Guía práctica para el nuevo perfil de archivero/a ante el archivo digital

Kit de supervivencia

para afrontar los retos de la Ley Foral 9/2026 de Archivos de Navarra



Gobierno de Navarra
Nafarroako Gobernua

Índice

BLOQUE 10. PRESERVACIÓN DE LA DOCUMENTACIÓN ELECTRÓNICA 3

FINALIDAD DEL BLOQUE 4

CONTEXTO Y CONCEPTOS CLAVE 5

1. El archivo digital seguro 6

2. Preservación digital de los documentos y expedientes electrónicos 8

2.1. Estrategias de preservación 8

2.2. La conversión de formatos: la estrategia más extendida 9

3. Preservación digital de formatos especiales: audiovisuales y fotografías 11

4. Documentos esenciales y preservación 12

PARA SABER MÁS 13

ESCENARIOS Y SITUACIONES HABITUALES 14

Escenario 1. Inclusión de nuevos formatos de preservación en la herramienta de archivo digital seguro 15

Escenario 2. Implementación de una herramienta de archivo digital seguro 17

Bloque 10

Preservación de la documentación electrónica

Finalidad del bloque

Este bloque proporciona el conocimiento esencial para garantizar la autenticidad, integridad y accesibilidad a largo plazo de los documentos y expedientes electrónicos custodiados por las administraciones públicas.

Las personas profesionales de archivo deben ser capaces de llevar a cabo estrategias de preservación digital que aseguren que la documentación electrónica mantenga su valor probatorio y archivístico a lo largo del tiempo, con independencia de la evolución tecnológica.



Comprender

las estrategias y mecanismos de preservación digital de documentos electrónicos.



Identificar

los retos específicos de la preservación en el entorno electrónico.



Aplicar

técnicas de conversión y migración de formatos en el archivo digital seguro.



Gestionar

la preservación de formatos especiales.

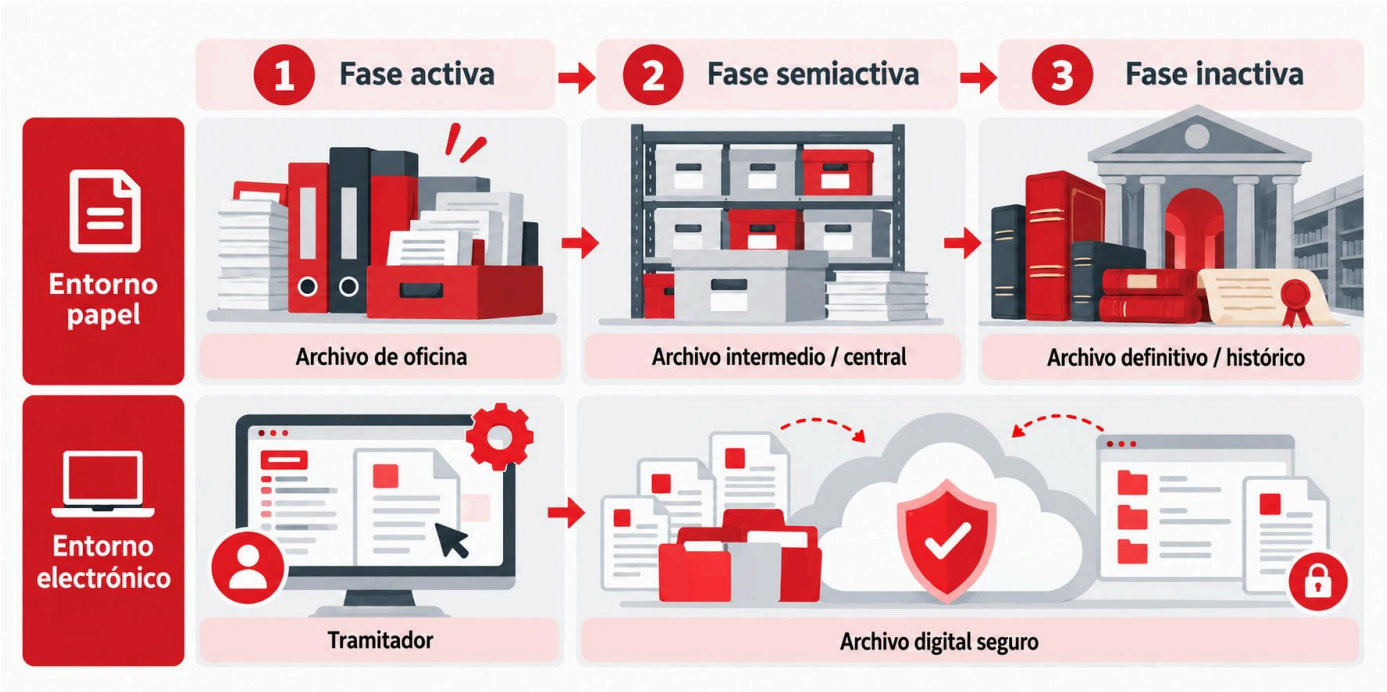
Contexto y conceptos clave



1. El archivo digital seguro

En el entorno papel, la documentación transitaba por una serie de archivos que respondían a las diferentes fases del ciclo de vida: el archivo de oficina, el archivo central o intermedio y el archivo definitivo o histórico.

En el mundo electrónico, esta estructura de archivos físicamente diferenciados ya no es necesaria: un único repositorio digital puede custodiar el expediente desde su cierre hasta su eliminación o conservación permanente. Es lo que se conoce como **archivo digital seguro** o **archivo electrónico único**.



El concepto de **plataforma de archivo digital seguro** procede de la Ley Foral 9/2026, la cual, en su artículo 3 ac), lo define como:

> **Un sistema de información que sirve de soporte a la gestión documental en una organización y que constituye el archivo electrónico único previsto en la legislación administrativa.**

El paralelismo entre archivo digital seguro y archivo electrónico único deriva de la regulación contenida en los artículos 24, 36 y 72 de dicha ley. En particular, el artículo 36.1 y 36.3 establece que:

> Las administraciones públicas de Navarra y sus sectores públicos institucionales se dotarán de una plataforma de archivo digital seguro, como repositorio corporativo con funcionalidad de archivo electrónico único, para la **gestión de los documentos y expedientes electrónicos en sus fases semiactiva o de vigencia e inactiva o histórica** […].
>
> La plataforma de archivo digital seguro garantizará el mantenimiento a largo plazo de las características de **autenticidad, fiabilidad, integridad** y **disponibilidad** de los documentos y expedientes electrónicos. Asimismo, proporcionará los servicios asociados a las funcionalidades que sean adecuadas en cada caso en cuanto a su accesibilidad, conservación y portabilidad entre distintas plataformas de archivo digital seguro.

El archivo digital seguro no es simplemente un repositorio de almacenamiento, sino un entorno tecnológico y organizativo que garantiza que los documentos y expedientes electrónicos que se custodian cumplen, a lo largo del tiempo, los siguientes **requisitos**:

Autenticidad

Los documentos son lo que dicen ser y han sido creados o enviados por quien se indica.

Fiabilidad

El contenido del documento puede considerarse una representación completa y precisa de las operaciones, actividades o hechos que testimonia, de modo que pueda confiarse en él en el curso de operaciones o actividades posteriores.

Integridad

Los documentos están completos y no han sido alterados.

Disponibilidad

Los documentos pueden recuperarse y visualizarse durante todo el tiempo que sea necesaria su conservación.

Trazabilidad

Existe un registro de todas las acciones realizadas sobre los documentos (ingresos, consultas, conversiones, eliminaciones…).



2. Preservación digital de los documentos y expedientes electrónicos

La preservación digital comprende el conjunto de actividades, políticas y estrategias orientadas a garantizar que los objetos digitales —documentos, expedientes, metadatos y firmas— se mantengan auténticos, íntegros y accesibles durante todo el tiempo que deban ser conservados.

A diferencia de la conservación en soporte papel, la preservación digital debe afrontar dos **retos específicos:**

Obsolescencia tecnológica

La obsolescencia tecnológica de los formatos y de los soportes de almacenamiento y, a su vez, la dependencia de software y hardware específicos para la interpretación de los documentos.

Un documento en un formato que ya no es compatible con ningún visor disponible es, en la práctica, ilegible.

Cadena de custodia y trazabilidad

La necesidad de mantener la cadena de custodia y la trazabilidad de todas las acciones realizadas sobre la documentación. A diferencia del papel, donde la custodia es física y visible, en el entorno electrónico la integridad y la autenticidad de los documentos dependen de mecanismos técnicos y organizativos que deben diseñarse y mantenerse de forma activa.

2.1. Estrategias de preservación

Existen diversas estrategias para garantizar la accesibilidad e interpretabilidad de los documentos electrónicos a largo plazo. Su elección depende del tipo de objeto digital, de su formato original, del horizonte temporal de conservación y de los recursos disponibles:

- **Conversión de formatos**

  Consiste en transformar los documentos de su formato original a otro con mejores garantías de preservación a largo plazo —generalmente un formato abierto y ampliamente adoptado—, generando una copia electrónica auténtica con cambio de formato.

  Es la estrategia más habitual y recomendada en el ámbito de las administraciones públicas.

- **Emulación**

  Consiste en reproducir el entorno tecnológico original —hardware y software— en el que fueron creados los documentos, de modo que puedan seguir siendo interpretados sin modificar el objeto digital.

  Es adecuada para objetos digitales complejos o interactivos que no pueden migrarse sin pérdida significativa de contenido.

  Su aplicación es más frecuente en archivos históricos.

- **Migración**

  Consiste en el traslado de documentos y expedientes electrónicos de un sistema o soporte a otro, garantizando la integridad de la información y la trazabilidad del proceso. ·

  Puede darse en diferentes supuestos: desde unidades de red o carpetas compartidas hacia el archivo digital seguro; desde soportes físicos de almacenamiento, como CD-ROM, DVD u otros medios externos, hacia el archivo digital seguro; o desde un archivo digital seguro hacia otro nuevo.

  No debe confundirse la migración con la conversión de formatos, que opera a nivel de fichero.

- **Soporte papel y microfilm**

  Para documentos con plazos de conservación muy prolongados o valor histórico, puede ser pertinente complementar la preservación digital con la generación de copias en soportes físicos de alta durabilidad.

  En este sentido, el microfilm constituye un soporte con garantías de durabilidad superiores al siglo, independiente de cualquier tecnología. Su uso no exime de preservar los documentos en formato electrónico, pero puede ser una medida adicional de seguridad para series documentales críticas.

ⓘ Las personas profesionales de archivo deben liderar la definición de la estrategia de preservación digital de la organización y coordinar su implementación con el área de TIC.

2.2. La conversión de formatos: la estrategia más extendida

La conversión de formatos es la estrategia de preservación más recomendada y extendida, ya que actúa directamente sobre el fichero y es compatible con la lógica de funcionamiento del archivo digital seguro. Se trata de un proceso de transformación de los documentos de un formato a otro que genera, por consiguiente, una **copia electrónica auténtica con cambio de formato**.

La conversión se lleva a cabo, normalmente, en la herramienta de archivo digital seguro. Este proceso comprende los siguientes pasos:

01

Detección

La plataforma de archivo digital seguro identifica de forma automática los documentos cuyos formatos están en riesgo de obsolescencia y envía un aviso a las personas profesionales de archivo para que autoricen la conversión y seleccionen los formatos de destino. Estos formatos deben adecuarse a lo establecido en el catálogo de formatos electrónicos corporativo.

NOTA: Muchas de las plataformas de archivo digital seguro del mercado ya proponen los formatos de conversión de destino cuando identifican formatos obsoletos.

02

Conversión y generación de la copia auténtica

Las personas profesionales de archivo seleccionan el formato de destino y autorizan la conversión, y el archivo digital seguro la ejecuta de forma automática. El documento resultante es una copia electrónica auténtica firmada con el sello electrónico de órgano de la organización, que debe identificarse como "EE02 – Copia electrónica auténtica con cambio de formato" mediante el metadato "Estado de elaboración".

03

Actualización del índice electrónico del expediente

La copia auténtica con cambio de formato se incorpora automáticamente al expediente. El índice ENI se actualiza en consecuencia, reflejando el nuevo documento, su *hash* y sus metadatos asociados.

04

Eliminación o conservación del original

La organización debe determinar, siguiendo su política de preservación, si el documento original en el formato obsoleto se elimina, conservando únicamente la copia auténtica, o si se mantienen ambos documentos en el expediente. En cualquier caso, debe quedar registro de la decisión y del proceso ejecutado.

Lo más recomendable en estos casos es mantener el documento electrónico original únicamente en el caso que la obtención de la copia implique una pérdida de calidad respecto al documento electrónico original. De no ser así, el original puede eliminarse.

3. Preservación digital de formatos especiales: audiovisuales y fotografías

Los documentos en formato audiovisual (vídeo y audio) y fotográfico presentan retos adicionales de preservación, tanto por el volumen que suelen ocupar como por la mayor diversidad de formatos y la dependencia de códecs específicos para su reproducción.

Para la preservación este tipo de objetos digitales, deben tenerse en cuenta las siguientes consideraciones:

- ## Selección de formatos de preservación

  Se recomienda utilizar formatos abiertos y ampliamente adoptados.

  - Para **fotografías**: los formatos TIFF (sin compresión) o PNG ofrecen garantías superiores al JPEG.
  - Para **vídeo y audio**: los formatos sin compresión o con compresión sin pérdida son preferibles; entre los más recomendados se encuentran FFV1 (vídeo), FLAC o WAV (audio).

  Dado que la evolución tecnológica permite obtener progresivamente copias de mayor calidad a partir del soporte original —especialmente en el caso de materiales de origen analógico digitalizados (cinta magnética, película)—, **se recomienda conservar siempre el original en documentos audiovisuales, con independencia de que se hayan generado copias en formatos de preservación**.

- ## Metadatos técnicos

  Además de los metadatos de gestión documental habituales, los objetos audiovisuales y fotográficos requieren la captura y conservación de metadatos técnicos específicos (resolución, códec, tasa de bits, perfil de color…) que son imprescindibles para garantizar su correcta interpretación en el futuro.

- ## Volumen y almacenamiento

  El tamaño de los ficheros audiovisuales puede ser muy superior al de los documentos textuales, lo que tiene implicaciones en términos de almacenamiento y de rendimiento del archivo digital seguro. Deben planificarse las necesidades de almacenamiento y, si procede, establecer estrategias de almacenamiento diferenciado para los objetos menos consultados.

- ## Consulta y acceso

  Debe garantizarse que el archivo digital seguro permite la visualización o reproducción de los documentos audiovisuales y fotográficos. En caso contrario, deberá preverse la generación de versiones de acceso que faciliten la consulta sin comprometer las copias de preservación.

4. Documentos esenciales y preservación

En el entorno electrónico, surge a menudo la pregunta de si los documentos esenciales necesitan medidas de preservación adicionales a las que ya aplica el archivo digital seguro. La respuesta requiere matizar.

El archivo digital seguro aplica medidas generales de preservación a **toda** la documentación que custodia, como copias de seguridad, control de integridad o registro de acciones. En este sentido, podría considerarse que los documentos esenciales no requieren, por su mera condición de esenciales, estrategias de preservación adicionales a las del resto de la documentación.

Sin embargo, sí puede ser pertinente adoptar **medidas adicionales de protección** para este tipo de documentos, orientadas no tanto a la preservación de su contenido como a garantizar su disponibilidad en situaciones excepcionales:

- ### Copias de seguridad reforzadas

  Copias de seguridad con mayor frecuencia o en ubicaciones geográficamente separadas (redundancia geográfica) o en servidores geográficamente distribuidos, para reducir el riesgo de pérdida ante desastres que afecten a las instalaciones físicas del archivo digital seguro.

- ### Inclusión en el plan de contingencia, continuidad y gestión de riesgos de la organización

  Los documentos esenciales deben estar expresamente contemplados en dicho plan, con procedimientos específicos que garanticen su accesibilidad prioritaria en situaciones de emergencia.

- ### Migración urgente de documentos esenciales fuera del sistema de gestión documental

  Si existen documentos esenciales almacenados fuera del archivo digital seguro —en unidades de red, soportes físicos u otros sistemas—, su migración debe abordarse de forma prioritaria. La organización debe tener previamente identificados estos documentos mediante el catálogo de documentos esenciales.

Para que el archivo digital seguro pueda identificar automáticamente los documentos esenciales, es imprescindible que el metadato eEMGDE13.4 – Documento esencial, esté correctamente informado desde la fase de tramitación (véase el **bloque 5. Diseño del sistema de gestión documental e implantación de los instrumentos de gestión documental, apartado 8. Documentos esenciales**).

Para saber más

Normativa

- 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 Foral 9/2026, de 20 de mayo, de Archivos, Gestión de Documentos y Patrimonio Documental de Navarra.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de Estándares.

Estándares UNE-ISO

- UNE-ISO 15489-1:2016. Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios.
- UNE-ISO 14721:2015. Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.

Escenarios y situaciones habituales

Escenario 1. Inclusión de nuevos formatos de preservación en la herramienta de archivo digital seguro

Situación

La aparición de un nuevo formato de preservación –ya sea por su inclusión en la Norma Técnica de Interoperabilidad de Catálogo de Estándares, por ofrecer mayores garantías que los formatos admitidos hasta ese momento o por la necesidad de gestionar nuevos tipos de objetos digitales–, requiere una revisión y actualización del catálogo de formatos electrónicos de la organización, así como su configuración en la herramienta de archivo digital seguro para permitir su uso.

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Análisis de la necesidad de incorporación. Determinar si existe una necesidad real de incorporar el nuevo formato, ya sea por requerimientos de herramientas corporativas o por la necesidad de gestionar nuevos tipos de objetos digitales.

Asimismo, debe evaluarse si los requisitos identificados pueden satisfacerse mediante alguno de los formatos ya incluidos en el catálogo de formatos de la organización. La incorporación de nuevos formatos debe realizarse de forma restrictiva, evitando incrementar innecesariamente la diversidad de formatos admitidos cuando existan alternativas equivalentes ya contempladas en el catálogo.

2. Evaluación técnica del nuevo formato. Antes de incorporarlo al catálogo de la organización, debe analizarse si el formato está reconocido en la Norma Técnica de Interoperabilidad de Catálogo de Estándares –salvo que el propio formato haya sido introducido por una actualización de dicha norma– o en el registro internacional PRONOM, y si cuenta, por consiguiente, con garantías de preservación a largo plazo. Esta evaluación debe realizarse en coordinación con el área de TIC.

3. Actualización del catálogo de formatos. La inclusión de un nuevo formato de preservación implica la actualización del catálogo de formatos.

4. Configuración de la herramienta. Una vez aprobado el nuevo formato, el área de TIC procederá a su configuración en el archivo digital seguro, de modo que la herramienta lo reconozca y pueda gestionar los documentos con ese formato.

5. Comunicación del cambio. El personal tramitador debe ser informado de los nuevos formatos admitidos, especialmente si el cambio afecta a los formatos en los que se debe presentar la documentación en el marco de los procedimientos administrativos.

Escenario 2. Implementación de una herramienta de archivo digital seguro

Situación

La organización debe implementar una herramienta de archivo digital seguro. Este escenario puede responder tanto a la necesidad de implantar una solución por primera vez como a la de sustituir la herramienta actualmente en uso.

> La contratación de una nueva herramienta de archivo digital seguro requiere que las personas profesionales de archivo lideren el proceso o, como mínimo, participen activamente en él. El área de TIC no puede decidir de forma unilateral, ya que tiene implicaciones archivísticas y documentales que van más allá de la infraestructura tecnológica.

> En este escenario se dan unas pautas básicas sobre los pasos a seguir para contratar una herramienta de archivo digital seguro. Dado que la implementación de una plataforma de estas características constituye un proceso complejo, se ha redactado un bloque específico sobre esta materia. **Véase bloque 17. Hacia un archivo digital seguro: hoja de ruta.**

Decisiones operativas

Antes de preparar la licitación, se identificarán los criterios mínimos tanto de la metodología a seguir por el proveedor como de la herramienta a contratar. En este sentido, es recomendable:

1. Establecer el alcance del proyecto. ¿Se tratará únicamente de una integración del archivo digital seguro con el gestor de expedientes, o incluirá también migración de documentos desde otros sistemas o aplicaciones? En el caso de migración, ¿cuáles serán las aplicaciones desde las que se deberán migrar los documentos? ¿Cuál será el volumen aproximado de documentación a migrar?

2. Identificar los requisitos mínimos funcionales que debería cumplir una herramienta de archivo digital seguro. Algunos de ellos son los siguientes:

- Tener un proceso de ingesta que, a través de un conjunto de procesos, permita incluir y almacenar objetos digitales en la plataforma.

- Contar con procesos internos de preservación proactivos que aseguren la ejecución controlada de los procesos de conversión de formatos, el resellado de firmas y otros procesos (por ejemplo, control de consistencia de *hash*) que puedan necesitar aplicarse a objetos digitales para garantizar su preservación y preservación a largo plazo.
- Contar con mecanismos de recuperación que permitan la búsqueda e identificación de objetos digitales, tanto contenido como metadatos.
- Contar con un sistema que le permita explotar información contextual y generar informes de actividad.
- Contar con medidas de seguridad y control para garantizar la protección de los objetos digitales frente a la alteración intencionada o accidental de su contenido, estructura y contexto.
- Permitir la creación y gestión de un número ilimitado de colecciones documentales.
- Permitir crear, añadir y mantener clasificaciones para cada fondo.
- Permitir la definición y configuración del esquema de metadatos especificando la naturaleza obligatoria, opcional y condicional de cada metadato.
- Incorporar los metadatos mínimos obligatorios definidos en la Normas Técnicas de Interoperabilidad de Documento y Expediente Electrónicos, la Norma Técnica de Interoperabilidad de Digitalización de Documentos y la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como el resto de los metadatos del e-EMGDE.
- Incorporar esquemas específicos de metadatos para la preservación de objetos digitales, especialmente METS y PREMIS.
- Permitir el mantenimiento de los metadatos y la correcta gestión del historial de eventos de los objetos, de acuerdo con los planes de contingencia, en caso de obsolescencia del software o hardware que los contenía.
- Garantizar la aplicación de las tablas de valoración y acceso a documentos y del calendario de conservación.
- Certificar la eliminación de objetos generando un informe de eliminación firmado electrónicamente o con sello electrónico de órgano con sello de tiempo que puedan descargarse del sistema, y que puedan certificar tanto la eliminación de un único documento electrónico o archivo electrónico o conjuntos de ellos, según lo solicite el usuario.
- Generar un registro de eliminación y todas las pistas de auditoría asociadas a la eliminación.
- Permitir las consultas y préstamos (PIT).
- Contar con un sistema que permita la difusión de la información contenida en el archivo a terceros, a través de una solución como un Portal, teniendo en cuenta las normas que afectan a la propiedad intelectual y la protección de datos.

3. Identificar las fases del proyecto, que, como mínimo, deberían contemplar:

- **Documentación preliminar.** Antes de iniciar el proyecto, el proveedor debe conocer cuál es la situación actual de la organización en materia de gestión documental (entorno tecnológico sobre el que se deberá implementar la nueva herramienta, procesos de gestión documental existentes en la organización…).

En el caso de existir una migración, será necesario, además, que se realice un inventario completo de los objetos a migrar: expedientes, documentos, metadatos, índices, históricos de acciones, tablas de valoración configuradas…

- **Instalación, parametrización e integración**. Se deberá contemplar una fase específica de instalación, configuración e integración del archivo digital seguro en. Se recomienda que la herramienta se pueda instalar en modalidad OnPremise y que la configuración se adecue a la política y modelo de gestión documental de la organización.
- **Migración**. En el caso que se contemple la migración en el proyecto, esta se realizará en fases, comenzando por series documentales menos críticas, para detectar y corregir posibles problemas antes de trasladar la documentación más sensible o voluminosa. Se deberá controlar que toda la información es migrada y que no existe pérdida de datos.

  Dada la complejidad de un proceso de migración, se recomienda que el proveedor establezca una hoja de ruta para llevarlo a cabo.

- **Definición del protocolo de validación o plan de pruebas.** Deben establecerse los criterios y las pruebas que permitirán verificar que todos los procesos se ejecutan correctamente: cotejo de *hash*, verificación de metadatos, comprobación de acceso a los documentos…
- **Mantenimiento del acceso al sistema antiguo.** En el caso de migración de un archivo digital seguro a otro, durante un período de tiempo suficiente tras la migración debe mantenerse el acceso al sistema antiguo en modo de solo lectura, a fin de poder recuperar cualquier documento o dato que pudiera no haberse trasladado correctamente.
- **Mantenimiento y soporte**. Una vez finalizada la integración y/o la migración, se deberá requerir mantenimiento y soporte continuado al proveedor para resolver dudas o realizar cualquier corrección en el sistema.
- **Formación**. Serán necesarias sesiones formativas dirigidas a diferentes tipos de usuario para garantizar que la nueva herramienta se pueda utilizar con autonomía por parte del personal de la organización.

⚠ Un proyecto de implementación de un archivo digital seguro, así como un proceso de migración mal planificado o ejecutado, puede comprometer de forma irreversible la integridad y la accesibilidad de la documentación. Por este motivo, **la participació activa y continuada del personal responsable de archivo constituye un requisito esencial para el éxito del proyecto,** debiendo intervenir en todas sus fases, desde la definición de requisitos y la contratación de la solución hasta la validación final de su implementación.