Introducción

La gestión documental y el control de la información constituyen una de las funciones clave en cualquier organización moderna, independientemente de su tamaño o sector de actividad. Tanto en la empresa privada como en la administración pública, disponer de un sistema de archivo eficiente, optimizado y seguro es un requisito esencial para garantizar la continuidad del negocio, cumplir con las obligaciones legales y facilitar la toma de decisiones.

En la actualidad, el volumen de datos que se genera y se procesa en las organizaciones crece de manera exponencial. A los tradicionales documentos en papel se suman los archivos electrónicos, los registros contables digitalizados, los correos electrónicos, las bases de datos y un sinfín de soportes que exigen nuevas competencias de gestión. Este cambio ha transformado por completo la manera de organizar, conservar y custodiar la información, obligando a integrar herramientas informáticas, normas de seguridad y criterios de confidencialidad en la práctica diaria.

Este manual ofrece una visión integral y didáctica de los tres grandes bloques de conocimiento necesarios para desenvolverse con solvencia en este ámbito:

- **Gestión de archivos públicos y privados**: se abordan las técnicas clásicas de archivo documental, los procedimientos de registro, acceso y recuperación de la información, y las medidas de seguridad necesarias para garantizar la confidencialidad y la protección de datos. También, se estudian los sistemas operativos desde el punto de vista de su aplicación a la organización de archivos electrónicos.

- **Optimización básica de sistemas de archivo electrónico**: se analiza el papel de los equipos informáticos, tanto en sus elementos de hardware como de software, así como las acciones necesarias para el mantenimiento y la prevención de anomalías. Se explican los fundamentos de los sistemas operativos monousuario, multiusuario y en red, junto con las medidas de seguridad informática indispensables para proteger la integridad de los datos y los derechos de autor.

- **Gestión básica de información en bases de datos**: se introduce al lector en el mundo de los sistemas gestores de bases de datos, explicando su estructura, funciones y aplicaciones prácticas. Se detallan los procedimientos de introducción, actualización, consulta y presentación de la información, así como la interrelación con otras aplicaciones de uso cotidiano en la empresa.

A lo largo de sus capítulos, el libro combina la teoría con ejemplos prácticos, cuadros comparativos, esquemas explicativos y actividades de autoevaluación, con el objetivo de que el lector no solo adquiera conocimientos, sino también competencias aplicables en su entorno laboral.

La normativa vigente en materia de **protección de datos y seguridad de la información** atraviesa de forma transversal toda la obra, ya que constituye uno de los pilares de la gestión documental en el siglo XXI. El cumplimiento de estas obligaciones legales no es solo una cuestión formal, sino una garantía de confianza frente a clientes, proveedores y organismos públicos.

Este manual está concebido como una herramienta de aprendizaje progresivo, especialmente orientada a estudiantes de formación profesional, opositores y profesionales en activo que deseen actualizar sus conocimientos. Al finalizar su estudio, el lector será capaz de:

- Organizar y conservar archivos físicos y digitales con criterios técnicos.
- Implementar medidas de seguridad y confidencialidad en el acceso a la información.
- Optimizar sistemas de archivo electrónico y gestionar recursos informáticos básicos.
- Administrar de forma correcta y segura información contenida en bases de datos.

En definitiva, se trata de una guía práctica que responde a las necesidades reales de las organizaciones y que prepara al profesional para desempeñar con eficacia una de las funciones administrativas más relevantes en la era digital: la gestión segura, ordenada y estratégica de la información.

1

Gestión de archivos públicos y privados

La gestión de archivos constituye un eje esencial dentro de la organización administrativa moderna. En un entorno en el que la información se genera y circula de forma constante, disponer de sistemas eficaces para clasificar, conservar y recuperar documentos se convierte en una condición imprescindible para garantizar la **eficiencia, la transparencia y la seguridad jurídica** tanto en entidades públicas como privadas.

No se trata únicamente de almacenar papeles o ficheros electrónicos: la gestión archivística implica **planificación, organización y control** de los documentos a lo largo de todo su ciclo de vida. Desde que un documento nace (una factura, un contrato, un expediente, un correo electrónico) hasta su conservación o eliminación, debe seguir un proceso que asegure su utilidad, legalidad y accesibilidad.

En este capítulo se abordarán los fundamentos teóricos y prácticos que permiten entender el papel de los archivos en las organizaciones. Se hará especial énfasis en:

- La **importancia de los archivos** como herramienta de gestión administrativa.
- Las **diferencias entre archivos públicos y privados**, en función de su titularidad, normativa y finalidad.
- Las **técnicas de archivo documental**, que permiten clasificar, ordenar y mantener actualizada la información.

- Los **procedimientos de acceso, consulta y conservación**, tanto en sistemas convencionales como informáticos.
- Las **medidas de seguridad y confidencialidad** que aseguran la protección de datos y el cumplimiento de la normativa vigente.

De este modo, el estudiante podrá adquirir una visión integral sobre cómo se gestiona la información archivada en cualquier organización, comprendiendo su utilidad no solo en el plano administrativo, sino también en el legal, histórico y estratégico.

1.1 LA GESTIÓN DE ARCHIVOS EN LA EMPRESA

La gestión de archivos constituye uno de los pilares fundamentales en cualquier organización, ya sea pública o privada. Los archivos no son meros depósitos de documentos: son el soporte sobre el cual se construye la memoria administrativa, legal y operativa de una entidad.

A través de ellos se garantiza la trazabilidad de las actuaciones, la transparencia en los procesos y la posibilidad de acceder a la información cuando se necesita.

En el ámbito empresarial, una correcta gestión archivística permite responder de manera rápida a clientes, proveedores o instituciones, minimizando riesgos derivados de pérdidas de información o incumplimientos normativos.

En la Administración pública, por su parte, los archivos aseguran la continuidad del servicio, la protección de derechos ciudadanos y el cumplimiento de la legislación vigente en materia de documentación y acceso a la información.

La evolución tecnológica ha transformado profundamente este ámbito. Los archivos ya no se limitan a expedientes en papel, sino que integran documentos digitales, bases de datos y sistemas de almacenamiento en red. Esta transformación plantea nuevas exigencias: desde la adopción de software especializado hasta la aplicación de protocolos de seguridad que protejan la confidencialidad de los datos.

En este punto introductorio se abordará la relevancia de los archivos dentro de la organización, estableciendo las diferencias principales entre archivos públicos y privados, y sentando las bases para comprender cómo se estructuran, clasifican y gestionan en el día a día.

Con ello, el estudiante podrá valorar su papel estratégico en la gestión administrativa y reconocer la necesidad de implantar buenas prácticas archivísticas como parte esencial de cualquier entidad.

1.1.1 Importancia en la organización administrativa

La gestión de archivos constituye uno de los pilares fundamentales en el funcionamiento de cualquier organización, ya sea pública o privada. Un archivo no es únicamente un conjunto de documentos almacenados, sino un **sistema organizado de información** que permite garantizar la trazabilidad, la transparencia y la continuidad de la actividad administrativa.

En la vida diaria de una empresa, por ejemplo, los documentos permiten demostrar el cumplimiento de obligaciones fiscales, justificar operaciones contables, acreditar la relación laboral de los trabajadores o dar soporte legal a contratos y acuerdos comerciales. En el ámbito de la Administración pública, los archivos garantizan que los ciudadanos puedan ejercer su derecho de acceso a la información, que se cumplan

los principios de publicidad y transparencia y que las decisiones de los órganos de gobierno puedan revisarse en cualquier momento.

La importancia de la gestión documental puede resumirse en tres funciones esenciales:

- **Función administrativa:** los documentos sirven como prueba de las actuaciones realizadas y facilitan la toma de decisiones.
- **Función jurídica:** actúan como respaldo legal frente a reclamaciones o litigios, al acreditar derechos y obligaciones.
- **Función histórica y cultural:** en el caso de los archivos públicos, los documentos adquieren valor patrimonial, ya que conservan la memoria colectiva de la sociedad.

Ejemplo

Una pyme que organiza correctamente sus facturas y contratos puede atender una inspección de la Agencia Tributaria de forma rápida y sin sanciones. Por el contrario, si carece de un sistema de archivo eficiente, puede verse obligada a realizar búsquedas manuales interminables, con el riesgo de perder documentos clave.

Beneficios de una adecuada gestión de archivos

Beneficio principal	Ejemplo
Rapidez en la localización.	Encontrar un contrato en segundos gracias a un sistema de clasificación digital.
Cumplimiento normativo.	Conservar facturas durante los plazos exigidos por la Ley General Tributaria.
Seguridad de la información.	Proteger datos personales conforme a la LOPDGDD y al Reglamento Europeo de Protección.
Continuidad de la actividad.	Acceder a documentos digitales tras un siniestro gracias a copias de seguridad.

1.1.2 Diferencias entre archivos públicos y privados

Aunque los principios de organización archivística son comunes, es necesario distinguir entre **archivos públicos** y **archivos privados**, ya que responden a finalidades y normativas diferentes.

1. **Archivos públicos:**
   - Son gestionados por Administraciones públicas (ministerios, ayuntamientos, universidades, hospitales, etc.).
   - Están regulados por normas específicas, como la Ley 16/1985 del Patrimonio Histórico Español y la Ley 19/2013 de Transparencia, acceso a la información pública y buen gobierno.
   - Su finalidad trasciende la gestión administrativa: cumplen una función social, cultural y de conservación histórica.
   - Su acceso está garantizado a los ciudadanos, salvo en casos de información reservada o protegida por motivos de seguridad o privacidad.

Ejemplo

Los archivos municipales custodian los padrones de habitantes, registros de acuerdos plenarios y licencias urbanísticas, todos ellos accesibles bajo condiciones de consulta.

---

2. **Archivos privados:**
   - Son gestionados por empresas, asociaciones, colegios profesionales o particulares.
   - Su regulación deriva del Código Civil, el Código de Comercio y la normativa laboral y fiscal que obliga a conservar ciertos documentos durante plazos mínimos.
   - Su finalidad es eminentemente operativa y de respaldo legal.
   - El acceso es restringido, limitado a empleados, socios o personas autorizadas.

Ejemplo

En una empresa, los contratos con proveedores o las nóminas de los trabajadores son parte del archivo privado, y su consulta solo corresponde a personal autorizado.

Diferencias entre archivos públicos y privados

Aspecto	Archivos públicos	Archivos privados
Titularidad.	Administraciones públicas (Estado, CCAA, municipios).	Empresas, asociaciones, particulares.
Finalidad.	Gestión administrativa + conservación histórica y cultural.	Gestión operativa y respaldo legal.
Regulación normativa.	Ley 16/1985, Ley 19/2013, normativas autonómicas.	Código de Comercio, normativa fiscal y laboral.
Acceso.	Generalmente público, con limitaciones por protección de datos.	Restringido a personas autorizadas.
Valor documental.	Administrativo, jurídico, histórico y patrimonial.	Administrativo y jurídico principalmente.

Nota

Un buen profesional debe saber identificar si un documento pertenece a un archivo público o privado, ya que de ello dependerán los plazos de conservación, el acceso permitido y el tratamiento de seguridad de la información.

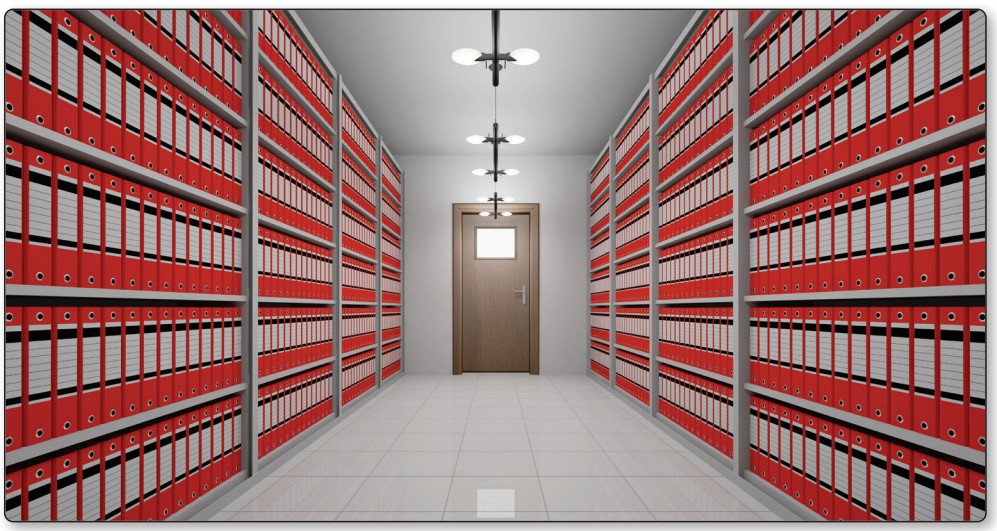
1.2 TÉCNICAS DE ARCHIVO DOCUMENTAL

La gestión de documentos en una organización no es un simple acto de almacenar papeles o archivos digitales. Se trata de un **proceso estratégico**, que garantiza que la información esté disponible, organizada, segura y actualizada para su uso cuando se necesite.

En este sentido, el archivo cumple un doble papel:

1. **Conservar la memoria institucional**: ya que un documento puede ser requerido muchos años después de haberse generado.
2. **Apoyar la toma de decisiones**: porque disponer de la información correcta, en el momento oportuno, permite trabajar con mayor eficacia y competitividad.

Para cumplir con esta misión, se aplican técnicas específicas que abarcan desde la **clasificación y ordenación** de los documentos, hasta la elaboración de **índices de consulta**, el empleo de **manuales internos de archivística** y la implantación de **sistemas de mejora continua**.



Un buen sistema archivístico es aquel que logra responder con rapidez y precisión a cuestiones tan prácticas como:

- ¿Dónde se encuentra un expediente determinado?
- ¿Quién tiene autorización para consultarlo?
- ¿Qué tiempo debe conservarse antes de ser eliminado?
- ¿Qué medidas garantizan la seguridad de la información contenida?
- ¿Cómo se corrigen los fallos detectados en el sistema?

A continuación, se desarrollan las principales técnicas de archivo documental que todo profesional administrativo debe dominar.

1.2.1 Sistemas de clasificación y ordenación

La **clasificación** consiste en **agrupar documentos siguiendo un criterio lógico** (nombre, número, fecha, tema, etc.), mientras que la **ordenación** establece la **secuencia interna de cada grupo**.

Ambos procesos son inseparables: un archivo mal clasificado o desordenado se convierte en inservible, aunque conserve todos los documentos.

Principales sistemas de clasificación

Sistema	Características	Ventajas	Inconvenientes	Ejemplo de uso
Alfabético	Los documentos se agrupan por orden de nombres propios o entidades.	Fácil de aplicar, comprensible para todos.	Riesgo de confusión en apellidos.	Archivo de clientes o proveedores.
Numérico	Se asigna un número a cada expediente.	Ocupa poco espacio en etiquetas	Requiere un índice auxiliar para localizar.	Expedientes de personal numerados.
Cronológico	Se ordena por fechas de emisión o recepción.	Muy útil para correspondencia y facturas.	Puede complicar la búsqueda si no se conoce la fecha exacta.	Registro de facturas recibidas.
Geográfico	Los documentos se agrupan por ubicación territorial.	Permite analizar información por áreas o delegaciones.	Poca utilidad si no se tiene referencia territorial.	Archivos de oficinas provinciales.
Temático	Clasificación por materias o asuntos.	Flexible y adaptable a cualquier organización.	Riesgo de dispersión si no se definen bien los temas.	Expedientes de “fiscalidad”, “laboral”, “comercial”.
Mixto	Combina dos o más criterios.	Ofrece mayor precisión.	Más complejo de mantener.	Clientes clasificados por provincia y número correlativo.

Ejemplo

Un despacho profesional recibe diariamente decenas de facturas de proveedores. Para gestionarlas, aplica un sistema **cronológico** dentro de carpetas **temáticas** (electricidad, suministros, alquileres). De este modo, se puede localizar rápidamente una factura tanto por fecha como por tipo de gasto.

1.2.2 Finalidad y objetivos del archivo

El archivo no debe concebirse como un simple almacén donde se acumulan documentos, carpetas o soportes digitales. Muy al contrario, constituye un **sistema organizado de información**, cuyo valor estratégico es comparable al de cualquier otro recurso de la empresa, como la tesorería, los recursos humanos o la infraestructura tecnológica.

En el entorno actual, caracterizado por la rapidez en los procesos administrativos, la exigencia legal en materia de protección de datos y la necesidad de decisiones empresariales basadas en información fiable, la correcta gestión del archivo resulta **imprescindible para garantizar la continuidad operativa y la competitividad**.

Podemos decir que el archivo cumple una triple función:

1. **Función administrativa**: asegurar la disponibilidad inmediata de la información necesaria para realizar tareas diarias.
2. **Función legal**: conservar los documentos que sirven como prueba en procedimientos judiciales, fiscales o laborales.
3. **Función histórica o patrimonial**: preservar la memoria y el conocimiento acumulado de la organización.

A continuación, se desarrollan sus objetivos esenciales.

Objetivos esenciales del archivo

1. **Disponibilidad**

   La primera exigencia de cualquier sistema de archivo es que la información esté disponible **en el momento en que se necesita**.

   - No sirve de nada conservar miles de documentos si no se pueden localizar de forma ágil.
   - El tiempo empleado en buscar información se traduce en costes ocultos para la empresa.

Ejemplo

Un responsable de recursos humanos necesita acceder de forma urgente al contrato laboral de un trabajador para presentarlo en una inspección. Si el archivo está bien organizado, puede encontrarlo en cuestión de minutos, ya sea en soporte físico o digital.

2. **Conservación**

   Los documentos deben mantenerse en buen estado durante todo el tiempo que marque la legislación o que la organización considere útil.

   - En archivos físicos, la conservación implica utilizar mobiliario adecuado, condiciones de temperatura y humedad controladas, y procedimientos de manipulación seguros.
   - En archivos digitales, requiere realizar **copias de seguridad periódicas**, actualizaciones tecnológicas y migración de soportes cuando sea necesario.

Ejemplo

Una factura emitida en 2020 debe conservarse al menos seis años, según el Código de Comercio. Si el documento se deteriora o se pierde antes de ese tiempo, la empresa puede enfrentarse a sanciones en una inspección.

3. **Confidencialidad**

   El archivo es depositario de datos sensibles: nóminas, historiales médicos de trabajadores, información financiera, contratos, etc. Proteger estos documentos de accesos indebidos no es solo una buena práctica, sino una **obligación legal recogida en el Reglamento General de Protección de Datos (RGPD)** y la Ley Orgánica de Protección de Datos (LOPDGDD).

   - En archivos físicos: implica restringir el acceso a salas y armarios, disponer de sistemas de cerraduras o claves y registrar los préstamos de documentos.
   - En archivos digitales: se aplican contraseñas, cifrado de archivos, niveles de acceso por usuario y auditorías de seguridad.

Ejemplo

Si las nóminas de los empleados quedan accesibles a cualquier trabajador en una carpeta compartida sin control, la empresa estaría vulnerando gravemente la normativa de protección de datos.

4. **Fiabilidad**

   Un archivo debe garantizar que los documentos que custodia son **auténticos, completos y verificables**. Esto permite utilizarlos como pruebas válidas en procedimientos de control interno o externo, auditorías, litigios o reclamaciones.

   - La fiabilidad se logra mediante el registro adecuado de la entrada y salida de documentos, la conservación de copias íntegras y la aplicación de sistemas de trazabilidad.
   - Los justificantes electrónicos con **Código Seguro de Verificación (CSV)** son un ejemplo de garantía de fiabilidad en la Administración pública.

Ejemplo

Durante una auditoría financiera, los auditores solicitan las facturas emitidas a un cliente en 2021. Si el archivo entrega documentos completos, con su correspondiente número de asiento y justificante de envío, la empresa demostrará transparencia y rigor contable.

5. **Eficiencia**

   Un archivo bien gestionado permite **ahorrar espacio, tiempo y recursos**.

   - Se evitan duplicidades de documentos.
   - Se reducen los costes de almacenamiento.
   - Se optimizan los procesos de búsqueda, consulta y actualización.

Ejemplo

En lugar de guardar diez copias impresas de un contrato, basta con conservar un original firmado en papel y una copia digital certificada en el sistema de gestión documental.

Finalidad última del archivo

Más allá de sus objetivos inmediatos, un archivo bien gestionado se convierte en un **activo de valor añadido** para la organización.

- **Cumplimiento normativo**: garantiza que la empresa actúa conforme a la legislación vigente (fiscal, laboral, mercantil, de protección de datos).
- **Mejora administrativa**: agiliza procesos internos como facturación, gestión de personal o atención al cliente.
- **Apoyo financiero**: facilita la presentación de documentación ante bancos o inversores, generando confianza.

- **Valor estratégico**: la información archivada se convierte en fuente de conocimiento para planificar proyectos, analizar tendencias y tomar decisiones fundamentadas.

Nota

Podemos concluir que el archivo es un auténtico **sistema nervioso documental** de la organización. Si falla, se paralizan los procesos y se multiplican los riesgos. En cambio, si funciona correctamente, aporta seguridad, confianza y competitividad.

Objetivos del archivo

Objetivo	Descripción	Ejemplo
Disponibilidad.	Localizar la información de forma inmediata.	Localizar un contrato en minutos para una inspección.
Conservación.	Mantener documentos íntegros y accesibles durante el tiempo legal.	Guardar facturas 6 años según Código de Comercio.
Confidencialidad.	Proteger información sensible de accesos indebidos.	Nóminas restringidas a RR. HH.
Fiabilidad.	Garantizar autenticidad y validez de los documentos.	Facturas con CSV válidas en auditoría.
Eficiencia.	Evitar duplicidades y reducir costes de gestión.	Usar un original + copia digital en lugar de 10 impresiones.

1.2.3 Índices de archivo y su actualización

Un archivo sin índice es como una **biblioteca sin catálogo**: la información existe, pero resulta prácticamente inaccesible. El índice es el **instrumento de localización y referencia** que permite identificar de manera rápida dónde se encuentra cada documento, expediente o carpeta dentro del sistema de archivo.

En la práctica archivística, el índice es la **puerta de entrada al archivo**, y su fiabilidad determina en gran medida la eficiencia de la gestión documental.

Tipos de índices más comunes:

1. **Índice alfabético**
   - Ordena los documentos por orden alfabético (ejemplo: clientes, proveedores, instituciones).
   - Útil cuando se consulta con frecuencia información por nombre propio o denominación social.

Ejemplo

"Transportes Marín" aparecerá en la sección T, "Almacenes López" en la A.

---

2. **Índice numérico**
   - Los expedientes reciben un número correlativo y se consultan en función de esa numeración.
   - Muy práctico para expedientes judiciales, facturas o registros de entrada.

Ejemplo

Factura 2024/0001, Factura 2024/0002, etc.

---

3. **Índice cronológico**
   - Ordena los documentos por la fecha en que fueron emitidos, recibidos o archivados.
   - Recomendado en procesos que requieren secuencia temporal (p. ej. actas, resoluciones, contratos).

4. **Índice digital**
    - Gestionado mediante bases de datos o sistemas de gestión documental (SGD).
    - Permite vincular directamente el registro del índice con el documento electrónico.

Ejemplo

En un gestor documental, al introducir "Factura 2024/0002", se abre automáticamente el PDF digitalizado.

Importancia de la actualización del índice

Un índice desactualizado provoca **errores, confusión y pérdida de tiempo**. Por ello, debe mantenerse vivo, incorporando cada alta, baja o modificación en tiempo real.

Buenas prácticas en actualización:

- Todo nuevo documento debe reflejarse en el índice en el momento de su registro.
- Los documentos eliminados por **expurgo** deben suprimirse también del índice.
- Los cambios en la estructura organizativa (p. ej. creación de una nueva categoría temática) deben reflejarse de inmediato.

Ejemplo

En un archivo alfabético de clientes, si se da de baja "Transportes Marín" y no se elimina del índice, seguirá apareciendo como activo en las búsquedas, lo que generará confusión y pérdida de tiempo en futuras consultas.

Tipos de índices y utilidad

Tipo de índice	Características principales	Uso recomendado
Alfabético.	Orden por nombres o materias.	Clientes, proveedores, instituciones.
Numérico.	Numeración correlativa.	Facturas, expedientes, registros de entrada.
Cronológico.	Orden por fechas.	Actas, resoluciones, contratos.
Digital.	Bases de datos y enlaces directos al documento.	Archivos electrónicos, gestión integral.

1.2.4 Uso de manuales de ayuda en archivística

Los **manuales de ayuda archivística** son documentos internos que establecen las normas y procedimientos que debe seguir todo el personal que trabaja con archivos. Su finalidad es asegurar que la gestión documental se realice de manera **homogénea, ordenada y conforme a la normativa vigente**.

Se convierten así en una guía de referencia para prevenir errores, garantizar la trazabilidad de la documentación y mantener la coherencia en el tiempo, incluso aunque cambien los responsables del archivo.

Contenido habitual de un manual archivístico

- **Descripción de los sistemas de clasificación empleados**: explica si el archivo es alfabético, numérico, cronológico o digital.
- **Normas para la creación, ordenación y conservación de documentos**: estandariza cómo se nombran las carpetas, en qué soportes se guardan, y por cuánto tiempo.

Tipo de documento	Plazo de conservación	Observaciones
Facturas.	6 años.	Según el *Código de Comercio* y la *Ley General Tributaria*.
Nóminas.	4 años.	Obligación establecida por la *Ley sobre Infracciones y Sanciones en el Orden Social (LISOS)*.
Expedientes laborales.	Hasta 5 años tras la baja del trabajador.	Recomendado para atender posibles reclamaciones o inspecciones.

- **Plazos legales de conservación**: define la permanencia de cada tipo documental según la normativa vigente.
- **Protocolos de acceso y consulta**: determina quién puede acceder a qué tipo de documento, con qué autorizaciones y bajo qué registro de control.
- **Digitalización y copias de seguridad**: establece formatos estándar de escaneo, frecuencia de copias y ubicación de los respaldos.
- **Procedimientos de expurgo y destrucción segura**: especifica cuándo y cómo destruir documentos para cumplir con la Ley de Protección de Datos (destrucción certificada, borrado seguro de archivos digitales).

Ejemplo

Un manual de archivo en una empresa puede indicar que:

- Las facturas se archivan cronológicamente por trimestres.
- Se conservan en archivo activo durante **2 años**.
- Posteriormente se trasladan a archivo pasivo durante **2 años más**.
- Pasado ese plazo, deben ser destruidas de forma **segura y certificada** para garantizar el cumplimiento de la normativa de protección de datos.

Problemas frecuentes:

- Documentos mal clasificados o duplicados.
- Índices obsoletos o incompletos.
- Espacios físicos saturados.
- Sistemas digitales desorganizados (carpetas sin criterio, nombres confusos).
- Falta de control en los accesos.

Propuestas de mejora:

- Auditorías internas periódicas del archivo.
- Digitalización con metadatos estandarizados.
- Revisión y depuración de índices.
- Uso de software de gestión documental (ERP, GED).
- Formación continua en técnicas de archivo para el personal administrativo.

Ciclo de mejora en el archivo documental

Fase	Descripción	Resultado esperado
Detección.	Identificación de errores o fallos en el sistema.	Reconocimiento de problemas reales.
Propuesta.	Diseño de soluciones concretas.	Plan de mejora.
Implementación.	Aplicación de las medidas correctivas.	Nuevo sistema más eficiente.
Evaluación.	Revisión de resultados alcanzados.	Confirmación de mejoras.
Reinicio.	Nuevos ajustes según las necesidades.	Archivo dinámico y actualizado.

Importante

Archivar no es guardar: es organizar estratégicamente la información para que siempre esté disponible, segura y útil.

1.2.5 Detección de problemas de organización y propuestas de mejora

Ningún sistema de archivo es perfecto ni está libre de incidencias. Aunque se diseñe de acuerdo con las mejores prácticas, el uso cotidiano, la entrada constante de nuevos documentos y la evolución de la propia organización hacen que aparezcan errores, desajustes o deficiencias que deben corregirse. La **detección temprana de estos problemas y la aplicación de medidas de mejora continua** son fundamentales para asegurar que el archivo cumpla siempre su función estratégica: conservar, organizar y poner a disposición la información de manera fiable, accesible y segura.

Un archivo mal gestionado no solo entorpece el trabajo administrativo, sino que también puede generar **riesgos legales, económicos y reputacionales**. Por ejemplo, conservar documentos durante más tiempo del debido incumpliendo la normativa de protección de datos puede acarrear sanciones, mientras que la pérdida de documentos clave puede dejar a la empresa indefensa ante una inspección o litigio.

A continuación, se describen los principales problemas que suelen detectarse en la gestión de archivos, acompañados de propuestas de mejora que permiten mantener el sistema actualizado, seguro y eficiente.

Problemas comunes en la organización de archivos

1. **Sobrecarga documental**

   Con el tiempo, los archivos tienden a saturarse de documentos que ya no son útiles o cuyo plazo legal de conservación ha vencido. Esto genera **espacios innecesariamente ocupados, mayor dificultad de búsqueda y costes añadidos de almacenamiento**.

Ejemplo

Carpetas con facturas de hace más de 10 años que ya no tienen valor fiscal ni legal, pero siguen ocupando espacio físico o digital.

---

2. **Desactualización del índice**

   Si el índice del archivo no se mantiene actualizado, los registros dejan de reflejar la situación real de los documentos. Un índice obsoleto provoca **confusión, pérdidas de tiempo en las búsquedas y duplicación de esfuerzos**.

Ejemplo

Un cliente dado de baja que sigue apareciendo en el índice como activo.

3. **Clasificación incoherente**

   La falta de criterios uniformes en la clasificación hace que un mismo tipo de documento aparezca en categorías diferentes, lo que genera **desorden y dificultades de localización**.

Ejemplo

Las nóminas de los empleados archivadas unas veces en “Recursos Humanos” y otras en “Contabilidad”.

4. **Acceso inadecuado**

   En algunos sistemas, la información sensible está disponible para cualquier empleado, lo que constituye un **riesgo de confidencialidad y protección de datos**.

Ejemplo

Nóminas o expedientes disciplinarios que pueden ser consultados por cualquier usuario de la red sin restricción.

5. **Falta de digitalización**

   Cuando los archivos se mantienen solo en formato papel, se dificulta el acceso remoto, la trazabilidad y la protección frente a desastres (incendios, inundaciones, deterioro físico).

Ejemplo

Contratos guardados únicamente en archivadores físicos, sin respaldo digital.

Propuestas de mejora

Para superar estas incidencias, es necesario implementar medidas correctivas y preventivas que aseguren la calidad de la gestión documental:

1. **Expurgo periódico**
   - Definir un calendario de expurgo adaptado a la normativa legal y a las necesidades de la empresa.
   - Establecer criterios claros de qué conservar y qué destruir.
   - Asegurar que la destrucción de documentos se realice de forma certificada en el caso de información sensible.
2. **Revisión de índices**
   - Programar revisiones trimestrales o semestrales para verificar que el índice refleja fielmente la realidad del archivo.
   - Eliminar registros de documentos dados de baja o caducados.
   - Actualizar categorías y referencias en caso de cambios organizativos.
3. **Establecer auditorías internas**
   - Realizar controles periódicos para detectar incoherencias en la clasificación, accesos indebidos o deficiencias en la custodia de documentos.
   - Generar informes que permitan tomar decisiones de mejora y ajustar procedimientos.

4. **Implantación de software de gestión documental (SGD)**
   - Permite automatizar procesos de clasificación, indexación y búsqueda.
   - Facilita la trazabilidad de los documentos y el control de accesos según roles de usuario.
   - Reduce la dependencia de procedimientos manuales y el riesgo de errores humanos.
5. **Formación del personal**
   - Capacitar a los empleados en clasificación, confidencialidad y normativa de protección de datos.
   - Impartir talleres sobre el uso de herramientas digitales y buenas prácticas archivísticas.
   - Promover una cultura organizativa orientada al cumplimiento normativo y la mejora continua.

Problemas y soluciones en archivos

Problema detectado	Ejemplo	Propuesta de mejora
Sobrecarga documental.	Carpetas con facturas caducadas hace 10 años.	Expurgo anual según normativa.
Índice desactualizado.	Cliente dado de baja sigue en registros.	Revisión trimestral del índice.
Clasificación incoherente.	Nóminas archivadas en carpetas distintas.	Manual de archivo unificado y formación interna.
Acceso inadecuado.	Nóminas consultables por cualquier usuario en red.	Asignación de permisos y control por roles.
Falta de digitalización	Documentos solo en papel	Escaneo y archivo digital con copias de seguridad

Nota

La detección de problemas en archivos debe concebirse como parte de un ciclo de **mejora continua**. No basta con corregir un error puntual; es imprescindible establecer mecanismos permanentes de control, auditoría y actualización, para que el archivo siga siendo un recurso estratégico y fiable a lo largo del tiempo.

1.3 PROCEDIMIENTOS DE REGISTRO Y ARCHIVO

El **registro y archivo de documentos** constituye una de las funciones básicas en cualquier organización, ya que garantiza la trazabilidad, la disponibilidad y la custodia adecuada de la información. No se trata únicamente de un proceso técnico, sino de un **mecanismo estratégico** que asegura el cumplimiento de la normativa, la eficiencia administrativa y la fiabilidad de la gestión.

Registrar un documento significa **dotarlo de identidad administrativa propia**: asignarle una referencia única, incluirlo en un índice, establecer su ubicación y dejar constancia de su entrada, salida o generación interna. Archivar, por su parte, supone **ubicar el documento en el espacio físico o digital correspondiente**, siguiendo normas de clasificación, ordenación y conservación previamente establecidas.

Este proceso implica la combinación de tres dimensiones:

- **Recursos materiales**: soportes, mobiliario, contenedores, dispositivos de almacenamiento.
- **Recursos técnicos**: sistemas de indexación, programas de gestión documental, digitalización.
- **Recursos humanos**: personal administrativo formado y con capacidad para aplicar los protocolos de seguridad, confidencialidad y organización.

Un buen procedimiento de registro y archivo convierte a la información en un recurso **estratégico y operativo**, al servicio de la empresa y de las obligaciones legales.

1.3.1 Identificación de soportes, mobiliario y útiles de archivo

Cuando pensamos en un archivo, lo primero que suele venir a la mente son estanterías repletas de carpetas, cajas o incluso servidores llenos de documentos digitalizados. Sin embargo, detrás de esta imagen existe una organización mucho más compleja que se apoya en **soportes**

físicos y digitales, en **mobiliario especializado** y en un conjunto de **útiles y herramientas** que permiten que la información pueda almacenarse, clasificarse y consultarse de manera eficaz.

La identificación de estos elementos es fundamental porque constituyen la **infraestructura básica** de cualquier sistema de archivo. Un buen profesional administrativo no solo debe saber manejar documentos, sino también conocer cuáles son los soportes más adecuados según el tipo de información, qué mobiliario garantiza una conservación óptima y qué herramientas facilitan el acceso y la protección de los archivos.

En este sentido, los **soportes** hacen referencia al medio en el que la información se encuentra contenida: desde el papel tradicional hasta los discos duros, la nube o las memorias USB. El **mobiliario**, por su parte, se relaciona con los espacios y estructuras que permiten almacenar de forma ordenada esos soportes: archivadores, estanterías, armarios compactos o sistemas automatizados. Finalmente, los **útiles de archivo** incluyen todos aquellos materiales auxiliares que hacen posible la organización diaria, como carpetas, fundas, separadores, cajas clasificadoras, etiquetas o software de gestión documental.

Conocer y seleccionar correctamente estos recursos no es una cuestión menor: de ello depende la **eficiencia administrativa**, la **seguridad de la información** y la **durabilidad de los documentos**. Un soporte inadecuado, un mobiliario mal diseñado o la ausencia de herramientas apropiadas pueden dificultar el acceso a datos esenciales, generar pérdidas de tiempo o incluso ocasionar daños irreversibles en documentos de valor legal o histórico.

Por tanto, en este apartado exploraremos los principales tipos de soportes, mobiliario y útiles de archivo, sus características, ventajas, limitaciones y criterios de selección. El objetivo es que el estudiante comprenda que la gestión documental no solo consiste en ordenar papeles o ficheros digitales, sino en construir un **entorno físico y digital eficiente y seguro** que respalde todo el proceso de conservación y consulta de la información.

a) **Soportes documentales**

El primer paso es reconocer el soporte en que se encuentra la información:

- **Soporte papel**: tradicional en facturas, contratos, informes, expedientes. Sigue siendo indispensable en procesos legales y notariales.
- **Soporte digital**: archivos electrónicos en formatos como PDF, DOCX, XLSX o bases de datos. Permite rapidez en la consulta y distribución.
- **Soportes especiales**: microfichas, CD, DVD, cintas magnéticas, soportes audiovisuales y multimedia. Se utilizan en archivos históricos o técnicos especializados.

Ejemplo

Un hospital mantiene las historias clínicas en soporte digital con acceso restringido, pero conserva en papel los consentimientos informados firmados por los pacientes, debido a exigencias legales.

b) **Mobiliario de archivo físico**

El mobiliario no solo sirve para almacenar, sino para **facilitar el acceso y proteger la documentación**.

- **Archivadores verticales con carpetas colgantes**: ideales para expedientes activos en uso frecuente.
- **Estanterías metálicas y armarios cerrados**: pensados para cajas y carpetas menos consultadas.
- **Planeros o mapotecas**: diseñados para documentos de gran formato (planos, carteles, mapas).
- **Armarios ignífugos o de seguridad**: garantizan la protección frente a incendios, humedad o accesos no autorizados.

c) **Útiles de archivo**

Los pequeños recursos de organización permiten **ordenar y localizar documentos con mayor rapidez**:

- Carpetas, subcarpetas y separadores temáticos.
- Cajas normalizadas (ej. formato A4 o folio).

- Etiquetas con códigos de colores para identificar categorías (ej. verde para facturas, azul para contratos).
- Sellos de registro, numeradores y sistemas de codificación para controlar entradas y salidas.

Ejemplo

En un despacho de abogados, los expedientes judiciales se archivan en carpetas numeradas, con etiquetas que diferencian civil, penal y laboral. Además, se digitalizan y se suben a una plataforma de gestión documental con copia de seguridad.

1.3.2 Contenedores y su función

Los contenedores son **soportes de agrupación** que protegen los documentos, facilitan su transporte y aseguran un orden coherente.

Tipo de contenedor	Uso principal	Ventajas	Limitaciones
Cajas de archivo.	Documentos semiactivos o históricos.	Fáciles de transportar y almacenar.	Requieren espacio físico amplio.
Carpetas colgantes.	Expedientes activos de consulta frecuente.	Acceso rápido y orden visual.	Capacidad limitada.
Archivadores de anillas.	Agrupación de documentos seriados (facturas, informes).	Permite añadir/quitar documentos.	Se deterioran con uso continuado.
Carpetas simples.	Documentación de un único asunto.	Simples y económicas.	Menor protección.
Contenedores digitales.	Almacenamiento en servidores, nubes o software.	Acceso remoto, trazabilidad, copias de seguridad.	Riesgo de ciberataques, dependencia tecnológica.

Ejemplo

En una empresa de construcción, los planos de proyectos activos se conservan en planeros para consulta inmediata, mientras que los expedientes cerrados se digitalizan y se guardan en cajas de archivo que pasan a archivo histórico.

1.3.3 Reproducción y cotejo de información: del papel al formato digital

La digitalización ha transformado la gestión documental. Hoy, un archivo que no incorpora procedimientos electrónicos **pierde eficiencia y competitividad**.

a) **Digitalización**
   - **Escaneo de documentos individuales** en PDF o TIFF.
   - **Captura masiva con escáneres de alto rendimiento** para expedientes completos.
   - **Tecnología OCR (Reconocimiento Óptico de Caracteres)**, que convierte la imagen en texto editable y buscable.

b) **Cotejo de información**

   Digitalizar no basta: es necesario **verificar la exactitud de la copia electrónica** respecto al original.
   - El cotejo puede realizarse manualmente (comparación visual) o con software especializado.
   - En documentos con validez legal, puede requerirse **firma electrónica reconocida** o certificados digitales para garantizar autenticidad.

Ejemplo

Una universidad escanea expedientes de alumnos y coteja cada documento con el original. Posteriormente, los incorpora al sistema de gestión documental con firma digital del responsable administrativo.

c) **Ventajas de la digitalización**

- Ahorro de espacio físico.
- Acceso remoto desde distintos dispositivos.
- Mayor seguridad mediante copias de respaldo.
- Localización inmediata gracias a buscadores internos.

d) **Precauciones**

- Cumplimiento estricto de la **LOPDGDD** y el **RGPD**.
  - Establecer protocolos de copia de seguridad.
  - Implementar contraseñas, roles de acceso y encriptación.

Procedimientos de registro y archivo

Etapa	Acciones principales	Resultado esperado
Identificación de soportes.	Definir si es papel, digital u otro formato.	Clasificación inicial coherente.
Uso de mobiliario y útiles.	Carpetas, archivadores, software de gestión.	Organización y acceso ágil.
Contenedores adecuados.	Elección según formato y volumen.	Protección y custodia segura.
Digitalización y cotejo.	Escaneo + verificación.	Documento electrónico válido y accesible.
Registro en índice.	Asignar referencia única.	Localización rápida y trazabilidad.

Nota

Los procedimientos de registro y archivo deben revisarse periódicamente para adaptarse a los cambios tecnológicos y normativos. El **modelo híbrido** (papel + digital) es hoy el más extendido, pero la tendencia apunta a una transición progresiva hacia archivos electrónicos integrales.

1.4 ACCESO, BÚSQUEDA Y RECUPERACIÓN DE LA INFORMACIÓN ARCHIVADA

El archivo no tiene sentido si los documentos que contiene no pueden localizarse de manera rápida, segura y eficiente. La finalidad última de cualquier sistema de gestión documental es que la información esté **disponible en el momento en que se necesite**, sin pérdida de tiempo ni riesgo de error.

El acceso a la información archivada debe responder a tres principios fundamentales:

- **Rapidez**: localizar un documento en el menor tiempo posible.
- **Seguridad**: garantizar que solo las personas autorizadas pueden acceder a información sensible.
- **Fiabilidad**: asegurar que el documento recuperado es auténtico, completo y corresponde al solicitado.

De esta manera, la gestión de archivos se convierte en un proceso que equilibra la **eficiencia operativa** con la **protección de la información**.

1.4.1 Procedimientos de búsqueda y consulta

Los procedimientos de búsqueda dependen directamente del sistema de clasificación utilizado y de la calidad del registro y los índices. Un archivo sin índices actualizados es como una biblioteca sin catálogo: la información existe, pero resulta prácticamente inaccesible.

a) **Métodos de búsqueda más habituales**

- **Búsqueda alfabética**: se ordenan los documentos por nombre de empresa, cliente o tema.
- **Búsqueda numérica**: cada expediente recibe un número único y correlativo que facilita la localización.
- **Búsqueda cronológica**: los documentos se archivan por fecha de emisión, recepción o vencimiento.

- **Búsqueda digital**: realizada en bases de datos o gestores documentales mediante palabras clave, filtros, metadatos o códigos QR.

1.4.2 Actualización, conservación y custodia de la información

Un archivo no es estático: debe mantenerse **actualizado, seguro y conforme a la normativa vigente**. La obsolescencia de los datos o la pérdida de documentos comprometen tanto la operativa de la empresa como su seguridad jurídica.

a) **Actualización de la información**

- **Altas**: cada documento nuevo debe registrarse e incorporarse al índice.
- **Bajas**: los documentos caducados deben eliminarse siguiendo los plazos de conservación legal.
- **Modificaciones**: cuando un expediente cambia (ejemplo: nueva dirección de cliente), debe actualizarse en el registro y en el archivo.

Ejemplo

Si un cliente cambia de domicilio fiscal, el expediente archivado debe actualizarse para evitar que futuras comunicaciones se envíen a la dirección antigua.

---

b) **Conservación**

La conservación implica garantizar que los documentos se mantienen en buen estado y accesibles durante el tiempo necesario.

- **Conservación física**: uso de carpetas y cajas en condiciones adecuadas de temperatura, humedad y protección frente a incendios.

- **Conservación digital**: copias de seguridad, migración de formatos y almacenamiento en servidores seguros o en la nube.

Ejemplo

Las facturas deben conservarse al menos 6 años (según Código de Comercio). Una empresa puede archivarlas en papel, pero también digitalizarlas y mantener copias de seguridad en la nube.

c) **Custodia y seguridad**

La custodia se refiere a las medidas que garantizan que la documentación no se pierda, deteriore o acceda indebidamente.

- **Medidas técnicas**: contraseñas, encriptación, sistemas antivirus, firewalls.
- **Medidas organizativas**: control de accesos, protocolos de préstamo y devolución de expedientes.
- **Medidas legales**: cumplimiento de la **LOPDGDD** y el **RGPD**.

Conservación y custodia documental

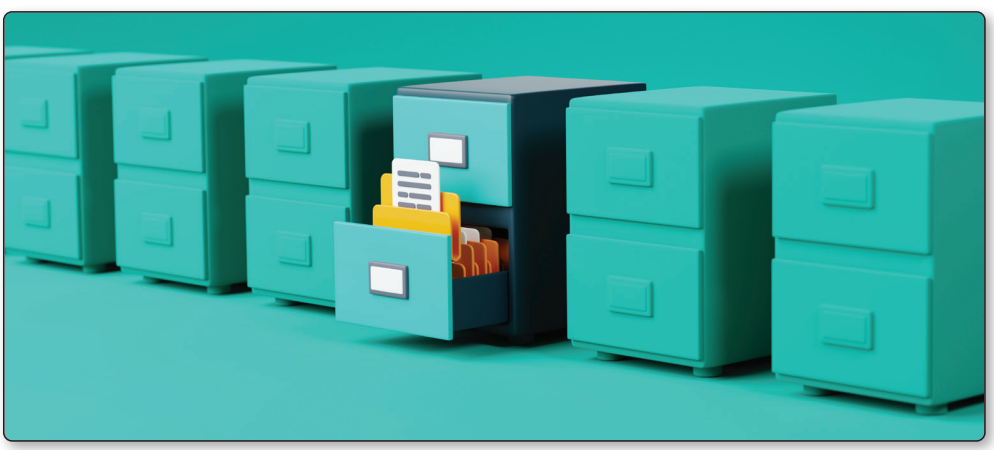
Aspecto	Documentación física	Documentación digital
Conservación.	Carpetas, cajas, armarios ignífugos.	Copias de seguridad, nube, servidores.
Accesibilidad.	Índices en papel, préstamo interno.	Buscadores, metadatos, filtros.
Seguridad.	Control de acceso a depósitos, llaves físicas.	Contraseñas, encriptación, roles.
Normativa.	Código de Comercio, Ley 39/2015.	RGPD, LOPDGDD, ENS.

Nota

La información mal custodiada no solo afecta a la operatividad diaria, sino que puede generar **responsabilidades legales** en caso de pérdida de datos personales o incumplimiento normativo. Por ello, actualizar, conservar y custodiar los documentos es una función esencial del técnico administrativo.

1.5 SISTEMAS OPERATIVOS Y GESTIÓN DE ARCHIVOS ELECTRÓNICOS

En la actualidad, el concepto de archivo ha evolucionado de manera radical. Durante décadas, la gestión documental se centraba en expedientes en papel, archivadores físicos y cajas de conservación. Sin embargo, el auge de las tecnologías de la información y la digitalización masiva de procesos ha transformado este escenario: hoy en día, más del 90 % de la información que se genera en una empresa es de origen electrónico y se gestiona a través de sistemas informáticos.



Esto implica que **el núcleo de la gestión documental moderna no se encuentra en el papel, sino en el entorno digital**, donde el **sistema operativo (SO)** actúa como la base que organiza y coordina todos los elementos necesarios para almacenar, acceder, compartir y proteger la información.

El sistema operativo puede definirse como el **conjunto de programas básicos que permiten que un ordenador o dispositivo funcione**. Es la capa intermedia entre el hardware (procesador, memoria, discos duros, dispositivos de red, periféricos) y el software de aplicación (programas de ofimática, bases de datos, navegadores, aplicaciones de gestión documental, etc.). Gracias a esta capa, los usuarios pueden interactuar con los equipos de manera sencilla y realizar operaciones como crear carpetas, copiar documentos, ejecutar aplicaciones o establecer permisos de seguridad.

Importancia de los sistemas operativos en la gestión documental

La relación entre sistemas operativos y gestión documental es directa y esencial. Cada archivo que se genera, cada documento que se guarda y cada acceso que se realiza se encuentra regulado por funciones del sistema operativo.

Las **ventajas de una gestión documental apoyada en un SO bien configurado** son múltiples:

- **Rapidez en el acceso a la información**: permite localizar un documento en segundos mediante rutas de acceso, buscadores o índices digitales.
- **Reducción de errores**: gracias a sistemas de nombres, jerarquías de carpetas y herramientas de verificación automática.
- **Conservación de versiones históricas**: el SO permite mantener copias previas de un mismo archivo o integrar herramientas de control de versiones.
- **Trazabilidad de cambios**: en entornos multiusuario, se puede identificar qué persona creó, modificó o eliminó un documento.
- **Cumplimiento normativo**: se facilita el respeto a leyes como la Ley de Protección de Datos Personales (LOPDGDD en España) o el Reglamento General de Protección de Datos (RGPD) en la Unión Europea.
- **Seguridad reforzada**: gracias a la asignación de permisos, cifrado de discos, autenticación de usuarios y control de accesos.

Ejemplo

En una asesoría fiscal, los sistemas operativos de sus ordenadores y servidores permiten que los técnicos puedan acceder únicamente a las carpetas de los clientes que gestionan. Los documentos de nóminas están protegidos con permisos de lectura restringida, mientras que los modelos fiscales trimestrales pueden ser modificados por el área de contabilidad, garantizando seguridad y eficiencia.

Papel del sistema operativo en el ciclo de vida de los documentos electrónicos

Todo documento digital pasa por un ciclo de vida en el que el sistema operativo tiene un rol fundamental:

1. **Creación** → mediante programas de ofimática, bases de datos o aplicaciones especializadas. El SO organiza su almacenamiento en carpetas o bases de datos.
2. **Clasificación** → asignación de nombres, metadatos y rutas de acceso que permiten su identificación.
3. **Acceso y consulta** → el SO gestiona permisos de usuario, búsqueda rápida y apertura de los documentos.
4. **Modificación y control de versiones** → se registran cambios, fechas y usuarios responsables.
5. **Conservación** → aplicación de medidas de seguridad, copias de respaldo y almacenamiento en servidores o nubes.
6. **Expurgo o eliminación** → una vez cumplidos los plazos legales o cuando deja de ser útil, el SO facilita su supresión definitiva, incluso con borrado seguro para datos sensibles.

Funciones clave del sistema operativo en la gestión documental

Función del SO	Aplicación en la gestión documental	Ejemplo
Creación y almacenamiento.	Permite guardar archivos en carpetas y asignar nombres únicos.	Guardar contratos de empleados en PDF en "RR. HH. 2024".
Organización jerárquica.	Facilita la estructuración en carpetas y subcarpetas.	Carpeta "Clientes" → Subcarpeta "IVA" → Facturas enero.
Seguridad y permisos.	Regula accesos según roles de usuario.	Solo dirección accede a informes financieros anuales.
Trazabilidad.	Registra quién y cuándo modificó un archivo.	Registro de auditoría de un expediente digital.
Copias de seguridad.	Integración con herramientas de backup.	Copia automática diaria en la nube corporativa.
Integración en red.	Comparte recursos entre usuarios y equipos.	Acceso de varios departamentos a una base de datos.

Nota

Comprender el papel de los sistemas operativos en la gestión documental es fundamental porque constituyen la **infraestructura invisible** que sostiene el archivo digital de una empresa. Un error en la configuración del sistema operativo puede poner en riesgo toda la información de la organización, mientras que un uso correcto garantiza eficiencia, seguridad y cumplimiento legal.

1.5.1 Funciones y características de los sistemas operativos

Los sistemas operativos (SO) son la base de cualquier infraestructura digital, tanto en el ámbito doméstico como en el empresarial. En gestión documental, su importancia es aún mayor, ya que actúan como el **"administrador invisible"** que regula la forma en que se crean, almacenan, protegen y comparten los archivos electrónicos de una organización.

Un SO no es un simple programa, sino un conjunto de instrucciones que gestiona el **hardware** (procesador, memoria, discos duros, periféricos)

y coordina el **software** (aplicaciones de gestión, bases de datos, programas ofimáticos). Su papel es garantizar que todo funcione de manera integrada, segura y eficiente.

Las funciones principales de los sistemas operativos aplicadas a la gestión documental son:

1. **Gestión de recursos**: regulan el uso de la memoria, el procesador, los dispositivos de almacenamiento y la red. Esto asegura que varios usuarios o programas puedan trabajar al mismo tiempo sin conflictos.
2. **Interfaz con el usuario**: facilitan el acceso a los archivos mediante entornos gráficos (Windows, macOS) o intérpretes de comandos (Linux, Unix). Gracias a ellos, es posible navegar por carpetas, buscar documentos y ejecutar aplicaciones de forma intuitiva.
3. **Ejecución de programas**: permiten abrir, modificar, guardar e imprimir documentos a través de aplicaciones ofimáticas, programas de contabilidad, software de bases de datos, etc.
4. **Gestión de archivos**: organizan la información en discos y servidores mediante carpetas, subcarpetas, atributos y metadatos. Sin este componente, localizar un documento sería casi imposible.
5. **Seguridad y permisos**: regulan qué usuarios pueden acceder, modificar o eliminar un archivo. Esto es fundamental para garantizar la **confidencialidad de la información**.
6. **Comunicación en red**: posibilitan que los archivos se compartan entre distintos equipos conectados a una red local (LAN) o a servidores en la nube, facilitando el trabajo colaborativo.

Ejemplo

En una empresa con 50 empleados, el servidor utiliza **Windows Server** para administrar carpetas compartidas. Gracias a los permisos de Active Directory, el departamento de contabilidad accede solo a sus expedientes, mientras que los técnicos de recursos humanos consultan únicamente nóminas. La dirección general, por su parte, tiene acceso global, pero en muchos casos en modo de solo lectura para evitar modificaciones no deseadas.

Sistemas operativos habituales en la gestión documental

Sistema operativo	Características principales	Uso típico en empresas
Windows.	Interfaz gráfica sencilla, gran compatibilidad, Active Directory para gestión de usuarios y permisos en red.	Oficinas administrativas, pymes, administración pública.
Linux.	Software libre, gran estabilidad, flexibilidad y seguridad. Muy utilizado en servidores.	Empresas tecnológicas, entornos académicos, servidores de red.
macOS.	Alta usabilidad, gran integración con diseño gráfico, edición multimedia y aplicaciones creativas.	Estudios de diseño, despachos profesionales, productoras.
Android / iOS.	Enfocados a dispositivos móviles, con aplicaciones de almacenamiento en la nube y gestión documental.	Trabajo remoto, movilidad, gestores comerciales.

1.5.2 Creación, copia y eliminación de archivos y carpetas

El manejo de archivos y carpetas es una **tarea básica pero esencial** en la gestión documental digital. Aunque a primera vista pueda parecer algo trivial, en realidad constituye el núcleo de la organización de la información en cualquier empresa.

- **Creación**: consiste en generar un archivo nuevo (ejemplo: un contrato en Word o una factura en Excel) o una carpeta que actúe como contenedor de documentos relacionados. La correcta denominación de archivos y carpetas es vital para mantener un orden coherente y evitar confusiones.
- **Copia**: permite duplicar documentos para hacer copias de seguridad, trasladarlos a otros dispositivos (USB, discos externos) o subirlos a la nube. Esta acción también se utiliza en planes de **backup corporativo**.
- **Eliminación**: supone borrar archivos o carpetas cuando han perdido su utilidad o han cumplido los plazos legales de conservación. La eliminación puede hacerse de manera simple (papelera) o de forma segura mediante software de borrado definitivo que evita la recuperación no autorizada.

Ejemplo

Un técnico administrativo crea la carpeta **"IVA 2024"** en el servidor, guarda en ella los modelos 303 trimestrales en formato PDF y realiza una copia de seguridad automática en la nube. Tras los 6 años de conservación obligatoria (según la normativa fiscal española), procede a la eliminación definitiva de los archivos, certificando su destrucción conforme a la LOPDGDD y al RGPD.

Operaciones básicas sobre archivos y carpetas

Operación	Herramienta en Windows	Herramienta en Linux	Finalidad
Crear archivo.	Menú contextual → Nuevo.	Touch.	Generar nuevos documentos.
Crear carpeta.	Menú contextual → Carpeta.	Mkdir.	Organizar documentos por categorías.
Copiar.	Ctrl + C / Ctrl + V.	Cp.	Duplicar o trasladar archivos.
Eliminar.	Supr o papelera.	Rm.	Suprimir definitivamente archivos.

1.5.3 Configuración de objetos en el sistema operativo

En un sistema operativo, los archivos no son elementos aislados: forman parte de una estructura jerárquica de carpetas, permisos y atributos que debe configurarse de forma coherente para garantizar accesibilidad, seguridad y trazabilidad.

a) **Atributos de archivos y carpetas**

Los SO permiten asignar atributos especiales que modifican el comportamiento de los documentos:

- **Solo lectura** → el archivo se puede abrir y consultar, pero no modificar.
- **Oculto** → el archivo no aparece en la vista normal, aunque sigue existiendo.
- **De sistema** → reservado para ficheros esenciales que no deben alterarse.

b) **Permisos de acceso**

En entornos multiusuario o en red, los permisos son clave para proteger la información sensible. Los más habituales son:

- **Lectura** → permite ver el documento, pero no modificarlo.
- **Escritura** → posibilita añadir o editar información.
- **Ejecución** → habilita abrir programas, scripts o aplicaciones vinculadas.

Ejemplo

En un servidor de asesoría fiscal:

- La carpeta **"Contabilidad"** es accesible solo por el equipo contable.
- La carpeta **"Nóminas"** está restringida al área de recursos humanos.
- La **Dirección General** accede a todas las áreas, pero con permisos de solo lectura, para preservar la integridad de la información.

c) **Organización de estructuras en red**

Un SO bien configurado permite crear **unidades de red compartidas** para departamentos o proyectos. Esto facilita la colaboración, evita duplicidades, centraliza las copias de seguridad y permite auditar los accesos de cada usuario.

Configuración de objetos en un SO

Elemento	Configuración recomendada	Beneficio principal
Atributos.	Documentos oficiales con "solo lectura".	Evita modificaciones indebidas.
Permisos.	Roles diferenciados por departamento.	Aumenta la seguridad y confidencialidad.
Carpetas en red.	Unidades compartidas con control de accesos.	Favorece la trazabilidad y eficiencia.
Copias de seguridad.	Automáticas y cifradas.	Conservación de la información a largo plazo.

Nota

Una gestión documental eficaz no depende únicamente de almacenar archivos, sino de hacerlo bajo **un sistema operativo bien configurado** que asegure orden, seguridad, trazabilidad y cumplimiento normativo.

Ejemplo

Un administrativo necesita localizar el contrato firmado con la empresa "Logística Pérez" en 2021. En un archivo físico con clasificación alfabética, acudirá a la letra "L" y dentro de ella a la subcarpeta de ese año. En un archivo digital, bastará con introducir "Logística Pérez 2021" en el buscador del software documental.

a) **Herramientas de consulta**

- **Índices físicos**: listados impresos que permiten localizar documentos en un archivo físico.
- **Índices electrónicos**: bases de datos que relacionan cada documento con su referencia, ubicación y metadatos.
- **Sistemas de gestión documental (SGD)**: aplicaciones que integran la digitalización, búsqueda avanzada, control de accesos y trazabilidad de cada consulta.

Ejemplo

En una asesoría laboral, la búsqueda de nóminas antiguas se realiza en el programa de gestión, introduciendo el nombre del trabajador y el periodo. El sistema devuelve el PDF con la copia de la nómina, evitando consultar manualmente cajas archivadas.

b) **Acceso controlado**

El acceso no puede ser indiscriminado: debe establecerse un **sistema de permisos y roles** para garantizar la confidencialidad.

- **Acceso libre**: para documentación pública o general.
- **Acceso restringido**: limitado a determinados departamentos (ejemplo: nóminas solo accesibles para Recursos Humanos).
- **Acceso confidencial**: solo autorizado a responsables designados (ejemplo: contratos de alta dirección o expedientes judiciales).

Niveles de acceso

Nivel de acceso	Tipo de documentación	Quién accede	Medidas de seguridad
Libre.	Informes públicos, manuales.	Todo el personal.	Carpeta compartida o intranet.
Restringido.	Nóminas, facturas, expedientes.	Área específica.	Contraseña, permisos de usuario.
Confidencial.	Contratos de directivos, litigios.	Dirección o responsables.	Encriptación, doble autenticación.

1.6 PROTECCIÓN DE ACCESOS Y SEGURIDAD DOCUMENTAL

La gestión de la información en una organización no se limita a archivar documentos o garantizar su conservación. En la sociedad actual, donde los datos constituyen un recurso estratégico y un activo de gran valor, proteger el acceso y la seguridad documental es una obligación legal, una responsabilidad ética y una necesidad práctica.

Un sistema de archivo, ya sea físico o electrónico, debe incorporar mecanismos que aseguren que solo las personas autorizadas puedan acceder a la información y que esta se mantenga íntegra, confidencial y disponible cuando se requiera. De lo contrario, se corre el riesgo de filtraciones, pérdidas de información, accesos indebidos o incluso sanciones administrativas por incumplimiento de la normativa vigente en materia de protección de datos (Reglamento General de Protección de Datos –RGPD– y

Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales –LOPDGDD–).

Este apartado analiza en detalle los principales mecanismos de seguridad en archivos físicos e informáticos, desde la definición de niveles de protección hasta el uso de contraseñas, las autorizaciones de acceso y la detección de errores en los procedimientos.

1.6.1 Niveles de protección en archivos físicos e informáticos

La seguridad documental no puede ser uniforme para todos los documentos, ya que no toda la información tiene la misma importancia o sensibilidad. Por ello, se establecen **niveles de protección** que determinan el grado de control y vigilancia necesario según la naturaleza de los datos.

Archivos físicos

En el caso de documentos en papel, los niveles de protección suelen organizarse en tres categorías:

- **Nivel básico**:

  Aplicable a documentación administrativa general (ejemplo: facturas ya pagadas, circulares internas, correspondencia comercial). Requiere un archivador cerrado, estanterías ordenadas y control de acceso a las instalaciones.

- **Nivel intermedio**:

  Aplicable a documentación de cierta sensibilidad (ejemplo: contratos con clientes, nóminas, expedientes laborales). Se recomienda archivado en **armarios con llave**, control de acceso a la sala y registro de préstamos de documentos.

- **Nivel alto**:

  Se aplica a documentos con información confidencial o estratégica (ejemplo: datos médicos de empleados, información de clientes protegida por la LOPDGDD, patentes o proyectos estratégicos). Se almacenan en **salas seguras**, con acceso restringido mediante tarjeta o huella digital, y vigilancia continua.

Archivos informáticos

En el entorno digital, los niveles de protección se establecen en función de la **sensibilidad y criticidad de los datos**:

- **Nivel básico**: documentos generales almacenados en carpetas de red o en la nube, protegidos con contraseña.
- **Nivel intermedio**: bases de datos de clientes o proveedores, accesibles solo para determinados departamentos. Se aplican restricciones de usuario, cifrado parcial y copias de seguridad periódicas.
- **Nivel alto**: información financiera, médica, jurídica o estratégica. Se exige cifrado completo, autenticación multifactor, registros de auditoría y monitorización en tiempo real.

Cuadro comparativo

Nivel de protección	Archivos físicos	Archivos informáticos
Básico.	Archivadores y estanterías ordenadas, acceso general controlado.	Carpetas protegidas con contraseña.
Intermedio.	Armarios cerrados, registros de préstamos.	Usuarios autorizados, cifrado parcial, copias de seguridad.
Alto.	Salas seguras con control biométrico, acceso restringido.	Cifrado completo, autenticación multifactor, auditoría y monitorización.

1.6.2 Uso de contraseñas y atributos de acceso

En la gestión documental digital, las contraseñas constituyen la **primera línea de defensa** frente a accesos indebidos. Sin embargo, no basta con "tener una contraseña": su eficacia depende directamente de cómo se diseñan, gestionan y utilizan. Una clave débil o compartida equivale a **dejar abierta la puerta del archivo**. Por ello, la seguridad informática actual combina contraseñas robustas con **atributos de acceso diferenciados** (roles y permisos), garantizando que cada trabajador acceda únicamente a la información que necesita para desempeñar su función.

Contraseñas seguras

Para que una contraseña sea eficaz debe reunir una serie de características mínimas:

- **Longitud adecuada**: se recomienda que tenga al menos entre 8 y 12 caracteres, aunque para información crítica puede ser mayor.
- **Complejidad**: incluir letras mayúsculas y minúsculas, números y símbolos especiales.
- **No previsibles**: evitar datos personales (fechas de nacimiento, nombres de hijos, palabras comunes).
- **Cambio periódico**: renovar cada 60 o 90 días según la política de la empresa.
- **No reutilización**: impedir que un mismo trabajador utilice contraseñas antiguas en diferentes periodos.

Ejemplo

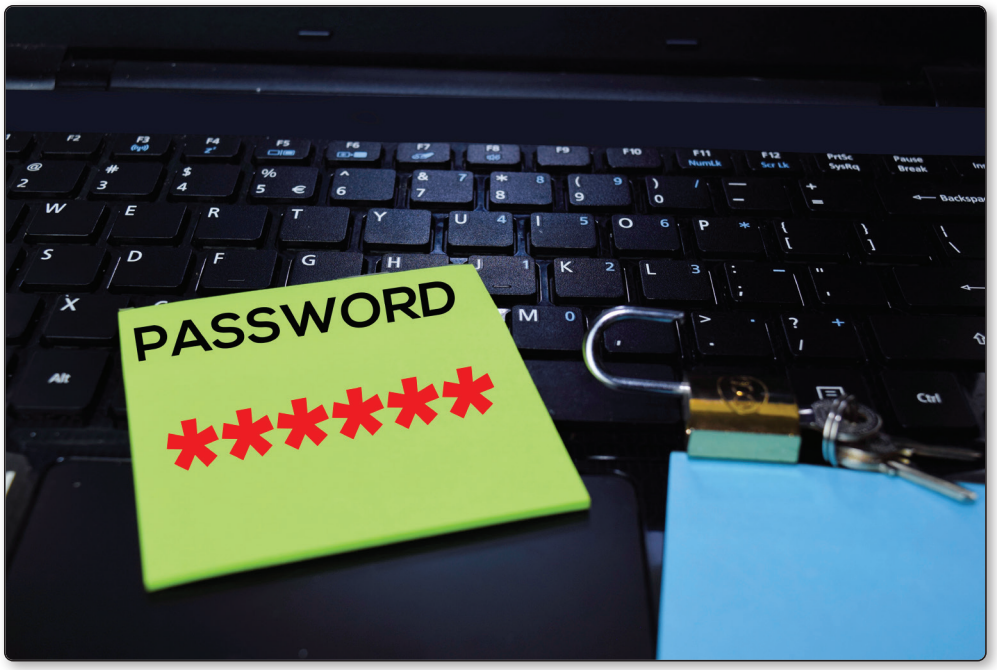
- Contraseña débil: 123456 o maria2023.
- Contraseña segura: M4r!@_27*G.

Política de contraseñas

Una buena gestión de contraseñas no depende solo de los usuarios, sino de la **normativa interna de la organización**. La empresa debe establecer una **política de contraseñas** que regule aspectos como:

1. **Periodicidad de cambio**: establecer un plazo máximo de vigencia (ej. 90 días).
2. **Bloqueo por intentos fallidos**: tras 3 o 5 intentos, el sistema debe bloquear temporalmente la cuenta.

3. **Almacenamiento seguro**: nunca se deben guardar contraseñas en documentos visibles o notas adhesivas en el escritorio.
4. **Autenticación adicional**: en accesos críticos, combinar la contraseña con otro factor (código SMS, aplicación móvil, huella digital).



Ejemplo de política interna

"Toda contraseña deberá tener al menos 10 caracteres, incluir 3 tipos distintos (mayúsculas, minúsculas, números o símbolos), renovarse cada 3 meses y no repetirse en los últimos 12 cambios".

Atributos de acceso

Además de las contraseñas, los sistemas modernos permiten aplicar **atributos de acceso**, también conocidos como **roles o permisos**. Estos determinan **qué puede hacer cada usuario** dentro del sistema de gestión documental.

- **Administrador**: acceso total a todos los documentos y configuración del sistema. Puede crear, modificar y eliminar registros.
- **Usuario avanzado**: puede leer y modificar archivos, pero no eliminarlos ni acceder a información de carácter confidencial.
- **Usuario básico**: solo puede visualizar determinados documentos, sin posibilidad de modificarlos ni descargarlos.

Ejemplo en un departamento de Recursos Humanos

- El **director de RR. HH.** tiene permisos de administrador para acceder a nóminas, contratos y evaluaciones.
- Los **técnicos de selección** solo pueden leer y modificar expedientes de candidatos, pero no acceder a nóminas.
- Los **empleados** tienen acceso restringido a sus propios documentos personales, como contratos o certificados.

Errores frecuentes

Pese a la importancia de la seguridad, en muchas empresas se cometen errores que comprometen la protección documental:

- Usar contraseñas obvias: “1234”, “admin”, “empresa2024”.
- Compartir la misma contraseña entre varios usuarios.
- No retirar permisos a empleados que abandonan la empresa.
- Mantener contraseñas apuntadas en papeles o archivos visibles.
- Permitir que un mismo usuario tenga permisos excesivos (ejemplo: un administrativo con acceso total a contabilidad).

Buenas prácticas

Para garantizar la protección real de la información, se recomienda aplicar las siguientes medidas:

- **Formación periódica** al personal en ciberseguridad básica.
- **Contraseñas individuales y no compartidas**.
- **Autenticación multifactor (MFA)** en accesos críticos.
- **Asignación de roles por necesidad** ("mínimo privilegio"): cada usuario solo accede a lo imprescindible.
- **Revisiones periódicas de permisos** para verificar que se mantienen actualizados.

Nota

Una contraseña débil es como una puerta con cerradura sin llave: **aparenta seguridad, pero no protege de verdad**. Por eso, la seguridad documental no se logra solo creando contraseñas, sino estableciendo un **sistema integral de gestión de accesos** que combine contraseñas robustas, roles de usuario y controles de auditoría.

1.6.3 Autorizaciones de acceso y detección de errores en el procedimiento

En cualquier sistema de gestión documental, ya sea físico o digital, el control de accesos es un pilar fundamental de la seguridad de la información. No basta con tener contraseñas seguras o archivadores cerrados: es imprescindible definir **quién puede acceder a cada tipo de información, en qué circunstancias y en qué condiciones**. Este control no solo garantiza la confidencialidad, sino también la trazabilidad y la responsabilidad individual de los usuarios.

La legislación vigente en materia de protección de datos (Reglamento General de Protección de Datos – **RGPD** y la **Ley Orgánica 3/2018 de Protección**

de Datos Personales y garantía de los derechos digitales) exige que toda organización disponga de mecanismos que aseguren que la información sensible solo es accesible a las personas autorizadas.

Autorizaciones de acceso

El acceso a la documentación debe estar regulado mediante **autorizaciones formales**. Estas autorizaciones pueden plasmarse en:

- **Documentos escritos**: listados firmados por la dirección donde se especifica qué empleados tienen acceso a qué documentación.
- **Registros digitales**: sistemas de gestión documental que asignan permisos personalizados a cada usuario.
- **Políticas internas**: manuales o protocolos que definen los niveles de acceso por departamentos o funciones.

Ejemplo

- El **departamento de Recursos Humanos** tiene acceso a expedientes laborales, contratos y nóminas.
- El **departamento de Contabilidad** puede acceder a facturas, balances y libros contables.
- El **equipo de Ventas** solo puede consultar información relativa a clientes activos y potenciales.

De esta manera, cada trabajador dispone únicamente de la información necesaria para desempeñar sus funciones, aplicando el principio de **mínimo privilegio**.

Registros de acceso

Un buen sistema de seguridad documental no solo concede permisos, sino que también **registra quién accede a la información, cuándo lo hace y qué operación realiza**.

- En **archivos informáticos**: el registro de accesos debe reflejar usuario, fecha, hora y acción realizada (lectura, modificación, descarga, eliminación).
- En **archivos físicos**: se puede llevar un **libro de control de préstamos**, donde cada empleado firma al retirar o consultar un documento y lo devuelve en el plazo establecido.

Estos registros permiten realizar **auditorías internas y externas**, detectar accesos indebidos y disponer de pruebas en caso de litigios o inspecciones.

Errores frecuentes en los procedimientos

En muchas organizaciones, los controles de acceso presentan debilidades que comprometen la seguridad documental. Entre los errores más habituales se encuentran:

- **Olvidar retirar autorizaciones a empleados que dejan la empresa**, lo que permite que sigan accediendo a datos sensibles.
- **Permitir el uso compartido de contraseñas**, lo que impide identificar al responsable de un acceso indebido.
- **No revisar periódicamente los registros de acceso**, dejando sin detectar posibles accesos sospechosos.
- **Archivar documentos confidenciales en ubicaciones comunes** sin restricciones de acceso, como servidores compartidos o archivadores abiertos.
- **No aplicar controles diferenciados por rol**, permitiendo que cualquier empleado pueda acceder a información crítica.

Ejemplo

Un empleado de una empresa accede sin autorización a la base de datos de clientes y descarga información confidencial para beneficio personal.

- Si la organización cuenta con un **registro de accesos**, podrá identificar qué usuario realizó la operación, a qué hora y desde qué dispositivo. Esto facilitará la depuración de responsabilidades y la aplicación de medidas disciplinarias o legales.
- En cambio, si no existen registros, la empresa no podrá determinar quién fue el responsable, lo que supondrá un **grave incumplimiento del RGPD**. Esta situación puede acarrear sanciones económicas de hasta **20 millones de euros o el 4 % de la facturación anual**, además del daño reputacional.

Buenas prácticas en la gestión de autorizaciones

Para evitar estos riesgos, las empresas deben aplicar un conjunto de **buenas prácticas**:

- Establecer **autorizaciones formales** por escrito o mediante sistemas digitales de gestión de accesos.
- Asignar permisos siguiendo el principio de **mínimo privilegio**.
- Actualizar los permisos cada vez que haya cambios en la plantilla o funciones.
- Realizar **revisiones periódicas** de los registros de acceso (auditorías trimestrales o semestrales).
- Implementar alertas automáticas en los sistemas digitales para detectar accesos sospechosos.
- Mantener **copias de seguridad** y protocolos de recuperación en caso de incidentes.

Nota

Conceder accesos sin control es como **dejar todas las llaves de la oficina en un cajón abierto**: cualquiera podría utilizarlas sin que sepamos quién lo hizo. Por eso, un buen sistema de autorizaciones no solo limita el acceso, sino que también **genera trazabilidad**, garantizando seguridad jurídica y confianza dentro de la organización.

Sistemas de control de accesos en archivos físicos y digitales

Aspecto a controlar	Archivos físicos	Archivos digitales
Identificación del usuario.	Firma manuscrita en libro de préstamos.	Usuario y contraseña personales.
Registro de accesos.	Libro de control con fecha, hora y documento.	Log automático con usuario, hora, IP y acción.
Limitación de permisos.	Llaves de archivo, armarios cerrados, sellos.	Roles diferenciados (lectura, escritura, borrado).
Revisión periódica.	Supervisión manual del responsable del archivo.	Auditorías automáticas y reportes programados.
Errores frecuentes.	Pérdida de documentos, préstamos no anotados.	Uso compartido de contraseñas, accesos no auditados.
Ventajas.	Sencillo, sin necesidad de tecnología.	Mayor trazabilidad, control remoto, alertas automáticas.
Inconvenientes.	Riesgo de pérdida física, acceso limitado a horarios.	Riesgo de ciberataques si no hay seguridad robusta.

Protocolo paso a paso para autorizar accesos en una empresa

Ejemplo

Empresa ficticia “Gestión Global S.L.”

1. **Solicitud formal de acceso**
   - El empleado solicita por escrito (correo electrónico o formulario interno) el acceso a determinada documentación.
   - El responsable del área debe justificar la necesidad (ejemplo: un administrativo solicita acceso a facturas del último trimestre).
2. **Evaluación de la solicitud**
   - El responsable de seguridad de la información o el responsable de archivo revisa si la petición es adecuada.
   - Se aplica el **principio de mínimo privilegio**: el empleado accede solo a lo que necesita.

3. **Aprobación o denegación**
   - Si la solicitud es válida, se aprueba y se registra la autorización.
   - Si no lo es, se informa al empleado explicando los motivos.
4. **Creación de permisos**
   - En archivos físicos: se entrega una llave, tarjeta de acceso o se habilita el préstamo con control.
   - En archivos digitales: el departamento de informática crea un usuario y asigna permisos concretos (ejemplo: solo lectura).
5. **Registro de accesos**
   - Cada consulta, préstamo o descarga queda registrada (en el libro de archivo o en el sistema informático).
   - Esto garantiza trazabilidad y permite auditorías futuras.
6. **Revisión periódica**
   - Cada 6 meses se revisan las autorizaciones concedidas.
   - Se eliminan accesos de empleados que hayan cambiado de puesto o hayan abandonado la empresa.
7. **Control ante incidentes**
   - Si se detecta un acceso indebido, se debe:
     - Bloquear inmediatamente el usuario o retirar la llave.
     - Investigar el incidente (revisando logs o libros de registro).
     - Notificar a la autoridad competente en caso de filtración de datos personales (AEPD en España).

Nota

Piensa en el sistema de autorizaciones como una **escalera con puertas en cada piso**. No todos los empleados necesitan subir hasta el último nivel; por eso, cada puerta se abre solo con la llave adecuada, y siempre queda constancia de quién la usó y cuándo.

1.7 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

La confidencialidad y la correcta protección de los datos constituyen hoy en día uno de los pilares fundamentales en la gestión documental de cualquier organización. Las empresas manejan a diario información sensible que puede abarcar desde datos personales de empleados y clientes hasta documentos financieros, contratos mercantiles, historiales médicos o registros estratégicos de negocio. Toda esta documentación no solo representa un activo esencial, sino que también está sujeta a un marco normativo estricto que obliga a custodiarla, conservarla y protegerla frente a accesos no autorizados, pérdidas accidentales o ciberataques.

En la era digital, la información se ha convertido en un recurso tan valioso como vulnerable. Una filtración, un mal uso o una pérdida de datos pueden tener consecuencias devastadoras: sanciones económicas, pérdida de confianza de clientes, deterioro de la reputación corporativa e incluso responsabilidades legales para los directivos. Por ello, resulta imprescindible que cualquier organización, independientemente de su tamaño o sector, implemente políticas claras de seguridad y confidencialidad documental.

Este apartado aborda dos cuestiones clave:

- **La normativa vigente en materia de protección de datos**, en especial el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) en España. Estas normas establecen derechos, obligaciones y medidas de seguridad que deben aplicarse en el tratamiento de datos personales.
- **Las copias de seguridad y la conservación documental**, entendidas como herramientas preventivas que aseguran la integridad, disponibilidad y trazabilidad de la información frente a incidentes técnicos, errores humanos o ataques externos.

En definitiva, garantizar la confidencialidad y la protección de datos no debe considerarse únicamente una obligación legal, sino una práctica estratégica que refuerza la confianza de clientes, trabajadores y socios comerciales, y que asegura la continuidad de las operaciones de la empresa en un entorno cada vez más digitalizado y regulado.

1.7.1 Normativa vigente sobre protección de datos

La gestión adecuada de la información en una organización no solo es una cuestión de eficiencia administrativa, sino también un **imperativo legal y ético**. Los datos personales que manejan las empresas —como nombres, direcciones, correos electrónicos, historiales laborales, nóminas o datos bancarios— están protegidos por una normativa que busca garantizar los derechos fundamentales de las personas, especialmente su **derecho a la privacidad**.

Principales marcos normativos

1. **Reglamento General de Protección de Datos (RGPD – Reglamento (UE) 2016/679)**

   1.1. Es la norma de referencia en toda la Unión Europea. Establece principios rectores que deben respetarse siempre que se traten datos personales:

      1.1.1. **Licitud, lealtad y transparencia:** el tratamiento debe estar basado en un fundamento jurídico (consentimiento, contrato, interés legítimo, etc.) y comunicarse claramente a la persona interesada.

1.1.2. **Limitación de la finalidad:** los datos solo pueden usarse para los fines para los que fueron recogidos.

1.1.3. **Minimización de datos:** no se deben recopilar más datos de los necesarios.

1.1.4. **Exactitud:** los datos deben mantenerse actualizados.

1.1.5. **Limitación del plazo de conservación:** no conservar información más allá de lo estrictamente necesario.

1.1.6. **Integridad y confidencialidad:** garantizar medidas de seguridad contra accesos no autorizados, pérdidas o alteraciones.

1.2. Establece **derechos de los interesados**, como acceso, rectificación, supresión, portabilidad, limitación del tratamiento y oposición.

1.3. Introduce la figura del **delegado de Protección de Datos (DPO o DPD)** en entidades que manejan grandes volúmenes de información o datos especialmente sensibles (ejemplo: hospitales, colegios, bancos).

1.4. Define un **régimen sancionador severo**, con multas de hasta **20 millones de euros o el 4 % de la facturación anual global**, lo que refuerza la importancia del cumplimiento.

2. **Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**

2.1. Esta norma adapta el RGPD al marco español. Sus aportaciones más destacadas son:

2.1.1. Reconocimiento del derecho a la intimidad y a la **desconexión digital** en el ámbito laboral, evitando abusos relacionados con la hiperconectividad.

2.1.2. Regulación de la videovigilancia en centros de trabajo y el uso de sistemas de geolocalización de empleados.

2.1.3. Protección reforzada de datos sensibles: salud, ideología, religión, orientación sexual, origen racial, etc.

2.1.4. Regulación del **consentimiento de menores**: en España, los adolescentes a partir de 14 años pueden dar consentimiento para el tratamiento de sus datos en servicios de la sociedad de la información (redes sociales, aplicaciones, etc.).

2.1.5. Regulación de los **canales de denuncia interna** (whistleblowing) para reportar irregularidades dentro de la empresa.

3. **Normativa sectorial complementaria**

3.1. En algunos sectores existen disposiciones adicionales:

3.1.1. En el ámbito sanitario: normas específicas sobre historia clínica (Ley 41/2002).

3.1.2. En el ámbito financiero: exigencias de confidencialidad en relación con la Ley de Servicios de Pago.

3.1.3. En educación: medidas de protección reforzada para datos de menores.

Ejemplo

Una consultora gestiona bases de datos de clientes y proveedores. Para cumplir con la normativa:

- Solicita el consentimiento expreso de los clientes antes de enviarles campañas comerciales.
- Mantiene un registro de actividades de tratamiento, donde especifica qué datos maneja, con qué finalidad y durante cuánto tiempo.
- Limita el acceso a los expedientes digitales a determinados perfiles autorizados mediante roles en el sistema informático.
- Establece un protocolo de respuesta en caso de **brecha de seguridad**, que incluye notificar a la Agencia Española de Protección de Datos (AEPD) en un máximo de 72 horas.

Nota

No cumplir con la normativa no solo implica riesgo de sanciones económicas, sino también **pérdida de reputación**, lo cual puede dañar gravemente la confianza de clientes, empleados y proveedores.

1.7.2 Copias de seguridad y conservación documental

La **protección de la información** no consiste únicamente en blindarla frente a accesos indebidos, sino en garantizar que esté siempre disponible, íntegra y en buen estado, incluso cuando ocurren incidentes graves como fallos técnicos, ataques informáticos, incendios o desastres naturales. Una organización puede invertir en seguridad perimetral, contraseñas robustas o antivirus, pero si pierde su información crítica sin posibilidad de recuperación, su operatividad quedará seriamente comprometida.

Por este motivo, las **copias de seguridad (backups)** y las políticas de **conservación documental** se convierten en dos pilares básicos de cualquier estrategia de gestión documental moderna. Ambas son obligatorias, no solo por criterios de eficiencia interna, sino por imposiciones legales recogidas en la **normativa mercantil, fiscal, laboral y de protección de datos**.

Copias de seguridad

Una **copia de seguridad** es la reproducción de los datos originales que se guarda en soportes alternativos. Su finalidad es permitir que, en caso de pérdida o corrupción de los datos, la empresa pueda restaurarlos con rapidez y minimizar el impacto en la actividad.

Tipos principales de copias de seguridad

- **Copia completa**:

  Se duplica la totalidad de los archivos o del sistema. Su ventaja es que la recuperación es sencilla e inmediata, aunque requiere mucho tiempo y espacio de almacenamiento. Se recomienda hacerla periódicamente (por ejemplo, una vez a la semana o al mes).

- **Copia incremental**:

  Solo guarda los archivos que han cambiado desde la última copia (sea completa o incremental). Requiere menos tiempo y espacio, pero la restauración es más compleja, pues debe combinar la última copia completa con todas las incrementales intermedias.

- **Copia diferencial**:

  Registra todos los cambios desde la última copia completa. Es un término medio: consume más espacio que la incremental, pero la recuperación es más ágil porque basta con combinar la última copia completa y la última diferencial.

- **Copias en espejo (mirror backup)**:

  Replican en tiempo real el contenido de un sistema en otro, garantizando una sincronización constante. Su principal desventaja es que, si se borra un archivo por error, también se borra en el espejo.

- **Copias en la nube**:

  Servicios externos que almacenan la información en servidores remotos con acceso cifrado. Permiten escalabilidad y acceso desde cualquier ubicación, pero requieren garantizar que el proveedor cumple con la normativa de protección de datos (RGPD y LOPDGDD).

Buenas prácticas en las copias de seguridad

1. **Aplicar la regla 3-2-1**:
   a) Tener al menos **3 copias** de la información.
   b) Guardarlas en **2 soportes distintos** (por ejemplo, un servidor local y un dispositivo externo).
   c) Mantener **1 copia fuera de la sede principal**, preferiblemente en la nube o en otra oficina, para casos de catástrofes físicas.

2. **Definir periodicidad según criticidad**:
   a) Información crítica (contabilidad, nóminas, contratos): copias **diarias**.
   b) Información de gestión interna menos sensible: copias **semanales** o mensuales.

3. **Cifrado y protección de las copias**:

   Los backups deben estar **cifrados** para evitar que, en caso de pérdida o robo del soporte, los datos puedan ser leídos.

4. **Pruebas periódicas de restauración**:

   Una copia de seguridad solo es útil si puede restaurarse. Es imprescindible realizar simulaciones de recuperación, verificando que los archivos no están dañados y que los tiempos de restauración cumplen con los requisitos de la empresa.

5. **Automatización del proceso**:

   El uso de software especializado evita que las copias dependan de la memoria humana. La automatización reduce errores y garantiza una mayor fiabilidad.

Conservación documental

La **conservación documental** consiste en mantener los documentos, en formato físico o digital, durante los plazos que establece la legislación vigente o mientras resulten útiles para la organización. La gestión correcta de los plazos permite un equilibrio entre seguridad jurídica y optimización de recursos de almacenamiento.

Plazos legales de conservación más habituales

Tipo de documento	Plazo mínimo de conservación	Normativa aplicable
Facturas, albaranes, libros contables.	6 años.	Código de Comercio.
Documentación fiscal (IVA, IRPF, IS).	4 años.	Ley General Tributaria.
Nóminas y seguros sociales.	4 años.	Estatuto de los Trabajadores / Seguridad Social.
Contratos laborales y expedientes de empleados.	Hasta 4 años después de la finalización.	Normativa laboral.
Historias clínicas.	5 años mínimo (más en casos específicos).	Ley de Autonomía del Paciente.
Datos de candidatos no contratados.	Máx. 2 años.	LOPDGDD.

Eliminación segura de documentos

Una vez transcurridos los plazos legales, los documentos **no deben conservarse indefinidamente**, ya que esto incrementa riesgos legales y de seguridad. La destrucción debe realizarse de forma que se imposibilite su recuperación:

- **En papel**:
  - Uso de destructoras de alta seguridad (nivel P-4 o superior, con triturado cruzado).
  - Servicios externos certificados que entregan un **acta de destrucción**, imprescindible en auditorías.
- **En formato digital**:
  - Uso de software de borrado seguro que sobrescribe varias veces los datos.
  - Eliminación de discos duros mediante **desmagnetización** o destrucción física.

Ejemplo

Una **empresa de distribución alimentaria** debe cumplir con obligaciones legales y proteger su información:

- Realiza **copias diarias** de contabilidad y nóminas en un servidor local y **copias semanales cifradas** en la nube.
- Conserva facturas y libros contables **6 años** en su archivo digital.
- Al terminar ese periodo, contrata a una empresa especializada que destruye la documentación física y entrega un certificado oficial.
- Los currículums de candidatos no seleccionados se eliminan automáticamente a los **24 meses**, cumpliendo con la LOPDGDD.

Nota

Una copia de seguridad no probada equivale a no tener copia. De nada sirve acumular documentos si no se establece un sistema de revisión, recuperación y eliminación segura. La seguridad documental no es solo **guardar**, sino **gestionar inteligentemente todo el ciclo de vida de la información**.

Conclusión

La gestión de copias de seguridad y la conservación documental garantizan la continuidad del negocio, el cumplimiento legal y la confianza de clientes, proveedores y empleados. Una empresa que cuida sus datos protege su patrimonio más valioso: la información.

1.8 CUESTIONARIO – CAPÍTULO 1

1. **La principal finalidad de la gestión de archivos dentro de una organización es:**
   a) Aumentar la cantidad de documentos almacenados.
   b) Garantizar la conservación, localización y uso eficiente de la información.
   c) Sustituir los archivos digitales por físicos.
   d) Facilitar el control fiscal de la empresa.

2. **Los archivos públicos se diferencian de los privados principalmente en que:**
   a) Solo almacenan documentos de carácter histórico.
   b) Están sujetos a legislación específica sobre acceso y transparencia.
   c) Carecen de estructura jerárquica.
   d) No pueden conservar documentos confidenciales.

3. El sistema de clasificación alfabético en archivística se utiliza cuando:

a) Los documentos se ordenan por fechas.
b) Los documentos se agrupan por materias.
c) Los documentos se ordenan según el nombre del cliente, empresa o entidad.
d) Se clasifican según el valor económico.

4. La finalidad principal del archivo en una empresa es:

a) Servir como almacén de documentos antiguos.
b) Facilitar el acceso rápido a la información para la toma de decisiones.
c) Limitar el acceso a la información a determinados empleados.
d) Eliminar los documentos una vez utilizados.

5. Los índices de archivo permiten:

a) Registrar la localización y estado de los documentos archivados.
b) Eliminar automáticamente documentos caducados.
c) Proteger los documentos frente a incendios.
d) Crear copias de seguridad de los documentos.

6. El uso de manuales de ayuda en archivística sirve para:

a) Establecer criterios uniformes en la organización y conservación de documentos.
b) Sustituir al personal del departamento de archivo.
c) Limitar el acceso al archivo a personal autorizado.
d) Clasificar documentos únicamente por fechas.

7. Un ejemplo de soporte de archivo físico sería:

a) Un disco duro externo.
b) Un archivador de anillas.
c) Una nube corporativa.
d) Un sistema operativo de red.

8. En un sistema operativo, eliminar un archivo implica:

a) Borrarlo físicamente de inmediato.
b) Moverlo a la papelera o área de eliminación temporal.
c) Crear una copia comprimida.
d) Enviarlo automáticamente a la red local.

9. Las contraseñas y atributos de acceso en los archivos informáticos tienen como finalidad:

a) Facilitar el intercambio libre de información.
b) Aumentar la velocidad de los equipos.
c) Proteger la confidencialidad de la información almacenada.
d) Eliminar los documentos obsoletos.

10. Según la normativa de protección de datos, las copias de seguridad deben realizarse:

a) Solo cuando se produce una pérdida de información.
b) Periódicamente y siguiendo un protocolo de conservación seguro.
c) Únicamente al final del ejercicio fiscal.
d) Cuando lo solicite la dirección de la empresa.

Respuestas correctas

1. b) Garantizar la conservación, localización y uso eficiente de la información.
2. b) Están sujetos a legislación específica sobre acceso y transparencia.
3. c) Los documentos se ordenan según el nombre del cliente, empresa o entidad.
4. b) Facilitar el acceso rápido a la información para la toma de decisiones.
5. a) Registrar la localización y estado de los documentos archivados.
6. a) Establecer criterios uniformes en la organización y conservación de documentos.

7. b) Un archivador de anillas.
8. b) Moverlo a la papelera o área de eliminación temporal.
9. c) Proteger la confidencialidad de la información almacenada.
10. b) Periódicamente y siguiendo un protocolo de conservación seguro.