# 2

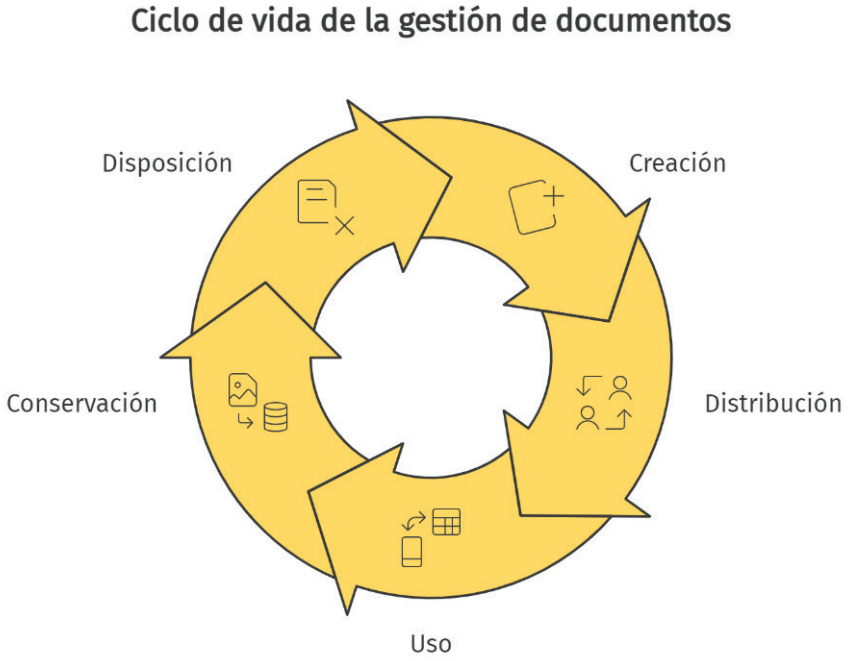
# Organización y archivo funcional de documentación administrativa

Se aborda el archivo como parte esencial de la gestión empresarial, destacando su finalidad, importancia y diversas modalidades, como el archivo centralizado o mixto. Asimismo, se explica la elección de los equipos y materiales necesarios para un archivo eficiente, el mantenimiento y la normativa asociada a la conservación y la destrucción de documentos, siempre bajo parámetros de confidencialidad y seguridad de la información.

## 2.1 COMPRENSIÓN DEL ARCHIVO EN LA EMPRESA

El archivo corporativo se concibe como un sistema dinámico que acompaña al documento desde su generación hasta su eliminación o transferencia histórica. Su propósito abarca la conservación de la memoria institucional, la garantía de la trazabilidad de cada procedimiento y el soporte a la toma de decisiones basada en evidencias.

Al integrar directrices de clasificación, valoración y acceso, se fomenta la coherencia entre las actividades diarias y los requisitos legales vigentes, al tiempo que se optimiza la disponibilidad de la información.

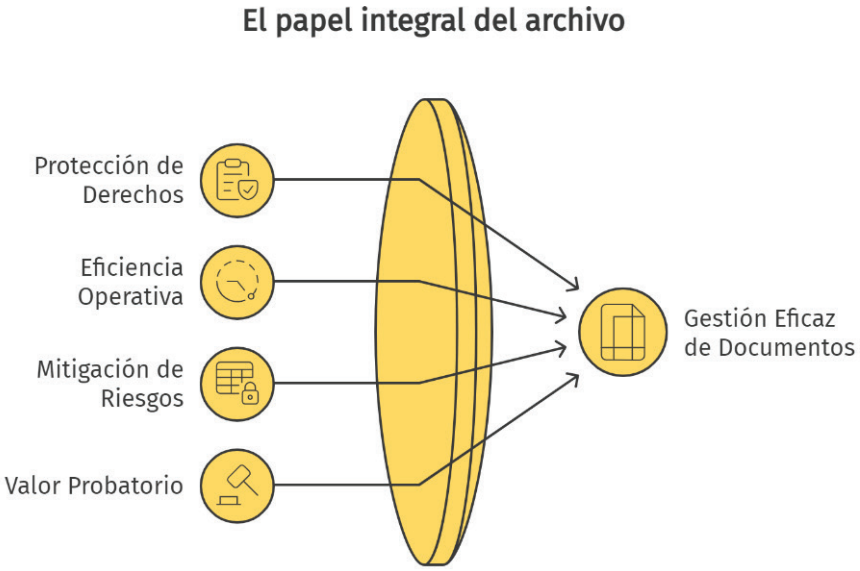



Cada fase del ciclo de vida documental —creación, distribución, uso, conservación y disposición final— se enlaza con políticas que aseguran la continuidad operativa, la transparencia y el cumplimiento normativo.

### 2.1.1 Finalidad y relevancia del archivo documental

La finalidad esencial del archivo consiste en custodiar documentos que respalden los derechos de la organización, de sus trabajadores y de terceros.

En este contexto, la relevancia se manifiesta mediante la agilización de consultas, la disminución de costes derivados de la búsqueda de información y la reducción de riesgos asociados a la pérdida o manipulación indebida de datos.

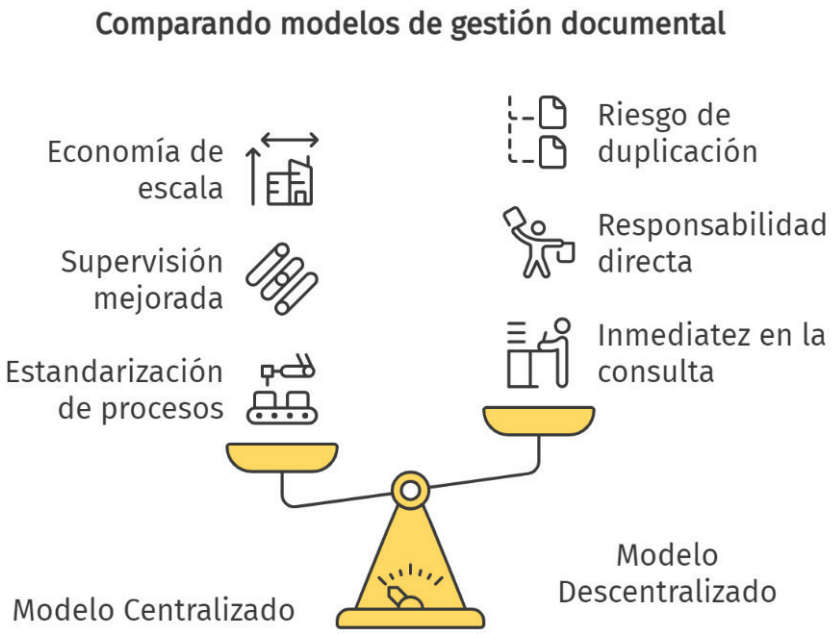



Asimismo, el archivo actúa como herramienta de defensa en procesos administrativos o judiciales, al proporcionar pruebas fehacientes sobre la actividad empresarial. Este valor probatorio requiere políticas de seguridad física y digital, un cuadro de clasificación coherente y un calendario de conservación que delimite plazos, garantizando que el expediente exacto se encuentre disponible cuando la normativa o la gestión lo demande.

### 2.1.2 Tipologías: archivo centralizado, descentralizado y mixto

El **modelo centralizado** concentra la documentación en un único depósito físico o virtual. Esta fórmula favorece la estandarización de procesos, facilita la supervisión y mejora la economía de escala en equipamiento y personal especializado. Sin embargo, la distancia geográfica entre el archivo y los usuarios puede ampliar los tiempos de respuesta y generar cuellos de botella en organizaciones con sedes dispersas.

El **esquema descentralizado** asigna a cada departamento la responsabilidad de conservar sus propios expedientes. Este enfoque incrementa la inmediatez en la consulta y refuerza la responsabilidad directa sobre la información, aunque conlleva riesgos de duplicación, criterios dispares de clasificación y mayor consumo de espacio o infraestructura.




El **modelo mixto** integra las ventajas de ambos sistemas: un fondo común destinado a los documentos inactivos o de conservación permanente, y depósitos de área para la documentación en uso frecuente. De este modo, se logra equilibrio entre rapidez de acceso y control normativo, al tiempo que se posibilita la implementación de software de gestión documental que armonice las taxonomías en todas las unidades administrativas.

## 2.2 SELECCIÓN DE EQUIPOS Y MATERIALES PARA ARCHIVO

La elección de equipos y materiales se define con base en el volumen documental, el soporte (papel o digital) y las condiciones ambientales requeridas.


En archivos físicos, se recomiendan estanterías metálicas con tratamiento antifuego y cajoneras deslizantes que aprovechen la altura del local, reduciendo pasillos fijos. Las cajas y carpetas, preferiblemente de cartón libre de ácido, preservan la integridad del papel al impedir la migración de sustancias nocivas. Para planos o documentos de gran formato se opta por gavetas horizontales que evitan dobleces.

En el ámbito digital, se recurre a servidores redundantes con alimentación ininterrumpida, matrices de discos configuradas en niveles RAID y copias externas periódicas en cintas LTO o en nubes certificadas por normas internacionales de seguridad de la información. El equipamiento se complementa con sistemas de climatización que mantengan temperatura y humedad estables, sensores de partículas para detectar riesgos biológicos y estaciones de limpieza con cepillos

suaves y aspiración filtrada. La incorporación de lectores RFID o códigos de barras agiliza los procesos de préstamo y devolución, mientras que los escáneres planetarios permiten convertir fondos en imágenes de alta resolución sin dañar encuadernaciones antiguas.

## Nota

Un servidor redundante con alimentación ininterrumpida describe una configuración donde dos o más máquinas idénticas trabajan en paralelo, de modo que si una falla la otra asume la carga sin interrupción; la energía llega a través de un sistema UPS (Uninterruptible Power Supply) que contiene baterías capaces de suministrar corriente durante cortes eléctricos y da tiempo para arrancar generadores o apagar el equipo con seguridad.

Las matrices de discos en niveles RAID (Redundant Array of Independent Disks) agrupan varios discos duros en un conjunto lógico y reparten la información siguiendo esquemas (RAID 0, 1, 5, 6, 10, entre otros) que priorizan desempeño, tolerancia a fallos o ambos aspectos; si un disco se avería, los datos permanecen accesibles porque la paridad o la réplica reside en los discos restantes.

Las copias externas en cintas LTO (Linear Tape-Open) consisten en guardar los ficheros en cartuchos magnéticos de gran capacidad que se almacenan fuera del sistema principal; la cinta, al permanecer desconectada de la red, protege frente a ransomware y ofrece ciclos de vida superiores a los de los discos convencionales, siendo apta para archivos de conservación prolongada.

Las nubes certificadas según normas internacionales de seguridad de la información se refieren a servicios que cuentan con acreditaciones como ISO 27001 o SOC 2; dichas certificaciones obligan al proveedor a mantener controles estrictos de confidencialidad, disponibilidad e

integridad mediante auditorías externas periódicas y cifrado de extremo a extremo en tránsito y en reposo.

Los sistemas de climatización para archivos regulan temperatura y humedad con precisión (habitualmente 18-22 °C y 45-55 % HR) a través de unidades HVAC dotadas de filtros HEPA y alarmas; su misión es reducir la expansión de hongos, la corrosión de soportes metálicos y la deformación del papel o los discos ópticos, preservando la calidad documental.

Los sensores de partículas miden en tiempo real la concentración de polvo, esporas y otros microrganismos en suspensión; al superar un umbral predefinido, envían avisos para que el personal investigue filtraciones de aire o focos de contaminación biológica que podrían dañar encuadernaciones, películas fotográficas o placas electrónicas.

Las estaciones de limpieza con cepillos suaves y aspiración filtrada proporcionan una superficie antiestática donde se retira suciedad antes de archivar o digitalizar; los cepillos de pelo natural separan residuos sin rayar, mientras que el aspirador equipado con filtros de alta eficiencia captura las partículas desprendidas, evitando su redistribución sobre otros materiales.

Los lectores RFID y de códigos de barras automatizan la identificación de cajas y carpetas: cada contenedor lleva una etiqueta con chip o código impreso; al escanear, el sistema actualiza préstamos, devoluciones y ubicaciones, manteniendo la trazabilidad de los movimientos y reduciendo errores humanos en el inventario.

Por último, los escáneres planetarios emplean una cuna en forma de “V” o superficie plana regulable que sostiene volúmenes delicados bajo una cámara de alta resolución montada en ángulo; la captura se realiza sin presionar el lomo, se evita la exposición prolongada a la luz intensa y se generan imágenes digitales exactas que sustituyen la manipulación física durante las consultas.

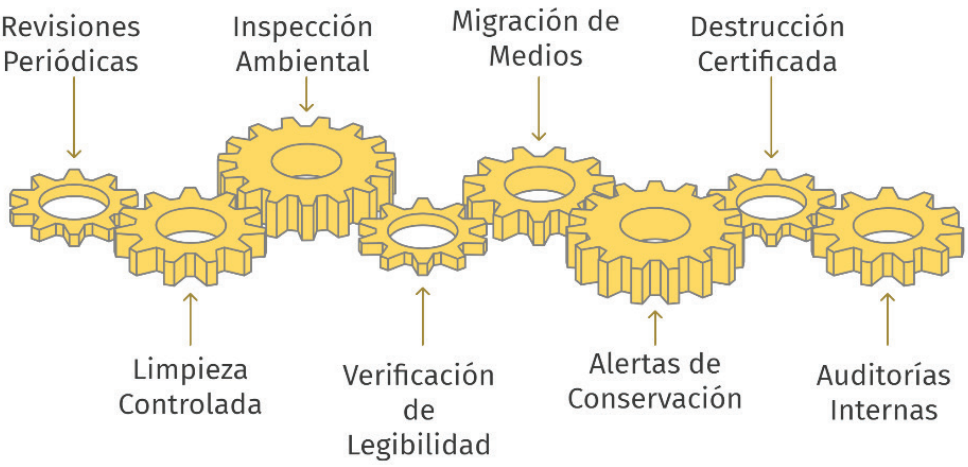
## 2.3 PROCEDIMIENTOS DE FUNCIONAMIENTO Y MANTENIMIENTO

El funcionamiento ordinario se apoya en un manual que describe la recepción de documentos, la clasificación según el cuadro autorizado y la asignación de signaturas únicas.


Cada ingreso se registra en un sistema de gestión que enlaza la referencia física o digital con metadatos completos: título, productor, fecha de origen, nivel de acceso y plazo de retención. Para las solicitudes de consulta, se habilitan formularios electrónicos que documentan la cadena de custodia y fijan plazos de devolución.

El mantenimiento comprende revisiones periódicas de estanterías y contenedores, limpieza controlada para prevenir polvo y plagas, inspección de condiciones ambientales y verificación de la legibilidad de soportes digitales.

**Proceso de mantenimiento de archivos**




Cuando se detectan medios magnéticos o formatos obsoletos, se procede a la migración a soportes contemporáneos, conservando la autenticidad mediante firmas digitales y registros hash. El calendario de conservación activa alertas automáticas que indican la transferencia de series semiactivas al depósito intermedio o su eliminación segura.

Para la destrucción certificada se emplean trituradoras de microcorte o servicios externos bajo contrato de confidencialidad, con emisión de actas que acreditan el proceso.

Para terminar, se programan auditorías internas que valoran la eficacia de los procedimientos y promueven la mejora continua, garantizando que el archivo mantenga su función estratégica dentro de la organización y cumpla las exigencias legales y operativas que se renuevan con el tiempo.

## 2.4 APLICACIÓN DEL PROCESO DE ARCHIVO

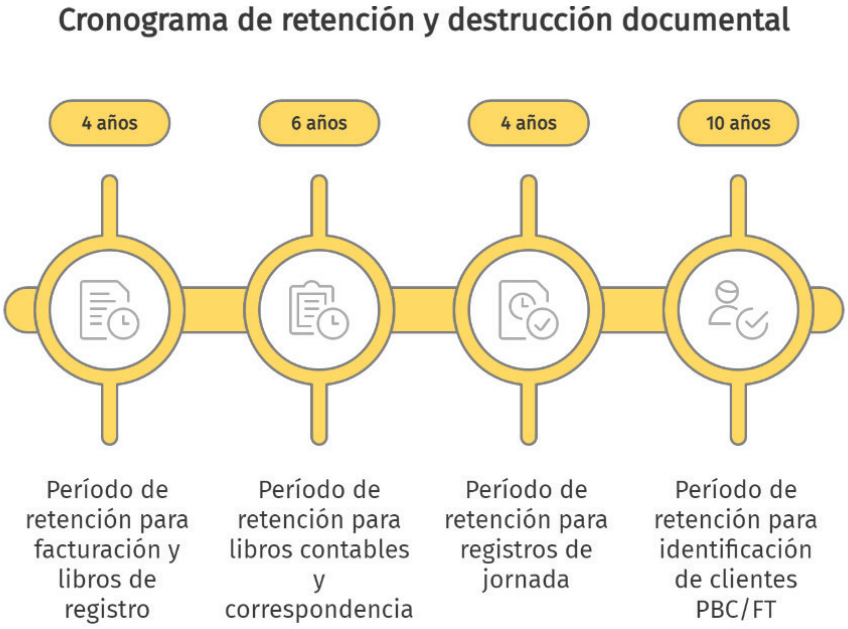
El proceso de archivo despliega una secuencia lógica que empieza con la recepción del documento y finaliza con su disposición posterior, ya sea la transferencia a un depósito histórico o la eliminación certificada. Su misión consiste en armonizar la continuidad administrativa con la protección de la memoria institucional, siempre bajo una pauta normativa que defina responsabilidades y plazos.

Cada paso incorpora procedimientos normalizados para la descripción, el registro, la digitalización —cuando procede— y la asignación de metadatos que faciliten la recuperación ágil del expediente. De forma transversal, intervienen controles que garantizan la autenticidad, la integridad y la trazabilidad, mediante firmas electrónicas, sellos de tiempo y registros de auditoría capaces de reconstruir la historia de cualquier acción efectuada sobre la información.

### 2.4.1 Conservación y destrucción según normativa vigente

La conservación documental se regula mediante calendarios que entrelazan requisitos legales, fiscales, laborales y de valor histórico-cultural. La norma ISO 15489-1:2016 dispone que el plazo de retención derive de la función que origina cada serie, mientras que la guía ISO 15489-2:2021 prescribe la revisión periódica de esos calendarios para adaptarlos a cambios normativos y a la evolución de los procesos de negocio.

En el ámbito tributario, el Real Decreto 1619/2012 exige custodiar facturas, justificantes y libros registro durante cuatro años, plazo que coincide con la prescripción establecida en la Ley 58/2003 General Tributaria; el Código de Comercio amplía a seis años la conservación de libros contables, balances y correspondencia.




La normativa laboral (Orden ESS/214/2018) fija en cuatro años el resguardo de los registros de jornada, y la Ley 10/2010 de prevención del blanqueo de capitales extiende a diez años la obligación de conservar la documentación de identificación de clientes y operaciones financieras. En materia de protección de datos, el Reglamento (UE) 2016/679 limita la retención al tiempo estrictamente necesario para la finalidad declarada y, una vez cumplido, la Ley Orgánica 3/2018 ordena bloquear los datos, dejándolos accesibles solo a autoridades competentes hasta que prescriban las responsabilidades asociadas.

La preservación electrónica descansa en repositorios certificados conforme a ISO 14721:2015 (OAIS) y ISO 16363:2020. Estos estándares exigen emplear formatos abiertos y autodocumentados —por ejemplo, PDF/A-2 para textos y TIFF 6.0 para imágenes—, programar migraciones controladas registradas en un plan de preservación, aplicar sumas de verificación SHA-256 de forma periódica y mantener una replicación geográfica con al menos tres copias independientes.

En la Administración española, el Real Decreto 203/2021 obliga a custodiar expedientes electrónicos en plataformas que cumplan el Esquema Nacional de Seguridad (ENS), nivel medio o alto, además de emitir sellos de tiempo cualificados cada vez que se firma o migra un documento, lo que refuerza la integridad y la trazabilidad a largo plazo.

La fase de destrucción se inicia cuando el expediente ha agotado su ciclo operativo y carece de valor histórico. El procedimiento se documenta mediante un acta que relaciona signaturas y series afectadas, firmada por la unidad de archivo y la autoridad competente. Para soportes en papel se emplean trituradoras de microcorte que reducen el material a tiras inferiores a cinco milímetros o prensas con compactación vigilada; los soportes ópticos y magnéticos se desmagnetizan con equipos de campo intenso o se pulverizan mecánicamente.

El ENS y el estándar NIST 800-88 definen niveles de sanitización digital que van del borrado lógico con sobreescritura múltiple a la destrucción física de los discos. La trazabilidad integral del proceso queda consignada en el sistema de gestión documental, de modo que la organización pueda demostrar cumplimiento durante auditorías internas, inspecciones fiscales o procedimientos judiciales.

### 2.4.2 Garantías de confidencialidad y seguridad de la información

La confidencialidad se estructura sobre un modelo de acceso escalonado, sustentado en perfiles y permisos vinculados al directorio corporativo. Cualquier solicitud de consulta debe quedar registrada en un circuito de autorización donde la identidad del usuario, el propósito de la consulta y el plazo de uso se validen antes de liberar el expediente.

En el ámbito físico, las áreas de archivo se equipan con cerraduras de alta seguridad, control de presencia mediante tarjetas de proximidad y cámaras con registro continuo; los contenedores de documentación sensible viajan en sobres opacos numerados y sellados, acompañados de un albarán que acredita la cadena de custodia.

En el dominio digital, la seguridad descansa en la autenticación multifactor, el cifrado AES-256 en reposo y TLS 1.3 en tránsito, así como en la segmentación de redes a través de VLAN protegidas por cortafuegos de inspección profunda. Los registros de acceso se alimentan a un SIEM (Security Information and Event Management) que detecta patrones anómalos en tiempo real y dispara alertas a los responsables de seguridad. La continuidad operativa se respalda con almacenamiento redundante en niveles RAID, réplicas remotas y planes de recuperación ante desastres con objetivos de punto (RPO) y de tiempo (RTO) definidos según el impacto en el negocio.

La confidencialidad contractual se asegura mediante acuerdos de confidencialidad (NDA) firmados por proveedores y personal interno, además de cláusulas de tratamiento de datos cuando intervienen terceros. Las sesiones formativas periódicas refuerzan la cultura de seguridad, explicando buenas prácticas de clasificación, técnicas de phishing y normativas vigentes en protección de datos.

# Ejemplo

## Ejemplo de acuerdo de confidencialidad (NDA) estándar

*(redactado para uso entre dos entidades,*
*"Parte Reveladora" y "Parte Receptora")*

1. Objeto y finalidad

   La Parte Reveladora entregará información de carácter técnico, comercial, financiero o estratégico con el propósito de evaluar oportunidades de cooperación. La Parte Receptora se compromete a utilizar dicha información exclusivamente para los fines de análisis previamente acordados.

2. Definiciones
   - Información Confidencial: todo dato, documento, prototipo, código fuente, especificación, plano, imagen, estudio o conversación, ya sea en soporte escrito, oral, electrónico o cualquier otro medio, que la Parte Reveladora identifique como confidencial o que, por su naturaleza, deba considerarse reservado.
   - Representantes Autorizados: empleados, directivos, asesores o subcontratistas de la Parte Receptora que necesiten conocer la Información Confidencial para cumplir con la finalidad descrita.

3. Obligaciones de confidencialidad
   a) Proteger la Información Confidencial con un nivel de cuidado, como mínimo, equivalente al que emplea para su propia información reservada y, en todo caso, conforme a buenas prácticas alineadas con ISO 27001.
   b) Limitar el acceso exclusivamente a Representantes Autorizados sujetos a obligaciones de confidencialidad equivalentes al presente acuerdo.
   c) No copiar, reproducir, desensamblar, revelar ni utilizar la Información Confidencial para fines distintos a los estipulados, salvo consentimiento previo y escrito de la Parte Reveladora.

4. Exclusiones

   Queda fuera del concepto de Información Confidencial aquella que:
   1. fuese de dominio público en la fecha de divulgación;
   2. llegue a ser de dominio público posteriormente sin incumplimiento de la Parte Receptora;
   3. obre ya en poder de la Parte Receptora con anterioridad y sin restricción;
   4. sea divulgada legítimamente por un tercero sin obligación de confidencialidad;

5. deba comunicarse por mandato legal, judicial o administrativo, siempre que la Parte Receptora notifique con antelación suficiente a la Parte Reveladora para permitir la adopción de medidas de protección.

5. Medidas de seguridad

   La Parte Receptora mantendrá controles técnicos y organizativos adecuados (cifrado AES-256 en reposo, TLS 1.3 en tránsito, control de acceso con MFA, registro de eventos en SIEM) y cumplirá el Esquema Nacional de Seguridad nivel medio o equivalente —cuando resulte aplicable— para prevenir pérdidas, accesos no autorizados o alteraciones de la Información Confidencial.

6. Plazo de vigencia y retención

   Las obligaciones de confidencialidad permanecerán vigentes durante cinco años desde la última recepción de Información Confidencial, salvo que la ley exija un periodo mayor. Transcurrido el plazo, o a petición escrita de la Parte Reveladora, la Parte Receptora devolverá o destruirá todos los soportes que contengan Información Confidencial y remitirá certificación escrita de su cumplimiento.

7. Propiedad intelectual y licencias

   Toda Información Confidencial, incluidas marcas, patentes, diseños, derechos de autor y know-how, seguirá siendo titularidad exclusiva de la Parte Reveladora. El presente acuerdo no otorga licencia ni cesión implícita de derechos de propiedad intelectual, salvo la necesaria para cumplir la finalidad del apartado 1.

8. Responsabilidad e indemnización

   La Parte Receptora responderá de los daños y perjuicios directos derivados de una divulgación no autorizada y mantendrá indemne a la Parte Reveladora frente a reclamaciones de terceros ocasionadas por dicho incumplimiento.

9. Legislación aplicable y jurisdicción

   El acuerdo se regirá e interpretará conforme a la legislación española. Para la resolución de cualquier disputa, las partes se someten, con renuncia expresa a cualquier otro fuero, a los juzgados y tribunales de la ciudad acordada (por ejemplo, Madrid).

10. Duración del acuerdo

    Entrará en vigor en la fecha de la última firma y permanecerá vigente hasta que todas las obligaciones aquí contenidas queden satisfechas.

Firma de las partes

| Parte Reveladora | Parte Receptora |
|---|---|
| Nombre: _____ | Nombre: _____ |
| Cargo: _____ | Cargo: _____ |
| Fecha: _____ | Fecha: _____ |
| Firma: _____ | Firma: _____ |

* Este modelo constituye un ejemplo general y puede necesitar adaptaciones específicas para sector regulado, tratamiento de datos personales, transferencia internacional de información o requisitos adicionales de la compañía.

Por último, auditorías internas y externas, basadas en ISO 27001 o ENS, revisan el grado de cumplimiento y generan planes de acción que perfeccionan las salvaguardas existentes, garantizando que la información permanezca íntegra, disponible y fuera del alcance de accesos indebidos durante todo su ciclo de vida.

## 2.5 IMPLEMENTACIÓN DE MODELOS DE ORGANIZACIÓN

Un modelo de organización documental articula reglas, espacios y tecnologías para vincular la producción diaria con la preservación a largo plazo. Su diseño requiere estudiar el flujo de información desde el instante en que se crea un expediente, identificando responsables, formatos y plazos de transferencia entre unidades.

Se definen procedimientos escritos que describen la captura de metadatos, los niveles de acceso, los hitos de valoración y los mecanismos de auditoría. El enfoque se apoya en un sistema de gestión capaz de mostrar, en tiempo real, qué documentos permanecen en uso operativo, cuáles pasan a consulta eventual y cuáles se conservan por motivos legales, fiscales o históricos.

Una cartografía de riesgos —que contemple ciberamenazas, desastres naturales y errores humanos— guía la asignación de copias de seguridad, réplicas geográficas y controles de integridad, garantizando que el modelo resista incidencias sin perder trazabilidad ni autenticidad.

### Ejemplo

Se diseña un mapa de riesgos para una empresa con sede principal en Sevilla y un centro de respaldo en Madrid. El análisis parte de tres vectores: amenazas lógicas, eventos naturales y fallos operativos.

En el apartado de ciberamenazas se valora el ransomware como riesgo de probabilidad alta e impacto muy alto; la respuesta asigna copias de seguridad incrementales cada cuatro horas en almacenamiento inmutable, una réplica asíncrona diaria hacia el centro de Madrid y pruebas mensuales de restauración completa en un entorno aislado.

Para desastres naturales, se observa que la sede sevillana se encuentra en zona fluvial con posibilidad moderada de inundación: se replica la totalidad de las máquinas virtuales a 550 kilómetros de distancia, se mantiene una copia semanal en un proveedor cloud europeo con certificación ISO 22301 y se contrata un generador diésel que garantiza 48 horas de autonomía eléctrica.

En la categoría de errores humanos se identifica la eliminación accidental de expedientes como riesgo recurrente; se implementa versionado automático con retención de 90 días, doble validación antes de borrar y un programa de formación semestral que instruye al personal sobre buenas prácticas de gestión documental.

Cada control queda vinculado en el plan maestro de continuidad, donde un panel de métricas registra el cumplimiento de las frecuencias de copia, la integridad verificada mediante hashes SHA-256 y los tiempos de recuperación reales frente a los objetivos definidos. De este modo, el modelo mantiene trazabilidad y autenticidad incluso si se materializa cualquiera de los escenarios contemplados.

---

### 2.5.1 Archivos activos, semiactivos e inactivos

Los **archivos activos** contienen la documentación imprescindible para la actividad corriente de la organización. Se ubican preferentemente en puntos próximos a las unidades productoras y en soportes que permitan recuperación instantánea (servidores de alto rendimiento o armarios de oficina con acceso restringido).

Los **archivos semiactivos** reúnen expedientes todavía necesarios, aunque con una frecuencia de consulta reducida. Estos fondos se trasladan a depósitos intermedios o a almacenamiento digital de segunda línea respaldado por discos de capacidad masiva, donde se optimiza el coste sin sacrificar la disponibilidad.

Por su parte, los **archivos inactivos** albergan materiales cuyo valor operativo ha concluido, pero deben mantenerse por exigencia legal o por interés histórico. Se conservan en depósitos externos, bóvedas climatizadas o repositorios digitales certificados, con esquemas de replicación y monitorización de largo plazo. Las transferencias entre etapas se apoyan en calendarios de conservación que disparan alertas automáticas para evitar retenciones innecesarias y liberar recursos.

## Ejemplo

Una serie de expedientes de contratación elaborados por el departamento de compras durante la presente campaña presupuestaria se considera archivo activo, pues el personal revisa las condiciones, aplica enmiendas y emite órdenes de pago a diario; la consulta frecuente exige mantener los documentos en la nube corporativa de acceso inmediato y en armarios cercanos al equipo gestor, garantizando agilidad en las operaciones de adquisición.

Las solicitudes de vacaciones y ausencias del año en curso, junto con los justificantes médicos emitidos en las últimas semanas, integran igualmente un archivo activo: el área de recursos humanos debe verificar saldos de días disponibles, calcular nóminas y responder a auditorías internas de personal en plazos muy breves, de modo que los formularios se almacenan en carpetas electrónicas con permisos específicos y en archivadores etiquetados por mes.

Los expedientes de inscripción de estudiantes que realizaron matrícula hace dos cursos académicos se clasifican como archivo semiactivo. Aunque las incidencias de consulta han disminuido, todavía se solicitan para trámites de becas o equivalencias; por ello, los documentos se transfieren a un servidor de capacidad masiva y a un depósito intermedio con acceso reglado, reduciendo coste de almacenamiento sin sacrificar tiempo de recuperación.

Los contratos de mantenimiento de maquinaria industrial firmados hace tres años —con vigencia inicial de cinco años y opción de prórroga— representan otro archivo semiactivo. El departamento de ingeniería requiere revisarlos de manera esporádica para verificar cláusulas de servicio, pero la frecuencia no justifica su permanencia en el servidor de proyectos activo; se archivan, por tanto, en un repositorio documental de segunda línea con índice de búsqueda.

Las declaraciones fiscales de la empresa correspondientes al último ejercicio cerrado y ya presentadas a la autoridad tributaria entran igualmente en la categoría de archivo semiactivo. El requerimiento legal obliga a conservarlas durante cuatro años, aunque las consultas disminuyen salvo que se reciba inspección; se decide almacenarlas en un sistema WORM (Write Once Read Many) con copias redundantes y acceso restringido a finanzas.

Los expedientes de expropiaciones urbanísticas tramitados hace quince años, cuyo plazo de recurso ha prescrito y que se conservarán únicamente para referencia histórica, constituyen un archivo inactivo. Se trasladan a una cámara climatizada con estanterías compactas y, además, se digitalizan en TIFF 6.0 para consulta interna sin manipular los originales.

Las actas de juntas generales correspondientes a la década de 1990 se consideran archivo inactivo por haber sobrepasado el margen mercantil de seis años y poseer valor histórico; se custodian en cajas libres de ácido dentro del depósito histórico y se incluyen en el catálogo patrimonial de la organización.

Los registros de sistemas biométricos de control horario que finalizaron su vida útil tecnológica hace ocho años, pero cuyas responsabilidades administrativas ya han prescrito, se clasifican como archivo inactivo; se mantienen bloqueados en soporte óptico de solo lectura y con hash registrado para conservar integridad hasta autorizar su eliminación definitiva según el calendario de conservación.

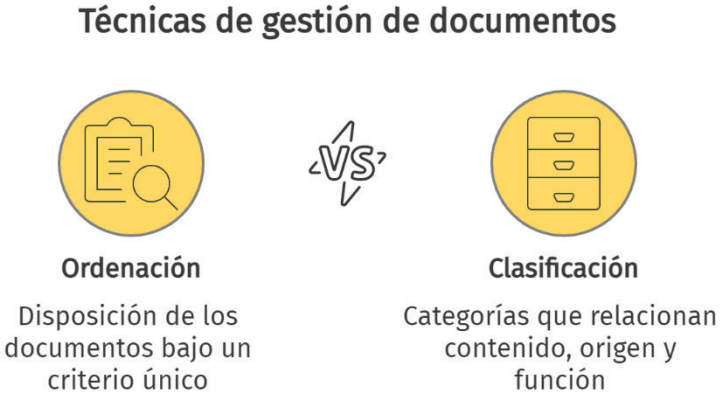
Los planos de construcción de una planta industrial que opera desde hace veinte años, sin modificaciones recientes, también pertenecen al archivo inactivo; la documentación conserva valor probatorio para seguros y reclamaciones estructurales, por lo que se almacena en gavetas horizontales y se replica en PDF/A para consulta técnica puntual.

Por último, los expedientes de subvenciones europeas liquidados totalmente y sin obligaciones de reembolso pendientes configuran otro

ejemplo de archivo inactivo. Al haberse cumplido el plazo de verificación comunitaria, se conservan en un repositorio digital con firma longeva para preservar autenticidad, pero quedan fuera del circuito habitual de gestión, accediéndose a ellos solo por requerimientos de transparencia o investigación histórica.

## 2.6 TÉCNICAS DE ORDENACIÓN Y CLASIFICACIÓN DOCUMENTAL

La **ordenación** constituye el acto de disponer física o lógicamente los documentos según un criterio único, mientras que la **clasificación** establece categorías que relacionan contenido, origen y función. Una técnica eficaz reduce tiempos de búsqueda, potencia la eficiencia administrativa y minimiza duplicidades.

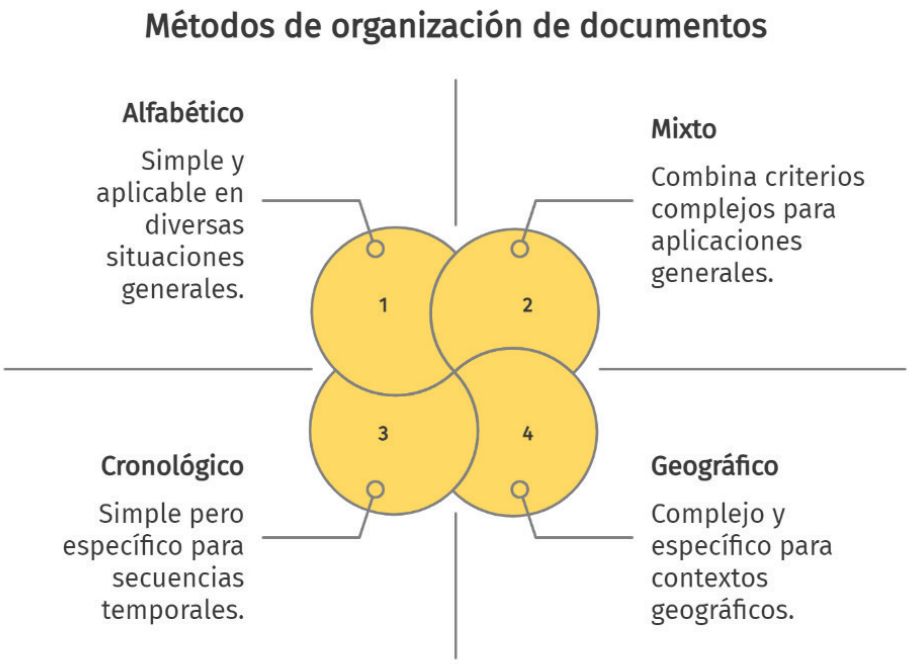



Para alcanzar ese propósito se combinan normas de descripción, cuadros de clasificación jerárquica y herramientas de etiquetado que enlazan cada registro con metadatos normalizados. Cuando el volumen aumenta, resultan indispensables los sistemas de referencia cruzada y los códigos alfanuméricos que facilitan reubicaciones y préstamos.

El cuadro de clasificación se revisa de forma periódica, incorporando series emergentes —por ejemplo, registros de redes sociales o evidencias de firma biométrica— y suprimiendo aquellas que ya no se generan.

### 2.6.1 Métodos alfabético, numérico, cronológico, geográfico, por materias y mixto

Algunos de los métodos de organización de documentos más populares son los siguientes:




- *Alfabético:* asigna la ordenación según la primera letra o secuencia de letras del nombre del productor, cliente o asunto. Es intuitivo y rápido de implementar en expedientes de personal, registros de proveedores o correspondencia general. Para evitar ambigüedades se normalizan prefijos, artículos y abreviaturas, y se aplica la regla de "archivo como se escribe".

- *Numérico:* otorga a cada expediente un identificador correlativo o un número estructurado que codifica departamento, serie y secuencia. Este sistema maximiza el espacio en estanterías móviles y simplifica la migración a bases de datos, dado que el localizador físico se corresponde con la signatura asignada.

- *Cronológico:* dispone los documentos por fecha de creación o recepción. Resulta idóneo para actas de reuniones, informes periódicos o diarios de obra, donde la secuencia temporal refleja la evolución de los procesos. Implica etiquetado claro de día, mes y año y el uso de contenedores con intervalos asignados (trimestrales o anuales).

- *Geográfico:* organiza según la región, país o área administrativa vinculada al contenido. Se aplica en proyectos de obras públicas, expedientes de exportación o informes de ventas por zona. Requiere listas oficiales de topónimos y niveles jerárquicos (continente → país → provincia → localidad) para asegurar la consistencia.

- *Por materias:* clasifica a partir de un tesauro o árbol de temas que refleja la actividad institucional. Cada documento recibe una clave temática y, cuando es necesario, subtemas y microtesoros que refinan la precisión. Este método favorece análisis transversales y recuperación conceptual en centros de documentación y bibliotecas especiales.

- *Mixto:* combina dos o más criterios para cubrir complejidades superiores. Un esquema frecuente adopta orden alfabético dentro de bloques cronológicos, o codificación numérica con sufijo temático. La clave se documenta en un manual que detalla precedencias y excepciones, garantizando que toda persona encargada del archivo interprete la misma lógica y mantenga la coherencia a lo largo del tiempo.