DEFINICIONES

Registro electrónico: Documento que registra datos o declaraciones y cuyo soporte es electrónico. **Se diferencia del documento electrónico en que soporta datos o declaraciones con naturaleza de prueba.**

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.

Firma electrónica: Datos en formato electrónico anejos o asociados de manera lógica con un documento electrónico que identifican al firmante de manera inequívoca y aseguran:

- la integridad del documento firmado,
- que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación,
- el no repudio del documento firmado (los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento).

Autenticación: Procedimiento de verificación de la identidad digital de un sujeto en sus interacciones en el ámbito digital, típicamente mediante factores tales como «algo que se sabe» (contraseñas o claves concertadas), «algo que se tiene» sean componentes lógicos (como certificados software) o dispositivos físicos (en expresión inglesa, tokens), o «algo que se es» (elementos biométricos), factores utilizados de manera aislada o combinados.

Firma electrónica avanzada: Es aquella que está basada en un certificado, sin entrar a definir qué certificado ni qué sistema de firma se usa. Puede usarse allí donde no sea necesario garantizar la equivalencia a la firma manuscrita, con todas las garantías legales y de seguridad de quien hizo la firma. Los requisitos que debe cumplir la firma avanzada están definidos en el artículo 26 del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Firma electrónica cualificada: Según el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE es una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. Solo puede realizarse con certificados digitales cualificados emitidos por un Prestador de Servicios de Confianza debidamente acreditado. **Tiene un valor legal completo y garantiza la exigibilidad de un documento frente a terceros**.

Marca de Tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Sello de tiempo: Asignación de una **Marca de Tiempo** con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del

documento. El sello de tiempo puede ser **avanzado**, si cumple requisitos de sello de tiempo avanzado, o **cualificado** si, además, usa dispositivos y prestadores de servicio cualificados.

Interoperabilidad: Habilidad de diferentes sistemas de información, tecnologías y aplicaciones para comunicarse e intercambiar datos, así como utilizar dicha información con el objetivo de alcanzar un mayor nivel funcional del sistema. En el entorno de la aeronavegabilidad esa facilidad de intercambio de información tiene que darse entre tres actores: proveedores de aeronavegabilidad, clientes de aeronavegabilidad y autoridad supervisora de aeronavegabilidad. Como ejemplo de un estándar aceptable está el Air Transport Association (ATA) Spec 2000 Chapter 16, que permite la interoperabilidad de datos para certificados de puesta en servicio (EASA Form 1 y FAA 8130-3).

Política de firma electrónica: Conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación**.**

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.

Firma en cascada (contrafirma): Es una firma múltiple en la que el orden en el que se firma es importante, ya que cada firma debe refrendar o certificar la firma anterior, en contraposición con la **cofirma**, en la que los firmantes se requieren sin ninguna prevalencia.

Prestador de Servicios de Confianza: Los Proveedores o Prestadores de Servicios de Confianza son las personas físicas o jurídicas que expiden certificados electrónicos o prestan otros servicios en relación con la firma electrónica. Los Proveedores de Servicios de Certificación tanto nacionales como europeos se pueden consultar a través de los siguientes enlaces:

- Listado proveedores españoles: https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx
- Listado proveedores europeos: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

VALIDe: Servicio online de validación de certificados españoles, y verificación y generación de firmas electrónicas. Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

El objetivo de este servicio es permitir a un usuario comprobar que el certificado español utilizado es un certificado válido y que no ha sido revocado. También permite comprobar la validez de una firma electrónica realizada mediante certificado digital emitido por un prestador de servicios de certificación reconocido, y realizar firmas mediante certificado digital del que se disponga de la clave privada correspondiente.

https://valide.redsara.es/valide/ejecutarValidarFirma/ejecutar.html

4. REQUISITOS GENERALES DE LOS REGISTROS ELECTRÓNICOS

Los procedimientos que desarrollen las organizaciones para la emisión y gestión de sus registros electrónicos deberán definir los siguientes aspectos principales:

- Sistema de soporte del registro y sus garantías. Seguridad de los datos.
- Gestión del registro electrónico dentro de la organización y sus propiedades.
- Interoperabilidad de los registros.
- Firma electrónica.

Todo ello se refleja en una **Política de gestión de documentos electrónicos** que deberá incluir **una Política de firma electrónica.**

4.1. Sistemas de garantía y comprobación de validez

Un sistema de registro electrónico de registros de aeronavegabilidad deberá contemplar:

- Definición del registro.
- Sistema de soporte que usará.
- Qué garantías se establecen en cuanto a:
    - Seguridad de datos (back-ups).
    - Seguridad de acceso.
    - Facilidad de acceso y universalidad del mismo.
- Qué sistemas de comprobación de validez para terceros se van a usar. Aplicable a aquellos registros que emite la organización, pero van destinados a terceros. Debe contemplar el modo en que el propio registro remite a un sistema de comprobación de validez de la firma electrónica.

4.2. Gestión del registro electrónico dentro de la organización

Deberá definirse cómo se da soporte electrónico a la información que el registro debe retener. También se incluirá en esa definición los requisitos de manejo del registro. Esto deberá incluir:

- Cómo se genera el registro en la organización y sus sistemas.
- Cómo se completa el registro.
- Consideraciones de flujo de trabajo, origen, asignaciones, destinarios y final del proceso que definan al completo la vida del registro. Firmas en cascada.
- Consideraciones en cuanto a la política de edición del registro, campos indispensables, campos opcionales, información anexa, etc.

4.3. Interoperabilidad de los registros

Deberá definirse de qué modo los registros electrónicos deben ser transferidos entre las partes de la organización y, si esto fuera necesario, con respecto a terceros. Eso se soportará con la adopción de los formatos de datos que permitan una interoperabilidad adecuada.

Deberá contemplarse especialmente la posibilidad de que los registros pueden ser auditados tanto por control de conformidad de la organización como por la Autoridad.

4.4. Firma electrónica

Deberá definirse la firma electrónica como sistema que da soporte a la necesidad de identificar al firmante de registros electrónicos (firma de puestas en servicio, workcards, etc.) y/o la capacidad de acceder a determinada información (documentación técnica, registros, etc.), así como la garantía de control de acceso a los registros.

Dentro de la organización se definirá una política de firma electrónica que diseñe los diferentes tipos de firma a usar y de qué modo (con qué sistemas) se realizarán las mismas. El diseño de la firma electrónica debe realizarse atendiendo a la necesidad de soporte legal a la firma de registros electrónicos. Dicha necesidad determinará el nivel de seguridad de la firma a usar.

En cualquier caso, deberá atenderse a la siguiente calificación:

- Registros con efectos a terceros y necesidad de pervivencia en el tiempo (p.e. EASA Form 1, Release to Service, acuerdo DO-PO, planos de diseño, declaración de aprobación de datos, Technical log book).
- Registros sin efectos a terceros, válidos solo en el entorno de la organización (p.e. firma de Workcards, validaciones de competencia, procesos internos, acceso a registros restringidos, orden de producción, configuración de diseño, etc.).

4.5. Definición de la política de firma electrónica

- Identificación del firmante y en su caso de la organización dentro de cuyo esquema se verifica la firma.
- Información que deberá incluir la firma, datos relevantes (hora, fecha, nº de autorización, etc.)
- Qué nivel de seguridad se aplicará a la firma.
- Estándar de Interoperabilidad de datos.

4.6. Sistema de gestión de firma electrónica

- Sistema de salvaguarda para evitar:
    - Firma de documentos en blanco,
    - Que las casillas que se definan como imprescindibles no queden nunca sin rellenar,

- Que, si hay un orden implicado en la edición de documentos y/o de las firmas, el sistema de edición respete esa cronología y no permita firmar o completar un paso sin haber sido rellenado o firmado el precedente. Firmas en cascada.

4.7. Niveles de firma electrónica

Siguiendo las directrices de la Ley 6/2020 del 11 de noviembre y el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y Del Consejo De 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, se establecen tres niveles de aplicabilidad de los tipos de firma electrónica en función de la responsabilidad exigida al documento electrónico firmado.

4.7.1. Nivel 3: firma simple

Se trata de un sistema firma electrónica que se aplicará a aquellos documentos que no tengan efectos a terceros y que constituyan solo partes de procesos internos de las organizaciones sin un componente de responsabilidad asociado o un componente de responsabilidad muy bajo.

Una firma electrónica simple es aquella en la que se firma usando datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

Es recomendable que se aplique a estos datos y su firma un estándar reconocido de interoperabilidad de datos. El ejemplo típico de este tipo de firma es el de mecanismos de usuario/contraseña.

El sistema de firma electrónica simple puede ser usado para control de acceso y autenticación, que también puede realizarse por sistemas sin firma electrónica (usuario y contraseña). Este nivel de seguridad deberá estar contemplado en la política de gestión de documentación electrónica dentro de la organización.

Ejemplos no exhaustivos:

- *Acceso a sistemas basados en certificados*
- *Sistemas de control de presencia.*
- *Sistemas de coordinación de turnos, comunicaciones entre trabajadores.*
- *Accesos a sistemas de solicitud de herramientas/materiales/información.*

4.7.2. Nivel 2: firma electrónica avanzada

Es una firma electrónica de responsabilidad media. Se aplicará a aquellos documentos que demuestran la voluntad y la responsabilidad del firmante en la ejecución de tareas, acuses de recibo o emisión de validaciones, serían registros que se asocian a responsabilidad dentro de la organización sin impacto en terceros.

La firma electrónica avanzada tendrá que garantizar (tal como define eIDAS):

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma, de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Es recomendable que:

- se aplique a los registros firmados un estándar reconocido de interoperabilidad de datos.
- que las garantías se aseguren con el uso de certificados de firma, ya que hacen más sencilla la demostración de cumplimiento con los requisitos.

Ejemplos no exhaustivos:

- *Firmas de procesos internos.*
- *Supervisión de tareas internas.*
- *Sign off tareas críticas.*
- *Evaluación de la Competencia.*
- *Firma de Certificados de cursos de formación.*
- *Firma de traspasos en tarjetas de trabajo por cambios de turnos.*
- *Firmas de actas de reuniones de calidad/sistema de gestión donde intervenga el Gerente Responsable/Director Responsable.*
- *Autorizaciones de Certificación.*
- *Chequeo/Visto Bueno de una orden de producción.*
- *Procedimientos complementarios al manual.*
- *Manuales de las organizaciones.*

4.7.3. Nivel 1: firma electrónica cualificada

Es el nivel de seguridad más alto. Se aplicará a aquellos documentos que tengan efectos de responsabilidad frente a terceros, es decir, fuera de la organización que emite el documento. A este nivel de firma se le aplicará un estándar que permita una interoperabilidad de datos, mientras que en los otros niveles esto es solo recomendable.

Es una firma electrónica avanzada a la que se le exige que los prestadores de servicios de certificación estén cualificados según requisitos de eIDAS.

Adicionalmente se recomienda añadir a la firma cualificada el uso de un sello de tiempo que garantice la fecha de firma usando los sistemas previstos en el reglamento eIDAS, de modo que la validez del documento firmado y su datación se extienda en el tiempo más allá de la caducidad de los certificados usados.

En todo caso, se establecerán los mecanismos pertinentes para garantizar que las salvaguardas de validez temporal establecidas en la norma se vean atendidas.

Ejemplos no exhaustivos:

- *Certificados de puesta en servicio (CRS, EASA Form 1 y TLB que soporte CRS de aeronave).*
- *Certificados de reconocimiento según formatos EASA 148 y 149 emitidos por las organizaciones Parte 147.*

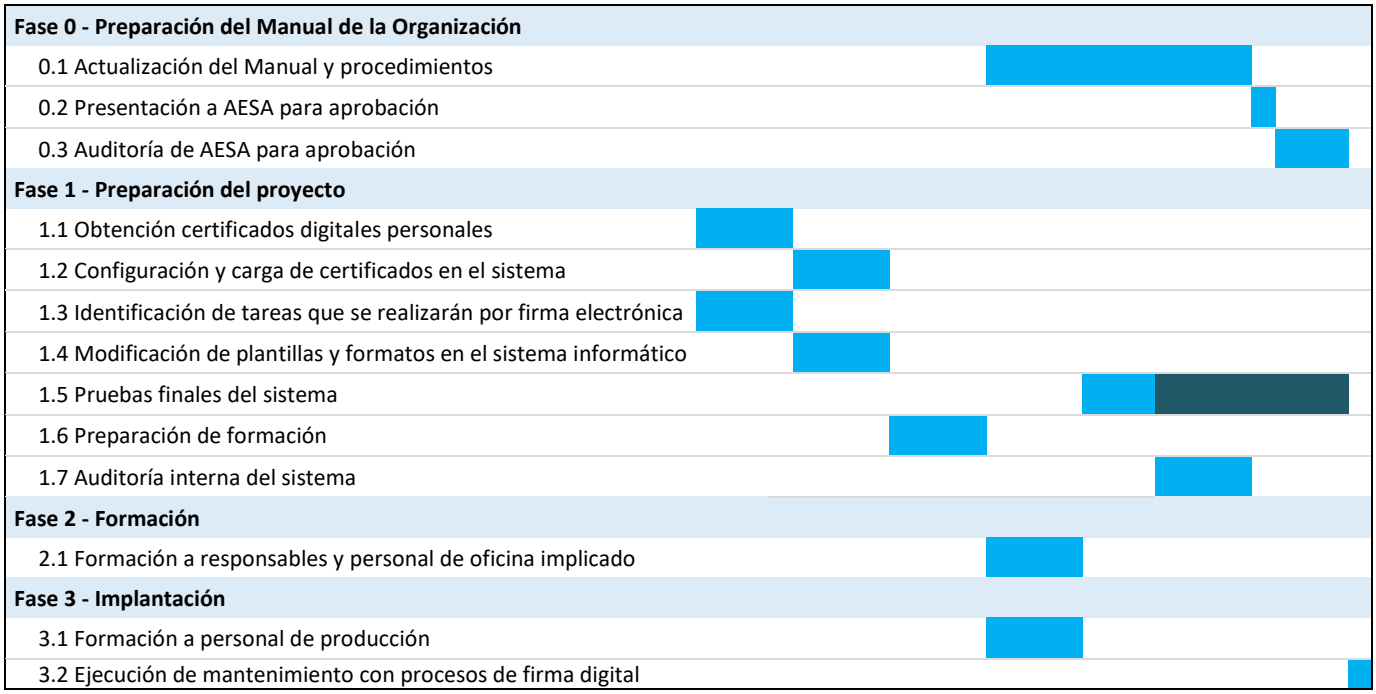
5. ANEXO I: PLAN DE TRANSICIÓN ORGANIZACIONES

A continuación, se traslada una propuesta de transición para la implementación del sistema de firma electrónica en una organización desde un sistema de firma tradicional manuscrita con sellos.

Esta propuesta deberá ser adaptada por cada organización, en función del alcance del sistema de firma electrónica propuesto y del tamaño de la propia organización, y a su vez, acordada con el Principal a cargo de la supervisión de AESA.

El plan de transición se podrá desarrollar en el propio manual o como un manual aparte siempre que esté acordado con el Principal a cargo de la supervisión de AESA y debidamente asociado al manual correspondiente (MOP, MOE, CAE, CAME, MTOE, POE, DOH).

La propuesta establece varias fases que pueden realizarse de manera simultánea. El siguiente diagrama de Gantt expresa la propuesta:



El punto **"1.5 Pruebas finales del sistema"** se ha dividido en dos bloques:

a) El primer bloque : debería consistir en trabajo de mantenimiento real, certificado de manera tradicional, realizado simultáneamente en el sistema de firma electrónica.

b) El segundo bloque : en función de la complejidad del sistema de firma electrónica implantado, representa que una vez superadas las pruebas finales del sistema, el personal de producción y de oficina continúe usando el sistema de firma electrónica paralelamente al método tradicional de firma manuscrita para no perder pericia en el uso del sistema de firma electrónica hasta su puesta en servicio definitiva.

El punto **“0.3 Auditoría de AESA”** evaluará el manual de la organización y la correcta implantación del plan de transición, y podrá entrar a supervisar en mayor detalle cualquier fase (ejemplo: evaluación in-situ de la subfase **“1.5 Pruebas finales del sistema”**).

6. CAMBIOS RELEVANTES DE ESTA EDICIÓN

Los principales cambios introducidos se encuentran indicados en el apartado “registro de ediciones”, en la información relativa a esta edición.