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 11. ACCESO, SEGURIDAD Y CONSULTA **3**

FINALIDAD DEL BLOQUE 4

CONTEXTO Y CONCEPTOS CLAVE 5

1. Principios y criterios de acceso a la documentación 6

2. Configuración del acceso a la documentación electrónica 7

3. Gestión de personas usuarias y roles 10

4. Funciones y responsabilidades del archivo en materia de acceso 13

5. Protección de datos en el acceso y difusión documental 14

6. Consulta en el entorno electrónico 16

PARA SABER MÁS 18

ESCENARIOS Y SITUACIONES HABITUALES 19

Escenario 1. Acceso indebido a documentación con datos personales 20

Escenario 2. Personas usuarias con permisos demasiado amplios 22

Escenario 3. Revisión de permisos tras un cambio de puesto de trabajo 24

Escenario 4. Solicitud de acceso o consulta de documentación 26

Escenario 5. Preparación de documentación con datos protegidos para consulta 28

Escenario 6. Modificación de reglas de acceso 30

Bloque 11

Acceso, seguridad y consulta

Finalidad del bloque

Este bloque proporciona el conocimiento esencial sobre seguridad, acceso y consulta a la documentación electrónica.

Comprender

conceptos clave sobre personas usuarias y roles en el entorno electrónico.

Identificar

situaciones que pueden suponer un riesgo sobre la seguridad de la documentación electrónica.

Aplicar

criterios coherentes en el acceso y la consulta a la documentación electrónica.

Contexto y conceptos clave



1. Principios y criterios de acceso a la documentación

En el entorno electrónico, el acceso a la documentación no depende de dónde se encuentra físicamente el expediente, sino de **sus permisos, roles, metadatos y controles automáticos.** Para las personas profesionales de archivo, el cambio principal es operativo: **los criterios que ya se aplican en papel deben trasladarse al sistema para que este permita o impida la consulta de forma coherente**.

El acceso documental debe equilibrar **disponibilidad, seguridad, confidencialidad, protección de datos, transparencia** y **rendición de cuentas**. Por tanto, permitir o denegar un acceso debe tener en cuenta la finalidad de la consulta, la naturaleza de la información y las limitaciones aplicables.

Principio de necesidad de conocer

Cada persona usuaria debe acceder solo a la información necesaria para cumplir una función concreta, resolver una solicitud o ejercer un derecho. En el entorno electrónico, un permiso excesivo puede conllevar accesos indebidos, modificaciones no autorizadas o dificultades para reconstruir responsabilidades.

Protección de datos desde el inicio

Antes de permitir una consulta debe comprobarse si la documentación contiene datos personales, si la persona solicitante está legitimada para acceder a ellos y si todos esos datos son necesarios para la finalidad de la consulta.

Principio de minimización de datos

Facilitar solo los datos mínimos necesarios. Si la finalidad puede satisfacerse con un solo documento, una copia parcial o una versión con datos de terceras personas ocultos, no debería entregarse más información.

Antes de permitir una consulta, conviene revisar la finalidad del acceso, la condición de la persona solicitante, el contenido de la documentación, la presencia de datos personales y las restricciones aplicables. Esta revisión busca que el acceso sea seguro, proporcionado y coherente.



2. Configuración del acceso a la documentación electrónica

Configurar el acceso significa convertir los criterios definidos por la organización en reglas aplicables dentro de la herramienta. En papel, la restricción de acceso podía ser una llave para abrir una habitación o un armario dentro del archivo.

En el entorno electrónico, las restricciones se traducen en permisos, metadatos y reglas de visibilidad para que el sistema permita o impida determinadas acciones.

La configuración debe distinguir, como mínimo, entre tres tipos de permisos:

Acceso de lectura

Permite consultar el expediente, el documento o sus metadatos, pero no modificarlos. Es el permiso habitual para consultas internas, revisiones, tareas de control o acceso a documentación ya cerrada.

Acceso de edición

Permite modificar determinados contenidos o metadatos, incorporar documentación o intervenir en la tramitación del expediente. Debe limitarse a quienes participan activamente en la gestión o tramitación.

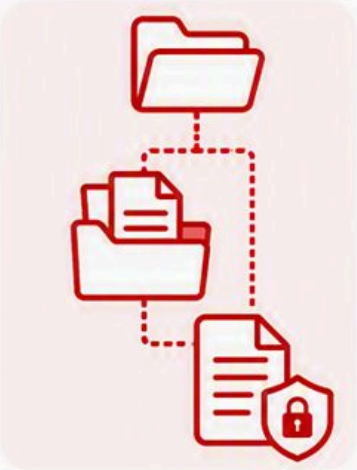
Acceso de eliminación

Permite suprimir documentos o expedientes en los casos autorizados. Debe ser el más restringido y no debe utilizarse sobre documentos definitivos.

El punto de partida debe ser la **serie documental** o el **procedimiento**. No conviene decidir el acceso documento por documento, sino a partir del tipo de expedientes generados en una misma actividad administrativa. Si una serie contiene información reservada, datos personales o documentación sensible, esa característica debe reflejarse en su configuración general.

Para ello son esenciales los **metadatos de control de acceso**, que indican si una serie, expediente o documento es de acceso público, restringido o confidencial; si contiene datos personales; si existen motivos para limitar la consulta; o si determinadas personas o unidades están autorizadas.

HERENCIA DE PERMISOS



También debe controlarse la **herencia de permisos**: los expedientes suelen heredar las condiciones de la serie y los documentos las del expediente.

Esta lógica facilita la coherencia, pero no debe impedir aplicar restricciones adicionales cuando un expediente o documento requiera mayor protección.

Por este motivo, al revisar la configuración de acceso conviene comprobar siempre **tres niveles:**



1 NIVEL 1 · SERIE DOCUMENTAL

La serie marca la regla general

- Define los permisos base para la serie.
- Se aplica a todos los expedientes de la serie.



2 NIVEL 2 · EXPEDIENTE

El expediente puede introducir una excepción

- Permite ajustar o restringir el acceso cuando es necesario.
- Adapta los permisos al contenido y contexto del expediente.



3 NIVEL 3 · DOCUMENTO

El documento puede requerir una protección específica

- Determinados documentos pueden necesitar medidas adicionales de protección.
- El acceso puede ser más restrictivo que el del expediente.

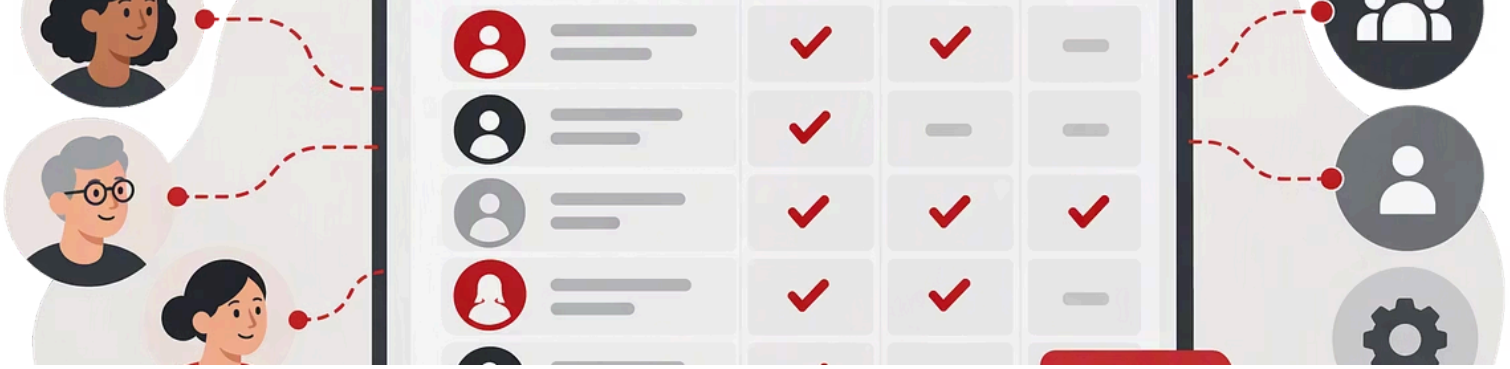


La herencia de permisos garantiza la coherencia, pero no debe impedir aplicar restricciones adicionales cuando la sensibilidad de la información lo requiera.

Las herramientas también deben registrar las acciones realizadas sobre expedientes y documentos. Estas **pistas de auditoría** permiten saber quién ha accedido, cuándo y qué acción ha realizado: consulta, edición, incorporación, modificación de metadatos, descarga o eliminación, según las funcionalidades disponibles.

El registro de accesos y acciones es una garantía de control: permite detectar accesos indebidos, modificaciones no autorizadas, eliminaciones improcedentes o usos anómalos, y reconstruir lo ocurrido en caso de incidencia.

Por ello, la configuración del acceso debe completarse con comprobaciones y auditorías periódicas. Estas revisiones ayudan a corregir errores y a mantener el sistema alineado con las necesidades reales de la organización.



3. Gestión de personas usuarias y roles

En el entorno electrónico, el acceso se gestiona mediante personas usuarias identificadas y roles asignados. El sistema debe saber quién accede y qué función cumple dentro del proceso documental.

Una **persona usuaria** es la identidad concreta que accede al sistema y debe ser individual, trazable y no compartida. Un **rol** es el conjunto de permisos asociados a una función. Esta separación permite revisar y ajustar permisos sin depender solo del nombre o cargo de cada persona.

Conviene diferenciar entre **roles funcionales**, vinculados a tramitación, consulta o aportación de documentación, y **personas usuarias de sistema**, con funciones transversales de administración, conservación, mantenimiento o soporte técnico.

En la tabla siguiente se resumen los roles funcionales más comunes:

Tipo	Finalidad práctica	Qué puede hacer normalmente	Precaución principal
Personal tramitador	Gestiona los expedientes durante la tramitación.	Crear expedientes, incorporar documentos, modificar metadatos editables, tramitar actuaciones y cerrar expedientes, según la fase y los permisos asignados.	No debe conservar permisos de edición cuando ya no participa en la tramitación o cuando el expediente pasad a fase archivística.
Consulta restringida	Permite consultar documentación no pública cuando existe una necesidad funcional justificada.	Consultar expedientes, documentos y metadatos, normalmente sin capacidad de modificación ni eliminación.	Debe limitarse a personas concretas, durante el tiempo necesario y sobre documentación específica.

Tipo	Finalidad práctica	Qué puede hacer normalmente	Precaución principal
Consulta	Permite el acceso a documentación que puede ser consultada de forma general.	Consultar documentos o metadatos definidos como públicos o de libre acceso.	Debe verificarse que no existan datos personales, información reservada o restricciones aplicables.
Terceras partes	Representan a personas interesadas, ciudadanía u otras entidades externas.	Consultar documentación cuando acreditan legitimación o condición de parte interesada.	Debe comprobarse la identidad, la legitimación y si procede aplicar anonimización o acceso parcial.
Aplicaciones	Permiten que una herramienta o sistema externo interactúe automáticamente con el gestor documental.	Crear expedientes, incorporar documentos o actualizar metadatos cuando el procedimiento lo requiere.	Su uso debe estar controlado, documentado y asociado a procesos concretos.

En la siguiente tabla se resumen las personas usuarias de sistema principales:

Tipo	Finalidad práctica	Qué puede hacer normalmente	Precaución principal
Administrador de gestión documental	Gestiona la documentación en fase archivística y vela por su conservación, organización y aplicación de criterios documentales.	Intervenir sobre expedientes cerrados, aceptar transferencias, revisar metadatos, aplicar criterios de conservación y eliminación.	Debe actuar conforme a los calendarios, fichas de series y criterios de acceso aprobados.
Administración tecnológica	Garantiza el funcionamiento técnico del sistema y mantiene operativos los accesos y configuraciones.	Configurar perfiles, mantener cuentas de personas usuarias y resolver incidencias técnicas.	No debe decidir por sí mismo los criterios documentales de acceso; sus actuaciones deben estar justificadas y monitorizadas.

La asignación de roles debe responder a una necesidad real. Cada alta, modificación o baja de permisos debería poder justificarse: quién la solicita, quién la autoriza, sobre qué documentación se aplica y durante cuánto tiempo.

Asimismo, deben evitarse las cuentas genéricas o compartidas, porque impiden reconstruir con seguridad quién ha consultado, modificado o eliminado un documento. Las credenciales deben ser personales e intransferibles.

La gestión de personas usuarias y roles no debe ser solo una tarea informática: permite garantizar que las reglas de acceso se aplican correctamente durante todo el ciclo de vida documental, especialmente en expedientes con datos personales, información restringida o documentación confidencial.

Como pauta práctica, conviene revisar periódicamente:

- si las personas usuarias siguen necesitando los permisos concedidos;
- si existen cuentas genéricas, duplicadas o sin persona responsable clara;
- si los cambios de puesto o de funciones se han reflejado en el sistema;
- si las personas usuarias de sistema actúan solo dentro de las funciones autorizadas.



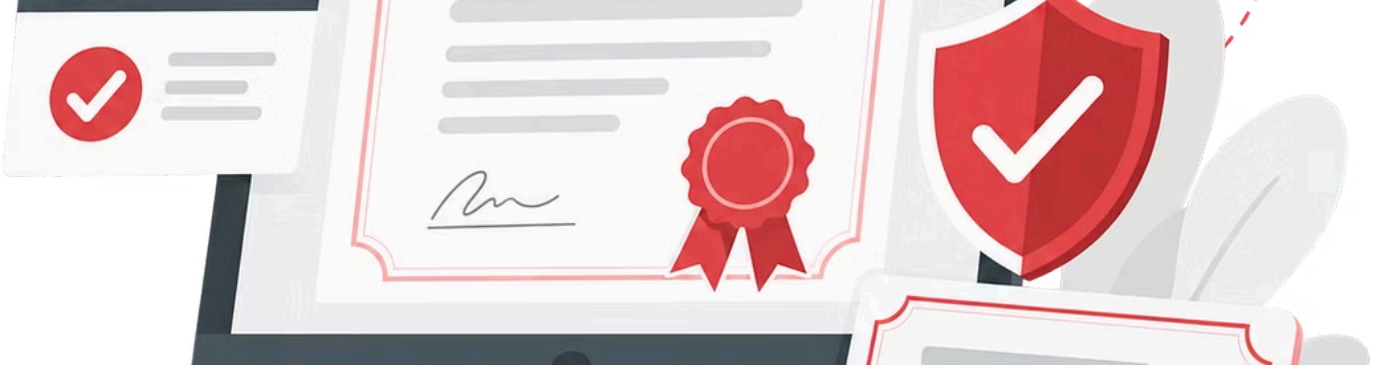
4. Funciones y responsabilidades del archivo en materia de acceso

El archivo debe participar en la definición, aplicación y supervisión de los criterios de acceso a la documentación electrónica. Su función es aportar criterio documental para que las reglas de acceso se apliquen de forma coherente durante todo el ciclo de vida, desde la tramitación hasta la conservación en el archivo digital.

En fase activa, la unidad tramitadora conserva la responsabilidad principal sobre el expediente, porque conoce el procedimiento y las necesidades reales de acceso. No obstante, el archivo debe intervenir cuando la configuración afecte a series documentales, metadatos de acceso, reglas de herencia o futuras transferencias al archivo digital. En fase de vigencia e histórica, su papel es más directo: aplicar las condiciones de acceso, revisar excepciones y asegurar que la consulta sea proporcionada y trazable.

Sus responsabilidades principales son:





5. Protección de datos en el acceso y difusión documental

La protección de datos debe integrarse en cualquier decisión de acceso, consulta o difusión documental. Debe analizarse qué información contiene la documentación, si identifica a personas físicas, si incluye datos especialmente protegidos y si puede facilitarse una versión parcial para resolver una determinada consulta.

A efectos prácticos, son **datos protegidos** aquellos que no pueden difundirse libremente porque afectan a la intimidad o a derechos fundamentales de las personas. Incluyen:

Datos identificativos

Nombre, DNI, dirección, firma, correo, teléfono, datos económicos, profesionales, familiares o de localización.

Datos especialmente sensibles

Salud, discapacidad, ideología, afiliación sindical, religión, orientación sexual, origen racial o étnico, datos biométricos o genéticos, infracciones, sanciones o situaciones de vulnerabilidad.

La identificación de datos protegidos no debe limitarse a los datos evidentes. Antes de facilitar una consulta o copia debe revisarse si el documento contiene datos de terceras personas, información no necesaria para la finalidad del acceso, información confidencial o elementos que permitan una identificación indirecta.

La **anonimización** y la **seudonimización** reducen riesgos en la consulta y difusión documental, pero tienen efectos distintos. La anonimización impide identificar a la persona por medios razonables; la seudonimización sustituye identificadores por códigos o seudónimos, pero permite reidentificar si se dispone de información adicional conservada por separado.

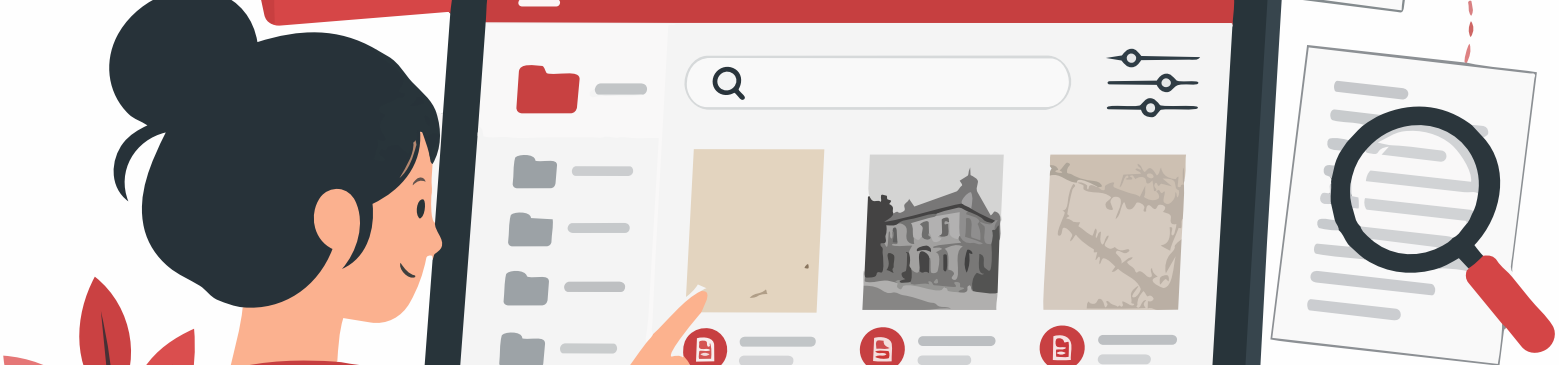
Cuando sea necesario compartir documentación con terceros, publicar información o facilitar una consulta parcial, puede generarse una **copia electrónica auténtica parcial** en la que se oculten, eliminen o sustituyan datos personales o información confidencial. Así se preserva el valor de la copia para la finalidad concreta y se reduce la exposición de información innecesaria. Para más información, véase el **bloque 8. Copias electrónicas**.

A continuación, se resumen las principales ventajas y desventajas de la anonimización y la seudonimización:

Técnica	Objetivo	Ventajas	Desventajas
Anonimización	Impedir que la persona pueda ser identificada directa o indirectamente.	Permite compartir o publicar información con menor riesgo. Útil cuando la identidad no es necesaria para la finalidad de la consulta.	Debe aplicarse de forma robusta. No basta con borrar nombres si otros datos permiten reidentificar a la persona. Puede reducir el detalle o utilidad de la información.
Seudonimización	Reducir la identificación directa sustituyendo datos identificativos por códigos o seudónimos.	Mantiene la posibilidad de relacionar registros o reconstruir la información cuando esté justificado. Útil para análisis o seguimiento interno.	La información sigue siendo dato personal si puede revertirse. La clave o tabla de correspondencia debe conservarse separada, protegida y con acceso muy restringido.

La elección entre anonimizar o seudonimizar depende de la finalidad del acceso. Si no es necesario identificar a las personas, es preferible una versión anonimizada o parcial; si se necesita relacionar la información con una persona concreta, puede usarse seudonimización con garantías reforzadas.

Estas técnicas deben aplicarse antes de la entrega, publicación o difusión. El archivo debe coordinarse con las unidades tramitadoras, servicios jurídicos, protección de datos e informática para determinar qué datos ocultar, qué versión conservar y qué evidencias registrar.



6. Consulta en el entorno electrónico

La consulta electrónica mantiene la misma finalidad que la consulta en papel: permitir el acceso a quienes tienen derecho o necesidad legítima. La diferencia es que en el entorno electrónico la documentación puede visualizarse, descargarse, compartirse o reproducirse con mucha más facilidad.

Cuando se genera una copia electrónica, esta es funcionalmente idéntica al documento original y no se devuelve al archivo. Una vez entregada, descargada o compartida, la organización pierde parte del control sobre su uso posterior. Por ello, debe definirse qué versión se facilita, durante cuánto tiempo, con qué restricciones y con qué evidencias de control.

Desde el punto de vista archivístico, pueden distinguirse varios tipos de consulta:

Consulta interna

Es la realizada por personal de la propia organización para ejercer funciones de tramitación, control, gestión, auditoría, asesoramiento jurídico, archivo o soporte técnico. Debe basarse en roles definidos y en el principio de necesidad de conocer.

Consulta ciudadanía / personas interesadas

Incluye las solicitudes de acceso formuladas por personas interesadas en un procedimiento, personas representantes, ciudadanía en general o personas solicitantes al amparo de la normativa de transparencia. Requiere comprobar identidad, legitimación, finalidad y posibles límites.

Consulta entre administraciones públicas

Se produce cuando otra administración necesita acceder a documentación para ejercer sus competencias, verificar datos o tramitar un procedimiento. Debe documentarse la finalidad, la base que justifica el acceso y el alcance concreto de la información facilitada.

Con independencia del tipo de consulta, el **procedimiento** debe seguir una secuencia común: recibir y registrar la solicitud, identificar quién solicita el acceso, qué documentación se pide y para qué finalidad, y verificar la identidad, legitimación o competencia de la persona o entidad solicitante.

Después, debe evaluarse si existen restricciones de acceso: régimen de la serie o expediente, datos personales, información confidencial, documentación reservada, derechos de terceras personas o límites normativos. Si procede, deben aplicarse medidas como anonimización, seudonimización, ocultación de fragmentos o copia parcial.

La documentación debe prepararse antes de la entrega: seleccionar los documentos pertinentes, comprobar la versión correcta, incluir los metadatos necesarios, generar una copia o paquete de consulta cuando proceda y dejar constancia de las transformaciones aplicadas.

Durante todo el proceso deben aplicarse **controles de consulta**: registrar quién solicita o consulta, qué documentación se entrega, cuándo, con qué finalidad, qué medidas de protección se aplican y si se permite visualización o descarga.

La información facilitada durante una consulta puede organizarse como un **Paquete de Información de Consulta (PIC)**, que agrupa la documentación objeto de acceso junto con los elementos necesarios para su interpretación, contextualización y control.

El **Paquete de Información de Consulta** o **PIC** es el conjunto organizado de información preparado para una consulta documental. Permite facilitar la documentación necesaria, junto con la información mínima para comprenderla, contextualizarla y verificar su integridad, sin exponer datos o documentos innecesarios.

El PIC no debe ser una simple descarga del expediente, sino una unidad preparada para la finalidad del acceso. Puede incluir documentos autorizados, metadatos, índice del expediente, relación de documentos, versiones anonimizadas o parciales y, cuando proceda, información sobre las limitaciones aplicadas.

Según la herramienta utilizada, el PIC puede tener un plazo limitado, una fecha máxima de consulta o permitir únicamente visualización de los documentos, sin descarga.

Para saber más

Normativa

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- 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.

Escenarios y situaciones habituales

Escenario 1. Acceso indebido a documentación con datos personales

Situación

Una persona profesional de archivo detecta, mediante auditoría, alerta del sistema o comunicación interna, que una persona usuaria ha accedido a documentación con datos personales sin una justificación evidente. El acceso puede afectar a un documento, expediente o serie, y deberse a permisos excesivos, clasificación incorrecta, regla de acceso mal aplicada o herencia automática de permisos.

Antes de actuar, el archivo debe revisar qué ha ocurrido y determinar si se trata de un acceso indebido, una configuración incorrecta o un acceso justificado no documentado.

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Revisar el detalle de lo sucedido.

Comprobar qué persona usuaria accedió, a qué documento, expediente o serie, cuándo y qué acción realizó: visualización, descarga, modificación, exportación u otra operación registrada.

2. Comprobar si los permisos de la persona usuaria eran correcto.

Verificar el rol asignado, los permisos concretos y si seguían justificados por las funciones actuales de la persona usuaria.

3. Comprobar si la clasificación del documento o expediente era correcta.

Revisar si el documento, expediente o serie tenía correctamente informado su nivel de acceso, restricciones, presencia de datos personales y régimen de consulta.

4. Valorar si el acceso estaba justificado o no.

Comprobar si existía una razón funcional, jurídica o técnica que justificara la consulta. Si existe, debe documentarse; si no, debe tratarse como incidencia.

5. Avisar a los ámbitos responsables.

Si el acceso no estaba justificado o existen dudas, avisar a Servicios Jurídicos e Informática. Si afecta a datos personales o puede suponer una brecha, activar también el circuito interno con protección de datos.

6. Aplicar medidas correctoras, si procede.

En función de la causa identificada, podrán adoptarse medidas como retirar o ajustar permisos, corregir la clasificación del documento o expediente, modificar los metadatos de acceso, revisar la herencia de permisos o bloquear temporalmente la consulta.

7. Documentar la actuación realizada.

Dejar constancia de la incidencia, comprobaciones, unidades informadas, conclusiones y medidas adoptadas.

8. Revisar si existen casos similares.

Tras resolver la incidencia, comprobar si el problema puede repetirse en otros documentos, expedientes o series y corregir la configuración general si procede.

Escenario 2. Personas usuarias con permisos demasiado amplios

Situación

Durante una revisión, auditoría o investigación de incidencia, el archivo detecta personas usuarias con permisos más amplios de los necesarios para sus funciones.

Puede tratarse de accesos generales a series, consulta restringida asignada de forma amplia, edición sobre expedientes cerrados, descarga de documentación sensible o permisos de administración no justificados.

Aunque no haya producido un acceso indebido, esta configuración supone un riesgo y debe revisarse según el principio de necesidad de conocer.

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Identificar a las personas usuarias y permisos afectados.

La persona profesional de archivo deberá revisar qué personas usuarias tienen permisos excesivos, sobre qué series, expedientes o documentos se aplican y qué acciones pueden realizar: consulta, edición o eliminación.

2. Comprobar la finalidad de los permisos asignados.

Verificar si responden a una función concreta y vigente: tramitación, archivo, control, auditoría, soporte técnico, asesoramiento jurídico u otra función justificada.

> ⚠ **¡ATENCIÓN!** No todos los accesos útiles son accesos necesarios. El hecho de que una persona usuaria pueda necesitar consultar ocasionalmente documentación de una unidad, serie o expediente no justifica que tenga acceso permanente.

3. Valorar el nivel de riesgo de la documentación afectada.

El análisis debe tener en cuenta si la documentación contiene datos especialmente protegidos. Cuanto más sensible sea la documentación, más restrictiva debe ser la configuración de permisos.

4. Coordinarse con otras unidades.

Si existen permisos excesivos, coordinarse con la unidad responsable, informática y, cuando proceda, servicios jurídicos o protección de datos para decidir qué mantener, modificar o retirar.

5. Aplicar medidas correctoras.

En función del análisis realizado, podrán adoptarse medidas como retirar permisos innecesarios, ajustar roles, revisar la herencia de permisos o crear roles nuevos específicos.

6. Documentar los cambios realizados.

Dejar constancia de los permisos revisados, cambios aplicados, autorización y criterio seguido.

7. Establecer revisiones periódicas.

Establecer revisiones periódicas de personas usuarias y roles, especialmente en series sensibles, para evitar acumulación de permisos injustificados.

Escenario 3. Revisión de permisos de personas usuarias tras un cambio de puesto de trabajo

Situación

Una persona usuaria cambia de puesto de trabajo, de unidad administrativa o de funciones dentro de la organización, pero conserva los permisos de acceso que tenía asignados en su puesto anterior. También puede ocurrir que una persona abandone la organización y su cuenta permanezca activa o siga teniendo permisos asociados en alguna herramienta.

Puede detectarse en revisiones periódicas, altas, modificaciones o bajas de permisos, auditorías o incidencias. También puede deberse a comunicaciones tardías, falta de circuito entre Recursos Humanos, unidad responsable, Informática y Archivo, o acumulación progresiva de permisos.

El riesgo radica en que la persona mantenga accesos que ya no necesita o, si ya no pertenece a la organización, que conserve usuarios activos. Esto compromete la seguridad, la protección de datos y la trazabilidad.

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Identificar el cambio producido.

Comprobar si se trata de cambio de unidad, puesto o funciones, sustitución temporal, baja de la organización o finalización de colaboración externa.

2. Revisar los permisos actuales.

Comprobar qué roles y permisos tiene asignados, sobre qué documentación se aplican y qué acciones permite realizar.

3. Coordinar la revisión con las unidades implicadas.

Coordinarse con unidad de origen, unidad de destino, Informática y, cuando proceda, Recursos Humanos, para confirmar permisos y asegurar bajas efectivas.

4. Retirar o ajustar permisos del puesto anterior.

Retirar permisos del puesto anterior cuando ya no estén justificados. Si se mantiene algún acceso temporal, debe limitarse en alcance y duración.

Si la persona ha abandonado la organización, el archivo debe comprobar, dentro de su ámbito, que no quedan permisos asociados a esa cuenta.

5. Asignar, si procede, los permisos del nuevo puesto.

Si el nuevo puesto requiere accesos, asignarlos según roles definidos y necesidad de conocer, evitando copiar permisos de otras personas o conceder accesos generales.

6. Revisar los mecanismos de comunicación y notificación de cambios.

Verificar que existen circuitos claros para comunicar cambios de puesto, funciones, adscripción o desvinculación de la organización a las unidades responsables de gestionar los permisos. En caso necesario, establecer medidas que garanticen una actualización oportuna de los accesos y eviten la acumulación de permisos no justificados.

Escenario 4. Solicitud de acceso o consulta de documentación

Situación

El archivo recibe una solicitud de acceso o consulta de documentación relativa a uno o varios expedientes. La solicitud puede proceder de una unidad interna, de una persona interesada o representante, de otra administración pública, o de una persona o entidad que formula una solicitud al amparo de la normativa de transparencia.

Aunque la documentación existe y está localizada, antes de facilitarla debe comprobarse si puede entregarse, con qué alcance, condiciones y canal, especialmente si hay dudas de legitimación, datos personales, información confidencial o restricciones de acceso.

El archivo debe aplicar una revisión ordenada para confirmar quién solicita el acceso, con qué finalidad, qué documentación necesita, qué restricciones existen y si procede facilitar documentación completa, parcial, anonimizada o un Paquete de Información de Consulta.

> El acceso por parte de las unidades tramitadoras a expedientes ya transferidos al archivo digital seguro presenta determinadas particularidades organizativas y tecnológicas. Estas se abordan específicamente en el escenario 5 del **bloque 9. Transferencia, ingesta y disposición documental.**

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Identificar quién solicita la documentación.

Comprobar si la solicitud procede de una unidad interna, persona interesada o persona representante, otra administración, órgano de control o solicitud de transparencia.

2. Verificar la identidad, representación o competencia.

Verificar identidad y, si procede, representación, competencia o finalidad que justifica la consulta.

3. Delimitar exactamente la documentación solicitada.

Si la solicitud es demasiado amplia o imprecisa, conviene acotarla antes de preparar la entrega. Debe identificarse qué expedientes o documentos se solicitan, evitando entregar más documentación de la necesaria.

4. Revisar el régimen de acceso y las restricciones aplicables.

El archivo deberá comprobar si la documentación tiene un régimen de acceso libre, restringido, confidencial o sometido a condiciones específicas.

5. Comprobar si contiene datos personales o información confidencial.

Revisar si contiene datos personales, datos especialmente protegidos, información reservada, datos de terceras personas u otra información que no deba comunicarse íntegramente.

6. Preparar la versión de consulta o entrega.

Decidir si se entrega toda la documentación, solo algunos documentos, una copia parcial o una versión anonimizada o seudonimizada, y generar el Paquete de Consulta. Evitar entregar el expediente completo si solo una parte es necesaria**.**

Escenario 5. Preparación de documentación con datos protegidos para consulta

Situación

El archivo debe preparar documentación para consulta, entrega, publicación o remisión a terceros, pero contiene datos personales, datos especialmente protegidos, información confidencial o datos de terceras personas.

La consulta puede estar justificada, pero no conviene facilitar el documento completo en su versión original cuando contiene, por ejemplo, datos de salud, económicos, DNI, direcciones, información sobre menores, denunciantes o información interna excluida de la entrega.

Este escenario se refiere a situaciones en las que ya se ha determinado que existe derecho de acceso, pero hay que revisar cómo preparar la documentación para que pueda consultarse o entregarse sin exponer más información de la necesaria.

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Identificar los datos protegidos presentes en la documentación.

Revisar qué datos personales o información confidencial contiene la documentación, incluidos datos que permitan identificación indirecta o revelen información sensible.

2. Determinar qué información es necesaria para la finalidad de la consulta.

Analizar qué parte de la documentación es necesaria. Si la finalidad puede satisfacerse sin identificar a determinadas personas o sin entregar ciertos documentos, preparar una versión limitada, parcial o anonimizada.

3. Decidir la técnica de protección más adecuada.

Elegir entre anonimización, seudonimización, ocultación de fragmentos, exclusión de documentos o copia electrónica auténtica parcial, según finalidad y tipo de información.

4. Preparar una copia o versión específica para la consulta.

Generar, cuando proceda, una copia parcial, versión anonimizada o PIC que incluya solo los documentos y metadatos necesarios.

5. Limitar las condiciones de acceso, si procede.

Si la herramienta lo permite, limitar a visualización sin descarga, fijar plazo máximo de consulta o restringir la disponibilidad del PIC.

6. Coordinar la decisión con los ámbitos competentes.

Coordinarse con la unidad responsable, servicios jurídicos, protección de datos e informática si hay dudas sobre datos a ocultar, copia parcial o derechos de terceras personas.

7. Documentar la versión facilitada y las medidas aplicadas.

Dejar constancia de la documentación revisada, datos ocultados o transformados, versión entregada, destinatario, canal, finalidad y plazo

Escenario 6. Modificación de reglas de acceso

Situación

El archivo detecta que debe modificarse el régimen de acceso de una serie documental, expediente o documento. La modificación puede consistir en restringir el acceso, ampliarlo, cambiar las condiciones de consulta o aplicar una regla específica a determinados documentos.

El cambio puede deberse a una modificación normativa, a la detección de datos personales o información sensible, a la finalización de un periodo de restricción, a una incidencia de seguridad, a una revisión archivística o a la necesidad de corregir una configuración que no refleja correctamente el criterio documental aprobado.

Antes de aplicar la modificación, el archivo debe comprobar qué regla estaba vigente, cuál debe aplicarse a partir de ahora, a qué nivel afecta y si debe aplicarse solo a nuevos expedientes o también a documentación ya existente.

Decisiones operativas

Se recomienda seguir los siguientes pasos:

1. Identificar el motivo de la modificación.

Comprobar si el cambio se debe a una modificación normativa, a una revisión de la serie, a la detección de datos personales o información confidencial, a la finalización de una restricción, a una incidencia o a una corrección de configuración.

2. Determinar a qué nivel se aplica el cambio.

Identificar si la nueva regla afecta a toda una serie documental, a expedientes concretos o solo a determinados documentos. Si existen documentos dentro de un expediente con una restricción diferente, deben tratarse como excepción.

3. Comparar la regla anterior y la nueva regla de acceso.

Documentar qué criterio estaba vigente, cuál se aprueba ahora, desde cuándo se aplica, qué documentación queda afectada y quién ha validado la decisión.

4. Valorar si afecta a expedientes existentes o solo a nuevos expedientes.

Comprobar si la modificación debe aplicarse de forma retroactiva a expedientes ya creados o solo a los que se creen a partir de la fecha de aplicación. Esta decisión es importante para evitar incoherencias entre expedientes de una misma serie.

5. Coordinar la modificación con los ámbitos implicados.

Coordinarse con la unidad tramitadora, Informática, Archivo, Servicios Jurídicos, las personas que ejercen como Delegado/a de Protección de Datos (DPD) y, cuando proceda, con las personas responsables de sede electrónica, portales de transparencia o aplicaciones de consulta.

6. Actualizar permisos, metadatos y reglas técnicas.

Verificar que la configuración técnica refleja la regla documental aprobada: permisos de lectura, edición o eliminación, metadatos de acceso, herencia de permisos, restricciones por perfil y condiciones de consulta o descarga.

7. Realizar pruebas con distintos perfiles de personas usuarias.

Comprobar que las personas usuarias autorizadas pueden acceder correctamente y que las personas usuarias no autorizadas no pueden consultar, descargar, modificar o eliminar documentación fuera de su permiso.

8. Mantener trazabilidad e histórico de reglas.

Registrar la modificación realizada, la fecha de aprobación y aplicación, las personas o unidades responsables, los accesos posteriores y, si procede, la fecha de revisión o finalización de la restricción.