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 9. TRANSFERENCIA, INGESTA Y DISPOSICIÓN DOCUMENTAL	**3**
FINALIDAD DEL BLOQUE	4
CONTEXTO Y CONCEPTOS CLAVE	5
1. Transferencia de documentación	6
2. Ingesta de documentación	9
3. Paquetes de información OAIS	10
4. Disposición documental	13
PARA SABER MÁS	21
ESCENARIOS Y SITUACIONES HABITUALES	22
Escenario 1. No se realizan transferencias desde las unidades tramitadoras	23
Escenario 2. Transferencia de expedientes incompletos o conformados incorrectamente	25
Escenario 3. Transferencia de expedientes de larga tramitación que deban seguir abiertos	29
Escenario 4. Ingesta de documentación procedente de otras fuentes distintas al gestor de expedientes	31
Escenario 5. Gestión del acceso a la documentación transferida por parte de las unidades tramitadoras	34
Escenario 6. Disposición de los expedientes híbridos	36

Bloque 9

Transferencia, ingesta y disposición documental

Finalidad del bloque

Este bloque tiene como finalidad comprender cómo se preparan y ejecutan las transferencias de expedientes desde las herramientas de tramitación al archivo digital seguro, tanto si el proceso está automatizado como si no lo está, así como las comprobaciones que se deben realizar desde el archivo para aceptarlas o rechazarlas.

Este bloque también tiene como objetivo facilitar que las personas profesionales de archivo comprendan la diferencia entre transferencia e ingesta, cómo se transforman los expedientes recibidos en paquetes de información para poder ser tratados y preservados por el archivo digital seguro, y cómo se debe gestionar la aplicación de las acciones de disposición sobre la documentación en el archivo digital seguro.



Comprender

los procesos de transferencia de expedientes desde las herramientas de tramitación al archivo digital seguro, tanto en entornos automatizados como no automatizados, así como las comprobaciones necesarias para su aceptación o rechazo.



Identificar

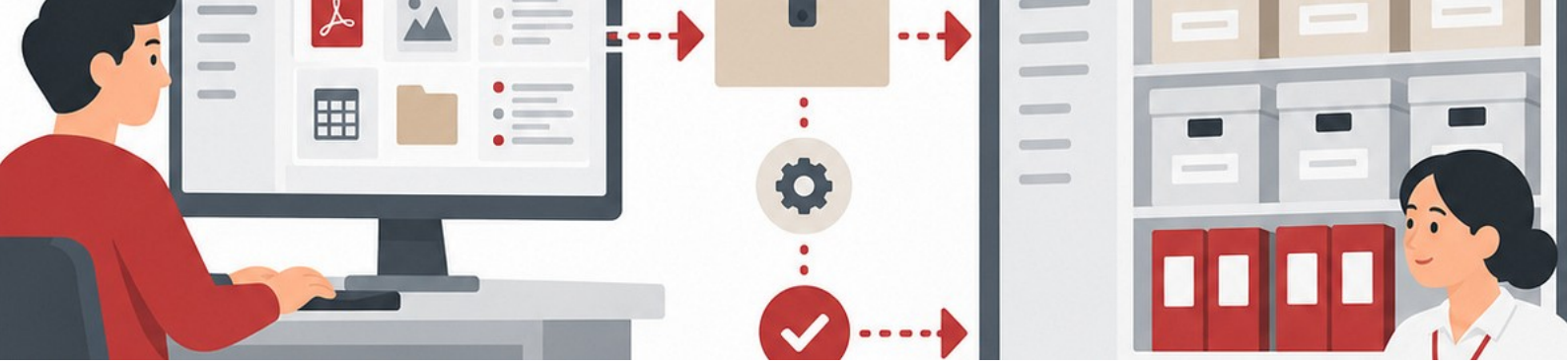
las diferencias entre los procesos de transferencia e ingesta, las características de los paquetes de información, así como los elementos relacionados con la disposición de la documentación.



Conocer

la transformación de los expedientes en paquetes de información para su tratamiento y preservación en el archivo digital seguro, así como la gestión y aplicación de las acciones de disposición sobre la documentación archivada.

Contexto y conceptos clave



1. Transferencia de documentación

La **transferencia** es el proceso mediante el cual se produce un cambio tanto en la custodia y responsabilidad sobre los documentos y expedientes electrónicos finalizados, que pasan de la unidad tramitadora al archivo, como en su ubicación, que pasa del gestor de expedientes al archivo digital seguro.

Las transferencias pueden ser:

Transferencia manual

Implica que el inicio del proceso de transferencia lo debe realizar, manualmente, una persona mediante la selección de los expedientes correspondientes y, posteriormente, peticionar la transferencia a través de los medios que correspondan para que la persona profesional de archivo la acepte o la rechace.

En este caso, corresponde al personal de la unidad tramitadora comprobar que los expedientes cumplen con los requisitos para ser transferidos.

Transferencia automática

En este supuesto no es necesario que una persona seleccione los expedientes y peticione su transferencia al archivo. El sistema aplica unas reglas previamente definidas para localizar todos los expedientes cerrados de ciertas series documentales que cumplan las condiciones para ser transferidos. El gestor de expedientes, automáticamente, identifica los expedientes a transferir, ejecuta las validaciones técnicas, genera los paquetes de información de transferencia y los remite al archivo digital seguro.

En ambos casos, deben distinguirse las siguientes responsabilidades en el proceso:

Unidad tramitadora

Es la responsable de finalizar correctamente el expediente, cerrarlo y asegurarse de que está en condiciones de ser transferido (constan todos los documentos de forma ordenada, no obran borradores o documentación de trabajo, están informados los metadatos, etc.).

Personal autorizado

En el caso de que la transferencia sea manual, la responsabilidad de iniciar y llevar a cabo el proceso de transferencia puede corresponder al personal de la unidad tramitadora o, si así se establece internamente, a las personas profesionales de archivo.



Gestor de expedientes

En el caso de que la transferencia sea automática, y en función de los parámetros configurados previamente, el gestor de expedientes es el responsable de ejecutar las validaciones correspondientes sobre los expedientes y, posteriormente, aplicar las reglas que permiten ejecutar el proceso.



Archivo

Le corresponde establecer los requisitos técnicos y archivísticos de aceptación de las transferencias, así como supervisar la ejecución del proceso, recibir, revisar y validar los paquetes de información y decidir si se acepta o se rechaza la transferencia.

⚠ A nivel organizativo y para asegurar la eficacia y eficiencia de la operativa, es recomendable que la unidad tramitadora sea la responsable de preparar, revisar y poner el expediente a disposición para su transferencia y el archivo de validar y aceptar, si corresponde, su ingreso.

Comprobaciones antes de ejecutar la transferencia

Antes de realizar las transferencias de la documentación, se deben llevar a cabo una serie de comprobaciones:

Comprobaciones automáticas

Antes de empezar el proceso de transferencia, la mayoría de las herramientas de **gestión de expedientes** llevan a cabo las siguientes comprobaciones y validaciones:

- Revisar si existen firmas electrónicas y si estas son válidas.
- Controlar los formatos de los documentos, tanto los aceptados como no aceptados por la administración, así como aquellos que son de preservación.
- Comprobar la integridad de la documentación que obra en el expediente.
- Constatar la existencia del índice electrónico y el foliado del expediente.
- Que los metadatos mínimos obligatorios estén informados.

Comprobaciones manuales

Antes de empezar el proceso de transferencia, la **unidad tramitadora** debe revisar y comprobar los siguientes aspectos:

- El procedimiento ha finalizado y el expediente está cerrado. Por consiguiente, se debe haber generado el foliado y el índice del expediente electrónico.
- El expediente está correctamente clasificado en la serie documental del Cuadro de Clasificación que les corresponde y contiene todos los documentos que deben formar parte de él, sin presencia de borradores, documentación de trabajo o auxiliar ni duplicados.
- Los documentos están correctamente ordenados, tienen informada correctamente la tipología documental, se corresponden a versiones definitivas y disponen de las firmas exigibles.
- Los documentos que constan en el índice coinciden con los que obran en el expediente y disponen de sus respectivos resúmenes criptográficos.
- Están correctamente informados los valores de los metadatos mínimos obligatorios a nivel de expediente y de documento, así como aquellos condicionales y complementarios.
- En caso de existir relaciones con otros expedientes u objetos del sistema, comprobar que las vinculaciones correspondientes existen y son vigentes.
- En el caso de expedientes híbridos, los documentos en soporte físico están debidamente vinculados con el expediente electrónico, identificados y localizados en la ubicación física correspondiente.

⚠ Si existen discrepancias o incongruencias después de realizar estas comprobaciones, la unidad tramitadora deberá revisarlas y solucionarlas antes de proceder al inicio de la transferencia.



2. Ingesta de documentación

La ingesta es el proceso que se lleva a cabo en el momento en que los **paquetes de información de transferencia (PIT)**, procedentes del gestor de expedientes, ingresan en el archivo digital seguro.

Es durante la ingesta que se realizan los **controles** sobre la estructura de los paquetes de información relativos a su integridad, los formatos de la documentación, la validez y vigencia de las firmas o la completitud de los metadatos, entre otros.

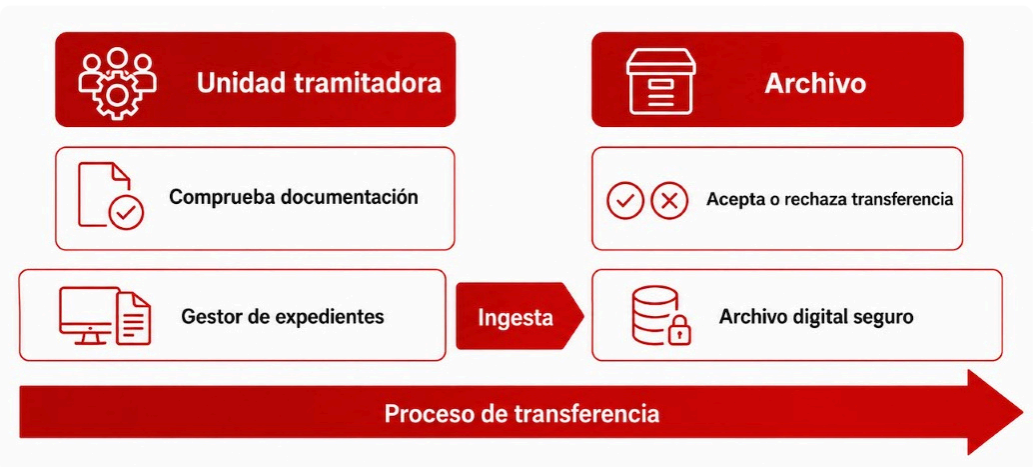
Si las comprobaciones son satisfactorias, la documentación es aceptada y se genera el correspondiente **paquete de información de archivo (PIA)**.

Si se detecta cualquier incongruencia o inexactitud, **se rechaza la ingesta** y se devuelve la transferencia a la unidad tramitadora.

Diferencias entre la transferencia y la ingesta

La **transferencia** se refiere a la totalidad del proceso de cambio de responsabilidad y ubicación de la documentación, desde que la unidad tramitadora la inicia hasta que el archivo la valida o rechaza. Incorpora el conjunto de comprobaciones que se llevan a cabo sobre el contenido y la estructura del expediente, por parte de la unidad tramitadora, con carácter previo a solicitar el envío de la documentación al archivo.

En cambio, la **ingesta** se refiere exclusivamente al proceso técnico en el que la documentación que se está transfiriendo desde el gestor de expedientes, en forma de paquetes de información, ingresa en la herramienta de archivo digital seguro.





3. Paquetes de información OAIS

El **modelo OAIS**, desarrollado en la **norma ISO 14721**, utiliza el concepto de paquete de información para representar la información, correspondiente a documentos u otros objetos digitales, que ingresa, se preserva y se difunde para su consulta en el archivo digital seguro.

Un **paquete de información** es una **agrupación lógica (contenedor)** que utilizan los sistemas de archivo digital para **mantener de forma agrupada un contenido (información principal)** junto con la **información** que lleva **asociada** y que es necesaria para **identificarlo, describirlo, interpretarlo,** comprobar su **integridad, preservarlo** y **recuperarlo** posteriormente.



Es importante destacar que un paquete de información **no tiene por qué corresponderse, necesariamente, con un fichero único**, sino que puede estar formado por varios objetos digitales con sus correspondientes metadatos, los cuales se relacionan y gestionan como una unidad.

En el ámbito de la documentación administrativa, por ejemplo, un paquete de información puede contener un expediente administrativo electrónico, integrado por sus documentos electrónicos, el índice electrónico, las firmas y los metadatos exigidos por el ENI y las NTI. En el momento de ingresar en el archivo digital seguro se puede incorporar, además, información específica relativa a su preservación.

Según el **modelo OAIS**, existen **tres paquetes de información** –ya mencionados anteriormente:

Paquete de información de transferencia (PIT)

Es el paquete que se genera en el gestor de expedientes y que contiene la documentación que el productor (la unidad tramitadora) remite al archivo para que esta ingrese en el archivo digital seguro.

Su característica principal es que todavía no constituye el paquete definitivo de preservación y, por consiguiente, durante el proceso de ingesta, puede ser rechazado o aceptado y, en caso de aceptación, puede ser complementado con la información correspondiente.

Este tipo de paquete puede incluir los siguientes elementos:

- Documentos y expedientes electrónicos.
- La estructura de estos y las relaciones entre ellos.
- Los respectivos metadatos.
- El índice electrónico del expediente.
- Información sobre las firmas electrónicas.
- Información relativa a la integridad, como los resúmenes criptográficos.
- Información necesaria para interpretar y validar la transferencia.

Paquete de información de archivo (PIA)

Es el paquete resultante de un proceso de ingesta satisfactorio y recoge la información que incorpora el PIT a la cual se le añade la información de preservación correspondiente en función de la estrategia de preservación por la cual se haya optado. Así pues, contiene el objeto que debe preservarse junto con la información necesaria para comprenderlo y conservarlo a largo plazo.

Este tipo de paquete puede incluir los siguientes ítems:

- Referencia: cómo identificar inequívocamente el objeto.
- Procedencia: de dónde procede y cuál ha sido su historia.
- Contexto: por qué fue creado y cómo se relaciona con otros objetos del sistema.
- Integridad: información que permite comprobar que el objeto no ha sido alterado indebidamente.
- Derechos de acceso: condiciones que afectan a su utilización.
- Información necesaria para interpretar correctamente los formatos y ficheros digitales que integran el objeto.

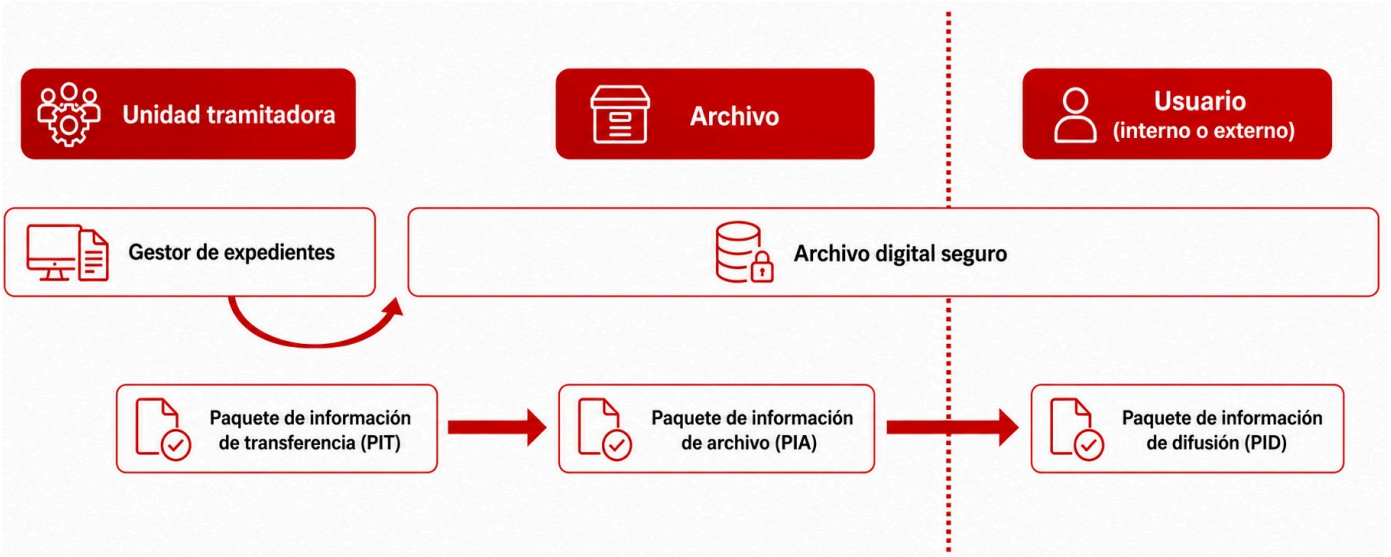
Paquete de información de difusión (PID)

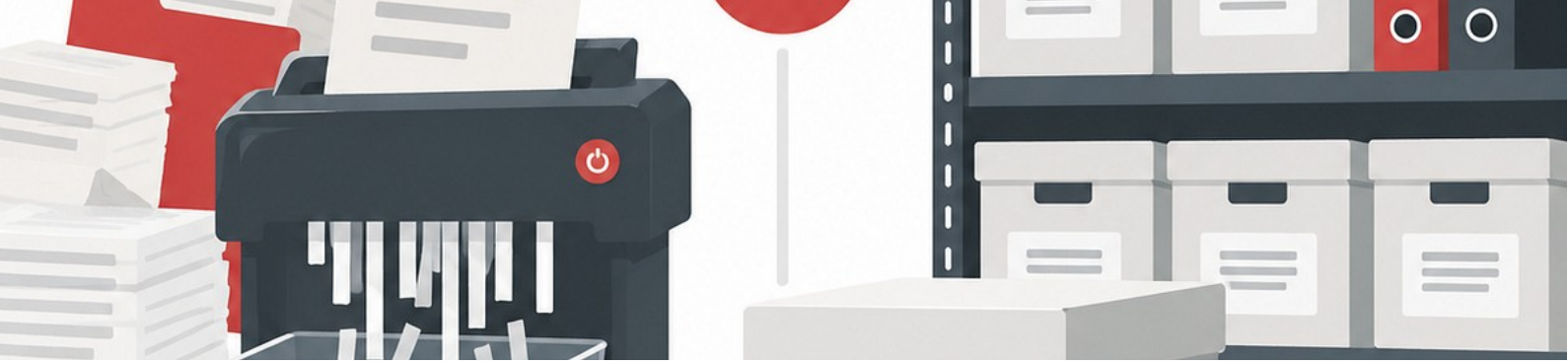
Es el paquete que genera el archivo digital seguro para proporcionar la información que solicita un usuario, sea interno de la organización o externo. Su razón de ser es servir la información solicitada sin alterar el paquete de archivo, que es el que sirve para asegurar la preservación de la información. A nivel lógico, el PIA permanece bajo custodia del archivo, mientras que el PID se genera, y comparte para satisfacer una necesidad concreta de acceso a un usuario.

Es importante destacar que, en este caso, el contenido de un PID tanto puede corresponderse al de un PIA, como a una parte de este o bien ser una agrupación de los contenidos de distintos PIA.

Este tipo de paquete puede incluir los siguientes elementos:

- El objeto de datos, que se puede corresponder con el propio documento o conjunto de documentos solicitados por el usuario y que deben estar en el formato correspondiente para entregarse al usuario, que puede ser distinto del formato de conservación del PIA.
- Información de representación que corresponde a la información necesaria para que el usuario pueda interpretar el contenido del objeto de datos.





4. Disposición documental

La **disposición** es el proceso que refiere a la decisión razonada sobre los plazos de conservación, eliminación o transferencia que debe tener cada serie documental, es decir, las acciones que se deben aplicar sobre los documentos, con independencia de su soporte, una vez estos han perdido su valor primario, y en base a un conjunto de análisis, decisiones y actuaciones previas.

Las acciones de disposición se ejecutan en el archivo digital seguro y pueden implicar la eliminación (destrucción), la conservación (retención) o la transferencia de los documentos a otra entidad y/o sistema.

Los principales estándares técnicos establecen, en concreto, **cuatro acciones de disposición**:

Eliminación

Se refiere a la destrucción, lógica o física, de la documentación u otros activos de información, de manera que no sea posible recuperar su contenido ni características.

Se trata de una acción irreversible, por lo que debe ejecutarse de forma controlada y segura y en base a lo que establezca la correspondiente tabla de valoración documental.

Conservación

Implica el mantenimiento, por un período de tiempo concreto o de forma indefinida, de la autenticidad, la integridad, la disponibilidad y el acceso al contenido y contexto de los documentos.

En el ámbito de la documentación electrónica, implica aplicar la/s estrategia/s de preservación correspondiente/s, de acuerdo con lo que se explica en el **bloque 10** de la presente guía, en la herramienta de archivo digital seguro, mientras que en el ámbito de la documentación en papel implica asegurar la condiciones ambientales y materiales para asegurar la conservación a largo plazo del soporte en cuestión.



Transferencia

Consiste en el traslado de la custodia, el control y la responsabilidad de la gestión de la documentación o los activos de información desde la organización productora –y sus sistemas de información– hacía a otra organización y/o sistema de información externo, garantizando en todo momento la continuidad de su autenticidad, integridad y accesibilidad tras el cambio de custodia.



Revisión

Consiste en llevar a cabo un nuevo análisis respecto a una serie, expediente, documento o activo de información con el fin revisar y, si corresponde, modificar la acción de disposición inicialmente prevista sobre este.

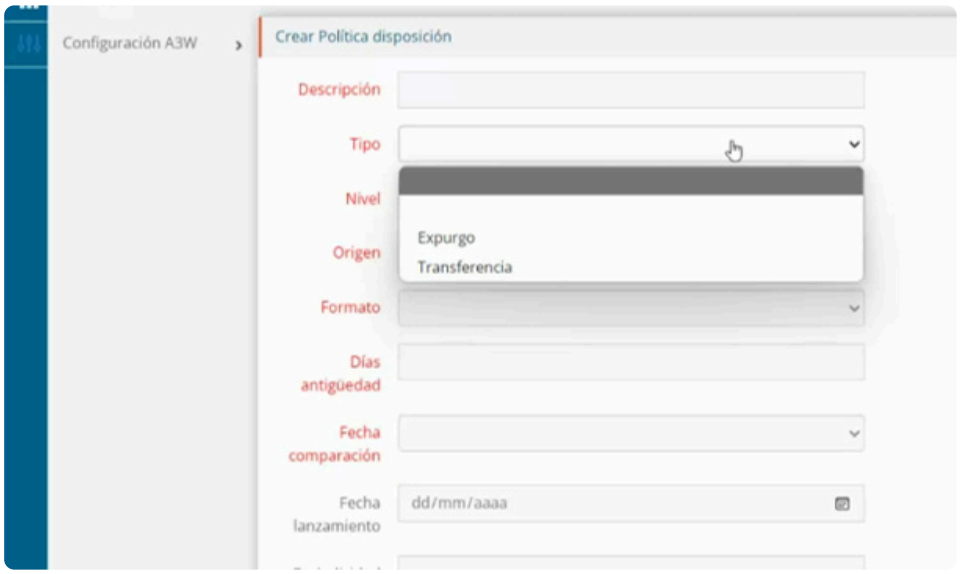
Como resultado de esta revisión puede decidirse ampliar el plazo de conservación, suspender temporalmente la disposición o bien confirmar de forma definitiva la aplicación de alguna de las otras tres acciones: eliminación, conservación o transferencia.

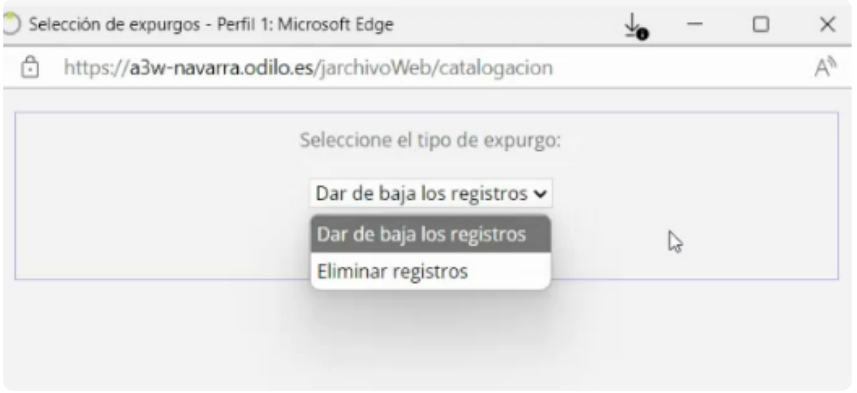
Vistas estas definiciones, las acciones de disposición deben responder a un conjunto de decisiones previamente analizadas, deliberadas y autorizadas, las cuáles se corresponden a la valoración documental, y deben estar debidamente documentadas. En el caso de las administraciones públicas, los instrumentos que recogen estas decisiones y establecen la disposición de los documentos son las tablas de valoración y acceso documental y el calendario de conservación.

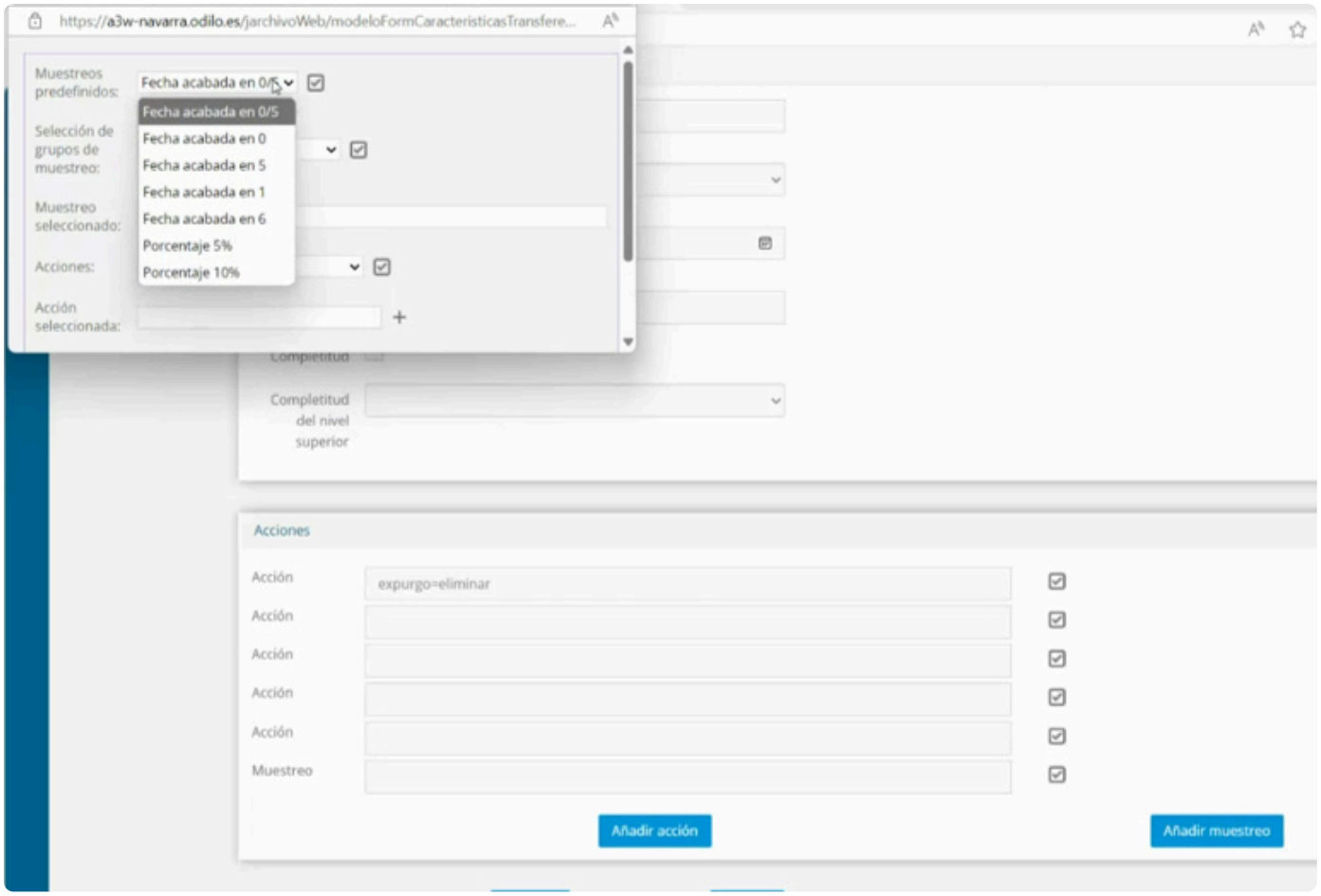
A nivel técnico, el archivo digital seguro debe de ser capaz de asociar reglas de disposición a los expedientes y documentos, así como a otros digitales –si les es de aplicación–, calcular sus plazos, impedir que se realicen eliminaciones cuando exista una suspensión concreta de la tabla de valoración o la serie documental no esté valorada, ejecutar de manera controlada la disposición, conservar las evidencias del proceso y mantener un registro de la documentación eliminada.

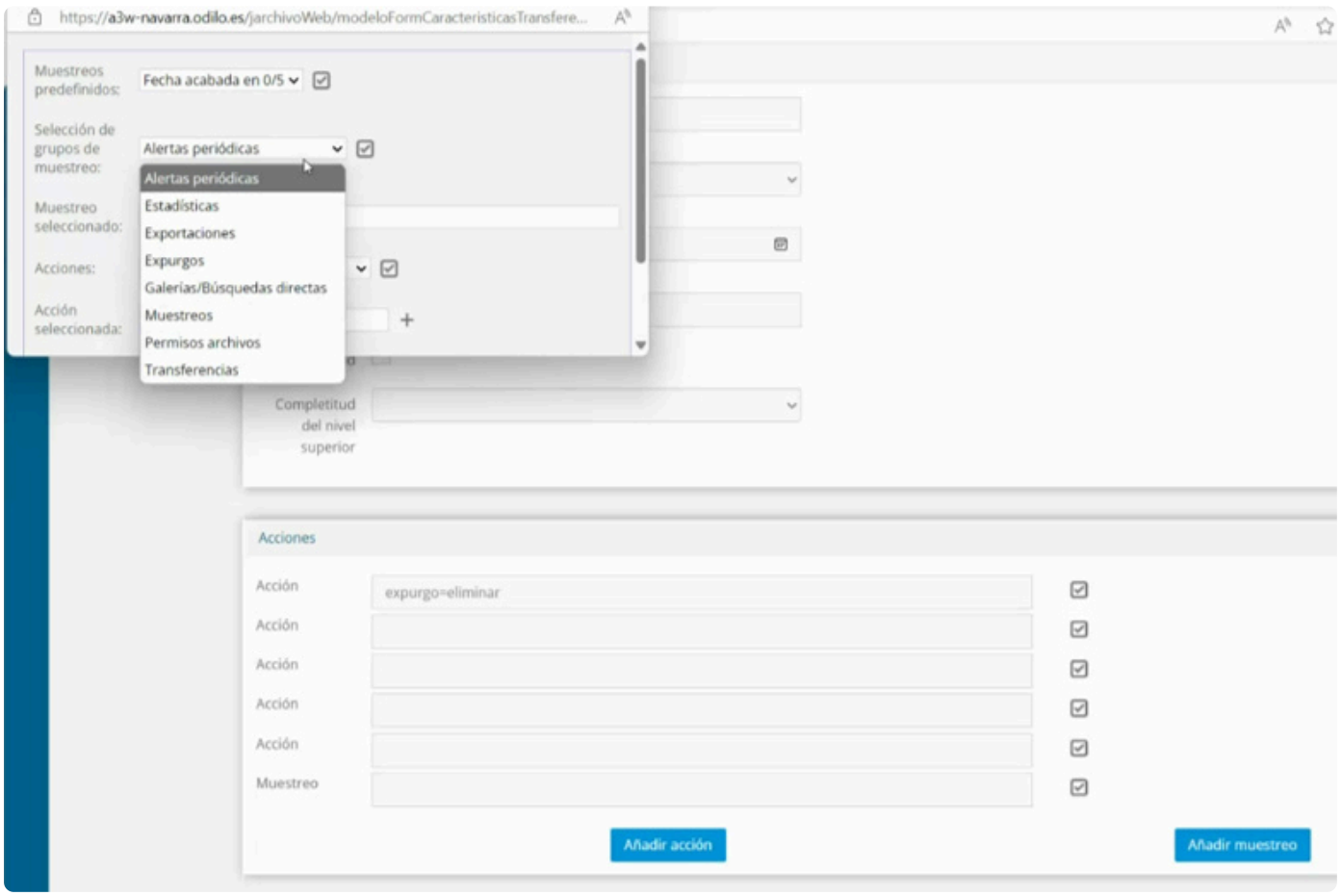
A continuación, se muestra la **configuración** de una **política de disposición** del Archivo Contemporáneo de Navarra (ACN) en la herramienta de archivo digital seguro de Letmino, de ODILO TID, S.L. –plataforma conocida anteriormente como ODILO:

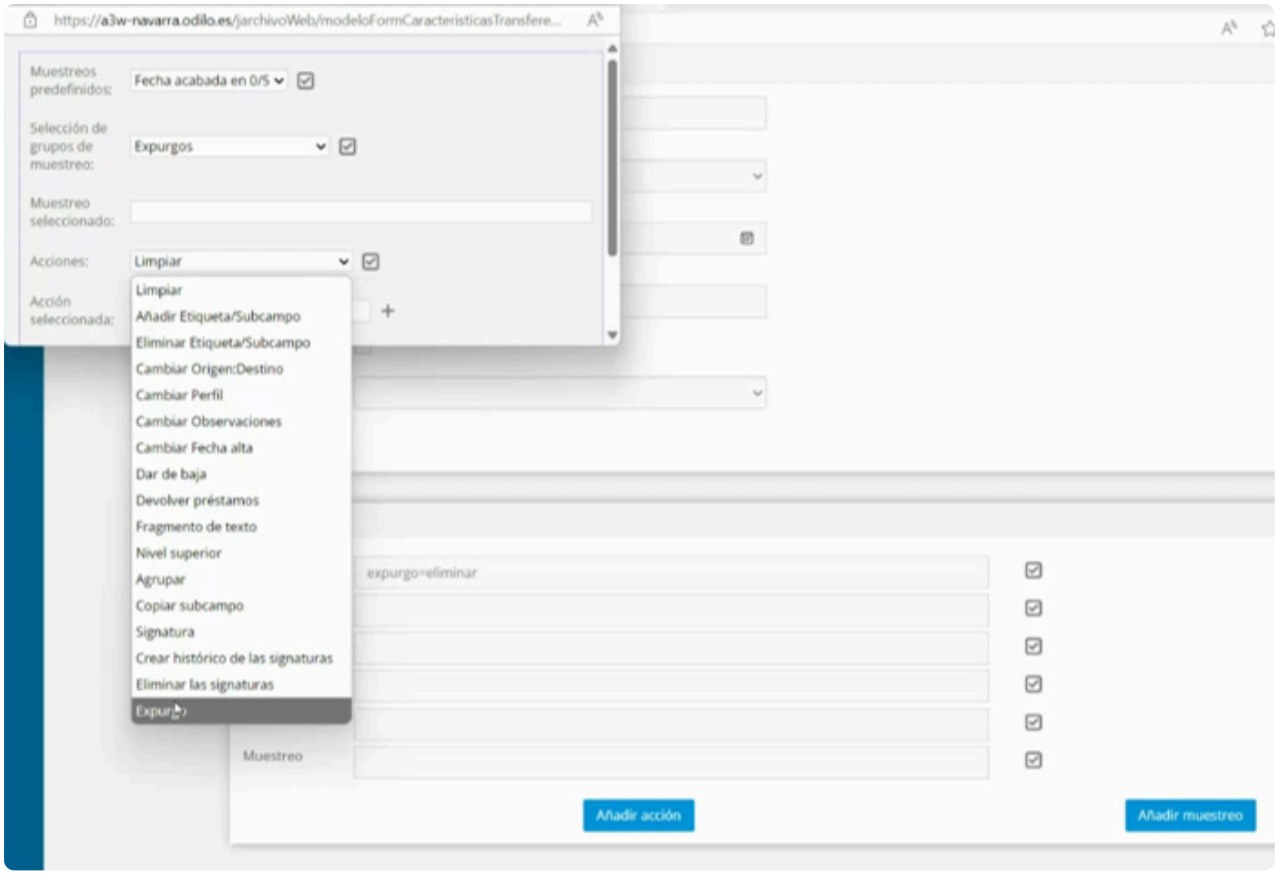

Editar Política disposición
Código
Descripción
Tipo
Nivel
Origen
Formato
Días antigüedad
Fecha comparación
Completitud
Expediente electrónico
Pieza electrónica
Pieza
Expediente
Fracción de Serie
Registros fotográficos
Vídeo
Audio
Caja
Pieza electrónica
1065
Fecha final


Configuración A3W
Crear Política disposición
Descripción
Tipo
Nivel
Origen
Formato
Días antigüedad
Fecha comparación
Fecha lanzamiento
Expurgo
Transferencia
dd/mm/aaaa


Selección de expurgos - Perfil 1: Microsoft Edge
https://a3w-navarra.odilo.es/jarchivoWeb/catalogacion
Seleccione el tipo de expurgo:
Dar de baja los registros
Dar de baja los registros
Eliminar registros


https://a3w-navarra.odilo.es/jarchivoWeb/modeloFormCaracteristicasTransfere...
Muestreos predefinidos:
Fecha acabada en 0/5
Selección de grupos de muestreo:
Muestreo seleccionado:
Acciones:
Acción seleccionada:
Fecha acabada en 0/5
Fecha acabada en 0
Fecha acabada en 5
Fecha acabada en 1
Fecha acabada en 6
Porcentaje 5%
Porcentaje 10%
Completitud del nivel superior
Acciones
Acción
expurgo=eliminar
Acción
Acción
Acción
Acción
Muestreo
Añadir acción
Añadir muestreo


https://a3w-navarra.odilo.es/jarchivoWeb/modeloFormCaracteristicasTransfere...
Muestreos predefinidos:
Fecha acabada en 0/5
Selección de grupos de muestreo:
Alertas periódicas
Muestreo seleccionado:
Acciones:
Acción seleccionada:
Alertas periódicas
Estadísticas
Exportaciones
Expurgos
Galerías/Búsquedas directas
Muestreos
Permisos archivos
Transferencias
Completitud del nivel superior
Acciones
Acción
expurgo=eliminar
Acción
Acción
Acción
Acción
Muestreo
Añadir acción
Añadir muestreo



Fuente: plataforma de archivo digital seguro de Letmino (anteriormente, ODILO), de ODILO TID, S.L.

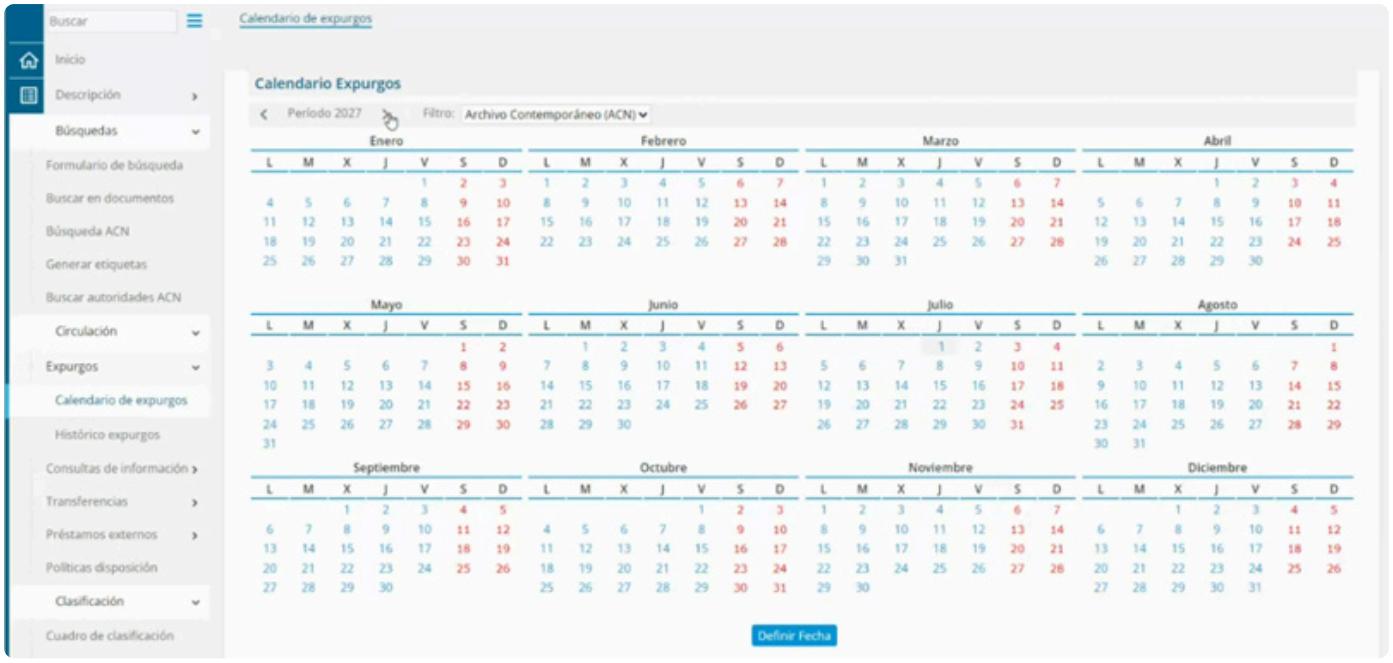
En relación con las acciones de disposición, hay que tener en cuenta los siguientes conceptos:

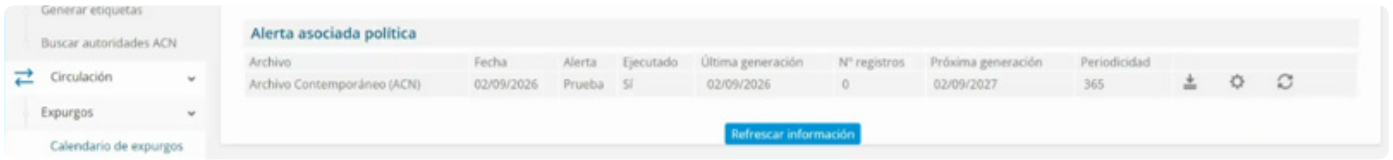
Calendario de avisos y eventos

Es el mecanismo dentro del archivo digital seguro que permite, una vez configuradas las tablas de valoración documental, llevar un control efectivo de los plazos de aplicación de las acciones de disposición programadas. Este recoge los eventos que están previstos que se lleven a cabo, previa autorización de las personas profesionales de archivo, y genera las correspondientes alertas para aceptarlos, denegarlos, bloquearlos, aplicarlos parcialmente o modificarlos.

Respecto la documentación física, el aviso de un evento no implica la disposición (básicamente la eliminación) automática de ésta, sino que se deben identificar las unidades afectadas, validar si procede ejecutar la acción correspondiente y, una vez ejecutada, se debe confirmar la acción en el archivo digital seguro para que quede constancia de esta.

Se incluye a continuación el calendario de expurgos que ofrece la herramienta de archivo digital seguro de Letmino, en el que se ha incorporado la política de disposición configurada en las imágenes anteriores:





Fuente: plataforma de archivo digital seguro de Letmino (anteriormente, ODILO), de ODILO TID, S.L.

Control de la ejecución de las acciones de disposición

En relación con el calendario de avisos y eventos, una vez salta el recordatorio de la aplicación de una acción de disposición en base a una tabla de valoración documental, las personas profesionales de archivo deben confirmar, rechazar, pausar o modificar el evento. Es importante que desde el archivo se disponga de una visión global de las acciones pendientes y las ejecutadas y, tanto para unas como otras, guardar la trazabilidad y el resultado final del proceso correspondiente. También acostumbra a existir la acción de suspensión o bloqueo, que impide automáticamente la ejecución de la disposición prevista cuando concurra alguna circunstancia en particular.

En la documentación en papel, el archivo digital seguro permite controlar y dejar constancia de todo el proceso de disposición que se le aplique, aunque la actuación se ejecute físicamente fuera del sistema. Las personas profesionales de archivo deben comprobar qué expedientes, cajas o unidades documentales resultan afectados, verificar que se cumplen los plazos y condiciones de aplicación y confirmar, rechazar o suspender la disposición. Si procede la eliminación, deberá coordinarse la retirada y destrucción física de forma segura y certificada de los documentos. Una vez realizada, se registrará en la herramienta su ejecución, fecha, documentación afectada, responsable, método de destrucción, resultado y referencia al acta o certificado correspondiente.

Registro de eliminaciones

Es el instrumento que permite dejar constancia de qué documentación ha sido eliminada, cuándo, por qué autorización y mediante qué procedimiento y debe incorporar, entre otros elementos, la serie documental en la que se clasificaba la documentación, el periodo cronológico afectado, el número o volumen de expedientes/documentos eliminados, la tabla de valoración, el tipo de eliminación (total o parcial), la fecha de la eliminación, el usuario responsable de la autorización, etc. Según la Ley Foral 9/2026, las administraciones públicas navarras deben publicar este instrumento.

Pista de auditoría de las acciones de disposición

Es el historial detallado y cronológico de las operaciones realizadas por el sistema en relación con la disposición, guardando evidencias de todo el proceso, como por ejemplo qué usuario dio el visto bueno, sobre cuantos ficheros u objetos digitales se ha aplicado, el resultado final, posibles incidencias, etc. En este caso, contiene más información que el registro de eliminaciones y la pista debe estar protegida frente a modificaciones y ser accesible únicamente a perfiles autorizados (normalmente administradores del sistema).

Conservación de metadatos después de la eliminación

Consiste en mantener, una vez eliminados los documentos o expedientes, un conjunto mínimo de metadatos que actúen como evidencia de su existencia y de la correcta aplicación de la disposición documental, tal y como recogen los principales estándares técnicos, como Moreq2010. Estos metadatos residuales permiten identificar qué documentación existió, conocer cuándo y conforme a qué autorización fue eliminada y acreditar que el proceso se ejecutó de forma controlada. Así pues, no es necesario conservar todos los metadatos originales, sino mantener únicamente aquellos necesarios para acreditar y garantizar la trazabilidad de la eliminación.

La recomendación general es que se conserven los siguientes metadatos del e-EMGDE.

eEMGDE1. Tipo de entidad eEMGDE2.1. Secuencia de identificador eEMGDE4.1. Fecha inicio eEMGDE4.2. Fecha fin eEMGDE6.1. ID entidad relacionada eEMGDE6.3. Rol de la relación	eEMGDE13.2.2. Acción dictaminada eEMGDE21.1.1. Descripción de la acción eEMGDE21.1.3. Objeto de la acción eEMGDE21.2. Motivo reglado eEMGDE21.3. Usuario de la acción	eEMGDE22.1. Código de clasificación eEMGDE22.2. Denominación de clase eEMGDE24. Órgano

⚠ **Los metadatos de trazabilidad asociados a las acciones efectuadas (eliminación) deberán conservarse obligatoriamente, así como la identificación de la documentación eliminada, con el fin de mantener evidencia de que dicha documentación existió, aunque haya sido posteriormente eliminada**.

Para saber más

Normativa

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- 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 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- Ley Foral 9/2026, de 20 de mayo, de Archivos, Gestión de Documentos y Patrimonio Documental.
- Orden Foral 18/2021, de 24 de mayo, de la Consejera de Cultura y Deporte, por la que se aprueban los requisitos tecnológicos y funcionales para implantaciones de archivo digital seguro de las entidades locales de Navarra y un modelo de auditoría.
- Orden Foral 51/2016, de 14 de junio, de la Consejera de Cultura, Deporte y Juventud, por la que se aprueban instrucciones para la evaluación y la eliminación de documentos de las Entidades Locales de Navarra.
- Resolución 476/2007, de 17 de julio, de la Directora General de Cultura, por la que se aprueba el texto con los criterios de conservación y eliminación y las instrucciones de seguridad y confidencialidad, propuestos por la Comisión de Evaluación Documental.

Escenarios y situaciones habituales

Escenario 1. No se realizan transferencias desde las unidades tramitadoras

Situación

Las unidades tramitadoras, una vez finalizan la tramitación de los expedientes electrónicos, deben cerrarlos para generar el índice y el foliado y que estén a punto para su transferencia. No obstante, en este contexto pueden ocurrir dos circunstancias:

- Que las unidades tramitadoras no cierren los expedientes, una vez finalizan su tramitación, y, por consiguiente, no sea posible iniciar el proceso de transferencia, en el supuesto que sea automatizado.
- Que las unidades tramitadoras cierren los expedientes, una vez finalizada su tramitación, pero que no ejecuten el proceso de transferencia (en caso de no estar automatizado).

Esto puede deberse al desconocimiento por parte de las unidades tramitadoras del procedimiento de transferencia, a la ausencia de responsabilidades claras en su ejecución, a la falta de automatización o al temor de las unidades a perder el acceso a sus expedientes una vez transferidos.

Estas circunstancias pueden implicar que los expedientes permanezcan, tanto abiertos como incluso cerrados, largos periodos de tiempo en el gestor de expedientes y que puedan producirse problemáticas importantes relacionadas con su integridad, la vigencia y validez de las firmas, la obsolescencia de los formatos, etc.

Decisiones operativas

Las personas profesionales de archivo deberán:

1. Identificar los expedientes, tanto abiertos como cerrados, pendientes de transferencia. Solicitar periódicamente al servicio de informática, o si archivo dispone de los permisos correspondientes, revisar el gestor de expedientes para poder obtener una relación de los expedientes, tanto abiertos como cerrados y por cada unidad de tramitación, que todavía permanezcan en el sistema de tramitación y deberían estar transferidos, diferenciándolos por unidad tramitadora, serie documental y fecha de finalización del procedimiento.

2. Determinar los motivos de la no ejecución de la transferencia. Comprobar si responde al desconocimiento de la unidad tramitadora, a su temor de perder el acceso a sus expedientes, a la falta de automatización del proceso, a la falta de asignación de responsabilidades, a incidencias técnicas, etc.

3. Establecer instrucciones claras para las unidades tramitadoras. Definir con claridad cuándo y cómo deben cerrase los expedientes –así como llevar a cabo controles de auditoria periódicos–, quién y cómo debe iniciar la transferencia, en qué momento, qué comprobaciones previas deben realizarse y mediante qué acciones, tanto dentro como fuera del gestor de expedientes –si corresponde–, se debe ejecutar el proceso.

4. Planificar la transferencia de los expedientes pendientes de transferir. Cuando exista un volumen importante de expedientes pendientes de transferir, es recomendable definir previamente y ejecutar las transferencias por lotes en función de las unidades productoras, las series documentales o los plazos de cierre y/o disposición de los expedientes. En este caso, es archivo quién debe encargarse de ejecutar estas transferencias de carácter masivo.

5. Promover la automatización del proceso. Siempre que sea técnicamente posible, junto con el servicio de informática, establecer las reglas y condiciones para que las transferencias se realicen automáticamente, a partir de ciertos eventos, plazos o condiciones, por parte del gestor de expedientes.

6. Realizar un seguimiento periódico. Archivo debe de ser el encargado de ir haciendo muestreos y auditorías periódicas, sobre las unidades tramitadoras, para comprobar que las transferencias se ejecutan correctamente en tiempo y forma. Asimismo, es recomendable disponer de indicadores de los sistemas, tanto de tramitación como de archivo digital seguro, que permitan saber cuántos expedientes se han cerrado, cuántos han sido transferidos, cuántos están pendientes, cuántos rechazados –y por qué motivos– y el tiempo transcurrido entre el cierre y la transferencia.

Escenario 2. Transferencia de expedientes incompletos o conformados incorrectamente

Situación

Durante la preparación o ejecución de una transferencia al archivo digital seguro pueden detectarse deficiencias que impidan considerar el expediente correctamente conformado. Entre las incidencias más habituales se encuentran:

- La ausencia de documentos que deberían formar parte del expediente.
- La incorporación de documentos duplicados, ajenos al procedimiento o que no constituyen documentos definitivos.
- La existencia de metadatos obligatorios ausentes, incorrectos o incoherentes.
- La utilización de formatos no admitidos o con riesgo de obsolescencia.
- La falta de firmas, sellos electrónicos, evidencias de validación o información necesaria para comprobar la autenticidad e integridad de los documentos.
- La falta de correspondencia entre los documentos, el índice electrónico y los metadatos del expediente.
- La aplicación incorrecta de la clasificación archivística o los plazos de disposición.

Estas incidencias pueden ser detectadas por la unidad tramitadora al preparar la transferencia, por las personas profesionales de archivo durante su revisión en el proceso de ingesta o por las validaciones automáticas del gestor de expedientes o el archivo digital seguro.

Como criterio general, no deberá aceptarse la transferencia cuando las deficiencias afecten a la identificación, autenticidad, integridad, disponibilidad, recuperación, clasificación o conservación del expediente en cuestión.

Decisiones operativas

1. En caso de que falten documentos:

Las personas profesionales de archivo deberán:

- Comprobar, de acuerdo con el procedimiento y con su configuración documental, qué documentos deberían integrar el expediente.
- Identificar de forma concreta los documentos ausentes.
- Devolver o rechazar la transferencia, indicando las incidencias detectadas.
- Requerir a la unidad tramitadora que incorpore los documentos que falten.

Cuando el documento no exista y no pueda incorporarse, la unidad tramitadora deberá justificar esta circunstancia mediante una diligencia, informe, nota interna u otra evidencia adecuada, según la naturaleza de la ausencia.

No deberán incorporarse documentos creados posteriormente simulando que fueron generados durante la tramitación. Cualquier actuación de subsanación deberá quedar debidamente documentada, identificada y aprobada por el órgano o cargo correspondientes y con constancia de su fecha.

2. En caso de que existan documentos duplicados, provisionales o ajenos al expediente:

La unidad tramitadora deberá revisar el contenido del expediente y:

- Eliminar los duplicados que no aporten valor documental.
- Excluir borradores, versiones de trabajo y documentos auxiliares que no deban formar parte del expediente definitivo.
- Retirar aquellos documentos incorporados por error o pertenecientes a otros expedientes.
- Mantener las versiones que deban conservarse como evidencia de la tramitación.

La eliminación o exclusión de documentos deberá realizarse antes del cierre del expediente y de acuerdo con las reglas del gestor de expedientes, dejando la correspondiente trazabilidad cuando el sistema así lo requiera.

3. En caso de metadatos ausentes o incorrectamente informados:

Deberá determinarse si la incidencia afecta a metadatos esenciales para identificar el expediente o los documentos en cuestión, identificar los metadatos en cuestión y requerir a la unidad tramitadora que los informe debidamente.

Mientras el expediente permanezca abierto, debe ser la unidad tramitadora quién corrija o informe los metadatos en el sistema de tramitación. Las personas profesionales de archivo podrán identificar los errores, indicar los criterios y/o acciones a aplicar y, posteriormente, comprobar que la corrección se ha realizado satisfactoriamente.

En este supuesto, no es recomendable que las personas profesionales de archivo modifiquen directamente los metadatos relativos a la tramitación, salvo que esta función la tenga expresamente atribuida y el sistema permita ejecutarla.

4. En caso de documentos sin firma o con problemas de validación:

Deberá analizarse si el documento en cuestión requiere una firma o sello electrónico. En el caso que sí:

- Se devolverá el expediente a la unidad tramitadora para que regularice la situación.
- No deberá sustituirse la firma ausente por una firma posterior que altere indebidamente el momento o las condiciones en que se produjo la actuación.
- Cuando no sea posible obtener nuevamente la firma, deberá documentarse la incidencia y valorar qué otras evidencias permiten acreditar la actuación realizada.

Cuando la firma exista, pero no pueda validarse por problemas técnicos, deberán conservarse el documento, la firma y las evidencias disponibles, y aplicarse los mecanismos previstos para preservar o acreditar su validez a largo plazo en el archivo digital seguro.

5. En caso de formatos no admitidos:

Deberá comprobarse si el formato:

- Está incluido entre los formatos admitidos por la política de gestión documental o el catálogo de formatos de la administración.
- Puede ser procesado por el archivo digital seguro.
- Permite conservar el contenido, la estructura, el contexto y, cuando proceda, la apariencia del documento.
- Presenta dependencias de software, componentes externos o tecnologías obsoletas.

Una vez en el archivo digital seguro, se deberán ejecutar las acciones de conversión de formatos correspondientes para asegurar la transferencia del contenido y contexto del documento en cuestión al nuevo formato de preservación.

6. En caso de clasificación archivística incorrecta:

Si el expediente está asociado a una serie documental o procedimiento incorrectos, deberá devolverse a la unidad tramitadora para que se revise su clasificación. Es importante recordar que la clasificación deberá corregirse antes de la transferencia, ya que condiciona:

- Los metadatos aplicables.
- Los permisos de acceso.
- Los plazos de disposición.
- La eventual eliminación o conservación permanente.
- La recuperación posterior del expediente.

En el caso que acabe ingresando un expediente mal clasificado en el archivo digital seguro, siguiendo el procedimiento establecido y con la autorización de la autoridad competente, se procederá a su reclasificación teniendo en cuenta las funcionalidades de las que este disponga.

7. Si la incidencia no puede subsanarse:

Cuando no sea posible corregir o subsanar la incidencia detectada en un expediente o en sus documentos, deberá:

- Documentarse de forma detallada la incidencia y sus motivos.
- Identificarse su alcance y sus posibles consecuencias.
- Incorporarse, cuando proceda, una diligencia o informe explicativo.
- Valorar medidas adicionales de conservación, acceso o control sobre el expediente y sus documentos.

La imposibilidad de corregir o solucionar una incidencia no deberá ocultarse ni resolverse mediante la alteración de los documentos o los metadatos. El objetivo debe ser conservar el expediente en su forma original, junto con las evidencias necesarias para comprender las deficiencias detectadas.

Escenario 3. Transferencia de expedientes de larga tramitación que deban seguir abiertos

Situación

Determinados procedimientos pueden permanecer abiertos durante largos períodos de tiempo y, de mientras, ir incorporando documentos en el expediente. Mientras este continúa en estado de tramitación, no se produce la transferencia al archivo digital seguro, ya que esta exige, con carácter general, que el expediente esté cerrado y foliado. Esta situación puede comportar riesgos para la integridad, el acceso y/o la preservación de los documentos y las firmas asociadas.

En este supuesto, es necesario valorar que acciones deben llevarse a cabo para asegurar la vigencia de la documentación sin alterar el estado del expediente ni aplicar de forma prematura la disposición.

Decisiones operativas

Las personas profesionales de archivo deberán:

1. Identificar los procedimientos de larga tramitación. Con la ayuda de las unidades tramitadoras, se deberá elaborar un inventario que identifique aquellos procedimientos cuyos expedientes puedan o deban mantenerse abiertos durante un período de tiempo prolongado, así como determinar los posibles riesgos de mantener la documentación, exclusivamente, en el gestor de expedientes.

2. No cerrar el expediente antes de tiempo para poder transferirlo. El expediente deberá permanecer abierto mientras continúe realmente su tramitación. En este sentido, la Orden Foral 18/2021 establece como requisito para la transferencia ordinaria al archivo digital seguro que los expedientes estén cerrados, foliados y dispongan de sus correspondientes metadatos. No obstante, en coordinación con el servicio de informática y si se considera viable, se puede plantear hacer una exportación en formato paquete ENI del expediente, con el estado de “cerrado para remisión”, e ingresarlo en el archivo digital seguro, manteniendo el expediente original en tramitación en el gestor de expedientes.

3. Valorar si realmente debe existir un único expediente durante todo el periodo. Junto con la unidad tramitadora y, si corresponde, con el soporte del servicio jurídico, deberá analizarse si la normativa permite organizar la tramitación del procedimiento mediante expedientes o agrupaciones documentales diferenciadas (subexpedientes o expedientes relacionados) por anualidades, fases, actuaciones u otros hitos.

Los expedientes que puedan cerrarse de forma efectiva podrán transferirse al archivo digital seguro, siempre asegurando su vinculación lógica con los expedientes o agrupaciones documentales que se mantengan en el gestor de expedientes.

4. Establecer, cuando no sea posible subdividir el expediente, mecanismos de preservación anticipada. Si determinados documentos necesitan la aplicación de acciones de preservación a largo plazo antes del cierre del expediente, se deberá valorar su incorporación al archivo digital seguro. Esta actuación deberá entenderse como una medida de preservación extraordinaria y no como la transferencia ordinaria del expediente abierto.

5. Mantener la vinculación con el expediente original. Los documentos o agrupaciones documentales preservados/as anticipadamente deberán conservar su identificador, metadatos, firmas y relaciones con el expediente original almacenado en el gestor de expedientes. Debe evitarse la generación de copias sin control o duplicados y las formas de acceso a esta documentación, por parte del personal tramitador, se determinarán junto con el servicio de informática.

6. No iniciar anticipadamente la aplicación de los plazos de disposición. La preservación o ingesta anticipada de determinados documentos no supone el cierre del expediente. Cuando la tabla de valoración establezca que el plazo de disposición empieza con el cierre, resolución o finalización del expediente, este deberá calcularse a partir del momento en que se produzca formalmente.

7. Realizar la transferencia definitiva cuando finalice el procedimiento. Una vez el expediente se cierre, al finalizar la tramitación del procedimiento, se deberán realizar las comprobaciones correspondientes y proceder a su transferencia al archivo digital seguro. Una vez ingrese en el sistema, se aplicarán los plazos y acciones de disposición que indique la tabla de valoración.

Escenario 4. Ingesta de documentación procedente de otras fuentes distintas al gestor de expedientes

Situación

El archivo digital seguro es la herramienta única e integral de gestión de toda la documentación electrónica de una administración, en su fase histórica, y no únicamente la de carácter administrativo. En esta línea, el archivo puede recibir documentación electrónica, sea o no administrativa, procedente de otras fuentes distintas a los tramitadores de expedientes, como por ejemplo documentos almacenados en carpetas de red, unidades compartidas, repositorios u otras aplicaciones corporativas o externas. Asimismo, también puede recibir fondos documentales, ya sean electrónicos, digitalizados o incluso físicos, procedentes de otras entidades, instituciones o personas.

En estos casos, es probable que la documentación a ingresar en el archivo digital seguro no se encuentre estructurada ni descrita con metadatos, no se organice entorno a la figura del expediente –aunque igual sí otros tipos de agrupaciones documentales–, ni tampoco se encuentre debidamente clasificada y descrita, presente duplicidades, inconsistencias, formatos no admitidos, etc. Por ello, su incorporación al archivo digital seguro debe tratarse como una ingesta específica, precedida de tareas de identificación, preparación y control.

Decisiones operativas

Las personas profesionales de archivo deberán:

1. Identificar el origen y naturaleza de la documentación. En este caso será necesario discernir si la documentación ha sido producida por la misma administración o bien si procede de otra persona u organización. En función de la procedencia de la documentación, se deberán realizar unos u otros pasos, tal y como se desarrolla a continuación:

- **Si la documentación procede de la misma administración, pero se encuentra almacenada en otros repositorios:** determinar en qué sistemas se almacena, cuáles son sus características, quién es el órgano productor, qué funciones y actividades documenta, si dispone de metadatos, firmas u otros datos contextuales asociados, los motivos para incorporarla al archivo digital seguro y discernir si se trata de documentación administrativa –y si debería formar parte de un expediente– o no.

En este supuesto, la documentación se incorporará dentro de la instancia –y en consecuencia del fondo documental– de la propia administración y se clasificará en base al Cuadro de Clasificación corporativo.

- **Si la documentación procede de una persona u organización externa a la administración:** en primer lugar, formalizar el ingreso cuando proceda. Los fondos externos, sean públicos o privados, deberán contar previamente con el correspondiente acuerdo, acta, convenio, contrato u otro instrumento jurídico, debidamente suscrito por las partes interesadas, que regule el régimen jurídico del ingreso en el archivo, así como los derechos y obligaciones de las partes, la titularidad de la documentación y las condiciones de custodia, acceso, tratamiento, disposición, preservación, difusión y reproducción –respetando siempre la propiedad intelectual y los derechos de autor.

  En este supuesto, por parte del archivo, se valorará si la documentación, por su volumen, naturaleza, especificidad, etc., debe incorporarse en la instancia de la propia administración o si, por el contrario, se debe crear una nueva instancia –y, por consiguiente, un fondo documental– específica para la persona u organización que ha cedido la documentación y clasificarla en base al Cuadro de Clasificación correspondiente.

2. Analizar y depurar la documentación antes de la ingesta. En el caso de documentación generada por la propia administración, identificar posibles duplicados, borradores, versiones intermedias, ficheros temporales y documentación de apoyo, evitando convertir el archivo digital seguro en un repositorio que agrupe de manera indiscriminada cualquier documento electrónico de la administración o de terceros.

En el caso de la documentación procedente de otra persona u organización, analizar las tipologías documentales, los soportes y los formatos de los documentos, así como sus características esenciales y posibles particularidades, para valorar la mejor forma de proceder a su ingesta. También se deberán tener en cuenta los derechos de autor y propiedad intelectual, a efectos de su futura gestión, especialmente de los plazos, y respecto a su incidencia en la difusión pública, o no, de la documentación.

3. Clasificar y describir la documentación. Asignar la documentación a la instancia y fondo documental que le corresponda, en función de si se trata de documentación de la propia administración o de otra persona u organización, clasificándola en la serie documental pertinente, identificando el productor, las fechas, los identificadores y el resto de los metadatos contextuales que correspondan. No debe forzarse, artificialmente, el ingreso y almacenamiento de la documentación en una estructura de expediente administrativo cuando no sea necesario; deberá cercarse la mejor solución en base a otros tipos de agrupaciones documentales en base a los estándares y mejores prácticas archivísticas y las funcionalidades del archivo digital seguro, en especial, para aquella documentación no producida por la propia administración.

4. Realizar controles técnicos. Comprobar, de forma manual o automática, según las funcionalidades del archivo digital seguro, los formatos de los documentos, su integridad y legibilidad, la presencia de malware, de firmas electrónicas cuando existan, etc. Cuando sea posible, es recomendable generar resúmenes criptográficos que permitan comprobar, a posteriori, la integridad de esta documentación.

5. Preparar la ingesta. Estructurar la documentación y sus metadatos, en caso de haberlos, en un paquete de ingreso o PIT adecuado a las capacidades del archivo digital seguro, incorporando un inventario que identifique los objetos que se ingresan.

6. Realizar una ingesta de prueba. Para comprobar que los objetos se cargan correctamente en el archivo digital seguro y se clasifican en el fondo y series correspondientes, es recomendable hacer una prueba con un conjunto representativo de los objetos a ingresar, manteniendo siempre los originales en el sistema de origen por si el proceso fallase o hubiera incidencias que afecten al contenido de estos.

7. Llevar a cabo la ingesta y validar los resultados del proceso. Si las pruebas de ingesta son satisfactorias, el siguiente paso consiste en llevar a cabo la ingesta de la totalidad de los objetos y, posteriormente, validar los resultados para comprobar que no se haya producido ninguna incidencia.

Escenario 5. Gestión del acceso a la documentación transferida por parte de las unidades tramitadoras

Situación

Una vez transferidos los expedientes al archivo digital seguro, las unidades productoras pueden necesitar consultarlos para realizar actuaciones posteriores, atender consultas o consultar antecedentes. La administración debe decidir cómo proporcionar este acceso, en función de las funcionalidades de los diversos sistemas de gestión que intervienen:

- Manteniendo una copia de consulta en el gestor de expedientes.
- Permitiendo acceder al archivo digital seguro de forma transparente desde el mismo gestor.
- Que el personal tramitador, con la debida autorización, acceda al archivo digital seguro.

La ausencia de un modelo claro y ágil puede generar resistencia, por parte de las unidades tramitadoras, a la realización de las transferencias. La transferencia implica un cambio en la custodia y gestión del expediente, pero no debe impedir que los usuarios que lo necesiten por razón de sus funciones puedan seguir consultándolo.

Decisiones operativas

Se recomienda llevar a cabo las siguientes acciones:

1. Definir junto con el servicio informático el modelo de acceso. Siempre que técnicamente sea posible, la opción más sencilla para el personal tramitador es que el gestor de expedientes permita consultar, de forma transparente, el expediente custodiado en el archivo digital seguro, sin necesidad de acceder a través de la herramienta de archivo.

2. Evitar copias paralelas no controladas. En el caso de optarse por la generación de copias de consulta disponibles en el gestor de expedientes, estas deberán considerarse exclusivamente en modo de solo lectura y no generarse de manera indiscriminada y sin control. El expediente custodiado en el archivo digital seguro, en tanto que agrupación original, debe constituir el objeto sobre el que se apliquen las acciones de disposición.

3. Habilitar el acceso directo cuando sea necesario. En el caso de no existir la integración entre el archivo digital seguro y el gestor de expedientes, o en el supuesto de que esta no esté operativa o, incluso, que no permita la consulta transparente de los expedientes del archivo desde el gestor, con el soporte del servicio informático –en caso necesario–, se podrán facilitar o crear usuarios para que el personal tramitador, con los debidos permisos de acceso en base a los procedimientos que tramita, consulte directamente la documentación almacenada en el archivo digital seguro.

4. Gestionar los permisos de acceso en base a roles y funciones. Es importante mencionar que los perfiles y roles de acceso de los usuarios internos debe configurarse teniendo en cuenta la unidad tramitadora de la cual forman parte, sus funciones y responsabilidades a nivel de usuario y las series documentales a las cuales deberían poder acceder y a las que no. Asimismo, se recomienda establecer un período de tiempo concreto durante el cual los usuarios puedan acceder a la documentación y, una vez finalizado este, ya no sea posible que accedan.

5. Registrar las consultas a través de la pista de auditoria. El archivo digital seguro debe mantener una trazabilidad exacta de todos los accesos a la documentación y en base a distintos parámetros para poder llevar un control de las actividades y accesos de los usuarios, como, por ejemplo, el identificador del usuario, los expedientes y documentos consultados, las fechas de las consultas, las acciones realizadas, etc.

6. Explicar el modelo a las unidades. En función del modelo de consulta que se establezca, este debe explicarse con detalle a las unidades tramitadores para que comprendan el funcionamiento del proceso de consulta y, sobre todo, transmitir el mensaje de que transferir no significa perder el acceso al expediente.

Escenario 6. Disposición de los expedientes híbridos

Situación

Es probable que, en el marco de la operación del archivo digital seguro, en algún u otro instante, ingresen en el sistema expedientes híbridos, de acuerdo con las particularidades que estos tienen y que se han desarrollado en otros bloques de esta guía. En consecuencia, es necesario comprender la operativa que se debe llevar a cabo a la hora de aplicar las acciones de disposición sobre un expediente que se encuentra integrado por documentación electrónica y documentación en papel.

La dificultad consiste en garantizar que la preservación y la eliminación se apliquen de forma coherente sobre ambos soportes sin perder la relación y el contexto que permite reconstruir el expediente completo. En este sentido, la Ley Foral 9/2026 exige expresamente garantizar la integridad de la relación entre los componentes electrónicos y los conservados en otros soportes.

Decisiones operativas

Se recomienda llevar a cabo las siguientes acciones:

1. Identificar qué documentos son electrónicos y cuáles se encuentran en papel. El primer paso implica identificar, dentro del expediente, qué documentos se conservan electrónicamente y cuáles en soporte papel.

Es importante revisar la existencia de los registros y los metadatos, dentro del expediente electrónico, relativos a la ubicación física de cada uno de los documentos que se encuentran en soporte papel para mantener la relación y trazabilidad en todo momento.

2. Determinar si procede digitalizar la parte en papel. La digitalización será especialmente conveniente cuando facilite la reunificación del expediente en un solo soporte y la documentación en papel no presente particularidades que recomienden su conservación.

En el caso que se opte por la digitalización de la documentación en papel, con la voluntad de sustituirla por documentación electrónica con validez jurídica, el proceso que se siga deberá cumplir con lo establecido en la legislación vigente, muy especialmente las NTI de Digitalización y Copiado auténtico, así como el Decreto Foral 30/2015, y la documentación resultante en soporte electrónico deberá contener todos los elementos técnicos (metadatos, firmas, resolución, etc.) que esta misma normativa específica.

3. Aplicar una misma decisión de valoración. Tanto si la documentación en papel se digitaliza como si no, es importante destacar que las acciones de disposición, de acuerdo con lo que establezca la correspondiente tabla de valoración documental, se deberán aplicar por igual en ambos soportes, aunque la ejecución material, evidentemente, sea distinta (principalmente, borrado seguro vs destrucción certificada del papel o preservación digital vs conservación material, sin perjuicio que se pueda dictaminar la transferencia a otro sistema de información o a otro depósito de archivo).

4. Conservar la relación entre soportes cuando aplique la conservación permanente. En el supuesto que una parte de la documentación en papel sea de conservación permanente, y no se decida digitalizarla, del mismo modo que sobre la documentación electrónica se aplicarán las correspondientes acciones de preservación, sobre la documentación en papel se deberán aplicar las acciones de conservación ambiental y material en los depósitos del archivo.

Asimismo, a nivel descriptivo y de metadatos, se deberán mantener y preservar a lo largo del tiempo las relaciones entre la parte electrónica del expediente y la parte física, a efectos de trazabilidad.