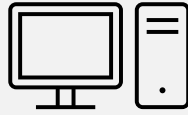


## Unidad 2



# Planificación e instalación de sistemas operativos en red



## EDITORIAL TUTOR FORMACIÓN

La implantación de un sistema operativo en red requiere una planificación previa rigurosa que tenga en cuenta las necesidades técnicas, organizativas y de crecimiento del entorno. Una instalación incorrecta o mal dimensionada puede derivar en problemas de rendimiento, seguridad o mantenimiento a medio y largo plazo, por lo que resulta imprescindible abordar este proceso de forma estructurada.

En esta unidad se estudian los criterios que intervienen en la planificación y en la instalación inicial del sistema operativo en red, desde el análisis de requisitos hasta la configuración básica tras la instalación. El enfoque se centra en entornos profesionales, evitando procedimientos propios de sistemas individuales y priorizando la coherencia del conjunto de la infraestructura.

# 1. Análisis de requisitos del entorno de red.

El **análisis de requisitos del entorno de red** constituye la fase inicial y más determinante en la implantación de un sistema operativo en red. Antes de instalar cualquier software o definir configuraciones, resulta imprescindible **comprender el contexto real** en el que el sistema va a operar. Un análisis incompleto o superficial suele traducirse en sistemas sobredimensionados, ineficientes o incapaces de adaptarse a la evolución de la organización.

Esta fase no es exclusivamente técnica. Implica identificar **necesidades organizativas, formas de trabajo, expectativas de crecimiento y limitaciones existentes**, para posteriormente traducirlas en requisitos técnicos claros. El sistema operativo en red debe responder al entorno, no forzar a la organización a adaptarse a una solución mal planteada.

## Objetivo del análisis de requisitos

El objetivo principal del análisis de requisitos es **definir con precisión qué debe hacer el sistema operativo en red**, bajo qué condiciones y con qué nivel de exigencia. Esto permite:

- Seleccionar el sistema operativo adecuado.
- Dimensionar correctamente la infraestructura.
- Definir una estructura lógica coherente.
- Anticipar problemas de escalabilidad.
- Reducir errores en fases posteriores.



### Recuerda

Los problemas más graves y difíciles de corregir en un sistema operativo en red suelen tener su origen en decisiones previas a la instalación, cuando aún se está definiendo qué se espera del sistema y cómo debe responder ante las necesidades de la organización. Una instalación técnicamente correcta no compensa un análisis de requisitos incompleto, ya que las carencias iniciales se traducen después en limitaciones estructurales, configuraciones forzadas o soluciones improvisadas.

Un análisis de requisitos riguroso permite tomar decisiones fundamentadas sobre arquitectura, escalabilidad y nivel de control, evitando errores que, una vez desplegado el sistema, resultan costosos de corregir. Pensar antes de instalar implica evaluar no solo la situación actual, sino también la evolución prevista del entorno. De este modo, el sistema operativo en red se construye sobre una base sólida, coherente y alineada con las necesidades reales, reduciendo significativamente los riesgos a medio y largo plazo.

## Identificación del tipo de organización

El primer paso consiste en analizar el **tipo de organización** para la que se diseña el sistema. No es lo mismo una empresa privada, un centro educativo, una administración pública o una asociación, ya que cada una presenta dinámicas distintas.

Algunos aspectos clave a considerar son:

- Finalidad de la organización.
- Grado de formalización de procesos.
- Nivel de rotación de usuarios.
- Dependencia del sistema informático para la actividad diaria.



Nota

Un sistema operativo en red para un centro educativo prioriza la gestión de grupos y perfiles temporales; uno para una empresa prioriza continuidad, control y trazabilidad.

### Número de usuarios y perfiles de uso

Determinar cuántos usuarios utilizarán el sistema y **cómo lo harán** es fundamental. No todos los usuarios tienen las mismas necesidades ni el mismo impacto en el sistema.

Se deben identificar:

- Número total de usuarios.
- Tipos de usuario (administración, técnicos, alumnado, personal temporal, etc.).
- Frecuencia de acceso.
- Nivel de autonomía permitido.

La clasificación habitual de perfiles es la siguiente:

Tipo de usuario	Características	Impacto en el sistema
Usuario básico	Uso de aplicaciones y archivos	Bajo
Usuario avanzado	Uso intensivo de recursos	Medio
Usuario administrativo	Acceso a información sensible	Alto
Usuario técnico	Cambios de configuración	Muy alto



Recuerda

El diseño de un sistema operativo en red debe partir del usuario más exigente, ya que es este perfil el que pone a prueba los límites de la infraestructura, la seguridad y la organización del entorno. Usuarios con acceso a información sensible, capacidad de modificar configuraciones o uso intensivo de recursos condicionan decisiones clave como la segmentación de permisos, la definición de políticas, el rendimiento necesario o los mecanismos de control y auditoría.

No obstante, diseñar para el perfil más exigente no significa complicar innecesariamente la experiencia del resto de usuarios. El reto consiste en equilibrar robustez y usabilidad, de modo que el sistema sea capaz de soportar cargas elevadas y operaciones críticas, mientras mantiene una experiencia fluida y controlada para los perfiles básicos o temporales. Una correcta clasificación de usuarios permite aplicar el principio de mínimo privilegio, optimizar recursos y garantizar un funcionamiento estable y seguro para todo el conjunto del sistema.

### Número y tipo de equipos

El análisis debe incluir los **equipos que formarán parte del entorno**, ya que condicionan la carga del sistema operativo en red y el modelo de administración.

Aspectos a evaluar:

- Número total de equipos.
- Tipología (puestos fijos, portátiles, aulas, terminales compartidos).
- Uso simultáneo.
- Vida útil prevista.

Este análisis permite anticipar necesidades de:

- Gestión de perfiles.
- Aplicación de políticas diferenciadas.
- Escalabilidad futura.

### Recursos a gestionar desde el sistema operativo en red

El sistema operativo en red no solo gestiona usuarios, sino también **recursos compartidos** que deben identificarse desde el inicio:

- Carpetas compartidas.
- Almacenamiento centralizado.
- Impresoras de red.
- Perfiles de usuario.
- Configuraciones comunes.

Para cada recurso conviene determinar:

- Quién accede.
- Qué nivel de acceso necesita.
- Qué importancia tiene para la actividad diaria.



Ejemplo

Un recurso crítico (documentación de gestión) requiere permisos estrictos, copias frecuentes y trazabilidad, mientras que un recurso de uso general puede gestionarse con menor control.

### Grado de compartición y colaboración

No todas las organizaciones trabajan del mismo modo. Algunas requieren un alto grado de colaboración, mientras que otras mantienen información muy segmentada.

El análisis debe responder a preguntas como:

- ¿Se comparte información entre departamentos?
- ¿Existen proyectos transversales?
- ¿Hay información confidencial?
- ¿Se requiere acceso desde distintos equipos?

Este análisis influye directamente en:

- La estructura de carpetas.
- La organización de grupos.
- La definición de permisos.

### Requisitos de disponibilidad y continuidad

El grado de dependencia del sistema operativo en red determina los **requisitos de continuidad del servicio**. No todos los entornos toleran las mismas interrupciones.

Se debe evaluar:

- Impacto de una caída del sistema.
- Tiempo máximo aceptable de inactividad.
- Necesidad de copias de seguridad frecuentes.
- Prioridad de restauración.



#### Nota

Cuando la actividad de la organización depende directamente del funcionamiento del sistema operativo en red, la continuidad del servicio deja de ser un elemento opcional o deseable para convertirse en un requisito crítico. En estos casos, una interrupción no solo implica una incidencia técnica, sino una paralización real del trabajo, con impacto directo en la productividad, la atención al usuario o incluso en el cumplimiento de obligaciones legales y contractuales.

Evaluar correctamente los requisitos de disponibilidad permite definir medidas acordes al nivel de dependencia del entorno: desde copias de seguridad periódicas y procedimientos de restauración claros, hasta estrategias de alta disponibilidad y priorización de servicios críticos. Cuanto mayor es el impacto de una caída, mayor debe ser el nivel de planificación preventiva. Diseñar el sistema teniendo en cuenta estos factores reduce el riesgo operativo y garantiza que el entorno pueda recuperarse de forma controlada ante fallos inevitables.

### Requisitos de crecimiento y evolución

El análisis debe contemplar no solo la situación actual, sino la **evolución prevista del entorno**:

- Incremento de usuarios.
- Nuevos equipos.
- Cambios organizativos.
- Nuevas formas de trabajo.

Un sistema operativo en red debe planificarse con márgenes claros de crecimiento, asumiendo que el entorno cambiará con el tiempo. El aumento de usuarios, la incorporación de nuevos equipos, la reorganización interna o la adopción de nuevas formas de trabajo son procesos habituales que no deberían obligar a replantear toda la infraestructura. Cuando el diseño inicial no contempla esta evolución, cada cambio se convierte en una intervención compleja, costosa y propensa a errores.

Un sistema bien planificado permite crecer por extensión, añadiendo elementos, servicios o políticas sobre una base sólida ya existente. Esto implica definir estructuras lógicas flexibles, mecanismos de administración reutilizables y una arquitectura que admita ampliaciones sin romper el conjunto. De este modo, el sistema operativo en red acompaña a la organización en su evolución natural, en lugar de convertirse en un freno o en una fuente constante de reestructuraciones.

### Restricciones y limitaciones existentes

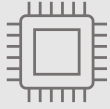
No todos los requisitos son deseables; algunos son **limitaciones** que deben asumirse:

- Presupuesto disponible.
- Infraestructura existente.
- Nivel técnico del personal.
- Políticas internas de la organización.

Estas restricciones condicionan las decisiones técnicas y deben documentarse para evitar expectativas irreales.

Los requisitos a analizar son:

Área	Preguntas clave
<b>Usuarios</b>	¿Cuántos? ¿Qué perfiles?
<b>Equipos</b>	¿Cuántos y de qué tipo?
<b>Recursos</b>	¿Qué se comparte y cómo?
<b>Organización</b>	¿Cómo se estructura el trabajo?
<b>Continuidad</b>	¿Qué ocurre si el sistema falla?
<b>Crecimiento</b>	¿Cómo evolucionará el entorno?
<b>Limitaciones</b>	¿Qué no se puede cambiar?



### Actividad 3

Se plantea un entorno con las siguientes características:

25 usuarios.

Dos departamentos diferenciados.

Documentación compartida con carácter sensible.

Previsión de crecimiento hasta 40 usuarios.

**Tarea:**

Identificar los requisitos más relevantes que debe cumplir el sistema operativo en red para dar respuesta a este entorno.

El análisis de requisitos no es una formalidad: es la **base sobre la que se construye todo el sistema**. Un análisis riguroso reduce errores, facilita la administración y garantiza que el sistema operativo en red responda a las necesidades reales de la organización.



## 2. Selección del sistema operativo en red según necesidades.

Una vez realizado el análisis de requisitos del entorno, el siguiente paso consiste en la **selección del sistema operativo en red** que mejor se adapte a dichas necesidades. Esta decisión es crítica, ya que condiciona la **arquitectura del sistema**, las **herramientas de administración disponibles**, el **modelo de gestión de usuarios y recursos** y la **capacidad de evolución futura** del entorno. Elegir un sistema inadecuado puede generar limitaciones difíciles de corregir sin una reimplantación completa.

La selección no debe basarse únicamente en criterios de popularidad o familiaridad, sino en una **evaluación objetiva de las características del entorno**, los requisitos técnicos y organizativos identificados y las capacidades reales del sistema operativo. En este proceso, resulta fundamental priorizar la adecuación funcional frente a soluciones genéricas o sobredimensionadas.

### Criterios generales de selección

La elección de un sistema operativo en red debe apoyarse en una serie de criterios que permitan comparar distintas opciones de forma estructurada. Entre los más relevantes se encuentran:

- Capacidad de **gestión centralizada** de usuarios y equipos.
- Soporte para **políticas de sistema**.
- Facilidad de **administración y mantenimiento**.
- Escalabilidad y adaptación al crecimiento.
- Compatibilidad con el entorno existente.
- Nivel de documentación y soporte disponible.



#### Recuerda

La selección de un sistema operativo en red no debe basarse en la acumulación de funcionalidades ni en su potencial máximo, sino en su adecuación real a las necesidades del entorno. Muchas plataformas ofrecen un amplio conjunto de posibilidades que, si no se utilizan, añaden complejidad innecesaria a la administración y dificultan el mantenimiento. Un sistema eficaz es aquel que cubre de forma fiable los requisitos definidos, sin exigir soluciones forzadas ni configuraciones excesivas.

Elegir en función de lo que realmente se necesita implica valorar la estabilidad, la facilidad de gestión y la coherencia con la infraestructura existente por encima de características avanzadas que pueden no ser relevantes. Un sistema operativo en red bien elegido simplifica el trabajo diario del administrador, reduce la probabilidad de errores y garantiza un funcionamiento predecible a largo plazo, incluso cuando el entorno crece o evoluciona.

### Adecuación al tamaño y complejidad del entorno

El tamaño del entorno influye directamente en la elección del sistema operativo en red. No todos los sistemas están pensados para los mismos escenarios.

- En entornos pequeños:
  - Se prioriza la simplicidad de administración.
  - Es importante minimizar la carga de mantenimiento.
  - Se valoran soluciones que no requieran una infraestructura compleja.
- En entornos medianos y grandes:
  - Se requiere una gestión avanzada de identidades.
  - Es fundamental el uso de políticas y automatización.
  - Se necesitan mecanismos de delegación administrativa.

Elegir un sistema diseñado para grandes entornos en una red pequeña puede resultar innecesariamente complejo; elegir uno limitado en un entorno en crecimiento genera problemas a medio plazo.

### Modelo de gestión de identidades

Uno de los aspectos más determinantes es el **modelo de gestión de identidades** que ofrece el sistema operativo en red. Este modelo define cómo se crean, gestionan y utilizan las cuentas de usuario y equipo.

Al evaluar este criterio conviene analizar:

- Centralización de cuentas.
- Gestión de grupos y roles.
- Aplicación de permisos.
- Integración de perfiles de usuario.
- Capacidad de administración delegada.



Nota

La gestión de identidades es el eje del sistema operativo en red: si este componente es débil, el resto del sistema se resiente.

### Herramientas de administración disponibles

El sistema operativo en red debe proporcionar **herramientas eficaces de administración**, que permitan gestionar el entorno de forma ágil y controlada. Estas herramientas pueden ser gráficas, basadas en consola o una combinación de ambas.

Aspectos a valorar:

- Facilidad de uso.
- Posibilidad de administración remota.
- Automatización de tareas.
- Gestión centralizada de configuraciones.
- Acceso controlado para distintos perfiles técnicos.



### Recuerda

Una buena herramienta de administración no sustituye al conocimiento técnico, pero reduce errores y ahorra tiempo.

### Compatibilidad con el entorno existente

La selección debe tener en cuenta la **infraestructura ya implantada**, para evitar problemas de integración o costes innecesarios.

Conviene analizar:

- Compatibilidad con los equipos clientes.
- Integración con otros sistemas operativos.
- Requisitos de hardware del servidor.
- Posibilidad de migración desde sistemas previos.

Ignorar este aspecto puede provocar interrupciones prolongadas o la necesidad de cambios no previstos en el entorno.

### Escalabilidad y evolución futura

El sistema operativo en red debe permitir **crecer sin redefinir el modelo de administración**. Para ello, se debe evaluar:

- Capacidad de añadir nuevos usuarios y equipos.
- Flexibilidad en la organización de recursos.
- Soporte para estructuras más complejas.
- Posibilidad de incorporar nuevas funciones en el futuro.



### Nota

La escalabilidad de un sistema operativo en red no se limita a la capacidad de soportar más usuarios o equipos, sino a la posibilidad de crecer sin alterar el modelo de administración definido. Un sistema bien diseñado permite ampliar el entorno incorporando nuevos recursos, servicios o estructuras lógicas sin necesidad de replantear la forma en que se gestiona, se documenta o se controla el sistema.

Además de la dimensión técnica, la escalabilidad tiene una vertiente organizativa y administrativa. El sistema debe seguir siendo manejable a medida que aumenta su tamaño, permitiendo delegar funciones, mantener la coherencia de las políticas y conservar la trazabilidad de los cambios. Si el crecimiento obliga a complicar en exceso la administración o a introducir excepciones constantes, el sistema deja de ser escalable en la práctica, aunque lo sea desde el punto de vista técnico.

### Coste y recursos disponibles

El coste asociado a un sistema operativo en red no se limita a la licencia. Deben considerarse:

- Requisitos de hardware.
- Coste de mantenimiento.
- Necesidad de formación del personal.
- Tiempo dedicado a la administración.

La solución elegida debe ser **sostenible** a largo plazo, tanto técnica como organizativamente. Se expone una tabla comparativa orientativa de criterios de selección:

Criterio	Aspectos a evaluar
<b>Tamaño del entorno</b>	Usuarios, equipos, crecimiento
<b>Gestión de identidades</b>	Centralización, roles, grupos
<b>Administración</b>	Herramientas, automatización
<b>Compatibilidad</b>	Infraestructura existente
<b>Escalabilidad</b>	Evolución futura
<b>Coste</b>	Licencias, mantenimiento

Seleccionar un sistema operativo en red es una **decisión estratégica**, no un paso técnico menor. Un análisis riguroso de las necesidades del entorno permite elegir una solución adecuada, flexible y sostenible, facilitando la administración y reduciendo problemas futuros.

### 3. Planificación de la instalación en entornos corporativos.

La **planificación de la instalación** de un sistema operativo en red en un entorno corporativo es una fase crítica que actúa como **punto entre el análisis de requisitos y la ejecución técnica**. Una instalación correctamente planificada reduce incidencias, evita improvisaciones y permite que el sistema entre en funcionamiento de forma progresiva y controlada. En entornos profesionales, la instalación no debe entenderse como un evento puntual, sino como un **proceso estructurado** con impacto organizativo.

Planificar implica **anticipar decisiones**, definir un orden lógico de actuación y establecer criterios claros antes de intervenir sobre el sistema. Esta fase resulta especialmente relevante porque, a diferencia de entornos pequeños, en contextos corporativos cualquier error puede afectar a múltiples usuarios y comprometer la continuidad del servicio.

#### Objetivos de la planificación de la instalación

La planificación persigue una serie de objetivos fundamentales:

- Garantizar que la instalación se ajusta a los requisitos definidos.
- Minimizar interrupciones en la actividad de la organización.
- Reducir riesgos técnicos y organizativos.
- Facilitar el mantenimiento posterior del sistema.
- Asegurar la coherencia del entorno desde el inicio.



#### Recuerda

Una instalación bien planificada es aquella que se desarrolla de forma previsible y controlada, sin generar impactos inesperados en la actividad diaria de los usuarios ni situaciones de urgencia para el equipo técnico. Cuando la planificación es adecuada, los cambios están anticipados, los tiempos de intervención son conocidos y las posibles incidencias cuentan con procedimientos definidos, lo que reduce la percepción de riesgo y mejora la aceptación del sistema por parte de la organización.

Además, una instalación que no “sorprende” es el resultado de decisiones tomadas con antelación: definición clara de fases, pruebas previas, comunicación interna y validación de los pasos críticos. Esta forma de trabajar transforma la instalación en un proceso ordenado y asumible, en lugar de un evento disruptivo. De este modo, el sistema operativo en red comienza su funcionamiento sobre una base estable, facilitando tanto su uso cotidiano como su mantenimiento a largo plazo.

#### Definición del alcance de la instalación

Antes de iniciar cualquier actuación técnica, es imprescindible definir **qué se va a instalar y hasta dónde llega la intervención**. En entornos corporativos, el alcance puede variar considerablemente.

Conviene concretar:

- Qué servidores se van a implantar.

- Qué funciones asumirá el sistema operativo en red.
- Qué recursos se gestionarán desde el inicio.
- Qué elementos se incorporarán en fases posteriores.

Esta delimitación evita expectativas irreales y permite una implantación progresiva.



### Nota

No todo debe estar operativo desde el primer día. Una implantación por fases reduce riesgos y facilita la adaptación del entorno.

### Planificación temporal y ventanas de intervención

La planificación debe incluir un **calendario de instalación**, teniendo en cuenta la actividad normal de la organización. En entornos corporativos, resulta esencial definir:

- Fechas de instalación.
- Ventanas de intervención con menor impacto.
- Tiempos estimados de parada o degradación del servicio.
- Momentos de validación tras cada fase.



### Ejemplo

Realizar la instalación inicial fuera del horario laboral reduce el impacto en los usuarios y facilita pruebas sin presión operativa.

### Preparación de la infraestructura previa

Antes de instalar el sistema operativo en red, debe verificarse que la **infraestructura está preparada** para soportarlo. Esta preparación incluye:

- Disponibilidad y estado del hardware del servidor.
- Recursos de almacenamiento adecuados.
- Conectividad de red funcional.
- Acceso físico y lógico controlado al sistema.

Cualquier carencia en esta fase puede comprometer la instalación o generar problemas posteriores difíciles de diagnosticar.

### Definición de la estructura lógica inicial

La planificación debe contemplar la **estructura lógica** que tendrá el sistema desde el inicio, aunque pueda ampliarse más adelante. Esto incluye:

- Organización básica de usuarios y grupos.
- Estructura inicial de recursos compartidos.
- Criterios de asignación de permisos.
- Convenciones de nombres.

Definir estos elementos antes de instalar evita cambios disruptivos una vez el sistema está en uso.

### Planificación de la incorporación de usuarios y equipos

En entornos corporativos, la incorporación de usuarios y equipos debe realizarse de forma **ordenada y controlada**. La planificación debe responder a cuestiones como:

- ¿Se incorporarán todos los usuarios a la vez o por fases?
- ¿Qué equipos se integrarán inicialmente?
- ¿Cómo se gestionará la transición desde sistemas previos?

Una incorporación progresiva permite detectar errores y ajustar configuraciones sin afectar a todo el entorno.



#### Nota

En entornos corporativos, la transición entre sistemas es una fase crítica que va más allá de la mera instalación técnica. Una incorporación desordenada de usuarios y equipos puede provocar confusión, interrupciones en el trabajo diario y rechazo hacia el nuevo entorno, incluso aunque el sistema esté correctamente configurado. Por este motivo, planificar cómo y cuándo se produce el cambio es tan importante como decidir qué se instala.

Una transición bien gestionada se apoya en incorporaciones progresivas, pruebas controladas y comunicación clara con los usuarios afectados. Este enfoque permite detectar problemas reales en condiciones de uso, ajustar configuraciones antes de un despliegue completo y facilitar la adaptación de las personas al nuevo sistema. Cuando la transición se cuida, el sistema operativo en red se percibe como una mejora y no como una imposición, favoreciendo su adopción y estabilidad a largo plazo.

### Estrategia de pruebas y validación

La planificación debe incluir una **estrategia de pruebas**, orientada a comprobar que el sistema funciona conforme a lo previsto antes de su uso generalizado.

Conviene definir:

- Qué elementos se van a probar.
- En qué orden.

## EDITORIAL TUTOR FORMACIÓN

- Quién valida cada fase.
- Qué criterios determinan que una fase se considere correcta.

Las pruebas permiten detectar errores tempranos y evitan que problemas menores se conviertan en incidencias generalizadas.

### Documentación del proceso de instalación

Toda instalación en un entorno corporativo debe ir acompañada de una **documentación mínima**, que incluya:

- Decisiones técnicas adoptadas.
- Configuraciones iniciales.
- Estructura lógica del sistema.
- Incidencias detectadas y soluciones aplicadas.

Esta documentación resulta esencial para el mantenimiento posterior y para la continuidad del servicio en caso de cambios de personal.



Recuerda

Un sistema sin documentación es un sistema difícil de mantener, independientemente de su calidad técnica.

En resumen, los elementos clave de la planificación son:

Elemento	Finalidad
Alcance	Delimitar qué se instala
Calendario	Minimizar impacto
Infraestructura	Garantizar viabilidad
Estructura lógica	Asegurar coherencia
Incorporación	Controlar la transición
Pruebas	Validar funcionamiento
Documentación	Facilitar mantenimiento

La planificación de la instalación no es un trámite previo, sino una **fase decisiva** que determina la calidad del sistema operativo en red a largo plazo. Invertir tiempo en planificar reduce errores, facilita la adopción y garantiza un entorno más estable y controlado.



## 4. Instalación del sistema operativo en red.

La **instalación del sistema operativo en red** constituye la fase en la que las decisiones tomadas durante el análisis y la planificación se materializan en un entorno operativo real. En contextos corporativos, esta instalación debe ejecutarse de forma **metódica, documentada y controlada**, ya que cualquier error en esta etapa puede afectar a la estabilidad del sistema y dificultar su administración futura.

A diferencia de la instalación de un sistema monopuesto, la instalación de un sistema operativo en red no persigue únicamente que el sistema “arranque”, sino que quede preparado para **asumir funciones de administración**, integrarse en la infraestructura existente y servir de base para la gestión centralizada de usuarios, equipos y recursos.

### Consideraciones previas a la instalación

Antes de iniciar el proceso de instalación propiamente dicho, es imprescindible verificar una serie de condiciones que garantizan que el entorno está preparado:

- Disponibilidad del hardware destinado al servidor.
- Acceso a los medios de instalación oficiales.
- Confirmación de la planificación realizada.
- Definición clara del rol inicial del sistema.
- Copias de seguridad de sistemas previos, si existen.



#### Recuerda

La instalación comienza antes de ejecutar el instalador. Preparar el entorno reduce errores y retrabajos.

### Preparación del servidor

El servidor que alojará el sistema operativo en red debe prepararse cuidadosamente, ya que se convertirá en un elemento crítico del entorno.

Aspectos clave en esta fase:

- Verificación del hardware y sus componentes.
- Configuración básica del firmware del sistema.
- Comprobación del almacenamiento disponible.
- Identificación de los dispositivos de red.

Esta preparación garantiza que el sistema operativo pueda instalarse y funcionar sin limitaciones técnicas ocultas.



*Infraestructura de servidores preparada para alojar servicios críticos en un entorno de red.*



### Nota

En un entorno profesional, el servidor es un punto crítico del sistema operativo en red, por lo que cualquier problema de hardware no detectado a tiempo puede tener consecuencias amplificadas una vez el sistema está en producción. Detectar una anomalía tras la instalación implica, en muchos casos, detener servicios, interrumpir el trabajo de los usuarios y rehacer configuraciones que ya estaban en uso, con la consiguiente pérdida de tiempo y aumento del riesgo operativo.

Una preparación cuidadosa del servidor permite anticipar fallos antes de que el sistema entre en funcionamiento real. Verificar el estado del hardware, el firmware y los dispositivos de red reduce la probabilidad de incidencias posteriores y facilita una instalación estable desde el inicio. Invertir tiempo en esta fase no retrasa el proyecto, sino que evita paradas innecesarias y correcciones urgentes que suelen resultar mucho más costosas una vez el sistema ya está operativo.

### Selección del tipo de instalación

Durante la instalación, el sistema operativo en red suele ofrecer distintas opciones o perfiles de instalación. Elegir correctamente es fundamental para evitar servicios innecesarios o carencias funcionales.

Conviene definir:

- Instalación mínima o completa.
- Componentes esenciales desde el inicio.
- Servicios que se activarán posteriormente.
- Configuración inicial orientada a servidor.

Esta selección debe alinearse con el **alcance definido en la planificación**.

### Configuración básica del sistema

Una vez iniciada la instalación, el sistema solicita una serie de parámetros básicos que determinan su comportamiento inicial:

- Identificación del sistema.
- Configuración regional y de idioma.
- Ajustes de fecha y hora.
- Configuración básica de red.
- Credenciales iniciales de administración.

Estas decisiones deben tomarse con criterios profesionales, ya que afectan a la coherencia del entorno y a la administración posterior.



#### Recuerda

Las decisiones tomadas durante la configuración básica inicial condicionan el comportamiento del sistema durante toda su vida útil. Aspectos como el nombre del sistema, la configuración regional, la zona horaria o los parámetros de red no son meros ajustes formales, sino elementos que influyen en la coherencia del entorno, en la integración con otros servicios y en la facilidad de administración futura.

Modificar estas decisiones una vez el sistema está en funcionamiento suele implicar interrupciones del servicio, reconfiguraciones adicionales o ajustes en otros componentes dependientes. Por ello, definir correctamente estos parámetros desde el inicio reduce la complejidad técnica posterior, evita inconsistencias y contribuye a un entorno más estable, predecible y fácil de mantener a largo plazo.

### Instalación orientada a entorno en red

La instalación de un sistema operativo en red debe realizarse con una **mentalidad de servicio**, no de uso individual. Esto implica:

- Evitar configuraciones orientadas a un único usuario.
- Priorizar estabilidad frente a personalización.
- Activar mecanismos de administración remota.
- Preparar el sistema para la gestión centralizada.

El objetivo es obtener un sistema **predecible, controlable y mantenible**, incluso antes de añadir usuarios y recursos.

### Verificación inicial tras la instalación

Una vez completada la instalación, es imprescindible realizar una **verificación inicial** para confirmar que el sistema está listo para las fases posteriores.

## EDITORIAL TUTOR FORMACIÓN

Entre las comprobaciones habituales se incluyen:

- Arranque correcto del sistema.
- Acceso administrativo funcional.
- Conectividad básica de red.
- Funcionamiento de los servicios esenciales.
- Registro correcto de eventos del sistema.

La verificación inicial tras la instalación es una fase clave para detectar errores en un momento en el que aún son fáciles de corregir. Continuar con configuraciones avanzadas sin confirmar que el sistema arranca correctamente, que el acceso administrativo es funcional o que los servicios básicos responden de forma adecuada puede ocultar fallos que reaparecerán más adelante, cuando el entorno sea más complejo y difícil de depurar.

Validar el sistema en este punto permite establecer una línea base estable, sobre la que se apoyarán el resto de configuraciones. Cualquier incidencia detectada posteriormente podrá compararse con este estado inicial validado, facilitando su diagnóstico. Omitir esta comprobación suele derivar en problemas encadenados cuya causa real resulta complicada de identificar, incrementando el tiempo de resolución y el impacto sobre el entorno.

### Registro y documentación de la instalación

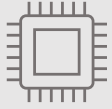
La instalación debe documentarse desde el primer momento, incluyendo:

- Fecha y versión del sistema instalado.
- Opciones de instalación seleccionadas.
- Configuraciones iniciales aplicadas.
- Incidencias detectadas y cómo se resolvieron.

Esta documentación es fundamental para el mantenimiento, las auditorías internas y la continuidad del servicio. Una instalación no documentada es un conocimiento que se pierde con el tiempo o con el cambio de personal.

Se sintetizan, a continuación, las fases de la instalación con sus objetivos:

Fase	Objetivo
<b>Preparación</b>	Garantizar viabilidad
<b>Selección</b>	Ajustar el sistema al entorno
<b>Configuración</b>	Definir parámetros base
<b>Orientación</b>	Enfoque a administración
<b>Verificación</b>	Confirmar funcionamiento
<b>Documentación</b>	Facilitar mantenimiento



### Actividad 4

Se plantea la instalación de un sistema operativo en red en un servidor nuevo, destinado a la administración de usuarios y recursos del entorno.

#### **Tarea:**

Enumerar los pasos previos a la instalación que deben verificarse antes de iniciar el proceso.

Explicar por qué la verificación inicial tras la instalación es esencial antes de continuar con la configuración del entorno.

La instalación del sistema operativo en red no es un fin en sí misma, sino el **punto de partida** de un proceso de administración a largo plazo. Ejecutarla de forma ordenada y documentada sienta las bases de un sistema estable, coherente y fácil de mantener.

## 5. Configuración inicial del sistema tras la instalación.

La **configuración inicial del sistema tras la instalación** es la fase en la que el sistema operativo en red pasa de estar simplemente instalado a encontrarse **preparado para su uso real en un entorno corporativo**. Aunque la instalación haya sido correcta, un sistema sin una configuración inicial adecuada es funcionalmente incompleto y vulnerable a errores operativos, incoherencias de administración y problemas de mantenimiento.

Esta fase tiene un carácter **fundacional**: las decisiones que se adopten aquí condicionarán la forma en que se gestionarán usuarios, equipos y recursos en el futuro. Por ello, la configuración inicial debe abordarse de manera **estructurada, progresiva y documentada**, evitando configuraciones improvisadas o excesivamente personalizadas.

### Objetivos de la configuración inicial

La configuración inicial persigue varios objetivos claros:

- Preparar el sistema para la administración centralizada.
- Garantizar un funcionamiento estable y predecible.
- Establecer una base coherente para la incorporación de usuarios y equipos.
- Reducir la probabilidad de errores en fases posteriores.
- Facilitar el mantenimiento y la evolución del entorno.

Un sistema correctamente configurado desde el inicio requiere menos correcciones y menos intervenciones urgentes a lo largo de su vida útil.

### Configuración de parámetros básicos del sistema

Una de las primeras tareas tras la instalación es revisar y ajustar los **parámetros básicos del sistema**, asegurando que se alinean con el entorno corporativo.

Entre los ajustes habituales se encuentran:

- Nombre definitivo del sistema.
- Configuración regional y de idioma.
- Zona horaria y sincronización de hora.
- Parámetros de red definidos en la planificación.
- Ajustes básicos de rendimiento y almacenamiento.

Estos elementos, aunque parecen triviales, influyen en la coherencia del sistema y en la correcta interpretación de registros y eventos.



### Nota

Desajustes de hora o región pueden provocar problemas de autenticación, errores en registros y confusión en tareas de auditoría.

### Preparación del entorno para la administración

Antes de incorporar usuarios y equipos, el sistema debe quedar **preparado para ser administrado** de forma eficiente. Esto implica:

- Activar herramientas de administración remota.
- Verificar el acceso administrativo seguro.
- Definir cuentas administrativas iniciales.
- Limitar el uso de cuentas con privilegios elevados.

El objetivo es garantizar que la administración del sistema se realice de forma controlada y que las tareas críticas no dependan de una única cuenta o de configuraciones inseguras.



### Recuerda

El control de las cuentas con privilegios elevados es uno de los pilares de una administración segura y eficiente. Cuantas más cuentas con permisos administrativos existan, mayor es la superficie de riesgo y más difícil resulta identificar el origen de errores, cambios indebidos o problemas de seguridad. Reducir y justificar el número de estas cuentas facilita el seguimiento de acciones y refuerza la trazabilidad dentro del sistema.

Un entorno bien preparado prioriza el uso de cuentas diferenciadas, aplicando el principio de mínimo privilegio y reservando los accesos administrativos solo para tareas concretas y justificadas. Este enfoque no solo mejora la seguridad, sino que simplifica la gestión diaria, permite auditar con mayor claridad las intervenciones realizadas y contribuye a mantener un sistema operativo en red estable y bajo control a lo largo del tiempo.

### Definición inicial de la estructura lógica

La configuración inicial debe incluir una **estructura lógica mínima**, que sirva de base para el crecimiento del entorno. Esta estructura no tiene por qué ser definitiva, pero sí coherente.

Conviene definir desde el inicio:

- Organización básica de usuarios y grupos.
- Convenciones de nombres.
- Estructura inicial de recursos compartidos.
- Criterios generales de permisos.

Establecer estas reglas evita cambios disruptivos una vez el sistema entra en producción.

### Configuración de políticas iniciales

Las **políticas del sistema** permiten aplicar configuraciones comunes a usuarios y equipos. Durante la configuración inicial, conviene definir un conjunto mínimo de políticas orientadas a:

- Garantizar un comportamiento homogéneo del entorno.
- Limitar acciones que puedan generar incidencias.
- Facilitar la administración posterior.

Estas políticas deben ser **prudentes y progresivas**, evitando restricciones excesivas que dificulten el trabajo diario.



#### Nota

Es preferible comenzar con pocas políticas bien definidas e ir ampliándolas, que imponer un conjunto rígido difícil de mantener.

### Preparación para la incorporación de usuarios y equipos

Antes de añadir usuarios y equipos reales, el sistema debe quedar listo para integrarlos sin problemas. Esto implica:

- Verificar los procedimientos de alta y baja.
- Comprobar la aplicación correcta de políticas.
- Validar la estructura de grupos.
- Revisar la asignación de permisos por defecto.

Realizar estas comprobaciones evita errores repetitivos cuando el sistema entra en uso generalizado.



#### Ejemplo

Durante la fase previa a la incorporación masiva de usuarios, se crea un usuario de prueba y se integra en los grupos definidos por defecto. Al iniciar sesión, se comprueba qué recursos puede utilizar, qué aplicaciones tiene disponibles y qué permisos se aplican automáticamente. En este contexto, se detecta que el usuario tiene acceso a una carpeta que no corresponde a su perfil, debido a una asignación incorrecta de permisos en un grupo común.

Corregir este error en ese momento es rápido: basta con ajustar la pertenencia al grupo o modificar el permiso mal definido. Sin embargo, si el sistema ya hubiera incorporado a decenas de usuarios reales, el mismo fallo implicaría revisar múltiples cuentas, corregir accesos indebidos y gestionar posibles incidencias de seguridad. Este ejemplo muestra cómo las pruebas previas con usuarios y equipos de prueba reducen drásticamente el esfuerzo de corrección y previenen problemas que, una vez el sistema está en uso generalizado, resultan mucho más costosos de resolver.



### Pruebas funcionales iniciales

Una parte esencial de la configuración inicial es la realización de **pruebas funcionales**, que confirmen que el sistema responde conforme a lo esperado.

Estas pruebas pueden incluir:

- Inicio de sesión de usuarios de prueba.
- Acceso a recursos compartidos.
- Aplicación de políticas.
- Registro de eventos.
- Funcionamiento de herramientas administrativas.

Las pruebas deben documentarse y servir como referencia para futuras comprobaciones.

### Documentación de la configuración inicial

Toda la configuración realizada debe quedar reflejada en una **documentación inicial del sistema**, que incluya:

- Parámetros configurados.
- Estructura lógica definida.
- Políticas aplicadas.
- Resultados de las pruebas realizadas.

Esta documentación constituye el punto de partida para el mantenimiento y la evolución del sistema operativo en red.

La siguiente tabla detalla **qué aspectos críticos conviene asegurar en cada área durante la configuración inicial**, indicando su finalidad práctica y las consecuencias habituales de una preparación incompleta o apresurada del sistema:

## EDITORIAL TUTOR FORMACIÓN

Área	Finalidad práctica dentro del entorno	Aspectos que conviene comprobar en esta fase	Consecuencias de una configuración deficiente
<b>Parámetros básicos</b>	Garantizar coherencia temporal, regional y de red para una correcta interpretación de eventos y servicios	Sincronización horaria, coherencia de idioma y región, consistencia de la configuración de red	Errores de autenticación, registros inconsistentes, dificultades en auditorías y diagnóstico de incidencias
<b>Administración</b>	Establecer un modelo de control seguro y sostenible desde el inicio	Número y uso de cuentas administrativas, acceso remoto seguro, separación de cuentas de uso y de administración	Aumento del riesgo de errores críticos, dificultad para rastrear cambios y mayor superficie de ataque
<b>Estructura lógica</b>	Crear una base organizativa que permita crecer sin reestructuraciones bruscas	Convenciones de nombres, grupos iniciales, organización básica de recursos	Reorganizaciones costosas en fases posteriores, permisos heredados incorrectos y pérdida de coherencia
<b>Políticas</b>	Aplicar un comportamiento homogéneo mínimo sin bloquear la operativa diaria	Alcance real de las políticas, efectos sobre usuarios y equipos de prueba	Restricciones excesivas, incidencias recurrentes o rechazo por parte de los usuarios
<b>Pruebas</b>	Detectar errores estructurales antes de la entrada en producción	Pruebas con usuarios y equipos de prueba, verificación de accesos y aplicación de políticas	Correcciones masivas posteriores, incidencias repetitivas y mayor carga de soporte
<b>Documentación</b>	Fijar un punto de partida claro para el mantenimiento y la evolución del sistema	Registro de decisiones, parámetros aplicados y resultados de pruebas	Dependencia del conocimiento individual, dificultad para auditar y pérdida de trazabilidad

La configuración inicial es el **momento de consolidar el sistema**. Un sistema operativo en red correctamente configurado desde el principio facilita la administración, reduce errores y permite que el entorno crezca de forma ordenada y controlada.

## 6. Resumen de la unidad.



La planificación de un sistema operativo en red constituye una fase crítica que condiciona su estabilidad, seguridad y capacidad de crecimiento. Antes de cualquier instalación es imprescindible analizar el contexto organizativo, el número de usuarios y equipos, los recursos que se compartirán y el nivel de control requerido. Una planificación adecuada evita improvisaciones posteriores, reduce incidencias y permite que el sistema evolucione sin necesidad de rediseños estructurales.

El primer eje de la planificación es el análisis de requisitos. Este análisis incluye aspectos de hardware (capacidad de procesamiento, memoria, almacenamiento y redundancia), software (sistema operativo, servicios necesarios, compatibilidad) y red (direccionamiento, conectividad, segmentación y acceso). A ello se suman criterios de seguridad, como la necesidad de control de accesos, políticas de contraseñas, auditoría o copias de seguridad, que deben definirse desde el inicio y no como añadidos posteriores.

Otro aspecto fundamental es la selección del sistema operativo en red, que debe realizarse en función de su adecuación al entorno previsto. Se valoran factores como la escalabilidad, la facilidad de administración, el soporte a largo plazo, la compatibilidad con equipos clientes y la integración con otros servicios de la infraestructura TIC. La elección no debe basarse únicamente en criterios técnicos aislados, sino en la coherencia del conjunto y en la capacidad del sistema para adaptarse a futuras necesidades.

La planificación también contempla el diseño lógico del sistema, que incluye la estructura de almacenamiento, la organización de usuarios y grupos, la definición inicial de políticas y la previsión de servicios que se desplegarán. Este diseño actúa como guía durante la instalación y sirve de referencia para la documentación técnica posterior, facilitando la administración y el mantenimiento del entorno.

La instalación del sistema operativo en red debe seguir un procedimiento ordenado y controlado. Este proceso comienza con la preparación del hardware y los soportes de instalación, continúa con la configuración básica del sistema (idioma, zona, red, almacenamiento) y finaliza con la activación de los servicios esenciales. Durante esta fase es clave asegurar que la configuración inicial sea estable y coherente, ya que muchos problemas posteriores tienen su origen en decisiones tomadas en el primer despliegue.

Una vez instalado el sistema, se realiza la configuración inicial del entorno, que incluye la verificación del correcto funcionamiento de los servicios, la aplicación de ajustes básicos de seguridad y la comprobación de la conectividad con los equipos clientes. Esta etapa permite detectar errores tempranos y validar que el sistema responde a los requisitos definidos en la planificación.

La planificación e instalación de un sistema operativo en red no deben entenderse como tareas aisladas, sino como un proceso continuo orientado a garantizar la fiabilidad, la seguridad y la sostenibilidad del entorno. Un sistema correctamente planificado e instalado reduce la carga administrativa, mejora la calidad del servicio y sienta las bases para una gestión eficiente y profesional de la infraestructura en red.

## 7. Prueba de autoevaluación.

1. *¿Cuál es el objetivo principal del análisis de requisitos del entorno de red?*
  - A) *Instalar el sistema operativo más utilizado*
  - B) *Definir con precisión qué debe hacer el sistema operativo en red y bajo qué condiciones*
  - C) *Reducir el tiempo de instalación*
  - D) *Configurar directamente los servicios del sistema*
2. *¿Por qué el análisis de requisitos no se considera una fase exclusivamente técnica?*
  - A) *Porque depende del hardware disponible*
  - B) *Porque incluye únicamente decisiones de software*
  - C) *Porque implica necesidades organizativas y formas de trabajo*
  - D) *Porque se realiza después de la instalación*
3. *¿Qué consecuencia habitual tiene un análisis de requisitos incompleto?*
  - A) *Mayor simplicidad del sistema*
  - B) *Sistemas sobredimensionados o incapaces de adaptarse*
  - C) *Reducción del mantenimiento*
  - D) *Eliminación de la planificación*
4. *¿Qué aspecto debe analizarse en primer lugar al diseñar un sistema operativo en red?*
  - A) *El tipo de organización*
  - B) *El sistema de archivos*
  - C) *El software de virtualización*
  - D) *El modelo de licenciamiento*
5. *¿Qué factor distingue principalmente los distintos tipos de usuario en el análisis de requisitos?*
  - A) *El sistema operativo que utilizan*
  - B) *El impacto que tienen sobre el sistema*
  - C) *El número de equipos asignados*
  - D) *La antigüedad en la organización*
6. *¿Qué perfil de usuario tiene mayor impacto en el sistema operativo en red?*
  - A) *Usuario básico*
  - B) *Usuario avanzado*
  - C) *Usuario administrativo*
  - D) *Usuario técnico*

7. *¿Por qué el diseño del sistema debe partir del usuario más exigente?*

- A) Porque es el más numeroso*
- B) Porque simplifica la experiencia del resto*
- C) Porque pone a prueba los límites del sistema*
- D) Porque reduce los costes de licencias*

8. *¿Qué elemento NO forma parte del análisis de los equipos del entorno?*

- A) Número total de equipos*
- B) Tipología de los equipos*
- C) Vida útil prevista*
- D) Marca comercial del hardware*

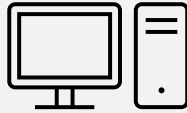
9. *¿Qué recurso requiere permisos más estrictos y mayor control?*

- A) Un recurso crítico para la actividad*
- B) Un recurso de uso general*
- C) Un recurso temporal*
- D) Un recurso local*

10. *¿Qué influye directamente en la estructura de carpetas y la organización de grupos?*

- A) El grado de compartición y colaboración*
- B) El presupuesto disponible*
- C) La versión del sistema operativo*
- D) El tipo de hardware del servidor*

## Unidad 3



# Estructura lógica y gestión del sistema



## EDITORIAL TUTOR FORMACIÓN

La organización interna del sistema operativo en red determina en gran medida su eficiencia y facilidad de administración. Una estructura lógica bien definida permite controlar el acceso a los recursos, optimizar el almacenamiento y mantener el orden en entornos con múltiples usuarios y equipos conectados simultáneamente.

Esta unidad aborda la gestión del sistema desde una perspectiva estructural, analizando la organización de los sistemas de archivos, los volúmenes y los mecanismos de control del uso del almacenamiento. Se presta especial atención a la asignación de permisos y a la auditoría básica, como elementos clave para una administración ordenada y coherente del entorno en red.

# 1. Organización del sistema de archivos en entornos de red.

La **organización del sistema de archivos en entornos de red** es uno de los pilares sobre los que se sostiene la administración eficaz de un sistema operativo en red. No se trata únicamente de decidir dónde se almacenan los datos, sino de **definir una estructura lógica, coherente y sostenible** que permita el acceso controlado a la información, facilite el trabajo colaborativo y reduzca los riesgos asociados a pérdidas, duplicidades o accesos indebidos.

En un entorno corporativo, el sistema de archivos deja de ser un espacio personal para convertirse en un **recurso compartido y estratégico**. Por ello, su organización debe responder a criterios técnicos y organizativos, no a preferencias individuales. Una estructura mal diseñada genera problemas persistentes: confusión entre usuarios, dificultad para asignar permisos, aumento de incidencias y dependencia de soluciones improvisadas.

## Función del sistema de archivos en un entorno en red

En un sistema operativo en red, el sistema de archivos cumple funciones que van más allá del simple almacenamiento:

- Centralizar la información corporativa.
- Facilitar el acceso compartido a documentos.
- Aplicar permisos y controles de acceso.
- Permitir la trazabilidad de cambios.
- Servir de base para copias de seguridad y restauración.

A diferencia del entorno monopuesto, donde los archivos suelen pertenecer a una sola persona, en el entorno en red **los datos tienen múltiples propietarios lógicos** (departamentos, proyectos, equipos), lo que exige una organización clara y consensuada.



### Recuerda

En un entorno de red, los archivos dejan de entenderse como propiedad individual para pasar a formar parte de un ámbito de trabajo compartido, vinculado a departamentos, proyectos o funciones concretas. Esta perspectiva es esencial para evitar estructuras basadas en personas concretas, que generan dependencias innecesarias y dificultan la continuidad cuando se producen cambios de personal o de organización.

Organizar los datos por ámbitos de trabajo permite asignar permisos de forma coherente, facilitar el acceso colaborativo y mantener el control sobre la información a lo largo del tiempo. Cuando los archivos se asocian a funciones y no a individuos, el sistema de archivos se convierte en un recurso estable y sostenible, alineado con la lógica de la organización y con los principios de una administración eficaz en entornos de red.