Índice

68 capítulos para comprender, practicar y consultar. Sigue el orden si empiezas desde cero o busca el tema que necesitas reforzar. Las fuentes, recursos y límites de las prácticas se explican en el capítulo 68.

Bloque 0. Aquí puedes empezar 5

01. No necesitas saberlo todo para empezar . . . 5

02. Descubre dónde están tus lagunas . . . 7

03. Tu laboratorio sin complicarte la vida . . . 9

04. Estudiar informática para poder explicarla . . . 11

Bloque 1. Las piezas que faltaban 13

05. Qué hace un ordenador cuando parece que «piensa» . . . 13

06. Bits, bytes y números que dejan de dar miedo . . . 16

07. Archivos, carpetas y discos: cada cosa en su sitio . . . 19

08. Cómo se hablan dos ordenadores . . . 22

Bloque 2. Montaje y mantenimiento de equipos 25

09. Reconocer los componentes y entender qué aportan . . . 25

10. Elegir componentes compatibles y justificar el presupuesto . . . 30

11. Montar sin improvisar . . . 33

12. Entender el arranque y el firmware . . . 35

13. Periféricos y mantenimiento preventivo . . . 37

14. Diagnosticar averías sin cambiar piezas al azar . . . 40

Bloque 3. Sistemas operativos monopuesto 43

15. Qué administra realmente un sistema operativo . . . 43

16. Instalar con un plan y saber qué has instalado 47

17. Usuarios, grupos y permisos: quién puede hacer qué 50

18. Terminal desde cero: entiende cada línea 53

19. Mantener el sistema con evidencias 56

20. Virtualización y recuperación: volver atrás con criterio 59

Bloque 4. Redes locales que puedes entender **63**

21. Las piezas de la red y el mapa que las une 63

22. OSI y TCP/IP: modelos para localizar problemas 65

23. IPv4: dirección, máscara y puerta de enlace 67

24. Subredes paso a paso, con cuentas que puedes comprobar 69

25. IPv6, vecinos y rutas: no todo se resuelve con una máscara 72

26. Ethernet y wifi: el medio también importa 75

27. Diagnosticar conectividad: una prueba, una pregunta 80

Bloque 5. Sistemas operativos en red **82**

28. Del grupo de trabajo al dominio 82

29. Organizar usuarios, grupos y políticas 85

30. Carpetas e impresoras compartidas: permisos efectivos 88

31. Administrar servidores y conectar sistemas distintos 91

Bloque 6. Servicios en red **96**

32. DHCP y DNS: configuración y nombres sin confundirlos 96

33. Servidor web: del nombre a una respuesta verificable 102

34. Transferir archivos y administrar a distancia 106

35. Correo, proxy, NAT y encaminamiento 111

36. Un servicio no está terminado hasta probarlo desde el cliente 117

Bloque 7. Seguridad y recuperación 119

37. Entender el riesgo antes de comprar herramientas . . . 119
38. Proteger equipos y cuentas con capas coherentes . . . 122
39. Cortafuegos, segmentación, wifi y VPN . . . 126
40. Copias que puedas restaurar . . . 130
41. Incidentes: actuar con orden y conservar evidencia . . . 133
42. Privacidad y responsabilidad profesional . . . 135

Bloque 8. Ofimática para trabajar y entregar bien 139

43. Documentos profesionales sin pelearte con el formato . . . 139
44. Hojas de cálculo: fórmulas que puedes explicar . . . 144
45. Bases de datos: relacionar sin repetirlo todo . . . 148
46. Presentaciones, imagen y vídeo que ayudan a explicar . . . 152
47. Correo, calendario y colaboración sin perder el control . . . 156

Bloque 9. Aplicaciones web 160

48. Qué ocurre detrás de una página . . . 160
49. HTML y CSS para comprender y modificar . . . 163
50. Instalar y administrar un CMS . . . 166
51. Plataformas colaborativas y de aprendizaje . . . 170
52. Publicar, migrar y mantener colaboración web . . . 173

Bloque 10. Resolver problemas y trabajar con otras personas 180

53. Diagnosticar sin ir dando palos de ciego . . . 180
54. Atender a una persona también es trabajo técnico . . . 184
55. Tickets, inventarios y documentación que sirven mañana . . . 187

Bloque 11. Inglés, empleabilidad y un trabajo sostenible 190

56. Inglés profesional para desenvolverte en informática . . . 190

57. Empleabilidad: aprender un oficio y construir tu camino . . . 196

58. Digitalización y sostenibilidad con resultados comprobables . . . 205

Bloque 12. Herramientas para seguir creciendo 212

59. Automatizar una tarea pequeña con Bash y PowerShell . . . 212

60. Git: guardar decisiones y entender los cambios . . . 216

61. Nube y contenedores sin confundir sus responsabilidades . . . 219

62. Monitorización y registros: ver problemas antes de adivinarlos . . . 222

63. IA para aprender y trabajar con criterio . . . 225

Bloque 13. Un proyecto que puedas explicar y entregar 228

64. Proyecto integrador: poner en marcha Aula Norte . . . 228

65. Prepararte para la formación en empresa . . . 234

Anexo de consulta. Las palabras que vas a encontrarte 237

66. Glosario para volver a lo importante . . . 237

Anexo de taller. Consulta, calcula y comprueba 252

67. Puertos, comandos y casos resueltos . . . 252

Anexo de recorrido. Sigue aprendiendo con criterio 258

68. Recursos, fuentes y mapa del temario . . . 258

Sobre el autor 261

Bloque 0. Aquí puedes empezar

01. No necesitas saberlo todo para empezar

Al terminar: sabrás cómo recorrer este manual y cómo distinguir una tarea aprendida de una tarea que solo has conseguido imitar.

Quizá sabes instalar programas, pero te pierdes cuando aparece la palabra partición. O puedes calcular una subred en un examen, aunque no sabrías qué comprobar cuando un equipo deja de navegar. Son situaciones distintas, y ambas tienen arreglo: encontrar el paso que falta y practicarlo con sentido.

SMR reúne conocimientos de hardware, sistemas, redes, aplicaciones y seguridad. No son compartimentos independientes. Un ordenador puede funcionar correctamente y no acceder a una carpeta porque su usuario carece de permisos. Una web puede estar encendida y resultar inaccesible porque su nombre no se resuelve. Antes de corregir algo conviene identificar dónde está el problema.

El mapa del libro

Primero conocerás el equipo y los datos. Después instalarás sistemas y conectarás máquinas. Más adelante administrarás usuarios, servicios y aplicaciones. La seguridad y la documentación acompañan todo el proceso. Al final reunirás esas capacidades en el caso de una pequeña empresa ficticia: **Aula Norte**, una academia con administración, profesorado y un aula de informática.

En cada práctica distinguiremos tres preguntas: ¿qué quiero conseguir?, ¿qué cambio voy a realizar? y ¿qué prueba demostrará que funciona? Por ejemplo, crear una carpeta no demuestra que un usuario pueda usarla. La prueba consiste en iniciar sesión con ese usuario y comprobar la operación concreta que necesita realizar.

Cómo leer sin agobiarte

Si empiezas desde cero, sigue el orden. Si buscas resolver una duda, utiliza el índice y vuelve al apartado de conocimientos previos cuando aparezca algo desconocido. No necesitas memorizar todas las opciones de un comando: sí necesitas saber qué hace, dónde se ejecuta y cómo consultar su ayuda.



Consejo de David

Configurar es elegir los valores con los que funcionará un sistema. Administrar es mantenerlo útil a lo largo del tiempo. Diagnosticar es reunir pruebas para explicar un fallo. Reparar es aplicar una solución y comprobarla.

Ejemplo: «ya sé crear usuarios»

Has seguido una captura y has creado una cuenta. Ahora intenta explicar por qué no debería ser administradora, qué carpetas puede modificar y cómo comprobarías que su contraseña funciona sin revelar esa contraseña. Si no puedes responder todavía, has aprendido una parte del procedimiento; las preguntas señalan lo que debes reforzar.

Vamos a probarlo

Necesitas un cuaderno o un documento de texto. Escribe una tarea informática que ya sepas realizar. Divídela en objetivo, requisitos, pasos, comprobación y forma de volver atrás. Pide a otra persona que siga tus instrucciones, o repítelas tú al día siguiente sin improvisar los pasos que falten.

Resultado esperado: otra persona entiende lo que necesita y reconoce cuándo ha terminado. Si depende de frases como «haz lo de siempre», concreta esas instrucciones.

¿Lo has pillado?

1. ¿Por qué una captura de la configuración no demuestra por sí sola que el servicio funciona?

2. ¿Qué haces si una explicación utiliza tres términos que desconoces?

3. ¿Es un error consultar el manual mientras trabajas?

Soluciones razonadas. 1) Puede mostrar valores correctos y existir otro fallo; hace falta probar el comportamiento desde el punto de uso. 2) Identificarlos y repasar la base correspondiente antes de añadir más pasos. 3) No: consultar documentación forma parte del trabajo. Lo importante es comprender y verificar lo aplicado.

02. Descubre dónde están tus lagunas

Al terminar: tendrás un mapa personal de repaso. Necesitas diez o quince minutos y responder sin buscar las soluciones.

Esta prueba no sirve para decidir si vales para la informática. Sirve para elegir por dónde empezar. Marca cada respuesta con «lo puedo explicar», «me suena» o «no lo sé». Si aciertas por casualidad, mantén la segunda marca.

Prueba de orientación

1. Un equipo tiene 16 GB de RAM y un SSD de 512 GB. ¿En cuál se conservan normalmente los documentos al apagarlo?
2. ¿Qué diferencia hay entre una carpeta y una partición?
3. Una conexión anuncia 100 Mb/s. ¿Su máximo teórico equivale a 100 MB/s?
4. ¿Qué función principal cumple el sistema operativo?
5. ¿Cambiar la extensión de una imagen de .jpg a .pdf la convierte en PDF?
6. ¿Puedes tener conexión wifi y no tener acceso a Internet?
7. ¿Para qué sirve DNS?
8. ¿Todos los usuarios deben ser administradores para trabajar cómodamente?
9. ¿Qué protege una copia que está en el mismo disco que el original si ese disco se rompe?
10. ¿Cuál es mejor descripción de un fallo: «esto va mal» o «desde esta mañana no puedo abrir la carpeta del servidor; otros dos usuarios sí»?
11. Si un programa muestra «acceso denegado», ¿significa necesariamente que está mal instalado?
12. ¿Qué deberías comprobar después de reparar una impresora?

Respuestas y rutas de repaso

1. En el SSD. La RAM habitual pierde su contenido al quedarse sin alimentación. Repasa componentes y almacenamiento.
2. Una carpeta organiza entradas del sistema de archivos; una partición delimita una región lógica de una unidad. Repasa archivos y almacenamiento.
3. No. Ocho bits forman un byte: 100 Mb/s son 12,5 MB/s antes de descontar sobrecargas. Repasa unidades.
4. Gestionar recursos y proporcionar servicios a los programas. Repasa sistemas operativos.
5. No. Cambia el nombre, no la estructura interna del archivo. Repasa formatos.
6. Sí. El enlace inalámbrico puede funcionar y fallar la salida a Internet u otro servicio necesario. Repasa redes.

7. Resolver nombres y consultar otros datos del sistema de nombres de dominio. Repasa servicios en red.
8. No. Conviene trabajar con los permisos que requiere la tarea. Repasa cuentas y seguridad.
9. No protege frente a esa avería física. Repasa copias y recuperación.
10. La segunda: delimita el síntoma y aporta comparaciones útiles. Repasa soporte.
11. No. Puede faltar un permiso o existir una política que impida la operación. Repasa usuarios.
12. Una impresión real desde el equipo y la cuenta afectados, además del estado del dispositivo. Repasa periféricos y diagnóstico.

Convierte el resultado en un plan

Elige tres respuestas dudosas. En tu cuaderno anota qué no comprendes y una prueba pequeña que podrías hacer. Para la pregunta 5, puedes duplicar una imagen de prueba, cambiar la extensión de la copia y observar que no has creado un PDF válido. Conserva el original para restaurar el nombre si hace falta.



Ojo con este error

Reconocer una palabra no equivale a entenderla. Una buena prueba consiste en inventar un ejemplo y explicar qué sucedería al cambiar una condición.

Autocomprobación: si te equivocas en ocho preguntas, ¿debes abandonar? No. Debes empezar por fundamentos y repetir la prueba después. Comparar tus propias explicaciones antes y después es más útil que competir por la puntuación.

03. Tu laboratorio sin complicarte la vida

Al terminar: podrás separar el entorno de aprendizaje de tus archivos importantes y preparar un inventario inicial.

Una práctica necesita espacio para equivocarse. Eso no significa asumir pérdidas innecesarias. Utilizaremos datos ficticios y, cuando sea posible, máquinas virtuales. Una máquina virtual es un ordenador simulado por software que utiliza parte de los recursos del ordenador físico, llamado anfitrión. El sistema que corre dentro es el invitado.

Tres formas de practicar

Equipo disponible. Puedes empezar observando componentes, creando documentos y consultando configuraciones sin cambiarlas. No exige virtualización.

Una máquina virtual. Permite instalar un sistema invitado y probar sus usuarios y aplicaciones. El anfitrión debe conservar memoria y almacenamiento suficientes para seguir funcionando.

Varias máquinas virtuales. Permiten representar clientes y servidores. Si tu equipo va justo, ejecútalas por turnos o utiliza instalaciones sin escritorio cuando la práctica lo permita. Más máquinas encendidas no significan más aprendizaje.

No hay una cantidad universal de RAM suficiente: depende del anfitrión, del invitado y de los servicios. Consulta sus requisitos antes de asignar recursos. Un disco virtual dinámico puede crecer hasta su límite configurado y llenar el almacenamiento físico.

Antes de instalar

1. Copia los documentos importantes a un soporte independiente y comprueba que puedes abrir algunos desde la copia.
2. Anota procesador, RAM instalada, espacio libre, sistema anfitrión y arquitectura.
3. Descarga instaladores desde sus fuentes oficiales. Comprueba la integridad cuando se publique una suma de comprobación.
4. Revisa que el sistema invitado admite la arquitectura del equipo. Una imagen para x86-64 no se convierte en ARM por meterla en una máquina virtual.
5. Crea una carpeta de prácticas con subcarpetas para evidencias, configuraciones y entregas.

La red del laboratorio importa

Con **NAT**, una máquina suele salir a otras redes a través del anfitrión; los detalles dependen del hipervisor. Con **puente**, puede aparecer como otro equipo de la red física. Una **red interna** permite comunicar invitados dentro del entorno virtual sin conectarlos directamente a la red doméstica. Una red de **solo anfitrión** suele conectar invitados y anfitrión, según configuración.

Para probar un servidor DHCP utilizaremos una red de laboratorio aislada. Si lo activas en la red de casa o del centro, podrías entregar configuraciones a equipos ajenos. La separación es parte de la práctica, no un trámite.

Instantánea y copia

Una instantánea permite volver a un estado del invitado según el funcionamiento del hipervisor. Puede depender de archivos que están en el mismo almacenamiento y no sustituye una copia independiente. Si el disco físico falla, podrías perder la máquina y sus instantáneas juntas.

Vamos a probarlo

Crea un inventario con estas columnas: identificador, uso, procesador, memoria, almacenamiento libre, sistema y observaciones. Registra únicamente tu equipo; omite números de serie o datos personales si vas a compartirlo. Añade una ficha de laboratorio con objetivo, estado inicial, cambios, resultado y recuperación.

Resultado esperado: puedes decidir si empezarás con observación, una máquina o varias. No necesitas instalar nada todavía para completar este primer inventario.

Si no funciona: si no encuentras un dato, indica «pendiente de consultar» y el método que utilizarás. No rellenes cifras de memoria. Si no puedes ejecutar virtualización, continúa con los ejercicios de papel y las prácticas que no modifican el sistema.

¿Lo has pillado?

1. ¿Por qué no debes entregar toda la RAM del anfitrión a un invitado?

2. ¿Qué red elegirías para experimentar con DHCP sin afectar al resto de equipos?

3. ¿Una instantánea protege necesariamente contra el fallo del disco físico?

Soluciones. 1) El anfitrión y el hipervisor también necesitan recursos; si faltan, el conjunto puede bloquearse o volverse muy lento. 2) Una red interna aislada y comprobada antes de iniciar el servicio. 3) No: puede compartir el mismo punto de fallo que el sistema original.

04. Estudiar informática para poder explicarla

Al terminar: convertirás una sesión de estudio en una evidencia de aprendizaje reutilizable.

Copiar un procedimiento puede ayudarte a empezar. Para aprender, añade una predicción antes de ejecutarlo: «espero que aparezca una carpeta aquí» o «esta consulta debería devolver la dirección del servidor». Después compara tu predicción con lo observado.

Una sesión de cuatro pasos

Entiende. Lee una sección pequeña y escribe su idea principal con tus palabras. Si aparece «permiso de escritura», concreta qué operación permitiría.

Haz. Ejecuta una práctica y registra el estado inicial. Cambia una cosa por vez para poder atribuir el resultado a una causa.

Explica. Cierra el libro y describe lo que ha pasado. Incluye por qué elegiste esos valores.

Repite con una variación. Cambia el usuario, el nombre del archivo o la dirección del ejemplo. Si solo funcionaba al copiar exactamente, has encontrado una dependencia que debes comprender.

Apuntes que sirven

Un apunte útil contiene el problema, el entorno, el procedimiento y la prueba final. Una lista de comandos sin contexto es difícil de reutilizar: no indica con qué permisos se ejecutaron ni si cambian datos. Incluye también lo que descartaste y la razón.

Guarda los errores completos en texto cuando puedas. Una captura recortada puede perder la instrucción que originó el fallo. Oculta contraseñas, tokens, información de clientes y cualquier dato personal antes de compartir evidencias.

Cómo pedir ayuda

«No me funciona Linux» obliga a adivinar. Una consulta útil sería: «En el invitado Linux del laboratorio, con esta versión y este comando, obtengo este mensaje. Esperaba crear una carpeta dentro de mi directorio personal. Puedo crearla desde el gestor de archivos. Ya comprobé la ruta».

No añadas veinte cambios al azar antes de preguntar: dificultan reconstruir el estado. Cuando recibas una solución, pregunta qué prueba la confirma y cómo deshacerla si no es adecuada.

Práctica de recuperación activa

Elige una de las doce preguntas del capítulo anterior. Respóndela sin mirar; consulta después la solución y marca qué parte faltaba. Repite al día siguiente con un ejemplo distinto. El objetivo no es recitar la frase: es aplicar la idea.



Truco de taller

Lleva una lista de «suposiciones que debo comprobar». Por ejemplo: «el servidor está encendido», «este cable funciona» o «estoy en la carpeta correcta». Una hipótesis escrita deja de confundirse con un hecho.

¿Lo has pillado?

1. ¿Por qué cambiar cinco ajustes a la vez dificulta aprender de un resultado?

2. ¿Qué falta en el apunte «reiniciar arregla la red»?

Soluciones. 1) Aunque mejore, no sabrás qué cambio ayudó ni cuál introdujo otro problema. 2) Síntoma, entorno, causa investigada, qué componente se reinició y comprobación. Reiniciar puede ocultar temporalmente un fallo sin explicar su origen.

Caso resuelto: una consulta de ayuda que permite avanzar

Situación. Marta está preparando un informe para una práctica. Ha seguido las instrucciones para guardar un archivo, pero después no lo encuentra. Su primer mensaje es «el ordenador me ha borrado todo».

Separar observación y conclusión. Marta sabe que el archivo no aparece en la carpeta que está mirando. Todavía no sabe que se haya borrado. Puede haberse guardado con otro nombre, en otra ubicación, con otra cuenta o en un almacenamiento sincronizado. La primera mejora de su mensaje es: «No encuentro el informe en la carpeta de entregas».

Añadir contexto. Utiliza un procesador de textos, recuerda el nombre aproximado y sabe a qué hora trabajó. Anota el sistema, la aplicación y si ha cerrado la sesión. No publica documentos personales ni contraseñas para explicar el caso.

Elegir pruebas. Primero revisa los documentos recientes de la aplicación, después consulta la ubicación del archivo si puede abrirlo y, si hace falta, busca por nombre y fecha en las ubicaciones adecuadas. Estas acciones reúnen información sin sobrescribir archivos. Crear inmediatamente otro documento con el mismo nombre podría complicar la comparación.

Resultado del ejemplo. El informe estaba en la carpeta Documentos. Marta lo abre, comprueba que contiene la versión esperada y guarda una copia en entregas. Después abre esa copia desde su ubicación final. La evidencia es el documento correcto en el destino previsto, no solo un aviso de guardado.

Apunte reutilizable. «Al guardar, comprobar la ruta completa y volver a abrir el archivo desde la carpeta de entrega». La próxima vez, Marta puede aplicar esa comprobación aunque cambien la aplicación o el nombre del informe.

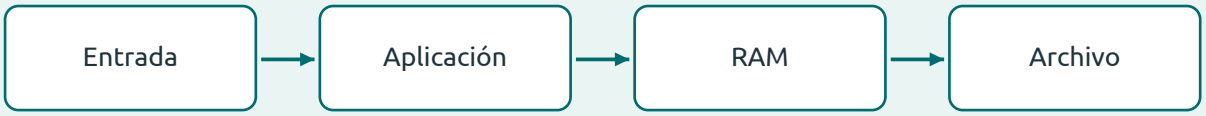
Tu turno. Reescribe «no me deja entrar» como una consulta útil sin inventar datos. Debes indicar a qué intentas acceder, desde dónde, qué mensaje aparece y qué esperabas. Si desconoces un dato, dilo. Una respuesta válida sería: «Desde mi cuenta del equipo de prácticas intento abrir la carpeta compartida del ejercicio y aparece “acceso denegado”. Puedo abrir mis carpetas locales. No he comprobado aún si otros usuarios acceden». Esa descripción delimita el caso y permite decidir la siguiente prueba.

Bloque 1. Las piezas que faltaban

05. Qué hace un ordenador cuando parece que «piensa»

Al terminar: podrás relacionar entrada, procesamiento, memoria, almacenamiento y salida con una tarea cotidiana. **Antes:** basta con saber abrir un programa.

DEL TECLADO AL ARCHIVO



La pantalla muestra el trabajo. Guardar permite recuperarlo.

Esquema simplificado: el sistema operativo coordina estas operaciones.

El recorrido de un dato al trabajar con un documento.

Cuando escribes una frase, el teclado envía eventos, el sistema los hace llegar a la aplicación y esta modifica una representación del documento en memoria. La pantalla muestra el resultado. Al guardar, se escribe información en un almacenamiento persistente. Ninguna de esas acciones requiere que el equipo comprenda el significado de la frase como una persona.

Cinco funciones para ordenar las piezas

La **entrada** recoge datos: teclado, ratón, micrófono, sensor o red. El **procesamiento** transforma datos siguiendo instrucciones. La **memoria principal** mantiene información que el procesador necesita utilizar. El **almacenamiento** conserva datos para usos posteriores. La **salida** entrega resultados: pantalla, impresora, altavoz o red.

Un componente puede participar en más de una función. La tarjeta de red recibe y envía; una pantalla táctil muestra información y recoge pulsaciones. Clasificar ayuda a entender, pero no convierte cada dispositivo en una caja con una única función.

Hardware, software y firmware

Hardware son los componentes físicos. **Software** son programas y otros elementos lógicos que permiten trabajar con información. El **firmware** es software asociado al control de un dispositivo, normalmente guardado en memoria no volátil. Una actualización de firmware modifica instrucciones, no añade físicamente otro chip.

El **sistema operativo** administra recursos, controla dispositivos mediante controladores y ofrece servicios a las aplicaciones. Un procesador de textos utiliza esos servicios para abrir

archivos o imprimir. Un **controlador** o driver facilita que el sistema trabaje con un dispositivo concreto.

No todo software cuesta dinero y no todo software gratuito permite modificar su código. El precio y la licencia son cuestiones diferentes. Antes de instalar o distribuir un programa conviene comprobar sus condiciones de uso.

Del botón de encendido al escritorio

La secuencia exacta varía, pero un esquema habitual es: alimentación, ejecución del firmware, comprobaciones iniciales, elección de una opción de arranque, ejecución de un cargador y puesta en marcha del sistema operativo. Después arrancan servicios y aparece un mecanismo de inicio de sesión.

Si no aparece ni el logotipo inicial, el problema pertenece a una etapa distinta de una contraseña rechazada. Esa distinción orienta las pruebas. No tiene sentido reinstalar un navegador para corregir que el equipo no recibe alimentación.

Ejemplo desarrollado: un documento perdido

Escribes media página y se va la luz antes de guardar. La RAM habitual es volátil: su contenido no se conserva al desaparecer la alimentación. La aplicación podría haber escrito una recuperación automática en disco, pero depende de su configuración y del momento del fallo. «Lo veía en pantalla» no demuestra que ya estuviera guardado.

Cuando pulsas Guardar, normalmente intervienen búferes y cachés. En una unidad extraíble, la expulsión segura ayuda a completar escrituras pendientes antes de desconectarla. El mensaje de guardado y la persistencia física no deben confundirse con una garantía frente a cualquier fallo.

Vamos a probarlo: sigue un dato

Necesitas un editor de texto y una carpeta de prácticas. Escribe una frase ficticia, guárdala como `prueba.txt`, cierra el editor y vuelve a abrir el archivo. Dibuja el recorrido teclado aplicación y memoria archivo aplicación pantalla. No simules un corte de corriente.

Resultado esperado: la frase reaparece porque se recupera del archivo. Explica qué etapa faltaría si cerraras sin guardar y no hubiera recuperación automática. Para volver al estado inicial, elimina solo el archivo de práctica después de comprobar su ubicación.

SOS: el programa se queda bloqueado

Observa si responde otra aplicación y si el sistema permite cambiar de ventana. Un bloqueo de un programa no demuestra que todo el equipo esté averiado. Registra la hora y la acción realizada antes de forzar el cierre: podrías perder cambios sin guardar. Más adelante aprenderás a consultar procesos y registros.

¿Lo has pillado?

1. ¿Un SSD es RAM porque ambos guardan datos?

2. ¿El firmware es hardware?

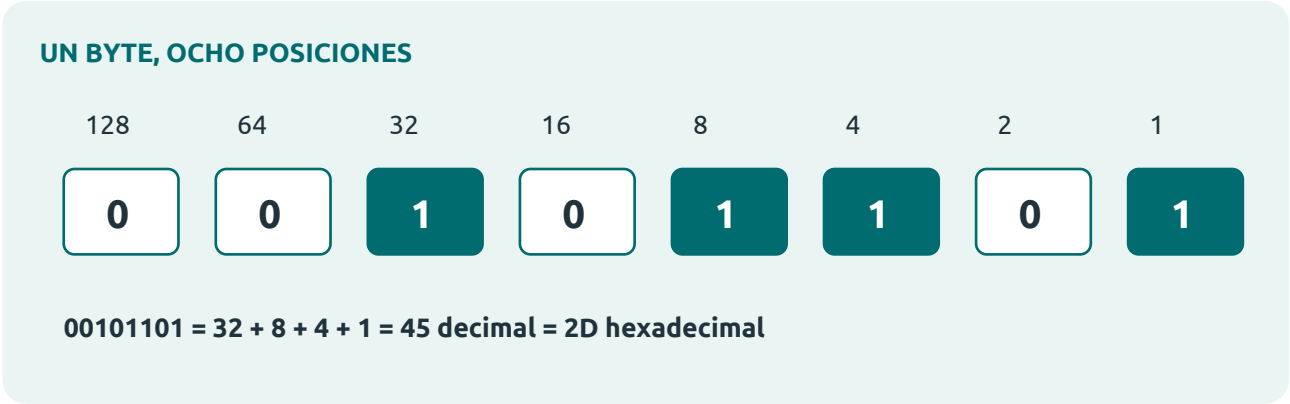
3. ¿Por qué conviene separar «no enciende» de «no inicia sesión»?

Soluciones. 1) No: cumplen funciones diferentes y presentan características de persistencia y acceso distintas. 2) Es software, aunque esté almacenado en un componente físico del dispositivo. 3) Corresponden a fases diferentes; requieren hipótesis y pruebas diferentes.

Glosario del capítulo: entrada, salida, memoria volátil, almacenamiento persistente, firmware, controlador y arranque.

06. Bits, bytes y números que dejan de dar miedo

Al terminar: convertirás unidades y representarás números pequeños en binario y hexadecimal.
Antes: multiplicar, dividir y reconocer potencias sencillas.



Cada posición binaria representa una potencia de dos.

Un **bit** representa dos posibilidades, que escribimos como 0 y 1. Un **byte** contiene ocho bits. Con ocho posiciones binarias se obtienen 256 combinaciones diferentes. Si se interpretan como enteros sin signo, representan valores de 0 a 255. Interpretarlos como una letra, un color o parte de una instrucción requiere una regla de codificación.

Leer binario de izquierda a derecha

En decimal, las posiciones valen unidades, decenas, centenas. En binario valen potencias de dos. Para un byte, de izquierda a derecha: 128, 64, 32, 16, 8, 4, 2 y 1. Cada 1 indica que sumamos el valor de su columna.

Por ejemplo, `00101101` representa 32 + 8 + 4 + 1 = 45. Los ceros iniciales no cambian el valor, pero permiten mostrar la anchura del dato.

Para convertir 45 a binario, busca la mayor potencia que cabe: 32. Quedan 13; cabe 8 y quedan 5; cabe 4 y queda 1. Activa esas posiciones. El resultado es `00101101`. Compruébalo sumando de nuevo: convertir en ambas direcciones detecta muchos despistes.

Hexadecimal: escribir lo mismo con menos cifras

El sistema hexadecimal utiliza dieciséis símbolos: 0-9 y A-F. A vale diez; F vale quince. Cada cifra hexadecimal equivale a cuatro bits. Divide `00101101` en `0010` y `1101`: obtienes 2 y D. Por tanto, 45 decimal = 2D hexadecimal. El prefijo `0x` es una convención frecuente para indicar hexadecimal: `0x2D`.

Esto aparece en direcciones MAC, colores y mensajes de diagnóstico. No necesitas efectuar todas las conversiones de memoria, pero sí saber qué representación estás leyendo.

Unidades decimales y binarias

En las unidades decimales, kB son 1.000 bytes, MB son 1.000.000 y GB son 1.000.000.000. En las binarias, KiB son 1.024 bytes, MiB son 1.048.576 y GiB son 1.073.741.824. Algunas interfaces usan etiquetas ambiguas; mira la definición, no solo las letras.

Un disco de 500.000.000.000 bytes equivale aproximadamente a 465,66 GiB. Esa diferencia de representación no significa que hayan desaparecido 34 GB. El espacio realmente utilizable puede reducirse además por particiones de recuperación, metadatos y otros usos.

Capacidad, tasa y frecuencia

Una capacidad indica cuánto cabe: 16 GB de RAM. Una tasa indica cuánto se transfiere por tiempo: 100 Mb/s. Una frecuencia indica ciclos por segundo: 3 GHz. Una cifra de GHz aislada no permite comparar el rendimiento global de dos procesadores distintos.

Presta atención a la mayúscula: `b` se utiliza para bit y `B` para byte. Una conexión de 100 Mb/s equivale a un máximo teórico de 12,5 MB/s. Si un archivo mide 250 MB, el tiempo ideal a esa tasa sería 250 / 12,5 = 20 segundos. El tiempo real será mayor si hay sobrecarga, congestión o límites en el servidor o el disco.



Truco de taller

Antes de dividir, escribe las unidades junto a las cifras. Si mezclas MB con Mb/s, convierte primero. «Me sale 2,5» no significa nada sin saber si son segundos, megabytes o una tasa.

Caracteres y codificación

Un texto necesita una correspondencia entre símbolos y valores. Unicode define caracteres y otros elementos; UTF-8 es una forma de codificarlos en bytes. Una letra no ocupa siempre un byte: depende del carácter y de la codificación. Por eso un texto con veinte caracteres puede ocupar más de veinte bytes, incluso antes de contar metadatos.

Si aparecen símbolos extraños al abrir un archivo, puede estar interpretándose con una codificación diferente. Cambiar la fuente tipográfica no siempre resuelve ese problema: una cosa es interpretar el dato y otra dibujar el carácter.

Vamos a probarlo

Resuelve en papel y comprueba después con una calculadora que admita bases:

1. Convierte 13 y 200 a binario de ocho bits.
2. Convierte `11110000` a decimal y hexadecimal.
3. Calcula el tiempo ideal para transferir 600 MB a 80 Mb/s.
4. Expresa 8 GiB en bytes.
5. ¿Cuántas combinaciones hay en cuatro bits?

Soluciones razonadas. 13 = 8 + 4 + 1, por tanto `00001101`. 200 = 128 + 64 + 8, por tanto `11001000`. `11110000` = 128 + 64 + 32 + 16 = 240 = F0. Para la transferencia: 80 / 8 = 10 MB/s; 600 / 10 = 60 s ideales. 8 GiB = 8 × 1.073.741.824 = 8.589.934.592 bytes. Cuatro bits permiten 2 elevado a 4 = 16 combinaciones.

SOS: siempre te falta un número. Si ocho bits ofrecen 256 combinaciones, el máximo sin signo es 255 porque se incluye el cero. Distingue cantidad de combinaciones y valor máximo.

07. Archivos, carpetas y discos: cada cosa en su sitio

Al terminar: distinguirás nombre, formato, ruta, sistema de archivos, partición y volumen.
Antes: comprende la diferencia entre memoria y almacenamiento.



Dispositivo, partición y organización de archivos son niveles diferentes.

Un **archivo** reúne datos que el sistema gestiona bajo una identidad y ciertos metadatos: nombre, tamaño, fechas, permisos y otros atributos. Una **carpeta** organiza entradas que permiten localizar archivos y otras carpetas. La interfaz puede mostrar iconos parecidos, pero un archivo comprimido que se abre como una carpeta sigue teniendo un formato propio.

El nombre no es el contenido

En `informe.pdf`, `.pdf` es una extensión que orienta sobre el formato. El contenido tiene una estructura interna. Renombrar `foto.jpg` como `foto.pdf` no convierte la imagen en un documento PDF válido. Para convertir hace falta una herramienta que lea un formato y escriba el otro.

El sistema puede asociar una extensión con un programa. Cambiar esa asociación cambia qué aplicación se abre, no transforma los datos. Un PDF puede abrirse con diferentes lectores sin dejar de ser PDF.



Ojo con este error

Si las extensiones están ocultas, un nombre como `factura.pdf.exe` puede verse de forma engañosa. Mostrar extensiones ayuda a inspeccionar archivos, aunque no sustituye otras medidas de seguridad.

Rutas absolutas y relativas

Una ruta indica cómo localizar algo. Una ruta **absoluta** parte de una raíz reconocible: `C:\Practicas\informe.txt` o `/home/alumno/practicas/informe.txt`. Una ruta **relativa** depende del directorio actual: `practicas/informe.txt`.

En muchas herramientas, `.` representa el directorio actual y `..` el superior. Una instrucción relativa ejecutada desde otro directorio puede operar sobre un lugar diferente o fallar. Antes de borrar o sobrescribir, comprueba dónde estás.

Los espacios y otros caracteres pueden necesitar comillas según el intérprete. Mayúsculas y minúsculas pueden ser significativas dependiendo del sistema de archivos y su configuración. No deduzcas el comportamiento solo por el aspecto de la ventana.

Del dispositivo al archivo

Una unidad física puede dividirse mediante una tabla de particiones. Una **partición** delimita una región lógica. Un **sistema de archivos** establece cómo organizar datos y metadatos: por ejemplo, NTFS, ext4 o exFAT. Un **volumen** es una unidad lógica de almacenamiento presentada al sistema; no siempre coincide uno a uno con una partición física.

Un **punto de montaje** permite acceder a un sistema de archivos dentro del árbol de directorios. En Linux puede ser `/mnt/datos`; en Windows una unidad puede aparecer mediante una letra y también existen puntos de montaje en carpetas. Una letra de unidad no identifica necesariamente un disco físico exclusivo.

Elegir formato según el uso

No existe un sistema de archivos mejor para todo. Considera compatibilidad, permisos, tamaños máximos, recuperación y funciones necesarias. FAT32 tiene un límite de archivo cercano a 4 GiB que explica por qué una unidad con espacio libre puede rechazar una imagen grande. exFAT se utiliza a menudo para intercambio entre sistemas, pero no ofrece las mismas funciones de permisos que NTFS o ext4.

Formatear crea estructuras de un sistema de archivos y puede hacer inaccesibles los datos anteriores. Un formato rápido no garantiza un borrado seguro. En este capítulo no necesitas formatear ningún soporte.

Ejemplo: «tengo sitio, pero no puedo copiar»

Quieres copiar un archivo de 6 GiB a una memoria con 20 GiB libres. Primero comprueba el tamaño real del archivo y el sistema de archivos del destino. Si es FAT32, el límite por archivo explica el fallo. La solución podría ser utilizar otro soporte compatible o cambiar el formato después de respaldar los datos y revisar los requisitos de los dispositivos. Borrar documentos para liberar espacio no elimina ese límite.

Vamos a probarlo sin tocar particiones

Crea `SMR-practicas`, y dentro `originales`, `trabajo` y `entregas`. Guarda un texto ficticio en `originales`. Haz una copia en `trabajo` y modifica solo esta. Anota las dos rutas y compara contenidos. En el gestor de archivos, consulta las propiedades de la unidad sin usar las opciones de formato.

Resultado esperado: distingues la copia y el original, y puedes explicar si una ruta es absoluta o relativa. Para recuperar, copia de nuevo el original sobre la copia de trabajo después de confirmar nombres y ubicación.

¿Lo has pillado?

1. ¿Un acceso directo es necesariamente otra copia del documento?

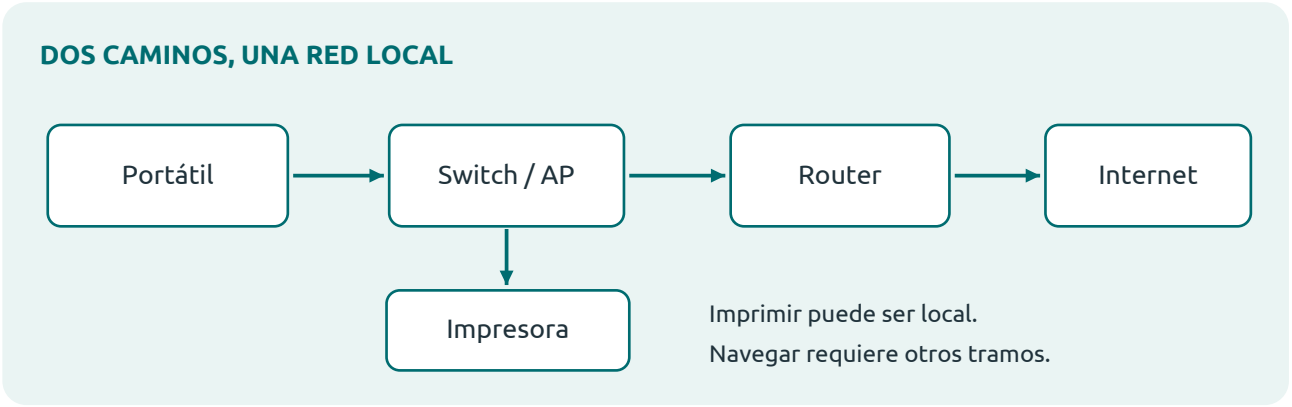
2. ¿Puedes asegurar que dos letras de unidad corresponden a dos discos físicos?

3. ¿Por qué una copia en otra carpeta del mismo disco no protege frente a la avería de ese disco?

Soluciones. 1) No: normalmente contiene una referencia; eliminarlo suele eliminar la referencia, no el destino. 2) No: pueden representar volúmenes del mismo dispositivo. 3) Porque original y copia comparten el componente que falla.

08. Cómo se hablan dos ordenadores

Al terminar: explicarás cliente, servidor, dirección, puerto y protocolo sin confundirlos con un aparato concreto. **Antes:** conoce archivos, programas y unidades de transferencia.



La impresión local y una web externa comparten solo parte del recorrido.

Una red permite intercambiar información entre dispositivos. Para hacerlo necesitan medios de comunicación y reglas compartidas. Un **protocolo** define reglas de intercambio: cómo se representan mensajes, qué significan y, según el protocolo, qué respuestas se esperan.

Cliente y servidor son papeles

Un cliente inicia una petición a un servicio; un servidor la atiende. Un ordenador puede ser cliente de una web y servir al mismo tiempo una carpeta a otros equipos. La palabra servidor puede referirse al equipo o al programa que ofrece el servicio: el contexto indica cuál.

Una dirección **IP** permite identificar una interfaz en el contexto de una red IP. Un **puerto** de transporte ayuda a distinguir comunicaciones y servicios dentro de un equipo. Decir «el servidor es 443» mezcla conceptos: 443 es un puerto habitual de HTTPS, no una dirección del servidor.

En TCP o UDP, el puerto es un número, no un conector físico. El conector Ethernet donde enchufas el cable también se llama puerto en otros contextos. Si hay duda, concreta «puerto TCP» o «puerto físico del switch».

Red local, Internet, web y wifi

Una **red local** conecta dispositivos dentro de un entorno limitado. **Internet** interconecta redes mediante protocolos compartidos. La **web** es un conjunto de servicios y recursos al que accedes normalmente con un navegador. **Wifi** proporciona una forma de conexión inalámbrica a una red local. Son conceptos relacionados, pero no intercambiables.

Puedes acceder a una impresora de la red local aunque se haya caído la conexión del proveedor. También puedes tener enlace wifi y no disponer de una configuración IP válida o no alcanzar el router. El icono inalámbrico describe una parte del camino.

Ejemplo: abrir una intranet

En Aula Norte escribes `https://intranet.aulanorte.test`. El navegador interpreta el esquema HTTPS y el nombre. El equipo necesita resolver el nombre, encontrar cómo llegar a la dirección obtenida y establecer la comunicación correspondiente. En una conexión HTTPS habitual sobre TCP, se establece TCP, se negocia TLS y se intercambian peticiones y respuestas HTTP protegidas. HTTP/3 utiliza QUIC sobre UDP: no todas las versiones de HTTP recorren exactamente la misma secuencia.

DNS no descarga la página y el router no se convierte por ello en servidor web. Cada elemento cumple una función. El dominio `.test` está reservado para pruebas; el laboratorio deberá configurar su resolución. Escribirlo en cualquier navegador no crea automáticamente la intranet.

Latencia y ancho de banda

El ancho de banda o la capacidad disponible se relaciona con cuánto puede transferirse por tiempo. La **latencia** expresa un retardo. Un enlace puede descargar archivos grandes deprisa y resultar incómodo para una conversación si el retardo es alto. La pérdida de paquetes y su variación temporal también afectan a la experiencia.

No concluyas «la red va bien» a partir de una única cifra. Pregunta qué tarea falla y entre qué equipos. Un servicio lento puede depender de disco, CPU, aplicación o resolución de nombres, además de la red.

Vamos a probarlo: dibuja antes de configurar

Dibuja un portátil conectado por wifi a un punto de acceso, este a un switch y el switch a un router con salida a Internet. Añade una impresora conectada al switch. Traza un camino hacia la impresora y otro hacia una web externa. El router doméstico puede integrar varias de esas funciones en una sola carcasa; separarlas en el dibujo ayuda a comprenderlas.

Resultado esperado: reconoces qué partes comparten ambos caminos. No hace falta modificar la red de casa. Si desconectas el acceso del proveedor en el dibujo, la impresión local podría seguir funcionando si todos sus servicios necesarios son locales.

SOS: tengo wifi, pero no navego

Empieza por delimitar: ¿afecta a un dispositivo o a todos?, ¿funciona una aplicación diferente?, ¿hay acceso a servicios locales? Más adelante comprobarás enlace, configuración IP, rutas, resolución de nombres y servicio. No cambies el DNS como respuesta automática a cualquier problema: primero necesitas indicios de un fallo de resolución.

¿Lo has pillado?

1. ¿Puede un mismo equipo actuar como cliente y servidor?

2. ¿Tener más Mb/s garantiza menor latencia?

3. ¿DNS y HTTPS cumplen la misma función?

4. ¿El puerto TCP 443 es la toma del cable de red?

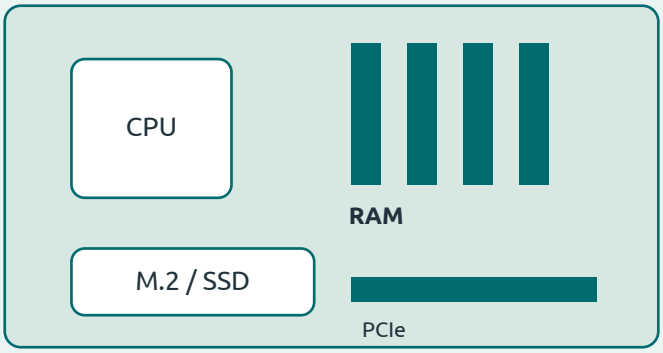
Soluciones razonadas. 1) Sí, son papeles de programas en comunicaciones concretas. 2) No: capacidad y retardo son magnitudes distintas. 3) No: DNS proporciona información de nombres; HTTPS permite intercambiar recursos web mediante una comunicación protegida. 4) No: es un identificador lógico de transporte; el conector es un elemento físico.

Bloque 2. Montaje y mantenimiento de equipos

09. Reconocer los componentes y entender qué aportan

Al terminar: explicarás la función de cada componente principal y qué datos consultar para sustituirlo. **Antes:** repasa hardware, memoria y almacenamiento.

UN MAPA PARA RECONOCER COMPONENTES



Placa: conecta las piezas.

CPU: ejecuta instrucciones.

RAM: datos de trabajo.

SSD: conserva archivos.

PCIe: permite expansión.

Ilustración conceptual: las posiciones reales dependen del modelo.

Los componentes se identifican por su función y por el manual del modelo.

Un ordenador no es «un procesador con una caja». Su rendimiento, compatibilidad y fiabilidad dependen del conjunto. Una CPU rápida con poca memoria disponible puede pasar mucho tiempo esperando. Un almacenamiento lento puede hacer que abrir programas resulte pesado aunque el procesador apenas trabaje.

Placa base, CPU y memoria

La **placa base** conecta y alimenta componentes y proporciona interfaces de comunicación. Tiene un formato físico, un zócalo de procesador, ranuras de memoria y conectores. El manual de su modelo es la referencia para identificar posiciones y compatibilidad.

La **CPU** ejecuta instrucciones. Los núcleos permiten ejecutar trabajo en paralelo cuando el programa y el sistema pueden aprovecharlos. Los hilos lógicos no equivalen a duplicar físicamente todos los recursos de un núcleo. Frecuencia, arquitectura, caché, consumo y refrigeración influyen en el resultado.

La **RAM** mantiene datos de trabajo. Su generación, formato, capacidad y configuración deben ser compatibles con la plataforma. Un módulo de una generación distinta no se vuelve compatible por tener una capacidad parecida. Forzar una pieza que no encaja puede dañarla.

La memoria **caché** acerca datos al procesador para reducir accesos más lentos. La **memoria virtual** permite administrar espacios de direcciones y utilizar almacenamiento como respaldo de

parte de la memoria. No convierte un SSD en RAM igual de rápida. Si el sistema intercambia continuamente páginas con el disco, puede perder mucha agilidad.

Almacenamiento y expansión

Un HDD guarda datos mediante mecanismos magnéticos con partes móviles; un SSD utiliza memoria no volátil sin ese mecanismo. La interfaz importa, pero también las características de la unidad y la carga de trabajo.

M.2 identifica un formato y un conector con variantes. **NVMe** es un protocolo de almacenamiento utilizado habitualmente sobre PCIe. Existen unidades M.2 SATA: que una unidad tenga esa forma no garantiza que sea NVMe ni que cualquier ranura M.2 la admita.

Las ranuras **PCIe** permiten instalar tarjetas de expansión. Su tamaño físico y el número de líneas eléctricas disponibles pueden ser distintos. Algunas placas comparten recursos entre conectores: instalar un dispositivo puede deshabilitar otro puerto. Esa información aparece en el manual.

Gráficos, alimentación y refrigeración

La GPU procesa trabajo gráfico y otras tareas adecuadas para su arquitectura. Puede estar integrada en la plataforma o en una tarjeta dedicada. Que la placa tenga una salida de vídeo no garantiza que la combinación instalada pueda utilizarla: depende, entre otras cosas, del procesador.

La fuente transforma y suministra alimentación. Hay que comprobar capacidad, calidad, conectores y adecuación al equipo. Una cifra grande de vatios por sí sola no demuestra calidad. En fuentes modulares, los cables del lado de la fuente no son universalmente intercambiables, aunque encajen.

El sistema de refrigeración transporta calor desde los componentes hacia el ambiente. Necesita montaje correcto, contacto térmico adecuado y circulación de aire. La pasta térmica ayuda a cubrir irregularidades microscópicas; no sustituye el disipador ni debe aplicarse sin seguir las indicaciones del fabricante.

Ejemplo de diagnóstico razonado

Un equipo tarda mucho en abrir aplicaciones. El procesador no está saturado, queda poca memoria disponible y el sistema realiza muchas operaciones de almacenamiento. Esa observación sugiere investigar presión de memoria y paginación. Comprar otra CPU sin medir nada no responde a la evidencia.

Vamos a probarlo

Sin abrir el equipo, consulta el inventario del sistema y registra modelo de CPU, RAM y unidades. Diferencia en tu ficha «dato observado», «dato obtenido del manual» y «dato no confirmado». Si puedes acceder al manual de la placa o del equipo, localiza la sección de memoria y las interfaces de almacenamiento.

Resultado esperado: una ficha que permita buscar una ampliación sin basarse en «es un ordenador bastante nuevo». No hace falta comprar ni desmontar nada.

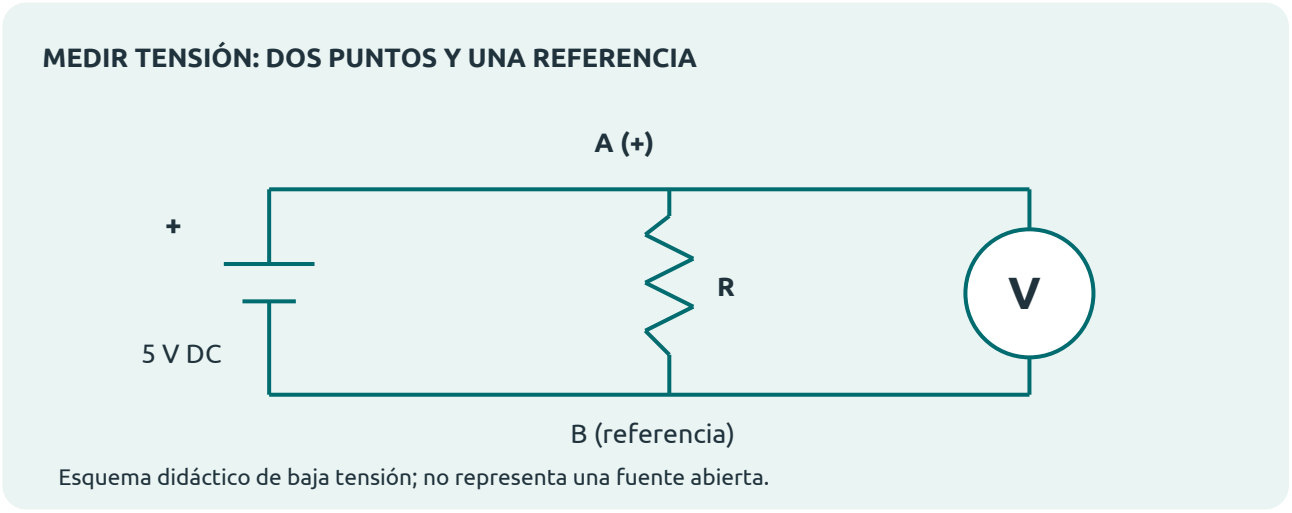
Taller de electricidad: entender qué estás midiendo

La **tensión** o diferencia de potencial se mide en voltios, V; la **intensidad**, en amperios, A; la **resistencia**, en ohmios; la **potencia**, en vatios, W. En un modelo resistivo de corriente continua, V = I × R y P = V × I. No utilices ese modelo simplificado como explicación completa de cualquier circuito electrónico o carga de corriente alterna.

Con 5 V sobre una resistencia de 1.000 ohmios, la intensidad ideal es 0,005 A, es decir, 5 mA, y la potencia 0,025 W. Una lectura se interpreta con unidad, punto de referencia, incertidumbre del instrumento y condiciones de funcionamiento. «Da cinco» no es un informe suficiente.

Corriente continua, DC, mantiene polaridad en el modelo sencillo; **corriente alterna, AC**, varía periódicamente en el caso habitual. Un multímetro en modo DC y otro en modo AC no responden a la misma pregunta. La lectura media no permite conocer por sí sola el rizado o transitorios de una fuente; para estudiar forma de onda se utiliza instrumental y preparación adecuados.

Medición guiada de una tensión continua baja



El voltímetro compara A y B en paralelo con la resistencia del ejemplo.

El ejercicio utiliza exclusivamente un módulo didáctico de baja tensión con puntos externos identificados por el docente, o una pila adecuada al instrumento. No se abre una fuente de PC, un cargador o un SAI ni se mide red eléctrica. Revisa el manual del multímetro y el estado de puntas y equipo antes de empezar.

1. Identifica magnitud, valor aproximado esperado y referencia. Para un punto de 5 V continuos, selecciona tensión DC y rango apropiado, superior al valor esperado si el instrumento no es automático.

2. Coloca la punta negra en COM y la roja en la entrada para tensión indicada por el fabricante, normalmente V. La entrada de intensidad A no sirve para esta conexión.

3. Conecta la medición de tensión **en paralelo**: negra en la referencia y roja en el punto positivo identificado del módulo. No provoques un puente entre contactos contiguos.
4. Lee signo, unidad y valor. Si inviertes la referencia puede aparecer un signo negativo; comprueba el montaje antes de concluir que existe una avería.
5. Retira las puntas, registra configuración y compara con el intervalo del ejercicio. No cambies a resistencia o continuidad sobre un circuito alimentado.

Ejemplo ficticio: el módulo especifica 5 V con tolerancia didáctica del 5 %. El intervalo es 4,75 a 5,25 V. Una medida de 4,92 V cae dentro; 4,60 V queda fuera. Antes de diagnosticar, revisa referencia, carga, escala y precisión. El 5 % pertenece a este supuesto, no es una tolerancia universal de cualquier salida.

La intensidad se mide con una conexión y entrada distintas, normalmente en serie con la rama preparada. Un amperímetro puesto directamente entre polos puede producir un cortocircuito. En este taller la intensidad se calcula; cualquier medición adicional se realiza en el circuito y procedimiento que prepare el docente, con límites y protección adecuados.

Fuente del procedimiento de tensión: Fluke, medición de tensión continua con multímetro. https://www.fluke.com/en/learn/blog/digital-multimeters/how-to-measure-dc-voltage-with-a-digital-multimeter

Fuente de alimentación y SAI: bloques y límites

Una fuente de PC transforma la alimentación de entrada en salidas adecuadas mediante etapas de filtrado, conversión, regulación y protección. En fuentes ATX multisalida son habituales líneas de 12 V, 5 V y 3,3 V, además de señales y alimentación de espera según el diseño. **ATX12VO** adopta otro reparto y entrega principalmente 12 V; parte de la conversión se realiza en la placa. Comprueba la especificación y el modelo, no solo el color de un cable.

El lado modular de una fuente no tiene un conexionado universal entre fabricantes o modelos. Utiliza los cables compatibles especificados. Un conector que encaja físicamente no demuestra compatibilidad eléctrica. Para comprobar salidas de una fuente se utiliza un útil de prueba externo apropiado, carga y procedimiento del taller; no improvises puentes para hacerla arrancar.

Un **SAI**, sistema de alimentación ininterrumpida, combina almacenamiento de energía y electrónica de alimentación para sostener cargas bajo condiciones definidas. Según topología puede incluir cargador/rectificador, batería, inversor, regulación y conmutación o bypass. Un equipo *line-interactive* y uno de doble conversión no tienen el mismo recorrido de energía ni las mismas prestaciones.

Consulta los límites de **W** y de **VA**: potencia activa y aparente. Deben respetarse ambos; no asumas una relación fija para cualquier carga. Ejemplo ficticio: un SAI admite 1.000 VA y 600 W; una carga de 700 W ya excede su límite aunque parezca caber mirando únicamente VA. La autonomía depende de carga, batería, estado y diseño: usa la curva del fabricante.

En el laboratorio se puede leer el panel o software autorizado del SAI: tensión de entrada/salida indicada, carga, estado de batería, eventos y autonomía estimada. Registra qué datos son

estimaciones y cuáles medidas reportadas por el equipo. Las señales en módulos didácticos se miden solo en los puntos de baja tensión previstos. No se accede al interior ni a bornes peligrosos.

Fuentes: Intel, guía ATX12VO, https://cdrdv2-public.intel.com/613768/613768_2.11.pdf; APC/Schneider Electric, selección de SAI, https://www.apc.com/us/en/support/product-support/ups-buying-guide-for-selecting-a-battery-backup-system.jsp.

Evidencia del taller y respuestas

Completa `recursos/hardware/ficha-medicion.md`: instrumento, magnitud, conexión, punto de referencia, rango, valor y comparación. Añade el cálculo del ejemplo y una ficha de SAI ficticia con W, VA y tarea de apagado ordenado. La lectura del capítulo no acredita una medición física realizada.

Preguntas: ¿dónde conectas un voltímetro?, ¿por qué no usas la entrada A para medir tensión?, ¿450 W garantizan autonomía de treinta minutos? Respuestas: en paralelo entre los puntos previstos; la entrada y circuito de intensidad pueden crear un cortocircuito con esa conexión; no, se necesita información de autonomía para carga y estado concretos.

¿Lo has pillado?

1. ¿M.2 y NVMe significan lo mismo?

2. ¿Más núcleos garantizan que cualquier programa tarde la mitad?

3. ¿Puedes reutilizar un cable modular de otra fuente porque el conector encaja?

Soluciones. 1) No: formato/conector y protocolo describen aspectos diferentes. 2) No: depende del trabajo paralelizable y de otros límites. 3) No sin compatibilidad expresa del fabricante: el cableado interno puede diferir y dañar componentes.

10. Elegir componentes compatibles y justificar el presupuesto

Al terminar: construirás una lista de comprobación antes de comprar. **Antes:** reconoce CPU, RAM, placa, fuente y almacenamiento.

El primer dato de un presupuesto no es una marca: es la necesidad. En Aula Norte, un puesto administrativo abre documentos, usa el navegador y participa en videollamadas. Un equipo de laboratorio debe ejecutar invitados virtuales. Ambos son ordenadores, pero la memoria, el almacenamiento y otras prioridades pueden ser diferentes.

Del uso a un requisito comprobable

Escribe tareas simultáneas, aplicaciones, periféricos, red disponible, espacio, ruido aceptable y posibilidades de ampliación. Distingue requisitos mínimos del software, una configuración confortable y deseos opcionales. Comprueba también licencias, garantía y mantenimiento.

Si el equipo debe ejecutar un sistema concreto, revisa sus requisitos oficiales y compatibilidad antes de seleccionar las piezas. No presupongas que cualquier equipo puede instalar cualquier versión de Windows o cualquier hipervisor.

La cadena de compatibilidad

1. CPU y placa: zócalo, familia admitida y versión de firmware necesaria.
2. RAM y placa: generación, formato, capacidad máxima, número de módulos y configuraciones admitidas.
3. Caja y placa: formato y posiciones de montaje.
4. Refrigeración: anclaje, altura, espacio y capacidad adecuada para la carga.
5. GPU: longitud, grosor, alimentación y espacio en la caja.
6. Almacenamiento: interfaz y ranura compatibles; recursos compartidos.
7. Fuente: conectores, formato, potencia adecuada y margen razonado.
8. Periféricos: puertos, controladores, resolución y usos necesarios.

Coste inicial y coste de uso

Un precio bajo puede esconder poca garantía, consumo elevado o una ampliación imposible. Un equipo reacondicionado puede ser una buena opción si cumple requisitos, presenta un estado adecuado y dispone de condiciones claras. Compara el coste total del periodo de uso, no solo el importe de la torre.

Las cifras del siguiente ejemplo son didácticas, no precios de mercado: opción A cuesta 500 unidades monetarias y necesita una ampliación de 100; opción B cuesta 570 e incluye esa capacidad. Si ambas satisfacen las mismas necesidades y garantías, la segunda puede resultar más económica en conjunto. Si no necesitas la ampliación, la comparación cambia.

Vamos a probarlo: dos propuestas para Aula Norte

Prepara una propuesta administrativa y otra de laboratorio. No hace falta poner modelos comerciales: usa requisitos técnicos verificables. Añade para cada componente «necesidad que resuelve», «compatibilidad que debo comprobar» y «fuente de la comprobación». Si incorporas precios reales, anota proveedor, impuestos y fecha.

Resultado esperado: una persona puede entender por qué asignaste más RAM al laboratorio sin recurrir a «porque es mejor». Incluye monitor, teclado, red, sistema y copias en el alcance; lo que se excluya debe quedar escrito.



Ojo con este error

La CPU es compatible, pero el equipo no arranca. Comprueba si la placa necesita una versión de firmware posterior a la instalada y qué método admite para actualizarla. No inicies una actualización a ciegas: necesitas el modelo exacto y el procedimiento del fabricante.

Elegir también el formato del equipo

Una torre facilita ciertas ampliaciones, pero ocupa espacio y necesita ventilación adecuada. Un **mini-PC** reduce volumen y puede limitar ranuras, potencia térmica, unidades y mantenimiento. Un **barebone** se entrega parcialmente montado; comprueba qué componentes faltan y qué admite antes de compararlo con un equipo completo.

Un **todo en uno** integra pantalla y ordenador: puede simplificar instalación y complicar algunas reparaciones. Un **HTPC** orientado a multimedia exige estudiar ruido, reproducción de formatos, salidas, control y espacio, además de potencia. Un portátil combina movilidad, batería, pantalla y condicionantes térmicos; una base de conexión no garantiza todas las funciones para cualquier equipo.

Los dispositivos móviles y sistemas integrados pueden servir como clientes ligeros, captura o control, con arquitecturas y gestión distintas. Una aplicación compilada para x86-64 no funciona necesariamente igual en ARM sin versión compatible o una capa de ejecución adecuada. Tampoco una ampliación soldada se sustituye como un módulo accesible.

El **modding** modifica apariencia o disposición. Debe respetar integridad estructural, aislamiento, ventilación y garantías/condiciones aplicables. Una ventana o iluminación no justifica retirar una protección ni alterar una fuente.

Práctica comparada: para un puesto fijo de administración, uno móvil y un terminal de consulta, justifica formato, mantenimiento, software, conectividad y vida útil. No hace falta elegir marcas ni comprar: utiliza fichas técnicas de modelos autorizados o requisitos ficticios. Resultado: tres elecciones justificadas y una limitación reconocida para cada una.

¿Lo has pillado?

1. ¿Basta con que coincida el zócalo?
2. ¿Por qué se debe comprobar el espacio de la caja además del conector de la GPU?
3. ¿Una cifra de consumo de un componente equivale a la potencia que consume siempre el equipo completo?

Soluciones. 1) No: importa la compatibilidad concreta y a veces el firmware. 2) Puede ser eléctricamente compatible y no caber. 3) No: depende de qué mide la cifra, del resto de componentes y de la carga.

11. Montar sin improvisar

Al terminar: podrás planificar un montaje y sus verificaciones. **Antes:** compatibilidad comprobada, manuales disponibles y práctica supervisada si no tienes experiencia.

Trabaja en una mesa estable, seca, despejada y con buena luz. Prepara destornilladores adecuados, recipientes para tornillos y un método de organización. Manipula las piezas por sus bordes y aplica medidas de protección electrostática siguiendo el equipamiento del puesto.

Antes de tocar el interior

Apaga el equipo, desconecta su alimentación y otros cables según el procedimiento de servicio. En portátiles, sigue las instrucciones para desconectar la batería interna. No abras fuentes de alimentación ni otros conjuntos con riesgo eléctrico: pueden conservar cargas peligrosas incluso desconectados.

Anota conexiones y haz fotografías de referencia si estás desmontando. La batería, las pestañas y las cintas flexibles requieren procedimientos específicos: un portátil no se desmonta igual que una torre.

Orden orientativo de montaje

El orden depende de la caja y los componentes. Una secuencia habitual es verificar piezas, instalar CPU y memoria según los manuales, colocar refrigeración, preparar separadores de la caja, fijar la placa, instalar fuente y almacenamiento, montar expansión y conectar alimentación, datos y panel frontal.

El procesador tiene una orientación definida. Comprueba marcas y mecanismo de retención; no fuerces contactos. Retira las protecciones que indique el disipador. Conecta el ventilador de CPU en la cabecera correspondiente y revisa si la refrigeración necesita otras conexiones.

Los separadores de la caja deben coincidir con los puntos de montaje de la placa. Un separador adicional bajo una zona sin orificio puede provocar un cortocircuito. Aprieta con firmeza moderada, sin deformar la placa ni dañar roscas.

Los conectores de alimentación de CPU y GPU pueden parecer semejantes. Comprueba etiquetas y manuales; no fuerces la inserción. Mantén cables alejados de ventiladores y evita tensiones sobre los conectores.

Lista antes del primer encendido

Verifica que no quedan tornillos sueltos, que la RAM está asentada, que CPU y disipador están instalados, que las conexiones principales de alimentación son correctas y que el monitor utiliza una salida válida. Confirma la conexión del botón de encendido en el panel frontal. Si una pieza no encaja, detente y revisa.

Primera comprobación

Tras encender, observa señales del firmware y comprueba que reconoce memoria y almacenamiento. Revisa que funcionan los ventiladores previstos y observa temperaturas de acuerdo con las indicaciones del fabricante. Los límites dependen del modelo: evita aplicar una cifra universal a todos los procesadores.

No continúes con la instalación del sistema si el equipo se apaga por temperatura o detectas olor, humo o un comportamiento eléctrico anómalo. Desconecta con seguridad y solicita revisión.

Práctica: ensayo de montaje sin alimentación

En un entorno de formación, identifica en una placa de prácticas el zócalo, ranuras, conexiones y puntos de fijación usando su manual. Prepara el orden y el material de cada paso antes de ejecutarlo. Si no dispones de piezas, realiza una ficha ilustrada basada en un manual oficial y marca lo que no puedes verificar físicamente.

Resultado esperado: un procedimiento específico para ese equipo, no una lista genérica que oculte conectores desconocidos. Al recoger, deja piezas protegidas y tornillos clasificados.

¿Lo has pillado?

1. ¿Por qué debes comprobar los separadores?

2. ¿Puedes encender brevemente sin disipador para «ver si funciona»?

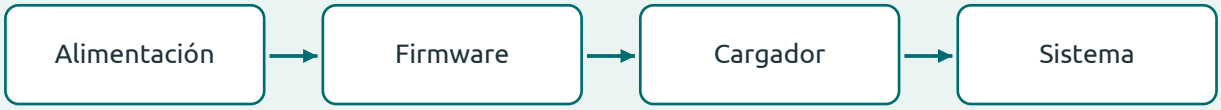
3. ¿Qué haces cuando necesitas mucha fuerza para insertar un módulo?

Soluciones. 1) Una fijación incorrecta puede dañar o cortocircuitar la placa. 2) No: instala la refrigeración requerida antes de alimentar el equipo. 3) Detenerte y comprobar orientación, compatibilidad y mecanismo; la fuerza no corrige una incompatibilidad.

12. Entender el arranque y el firmware

Al terminar: distinguirás detección de hardware, opción de arranque y carga del sistema. **Antes:** conoce firmware, particiones y almacenamiento.

CADA ETAPA NECESITA LA ANTERIOR



Que el disco esté detectado no demuestra que se pueda arrancar.

Secuencia orientativa; existen variaciones según plataforma y configuración.

El arranque se compone de varias etapas.

Al encender, el firmware prepara el entorno e inicia el proceso de arranque. **BIOS** y **UEFI** describen tecnologías de firmware diferentes, aunque algunas personas utilicen «BIOS» para cualquier pantalla de configuración. Identifica qué entorno y modos admite tu equipo.



Ojo con este error

El **POST** comprende comprobaciones iniciales. Luces de diagnóstico, códigos y sonidos pueden orientar, pero su significado depende del modelo. Busca la tabla del fabricante: un número de pitidos no tiene una interpretación universal.

Detectar un disco no significa poder arrancarlo

El firmware puede reconocer una unidad vacía. Para arrancar hace falta una cadena válida: una opción de arranque adecuada, los archivos o estructuras necesarios y un sistema compatible. En UEFI es habitual seleccionar una entrada del gestor de arranque, no simplemente «el primer disco».

GPT y **MBR** son esquemas de particionado. UEFI suele utilizar una partición de sistema EFI para los cargadores correspondientes. No confundas el estilo de partición con el sistema de archivos ni conviertas discos reales para probar sin copia y planificación.

Ajustes habituales y sus efectos

El menú puede permitir modificar fecha, orden de arranque, virtualización del procesador, comportamiento de ventiladores y funciones de seguridad. **Secure Boot** verifica componentes del proceso de arranque conforme a sus claves y políticas. No es un antivirus ni hace innecesaria la seguridad del sistema.

Cambiar opciones de almacenamiento, seguridad o arranque puede impedir el inicio o activar solicitudes de recuperación de cifrado. Antes de modificar, registra la configuración y asegúrate de disponer del procedimiento y de los medios de recuperación necesarios.

Actualizar firmware con criterio

Una actualización puede corregir fallos o ampliar compatibilidad. También exige seleccionar el archivo exacto y seguir el procedimiento del fabricante. Comprueba modelo y revisión, requisitos previos, suministro eléctrico estable y medidas relativas al cifrado. No apagues ni interrumpas la actualización salvo que el procedimiento indique qué hacer ante un fallo.

Ejemplo: vuelve siempre al instalador

Instalas el sistema desde una memoria USB y, al reiniciar, aparece otra vez la instalación. Antes de repetirla, comprueba si el equipo está arrancando de nuevo desde el USB. La instalación anterior puede estar correcta; la selección de arranque dirige a otro medio.

Vamos a probarlo

En una máquina virtual de prácticas, consulta el tipo de firmware y el orden de arranque. Guarda una captura sin datos sensibles y explica qué entrada debería usarse después de instalar. Si haces cambios, registra el valor inicial y restáuralo al terminar. En un equipo físico puedes limitarte a consultar el manual.

Resultado esperado: explicas la diferencia entre «la unidad está detectada» y «existe una opción válida para iniciar el sistema».

¿Lo has pillado?

1. ¿Secure Boot impide todos los programas maliciosos?

2. ¿GPT es un sistema de archivos?

3. ¿Una actualización sirve para cualquier placa de la misma marca?

Soluciones. 1) No: se ocupa de una parte del arranque y funciona con una configuración concreta. 2) No: describe el particionado. 3) No: se debe verificar el modelo y la revisión exactos.

13. Periféricos y mantenimiento preventivo

Al terminar: podrás instalar un periférico con comprobaciones y planificar un mantenimiento proporcionado. **Antes:** distingue dispositivos, controladores y aplicaciones.

Un periférico necesita una conexión física o de red, compatibilidad con el sistema y configuración adecuada. Conectar un cable puede bastar en algunos casos; en otros hay que instalar un controlador, elegir un protocolo o configurar una dirección.

Impresoras: separa dispositivo, cola y aplicación

La aplicación envía un trabajo, el sistema lo gestiona mediante una cola y el dispositivo lo recibe según la configuración. El controlador representa las capacidades de impresión. Si está mal elegido, puede faltar una función o producirse una salida incorrecta.

Una página de prueba generada por la impresora verifica parte de su funcionamiento. Una página enviada desde el sistema comprueba además la ruta de impresión correspondiente. Un documento de la aplicación afectada completa la comprobación del caso del usuario.

En una impresora de red, anota su dirección y el método de asignación. Si cambia inesperadamente y la cola apunta a la anterior, el equipo puede dejar de encontrarla. Una reserva DHCP o una configuración documentada puede ayudar, según el diseño de red.

Escáneres, pantallas y otros dispositivos

Para un escáner comprueba conexión, controlador, origen elegido y permisos de la aplicación. Para una pantalla revisa alimentación, entrada seleccionada, cable, salida del equipo y resolución. Un adaptador físico no garantiza todas las combinaciones de señal ni todas las resoluciones.

Las bases USB y otros accesorios comparten recursos y pueden requerir alimentación adicional. Una forma de conector no describe todas sus funciones: USB-C puede transportar diferentes capacidades según equipo, cable y dispositivo.

Plan de mantenimiento

Define tareas según ambiente y uso: inspección de polvo, ventilación, estado de cables, espacio libre, actualizaciones, copias y revisión de avisos. Registra fecha, responsable, observaciones y próxima revisión. Mantener no significa desmontar sin necesidad.

Limpia con el equipo apagado y desconectado, usando métodos y productos admitidos por el fabricante. Evita líquidos directos. Si utilizas aire para limpiar, sigue las instrucciones del equipo y del producto, controla el polvo y evita hacer girar ventiladores libremente a gran velocidad.

Una batería hinchada, dañada o con señales de fuga requiere dejar de utilizar el equipo y seguir las indicaciones de servicio y gestión del fabricante. No la perfores ni la comprimas para que vuelva a encajar.

Práctica: una impresora que se pueda dar por instalada

En una impresora de laboratorio autorizada, registra modelo, conexión y controlador. Comprueba suministros y estado. Imprime una página de prueba y un documento ficticio desde la cuenta que usará el dispositivo. Anota si funcionan funciones necesarias, como doble cara o tamaño de papel. No cambies direcciones ni configuración compartida sin planificar el efecto.

Resultado esperado: evidencia de la impresión y una ficha que permita repetir la instalación. Si no hay impresora, analiza un caso escrito y explica qué pruebas separarían un fallo físico de uno de cola.

SOS: el trabajo no sale

Revisa si afecta a todos, si la impresora informa de un error y si hay trabajos bloqueados. Borrar una cola elimina trabajos pendientes: avisa a las personas afectadas y sigue el procedimiento del entorno. No reinicies sin registrar el síntoma y sin considerar el uso compartido.

Consumibles y mecanismos: reconocer antes de sustituir

Una impresora de inyección y una láser emplean procesos y consumibles distintos. La láser utiliza elementos de imagen y fijación; el fusor puede alcanzar temperaturas elevadas. No confundas cartucho, tambor, depósito residual o kit de mantenimiento: su integración y sustitución dependen del modelo.

Ante un atasco, consulta recorrido y zonas accesibles del manual, detén la tarea y sigue su secuencia de enfriamiento/apertura. Retira el papel en la dirección indicada, sin forzar ni introducir herramientas en zonas no previstas. Comprueba que no quedan restos y cierra correctamente. Repetir atascos puede relacionarse con papel, bandeja, rodillos o mecanismos; registra evidencia antes de sustituir piezas.

Para cambiar un consumible: identifica referencia compatible, guarda configuración y estado si procede, prepara protección del área, retira/instala según manual y trata el residuo por su canal. Después comprueba reconocimiento, calidad y tarea original. Agitar, rellenar o limpiar de forma improvisada no es un procedimiento universal.

Captura, salida y usos profesionales

En un escáner, distingue superficie plana y alimentador, tamaño admitido, resolución óptica, profundidad de color, dúplex y formatos de salida. OCR interpreta texto; no demuestra que la lectura sea correcta. Revisa caracteres y disposición antes de utilizar el documento.

Una cámara añade resolución, frecuencia de imagen, enfoque, iluminación, interfaz y permisos de captura. Un micrófono y un altavoz necesitan revisar selección de entrada/salida, niveles y realimentación. En edición y reproducción, considera dispositivo, aplicación, controlador y formato por separado.

Fotocopiadoras multifunción, impresión de gran formato y equipos de producción pueden integrar contabilización, acabado o gestión de color. Su mantenimiento no se deduce del de una impresora doméstica; utiliza personal, procedimiento y consumibles específicos.

Práctica: crea un documento ficticio con texto, tonos y una línea fina. Obtén una impresión o usa las muestras facilitadas por el docente; escanea una página propia y guarda original y versión editada. Compara legibilidad, orientación, tamaño y OCR si lo utilizas. Documenta un fallo, hipótesis y prueba. No desmontes mecanismos para fabricar una avería.

¿Lo has pillado?

1. ¿Una página interna demuestra que la cola del usuario funciona?

2. ¿Un cable USB-C garantiza salida de vídeo?

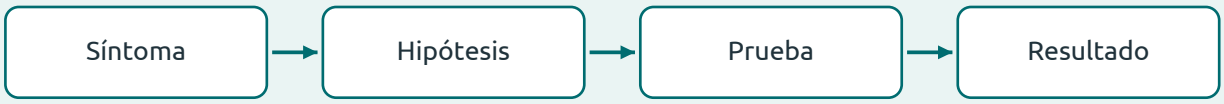
3. ¿Por qué hay que registrar una limpieza?

Soluciones. 1) No: aún falta probar la ruta desde su equipo y aplicación. 2) No: las capacidades dependen de todos los elementos. 3) Permite conocer lo realizado, comparar problemas y planificar mantenimiento.

14. Diagnosticar averías sin cambiar piezas al azar

Al terminar: construirás una secuencia de pruebas que separe síntoma, hipótesis y resultado.
Antes: conoce componentes, arranque y mantenimiento seguro.

UNA HIPÓTESIS DEBE PODER COMPROBARSE



¿La evidencia contradice la hipótesis? Revisa la explicación.

Si aplicas una solución: verifica la tarea original y documenta.

El diagnóstico convierte suposiciones en pruebas.

«No funciona» es el inicio de una conversación, no un diagnóstico. Pregunta qué ocurre, desde cuándo, qué cambió y qué parte sí funciona. Reproduce el síntoma cuando sea seguro. Anota el estado antes de intervenir.

Un método repetible

Describe el síntoma con precisión. Formula una hipótesis que pueda comprobarse. Elige una prueba con poco riesgo y que diferencie posibilidades. Aplica un cambio cada vez. Verifica la tarea original y documenta lo realizado. Si el resultado contradice tu hipótesis, actualízala en lugar de forzar la explicación.

Caso 1: no hay señales de encendido

Comprueba la toma y el cable por medios seguros, la conexión y el interruptor de la fuente si existe. En un equipo recién montado, revisa el panel frontal y las conexiones internas siguiendo el procedimiento sin alimentación. Una regleta apagada y una placa dañada producen síntomas parecidos, pero exigen actuaciones distintas.

No abras la fuente ni hagas puentes improvisados para probarla. Si no puedes verificar el suministro y el montaje con seguridad, deriva a una persona cualificada o utiliza el procedimiento y equipo de diagnóstico autorizados.

Caso 2: se enciende, pero no hay imagen

Comprueba pantalla encendida, entrada seleccionada y cable. Revisa que utilizas una salida válida para esa configuración. Observa códigos de diagnóstico. Si el procedimiento lo permite, comprueba el asiento de memoria y tarjetas con el equipo desconectado. No retires componentes con alimentación.

Una prueba con cable o pantalla conocidos como buenos puede aislar un tramo. «Conocido como bueno» significa comprobado, no simplemente nuevo. Cambiar simultáneamente cable, monitor y RAM impide saber qué resolvió el caso.

Caso 3: reinicios o apagados

Relaciona el momento con temperatura, carga, alimentación y cambios recientes. Consulta registros y herramientas de diagnóstico adecuadas. Las temperaturas deben compararse con límites del modelo. Si hay datos importantes y señales de fallo de almacenamiento, prioriza su protección antes de pruebas intensivas o reparaciones que escriban en el disco.

Un estado SMART sin alertas no garantiza que una unidad nunca vaya a fallar. Una alerta sí merece investigación. No prometas recuperar datos ni ejecutes herramientas destructivas sin comprender su efecto.

Caso 4: el equipo va lento

Observa uso de CPU, memoria, almacenamiento y red durante el síntoma. Distingue lentitud al arrancar, al abrir una aplicación o en una tarea concreta. Un equipo sin espacio libre necesita una investigación distinta a otro que espera una respuesta de red. Evita «limpiadores» que borran datos sin explicación.

Ejemplo completo: imagen ausente tras mover una torre

El monitor indica que no hay señal. Funciona con otro equipo y el cable está comprobado. Al inspeccionar las conexiones externas se descubre que el cable está en una salida de la placa que no ofrece vídeo con el procesador instalado. Se conecta a la tarjeta gráfica adecuada y aparece imagen.

La solución no es «mover el cable» como regla universal. El aprendizaje es verificar la ruta de vídeo de esa configuración. La comprobación final incluye arranque completo y resolución apropiada.

Vamos a probarlo: parte de intervención

Resuelve por escrito este caso: tras limpiar el escritorio, un equipo no navega; el resto sí, y sus aplicaciones locales funcionan. Redacta tres hipótesis y una prueba no destructiva para cada una. No presupongas que el fallo es de hardware: podría ser enlace, configuración o servicio.

Solución orientativa: comprobar enlace y conexiones; observar configuración IP sin cambiarla; contrastar resolución de nombres con conectividad hacia un destino autorizado. El orden depende de las observaciones. Una prueba debe explicar qué resultado apoya o descarta cada hipótesis.

¿Lo has pillado?

1. ¿Que un problema desaparezca al reiniciar demuestra su causa?

2. ¿Por qué comprobar un componente nuevo antes de usarlo como referencia?

3. ¿Cuándo termina una reparación?

Soluciones. 1) No: puede reiniciar estados y ocultar temporalmente el origen. 2) Nuevo no equivale a funcional ni compatible. 3) Cuando la tarea afectada funciona, se revisan efectos secundarios relevantes y queda documentado el resultado.

Caso de taller: el fallo vuelve después de la entrega

Un equipo se apaga durante una videollamada. Tras reiniciarlo, funciona durante diez minutos y se devuelve al usuario. Esa comprobación es demasiado breve si el fallo aparecía después de media hora de uso.

Recoger las condiciones. Anota duración aproximada, aplicaciones abiertas, conexión a alimentación y entorno. Pregunta si ocurre también con tareas locales. No atribuyas el caso a la cámara únicamente porque estaba encendida.

Elegir observaciones. Revisa ventilación, temperaturas según el modelo, alimentación y registros próximos al apagado. Una advertencia térmica es un indicio; una temperatura aparentemente normal después de enfriarse no describe lo que sucedía durante el fallo. Evita pruebas intensivas si hay señales de daño o riesgo.

Intervenir y verificar. Supongamos que se encuentra una obstrucción de ventilación y se corrige conforme al procedimiento del fabricante. Repite una carga representativa y segura durante un periodo adecuado, observa estabilidad y vuelve a probar la tarea del usuario. Documenta las condiciones: «funcionó una vez» aporta menos información que «se reprodujo la tarea, se supervisaron estos indicadores y no reapareció el apagado durante este intervalo».

Cerrar con honestidad. Si no reproduces el fallo, escríbelo. Puedes registrar comprobaciones correctas y recomendar seguimiento; no declares una causa demostrada que no has podido contrastar. Si reaparece, el registro anterior permite continuar la investigación en lugar de empezar de cero.

Bloque 3. Sistemas operativos monopuesto

15. Qué administra realmente un sistema operativo

Al terminar: relacionarás procesos, memoria, archivos, dispositivos y servicios con problemas observables. **Antes:** repasa los capítulos 05 y 07.



El escritorio es solo una de las interfaces del sistema.

Imagina que el navegador, el editor y el reproductor quieren utilizar el procesador, leer archivos y emitir sonido. El sistema operativo coordina el acceso a esos recursos, aplica reglas y proporciona interfaces a los programas. No es solo el escritorio que ves al iniciar sesión. Un servidor sin entorno gráfico también tiene sistema operativo.

Núcleo, espacio de usuario e interfaces

El **núcleo** o kernel realiza funciones centrales con privilegios especiales. Los programas ordinarios se ejecutan en un entorno más restringido y solicitan operaciones al sistema. Esa separación ayuda a evitar que una aplicación altere directamente la memoria de otra o controle cualquier dispositivo sin permiso.

La **interfaz gráfica** permite trabajar con ventanas. Una **shell** interpreta instrucciones. Un **terminal** ofrece una interfaz de entrada y salida para interactuar con una shell u otros programas. Puedes cambiar la interfaz sin cambiar todo el sistema operativo. Dos terminales de aspecto parecido pueden ejecutar lenguajes diferentes.

En Windows conviven distintas herramientas de línea de comandos, como PowerShell y el intérprete de comandos tradicional. En Linux hay diversas shells; los ejemplos de este manual identificarán Bash cuando utilicen su sintaxis. Copiar un comando entre ellas sin adaptarlo puede fallar.

Programa, proceso e hilo

Un programa es un conjunto de instrucciones y otros recursos. Un **proceso** es una instancia en ejecución con recursos y contexto propios. Abrir una aplicación puede crear varios procesos. Un **hilo** es una unidad de ejecución dentro de un proceso; los hilos de un proceso comparten parte de sus recursos.

El **planificador** decide qué trabajo utiliza el procesador. En un equipo con varias aplicaciones parece que todo sucede a la vez porque el sistema alterna o reparte la ejecución. El reparto debe atender prioridades y estados: un proceso que espera una lectura no necesita ocupar continuamente una CPU.

Un identificador de proceso, o **PID**, permite referirse a una instancia. Puede reutilizarse después de que termine. Antes de actuar sobre un PID, comprueba que sigue correspondiendo al programa que quieres gestionar.

Memoria y almacenamiento no son intercambiables

Cada proceso utiliza un espacio de direcciones. El sistema mantiene correspondencias entre direcciones y recursos de memoria, y puede trasladar determinadas páginas a almacenamiento de respaldo. La memoria virtual incluye más que el archivo de paginación: también proporciona abstracción y aislamiento.

Un uso alto de RAM no implica automáticamente un problema. Parte puede ser caché recuperable. Observa memoria disponible, actividad de paginación, tiempos de respuesta y carga. Del mismo modo, una CPU al 100 % durante un cálculo esperado no demuestra una avería; puede estar haciendo exactamente el trabajo solicitado.

Archivos, dispositivos y servicios

El sistema de archivos organiza nombres, contenido y metadatos. Los controladores permiten trabajar con dispositivos concretos. Los **servicios** realizan tareas en segundo plano, a menudo sin una ventana visible: impresión, registro o administración de red.

El estado de un servicio y su forma de inicio son datos distintos. Un servicio puede estar configurado para arrancar automáticamente y encontrarse detenido por un fallo. También puede estar detenido porque solo debe iniciarse bajo determinadas condiciones.

Ejemplo: la aplicación no responde

En Aula Norte una aplicación deja de aceptar clics, pero el reloj y otras ventanas siguen funcionando. La observación sugiere un problema localizado; no demuestra que el sistema completo esté bloqueado. Comprueba la aplicación, sus procesos y si espera un recurso externo. Forzar el cierre puede liberar la interfaz, pero pierde cambios pendientes y no identifica necesariamente la causa.

Vamos a probarlo: observar sin modificar

En Windows abre el Administrador de tareas; en Linux utiliza el monitor del sistema disponible. Anota la hora, abre un editor vacío y observa qué cambia. Después cierra el editor de forma normal. Identifica CPU, memoria y almacenamiento en las columnas disponibles. No finalices procesos desconocidos.

Resultado esperado: una ficha con al menos un proceso relacionado con una aplicación y una explicación de la diferencia entre el archivo del programa y su ejecución. Los valores concretos variarán entre equipos.

Recuperación: cierra las herramientas de observación. Si el editor pide guardar, cancela o descarta únicamente el documento ficticio que acabas de crear.

Del árbol de carpetas a las garantías del sistema de archivos

Una **ruta absoluta** parte de una raíz; una relativa depende del directorio actual. En Linux, `/` es la raíz del árbol, `/home` suele alojar datos personales, `/etc` configuración y `/var` datos variables como ciertos registros. La organización exacta depende de la distribución y del servicio. En Windows, una ruta como `C:\Users\Ana\Documents` parte de una unidad; el perfil y las carpetas conocidas pueden tener otra ubicación. No guardes tus documentos en directorios del sistema para evitar aprender a localizar tu perfil.

Un dispositivo, partición y punto de montaje son conceptos distintos. Un segundo sistema de archivos puede aparecer bajo un directorio del mismo árbol. Ver una carpeta no te dice en qué disco físico están sus datos. Consulta `lsblk -f` y `df -h` en el Linux de laboratorio, o Administración de discos y las propiedades del volumen en Windows, para relacionarlos sin modificar particiones.

Elegir formato. NTFS ofrece capacidades propias de Windows como sus ACL; ext4 es habitual en Linux; exFAT facilita ciertos intercambios entre sistemas compatibles; FAT32 conserva compatibilidad, pero tiene límites, entre ellos el tamaño de un archivo individual. Revisa soporte real de lectura/escritura, tamaño, permisos, recuperación y herramienta antes de formatear. No presupongas que cualquier formato conserva propietario y ACL al copiar entre sistemas.

Los **metadatos** describen el archivo y su organización: tamaño, fechas, atributos, permisos o referencias a sus bloques. Un sistema con **journal** registra operaciones para ayudar a recuperar coherencia tras ciertos fallos. En ext4 el alcance depende del modo: el comportamiento habitual protege operaciones de metadatos y no equivale a conservar todos los últimos cambios del contenido. Una transacción agrupa operaciones con garantías definidas; no convierte el sistema de archivos en una copia histórica completa. Sigue haciendo copias y apagando correctamente.

Fuente: documentación del kernel Linux, journal de ext4.

Práctica de rutas, atributos y compresión

En tu carpeta personal del invitado, crea una carpeta nueva `SMR-Archivos` con dos textos ficticios y una subcarpeta. Anota la ruta completa y la ruta relativa desde su carpeta padre. Muestra extensiones en el explorador y comprueba tamaño, fecha y permisos; un punto inicial en un nombre Linux o un atributo oculto en Windows no son un control de confidencialidad.

Selecciona la carpeta y crea un ZIP mediante la herramienta del sistema. Extrae en otra carpeta nueva y compara nombres, estructura, contenido y apertura. Un ZIP puede ocupar más que el original si los archivos son pequeños o ya están comprimidos; no inventes ahorro. Compresión de un archivo, cifrado y compresión transparente del sistema de archivos son funciones diferentes.

Por último, modifica solo el texto extraído y comprueba que el original y el ZIP anterior conservan su contenido. Entrega rutas, tamaños y una comparación. Recuperación: retira únicamente las carpetas propias del ensayo después de comprobar sus rutas. No cambies atributos de los archivos del sistema ni fuerces apagados para «probar el journal».

¿Lo has pillado?

1. ¿Un sistema sin escritorio carece de sistema operativo?

2. ¿Un PID identifica para siempre un programa?

3. ¿Un consumo alto de memoria justifica instalar un «limpiador» sin más pruebas?

Soluciones razonadas. 1) No: la interfaz gráfica es opcional en muchos sistemas. 2) No: identifica una instancia en un momento y puede reutilizarse. 3) No: hay que distinguir caché, presión de memoria y comportamiento real. Un cambio sin diagnóstico puede perjudicar el rendimiento.

16. Instalar con un plan y saber qué has instalado

Al terminar: prepararás una instalación reproducible y una comprobación posterior. **Antes:** capítulos 03, 07 y 12. **Entorno:** máquina virtual vacía o equipo de prácticas cuya modificación esté autorizada.

Instalar un sistema es preparar un entorno que pueda utilizarse, mantenerse y recuperarse. No termina al aparecer el escritorio. Faltan identificación de hardware, actualizaciones, cuentas, conectividad, aplicaciones necesarias y comprobaciones.

Define el destino antes de arrancar

Elige edición, versión, arquitectura y licencia o condiciones de uso. Comprueba el periodo de soporte en el momento de la práctica. «La última versión» deja de ser una instrucción reproducible: anota el nombre exacto y la fecha de descarga.

Windows 11 exige, entre otros requisitos, procesador compatible, al menos 4 GB de RAM y 64 GB de almacenamiento, firmware UEFI con capacidad de Secure Boot y TPM 2.0. Son mínimos, no una recomendación de comodidad. Los requisitos de conexión y cuenta durante la configuración dependen de la edición y el uso. Revisa la ficha oficial antes de preparar el invitado.

Fuente para comprobar requisitos: Microsoft, «Windows 11 specifications», https://www.microsoft.com/en-us/windows/windows-11-specifications. Consulta editorial: 5 de noviembre de 2026.

Para Linux selecciona una distribución mantenida y consulta sus requisitos e instrucciones. Los procedimientos de paquetes de este libro se orientan a Ubuntu con APT; no se aplican literalmente a todas las distribuciones. Anota si instalas escritorio o servidor.

Descarga, integridad y arranque

Descarga la imagen de la fuente oficial. Una suma criptográfica publicada permite comparar el archivo descargado con el valor esperado. La comprobación de una firma, cuando se ofrece, añade verificación de procedencia si las claves se obtienen y validan adecuadamente. No es suficiente comparar con una suma recibida del mismo origen desconocido que la descarga.

En una máquina virtual puedes adjuntar la imagen al lector virtual. Al preparar un USB físico, la herramienta puede borrar su contenido: identifica por capacidad y dispositivo, no por una letra que recuerdas de otra sesión. Mantén desconectados los soportes que no necesites.

Particionado y decisiones que conviene entender

En una instalación limpia sobre una máquina virtual nueva, el instalador suele poder crear automáticamente las particiones necesarias. Revisa antes el disco de destino. En un equipo con datos, no elimines particiones para «hacer sitio» sin conocer su función y disponer de recuperación.

El arranque UEFI, las particiones de sistema y el sistema de archivos son decisiones relacionadas, pero distintas. Un esquema Linux puede usar una partición raíz y otras opcionales. Windows puede crear particiones de sistema y recuperación además de la principal. El número y tamaño exactos dependen del entorno y de la versión.

El **cifrado** protege la confidencialidad de datos en reposo bajo condiciones concretas. Requiere gestionar claves y recuperación: perder la contraseña o clave necesaria puede impedir recuperar los datos. No actives cifrado en una práctica sin documentar cómo recuperarás el acceso.

Práctica guiada: una instalación limpia de laboratorio

1. Crea una ficha con imagen, arquitectura, edición, recursos del invitado, firmware y disco virtual nuevo. Comprueba que no has adjuntado un disco físico con documentos.
2. Inicia desde la imagen y elige idioma, teclado y zona horaria. Selecciona el disco virtual vacío. Si el estado no coincide con tu ficha, cancela y revisa.
3. Completa las decisiones de almacenamiento según el instalador y el plan. Crea las cuentas necesarias con credenciales de laboratorio que no reutilices fuera de él.
4. Reinicia hacia el sistema instalado. Retira la imagen del orden de arranque si vuelve a iniciar el instalador.
5. Comprueba nombre del equipo, fecha, versión, dispositivos, conectividad y espacio. Instala actualizaciones por el mecanismo oficial y reinicia si procede.
6. Instala una aplicación sencilla permitida y prueba una tarea completa: crear, guardar y volver a abrir un documento ficticio.
7. Apaga correctamente y vuelve a iniciar. Documenta el resultado y crea una base de recuperación conforme al capítulo 20.

Resultado esperado: el sistema arranca desde su unidad, muestra versión identificable, puede guardar y recuperar el documento y no presenta dispositivos necesarios sin atender. No basta con fotografiar la pantalla de bienvenida.

Recuperación: al trabajar solo sobre un invitado nuevo, puedes apagarlo y recrearlo desde cero. Antes de eliminarlo, confirma que sus discos no contienen evidencias o datos que quieras conservar.

SOS: el instalador no detecta la unidad

Comprueba primero que existe y está adjuntada al invitado. Después revisa el tipo de controlador virtual y su compatibilidad con el instalador. En hardware físico podría faltar un controlador o existir una configuración específica del almacenamiento. No cambies modos de controladora a ciegas en un equipo con un sistema ya instalado.

¿Lo has pillado?

1. ¿Cumplir el mínimo de RAM garantiza comodidad con varias aplicaciones?

2. ¿Por qué comprobar el disco aunque esté seleccionado «el primero»?

3. ¿En qué se diferencia una instalación limpia de una actualización?

Soluciones. 1) No: depende de la carga y otros recursos. 2) El orden puede cambiar y «primero» no identifica su contenido. 3) La limpia crea un entorno nuevo en el destino elegido; una actualización intenta mantener o migrar componentes y datos existentes según el procedimiento. Ambas requieren preparación y copia cuando haya datos relevantes.

17. Usuarios, grupos y permisos: quién puede hacer qué

Al terminar: interpretarás permisos básicos de Linux y distinguirás cuenta estándar, elevación y permisos de Windows. **Antes:** archivos, rutas y funciones del sistema.

PERMISOS TRADICIONALES DE LINUX

Propietario	Grupo	Otros
r w -	r - -	- - -
6	4	0

640: lectura/escritura · lectura · sin permisos tradicionales

Lectura vale 4, escritura 2 y ejecución 1 en cada categoría.

Una **cuenta** representa una identidad. La **autenticación** comprueba la identidad presentada; la **autorización** decide qué acciones puede realizar. Saber una contraseña válida no implica poder modificar cualquier archivo.

Los **grupos** permiten asignar permisos a conjuntos de cuentas. Si una persona cambia de función, ajustar su pertenencia puede resultar más claro que revisar permisos concedidos directamente en muchas carpetas. También existen cuentas de servicio que no representan a una persona que inicia sesión en el escritorio.

Administrar no exige trabajar siempre como administrador



Consejo de David

Utiliza una cuenta ordinaria para tareas cotidianas. La elevación concede privilegios para una acción cuando corresponde. En Windows, UAC participa en ese proceso; un aviso no demuestra que el programa sea seguro. Comprueba qué solicita privilegios y por qué.

En Ubuntu es habitual que una cuenta autorizada utilice `sudo` para ejecutar acciones concretas. El superusuario de Linux se llama `root`. No es necesario iniciar toda la sesión como root para leer documentos. La contraseña que solicita `sudo` en su configuración habitual es la de la cuenta autorizada que está actuando, no una contraseña universal del sistema.

La administración de cuentas locales no equivale a administrar identidades de un dominio: ese tema llegará en sistemas en red. Tampoco debes editar manualmente archivos internos de cuentas para una práctica inicial. Ubuntu documenta el uso de herramientas de gestión como `adduser`.

Fuente: documentación de Ubuntu, «User management», https://ubuntu.com/server/docs/how-to/security/user-management/.

Linux: propietario, grupo y otros

En los permisos tradicionales se distinguen propietario, grupo propietario y otros usuarios. `r` permite lectura, `w` escritura y `x` ejecución o recorrido, según se trate de un archivo o un directorio. Con `ls -l` puedes observar una representación como `-rw-r-----`: archivo ordinario, propietario con lectura y escritura, grupo con lectura y otros sin esos permisos.

Para obtener el número se suman 4 por lectura, 2 por escritura y 1 por ejecución. Por tanto, 6 significa lectura y escritura; 5 lectura y ejecución; 0 ninguna de esas tres. `640` describe los permisos del ejemplo. El primer carácter de la salida de `ls` representa el tipo y no forma parte de los nueve bits habituales mostrados después.

En un **directorio**, lectura permite listar nombres; ejecución permite recorrerlo y acceder a entradas conocidas cuando los demás permisos lo permitan. Escritura, normalmente junto con ejecución, permite crear o eliminar entradas. Poder escribir un archivo y poder eliminar su nombre del directorio son cuestiones distintas. También existen ACL, bits especiales y otros controles que pueden modificar el análisis.

Ejemplo seguro sobre un archivo propio

En Bash, dentro de una carpeta nueva de prácticas, crea un texto ficticio y limita sus permisos. No utilices estos comandos sobre carpetas del sistema ni sobre documentos compartidos.

BASH

```
mkdir smr-permisos-demo
cd smr-permisos-demo
printf 'Informe ficticio\n' > informe.txt
chmod 640 informe.txt
ls -l informe.txt
```

La salida debe mostrar lectura y escritura para el propietario, lectura para el grupo y ningún permiso tradicional para otros. El nombre de usuario, grupo y fecha variará. El usuario propietario aún puede leer y modificar el archivo. No has comprobado el acceso de otro usuario hasta probar con su identidad y considerar los permisos de todos los directorios de la ruta.

Para volver al permiso anterior, necesitas haberlo registrado. En este ejemplo el archivo es nuevo: puedes conservarlo como evidencia y, al terminar, borrar únicamente esa carpeta ficticia tras confirmar su ubicación. No apliques cambios recursivos para corregir un único archivo.

Windows: listas de control de acceso

En NTFS, las **ACL** contienen entradas que conceden o deniegan derechos a identidades. Los permisos pueden heredarse de carpetas superiores. Lectura, modificación y control total son conjuntos de derechos distintos. Control total suele incluir capacidad de cambiar permisos; no debe concederse solo para permitir editar un documento.

En la interfaz de seguridad de una carpeta puedes consultar identidades, herencia y permisos. La disponibilidad de herramientas depende de edición y entorno. Una denegación y pertenencias múltiples requieren revisar el acceso efectivo, no aplicar una regla simplista sin mirar las entradas. En carpetas compartidas se añaden permisos de compartición, tema del capítulo 30.

Práctica: separar cuentas y datos

En un invitado de laboratorio, crea por el mecanismo de administración del sistema una cuenta estándar ficticia para un alumno. Guarda un documento en su carpeta personal y comprueba desde esa sesión que puede modificarlo. Observa después una operación que necesita administración sin aceptarla. Registra qué cuenta y qué operación intervienen.

Resultado esperado: la cuenta realiza su trabajo ordinario y no se convierte en administradora para evitar un mensaje. Para retirar la cuenta, decide primero qué hacer con sus archivos y conserva la evidencia necesaria. Haz la eliminación solo en el invitado preparado para ello.

SOS: acceso denegado

Comprueba identidad real, ruta exacta, permisos del archivo y directorios superiores, herencia y posibles controles adicionales. No uses `chmod 777` ni concedas control total a todos como solución universal: amplía el acceso y puede ocultar el error de diseño.

¿Lo has pillado?

1. ¿Qué representa 750 en permisos tradicionales de Linux?

2. ¿Un usuario que puede leer un archivo puede necesariamente borrarlo?

3. ¿Crear una cuenta con el mismo nombre garantiza recuperar todos sus permisos anteriores?

Soluciones. 1) Propietario: lectura, escritura y ejecución; grupo: lectura y ejecución; otros: ningún permiso de esos tres. 2) No: la eliminación depende del directorio y de otros controles. 3) No: los sistemas usan identificadores internos; el nombre visible no basta. Debe revisarse la identidad y la propiedad real.

18. Terminal desde cero: entiende cada línea

Al terminar: crearás y consultarás archivos de práctica y distinguirás instrucciones de resultados. **Antes:** rutas absolutas y relativas. **Entorno:** Bash en Linux o PowerShell en Windows, sin elevación.

Una instrucción suele contener nombre de comando, opciones o parámetros y argumentos. En `mkdir practicas`, `mkdir` indica la acción y `practicas` el nombre. Las opciones cambian el comportamiento. Su sintaxis depende de la herramienta: no todos los comandos admiten las mismas abreviaturas.

Antes de pegar una instrucción

Comprueba qué shell estás utilizando, en qué directorio estás y qué datos modifica la línea. No copies el indicador del terminal: `$`, `PS>` y otros textos pueden ser parte del ejemplo visual, no del comando. Los bloques de este manual contienen solo lo que debes escribir.

Ejecuta línea a línea. Un salto de línea puede separar acciones; un carácter de continuación puede unirlas. Si una línea no funciona, conserva el mensaje completo antes de añadir otras.

Laboratorio A: Bash

Abre un directorio de trabajo autorizado. El nombre siguiente debe estar libre; si ya existe, elige otro y úsalo coherentemente. Empieza preguntando dónde estás y qué contiene el lugar.

BASH

```
pwd
ls
mkdir smr-terminal-demo
cd smr-terminal-demo
printf 'Primera prueba\n' > nota.txt
cat nota.txt
cp nota.txt copia.txt
ls -l
```

`pwd` muestra el directorio actual. `ls` lista entradas. `mkdir` crea una carpeta y `cd` cambia el directorio de la shell. `printf` produce texto y `>` dirige la salida a un archivo: puede sobrescribir su contenido si ya existe. `cat` lee el archivo y `cp` crea una copia en la ubicación elegida. `ls -l` presenta información ampliada.

Resultado esperado: aparecen `nota.txt` y `copia.txt`, y leer cualquiera devuelve `Primera prueba`. La hora y los permisos pueden variar.

Laboratorio B: PowerShell

Utiliza una sesión sin elevación y una carpeta en la que puedas crear archivos. En PowerShell, los cmdlets suelen tener nombres verbo-sustantivo y parámetros con un guion. Aunque algunos alias recuerden a Unix, no garantizan la misma sintaxis.

POWERSHELL

```
Get-Location
Get-ChildItem
New-Item -ItemType Directory -Path smr-terminal-demo
Set-Location smr-terminal-demo
Set-Content -Path nota.txt -Value 'Primera prueba'
Get-Content -Path nota.txt
Copy-Item -Path nota.txt -Destination copia.txt
Get-ChildItem
```

`Set-Content` escribe el contenido indicado y puede reemplazar el anterior. `Get-Content` lo lee; en su funcionamiento habitual devuelve las líneas como elementos. La codificación predeterminada puede variar entre versiones de PowerShell: regístrala si vas a intercambiar archivos o comparar bytes.

Fuente de consulta: Microsoft Learn, «Get-Content», https://learn.microsoft.com/powershell/module/microsoft.powershell.management/get-content. Para parámetros y comportamiento exacto, utiliza la documentación de tu versión.

Buscar ayuda y encontrar un error

En Linux, `man ls` abre el manual cuando está instalado; normalmente puedes salir con `q`. Muchas herramientas admiten `--help`, pero compruébalo. En PowerShell utiliza `Get-Help Get-Content` y consulta `Get-Command` para localizar comandos. La ayuda disponible localmente puede necesitar actualización autorizada.

«No se reconoce el comando» sugiere revisar nombre, shell, instalación y búsqueda en PATH. «No existe el archivo» apunta a ruta, nombre y directorio actual. «Acceso denegado» requiere analizar permisos. No respondas a cualquier mensaje añadiendo privilegios.

Tuberías: no transportan siempre lo mismo

Una tubería conecta la salida de una operación con la entrada de otra. En una shell Unix muchas herramientas intercambian flujos de bytes que suelen representar texto. PowerShell trabaja habitualmente con objetos cuando conecta cmdlets; los programas externos introducen matices. Entender esa diferencia evita copiar filtros de una shell a otra sin adaptación.

Ejemplo Bash: `cat nota.txt | wc -l` cuenta líneas terminadas con salto de línea. En este ejemplo existe una. Puede hacerse sin la tubería mediante `wc -l < nota.txt`; el símbolo `<` entrega el archivo como entrada. En PowerShell, `Get-Content nota.txt | Measure-Object -Line` mide las líneas de texto devueltas. No confíes en que ambas herramientas cuenten igual todos los archivos vacíos o sin salto final.

Práctica con una variación

Añade una segunda línea al archivo original. En Bash usa `printf 'Segunda prueba\n' >> nota.txt`; `>>` añade al final. En PowerShell usa `Add-Content -Path nota.txt -Value 'Segunda prueba'`. Lee original y copia. La copia conserva el estado anterior porque copiar no creó una sincronización automática.

Resultado esperado: original con dos líneas y copia con una. Para recuperar la prueba inicial, puedes copiar el archivo de copia sobre el original después de confirmar que ambos son los ficticios correctos. Eso reemplaza la modificación: explica por qué es adecuado solo en esta práctica.

¿Lo has pillado?

1. ¿`>` añade siempre al final?

2. ¿`cd` cambia el contenido de un archivo?

3. ¿Un comando que funciona en Bash funciona necesariamente en PowerShell?

4. ¿Por qué comprobar la ubicación antes de copiar sobre un archivo existente?

Soluciones. 1) No: normalmente redirige reemplazando; `>>` añade en las shells descritas. 2) No: cambia el directorio de trabajo. 3) No: lenguaje y herramientas difieren. 4) Porque una ruta relativa se interpreta desde el directorio actual y podrías sobrescribir otro archivo.

19. Mantener el sistema con evidencias

Al terminar: diferenciarás actualización, instalación, proceso, servicio, registro y tarea programada. **Antes:** cuentas, privilegios y terminal.

El mantenimiento reúne acciones periódicas y respuestas a problemas. Debe tener un objetivo, una ventana adecuada, una recuperación prevista y una comprobación. Instalar todas las herramientas que encuentras no es un plan de mantenimiento.

Software y repositorios

Un **paquete** reúne software y metadatos para su instalación. Una **dependencia** es un componente necesario para que otro funcione. Un **repositorio** distribuye paquetes e información. La firma y el origen ayudan a decidir en qué confiar, pero no convierten cualquier paquete en apropiado para tu sistema.

En Ubuntu y sistemas relacionados, APT permite consultar e instalar paquetes de repositorios configurados. Otros sistemas utilizan gestores diferentes. No añadas repositorios desconocidos para resolver el primer error: estás modificando las fuentes de software del equipo.

Para consultar sin cambiar nada puedes usar `apt list --installed` o `apt show nombre-del-paquete`, sustituyendo el nombre por uno real que quieras examinar. No escribas literalmente ese nombre descriptivo esperando un paquete del manual.

`sudo apt update` actualiza la información de paquetes disponibles; no equivale a actualizar todos los programas. `sudo apt upgrade` propone aplicar actualizaciones y puede modificar paquetes y dependencias según las reglas de la herramienta. Lee el resumen antes de aceptar y revisa si se requieren reinicios. Estas acciones necesitan conectividad, permisos y un entorno preparado.

Fuente: Ubuntu, «Install and manage packages», https://ubuntu.com/server/docs/how-to/software/package-management/. La organización de las fuentes puede variar según la versión; no sobrescribas archivos de configuración copiando instrucciones de otra edición.

Mantenimiento en Windows

Utiliza Windows Update y los mecanismos oficiales de actualización de aplicaciones. Identifica qué requiere reinicio y acuerda cuándo se realizará si el equipo está en uso. Un controlador procede del fabricante del dispositivo o del canal oficial correspondiente, no de un sitio que promete arreglar cualquier driver.

Anota versión antes y después si investigas un cambio. Actualizar el sistema, una aplicación y el firmware al mismo tiempo puede ser necesario en un plan, pero dificulta atribuir después un fallo a una causa. Registra el conjunto de cambios y prepara recuperación.

Observar procesos y servicios

En Linux, `ps` muestra información de procesos según sus opciones; `top` proporciona una vista interactiva si está instalado. En sistemas que utilizan systemd, `systemctl status nombre.service` consulta un servicio concreto. Sustituye el nombre por el servicio real de tu equipo. No todos los sistemas Linux utilizan systemd.

En PowerShell puedes consultar procesos con `Get-Process` y servicios con `Get-Service`. Detener un proceso no es equivalente a detener un servicio de forma ordenada. Puede haber dependencias, pérdida de trabajo y recuperación automática.

Registros: contexto antes de conclusiones

Un registro recoge eventos. Busca la hora del síntoma, la fuente, el mensaje y los eventos relacionados. Un evento clasificado como error puede no explicar el problema que investigas. Un identificador aislado encontrado en Internet no demuestra una causa.

En Windows utiliza el Visor de eventos y los registros de la aplicación. En Linux con systemd, `journalctl -b` consulta eventos del arranque actual; el acceso y la cantidad de información dependen de los permisos y la configuración. No publiques registros completos sin revisar datos personales, nombres internos y secretos.

Tareas programadas

Una tarea necesita acción, calendario, identidad, permisos y condiciones. Debe registrar si terminó bien. Si funciona manualmente y falla programada, compara cuenta, directorio de trabajo, variables, acceso a red y disponibilidad de archivos.

Windows ofrece el Programador de tareas. En Linux pueden emplearse cron o temporizadores de systemd. Los formatos y reglas varían; documenta zona horaria y comportamiento cuando el equipo está apagado. Programar una copia no demuestra que la copia sea recuperable.

Práctica: ficha de salud del invitado

Registra espacio libre, versión, actualizaciones pendientes y un proceso observado. Elige un servicio instalado y consulta su estado sin detenerlo. Localiza un evento de la sesión actual y explica qué dice y qué no permite concluir. Revisa una tarea existente sin modificarla o prepara en papel una tarea ficticia que escriba la fecha en un archivo de laboratorio.

Resultado esperado: una ficha con observaciones fechadas y acciones propuestas justificadas. Si aplicas una actualización en el invitado, verifica después arranque, red y aplicación de prueba. Conserva una base de recuperación y no interrumpas el gestor de paquetes durante una operación.

SOS: falta espacio

Comprueba qué volumen está lleno y qué datos ocupan espacio. Vaciar una papelera o retirar archivos temporales mediante las herramientas adecuadas puede ayudar. No borres directorios del sistema o cachés internas sin saber cómo se gestionan. Un disco virtual que crece dinámicamente puede agotar el anfitrión aunque el invitado todavía muestre espacio lógico disponible.

¿Lo has pillado?

1. ¿`apt update` instala todas las versiones nuevas?

2. ¿Un servicio configurado como automático está necesariamente funcionando?

3. ¿Por qué una tarea debe usar rutas explícitas?

Soluciones. 1) No: actualiza la información de paquetes. 2) No: puede haber fallado o estar condicionado por su diseño. 3) Su contexto puede diferir del interactivo; una ruta relativa puede resolver hacia otro lugar o no existir.

20. Virtualización y recuperación: volver atrás con criterio

Al terminar: elegirás entre instantánea, copia de archivos, imagen y reinstalación. **Antes:** laboratorio, almacenamiento y cuentas.

ELIGE SEGÚN LO QUE QUIERES RECUPERAR

Instantánea	Copia de archivos	Imagen
Estado del invitado	Datos seleccionados	Volumen o sistema

Ninguna opción sustituye comprobar la restauración y su alcance.

La elección depende del alcance de la recuperación.

La virtualización permite que uno o varios invitados compartan recursos del anfitrión mediante un **hipervisor**. No crea capacidad física: si asignas más de lo disponible o saturas el almacenamiento, todos pueden sufrir. Además de CPU y RAM, considera espacio de imágenes, instantáneas y copias.

Qué virtualizas y con qué límites

Hay hipervisores integrados directamente en una plataforma de virtualización y otros utilizados como aplicaciones del sistema anfitrión. Las clasificaciones ayudan, pero para trabajar debes conocer el producto concreto: dispositivos virtuales, modos de red, compatibilidad y formatos.



Ojo con este error

Una máquina virtual no garantiza aislamiento perfecto. Carpetas compartidas, portapapeles, dispositivos USB y redes puente crean vías de intercambio. Activa solo lo que necesita la práctica. Un invitado con un servicio vulnerable no debe exponerse innecesariamente a la red física.

Una **clonación** crea otra instancia a partir de un estado. Debe revisarse identidad de equipo, direcciones y otros identificadores. Dos clones con el mismo nombre o dirección fija pueden causar conflictos. Copiar archivos de una máquina encendida sin el procedimiento apropiado puede producir una copia incoherente.

Cuatro herramientas, cuatro objetivos

Una **instantánea** permite volver a un estado dentro del mecanismo del hipervisor. Puede incluir o no memoria y depender de discos base. Es útil antes de experimentar, pero no es una copia independiente.

Una **copia de archivos** protege datos seleccionados. Debe incluir lo necesario, conservar metadatos cuando importen y tener una restauración comprobada. Copiar documentos no preserva por sí solo toda la configuración de una aplicación.

Una **imagen** representa un conjunto más amplio, como un volumen o un sistema, según la herramienta. Su restauración puede reemplazar el destino y exige compatibilidad, almacenamiento y medios de recuperación.

Una **reinstalación** reconstruye el sistema. Necesita instaladores, licencias, configuraciones y datos recuperables. Si solo conocías una contraseña guardada dentro del sistema perdido, la reinstalación no resuelve ese secreto.

El procedimiento empieza antes del fallo

Define qué puedes perder y cuánto tiempo puede tardar la recuperación. Identifica datos, configuraciones y dependencias. Realiza una copia y una prueba en un destino separado. Si hay cifrado, conserva de forma protegida las claves necesarias y prueba el proceso autorizado de recuperación.

Un plan que dice «restaurar la copia» está incompleto si nadie sabe dónde está, quién puede acceder o si hace falta un programa que solo estaba instalado en el equipo averiado.

Práctica A: recuperar un documento ficticio

1. Crea una carpeta de trabajo y otra de copia de laboratorio. Guarda un documento con la frase «versión inicial».
2. Copia el documento y comprueba que la copia se abre. Registra tamaño, fecha y, si utilizas una herramienta de hash, su resultado.
3. Modifica el documento de trabajo a «versión modificada». Confirma que la copia sigue conservando la inicial.
4. Restaura primero en una tercera carpeta, sin sobrescribir el trabajo. Abre el restaurado y compara.
5. Documenta qué recuperaste y qué cambios posteriores a la copia no están incluidos.

Resultado esperado: el restaurado contiene la versión inicial. Esta práctica demuestra recuperación lógica de un archivo, no resistencia ante un fallo físico si todas las carpetas están en el mismo disco. Para protegerte frente a ese fallo necesitas una ubicación independiente adecuada.

Práctica B: una instantánea de laboratorio

Con un invitado apagado y sin discos físicos compartidos, crea una instantánea según el hipervisor. Inicia y añade un archivo ficticio claramente identificado. Apaga y restaura la instantánea conforme al procedimiento. Antes de confirmar, comprueba qué se perderá y si otros discos o carpetas compartidas quedan fuera del alcance.

Resultado esperado: el invitado vuelve al estado registrado para los recursos incluidos; el archivo creado después no estará en ese estado restaurado. Si estaba en una carpeta del anfitrión, puede seguir existiendo: demuestra por qué hay que conocer el alcance.

Recuperación del ejercicio: conserva el punto base y retira las instantáneas solo con el procedimiento del producto. «Eliminar instantánea» no significa siempre «volver a ella»: puede consolidar cambios. Lee la acción que vas a ejecutar.

SOS: la copia existe, pero no se abre

Comprueba integridad, contraseña, permisos, herramienta y versión, y si faltan partes o discos base. No modifiques tu única copia para intentar repararla: trabaja sobre un duplicado cuando sea posible. Registra el mensaje exacto y evita sobrescribir el original al restaurar.

Taller guiado: una imagen que realmente se pueda restaurar



El disco fuente, el repositorio de imagen y el destino son papeles distintos.

Utiliza una **VM desechable** con Linux y discos virtuales dedicados. La restauración sobrescribirá el disco de destino de la práctica. El host y sus discos físicos no se añaden como dispositivos a esta VM. Necesitas una imagen de arranque de Clonezilla Live obtenida de su proyecto y espacio suficiente para almacenar la imagen del sistema.

Prepara un disco virtual de sistema, otro de repositorio y, posteriormente, un destino vacío de capacidad igual o mayor que el original para simplificar. Los tamaños y nombres dependen del hipervisor. Registra identificadores y capacidades; `sda` o `sdb` pueden variar al cambiar el orden de conexión. Crea en el invitado un archivo marcador ficticio y anota su contenido o hash antes de apagar.

1. Arranca la VM desde Clonezilla Live. Elige idioma/teclado y el modo de trabajo con **imagen de dispositivo**, `device-image`.
2. Selecciona repositorio local, `local_dev`, e identifica el disco/partición destinado a imágenes. Verifica que no es el disco fuente. El repositorio necesita un sistema de archivos compatible y espacio libre adecuado.

3. Elige guardar el disco, `savedisk`, indica un nombre reconocible e identifica el **disco fuente** por datos registrados. Revisa los avisos y las opciones de comprobación; no fuerces un sistema de archivos con errores sin investigar.

4. Finaliza la imagen, conserva registros y utiliza la verificación de integridad disponible. Apaga correctamente y guarda evidencia de qué se ha incluido.

5. Para ensayar recuperación, retira de la VM el disco original conservándolo intacto y añade un destino virtual vacío. Mantén el repositorio y el mismo modo de firmware para este primer ensayo.

6. Arranca otra vez desde Clonezilla; selecciona el repositorio, `device-image` y **restaurar disco**, `restoredisk`. Comprueba imagen y destino, que perderá su contenido, antes de confirmar.

7. Termina, retira el medio de arranque y prueba el sistema restaurado. Comprueba inicio, archivo marcador, aplicaciones necesarias y estado relevante. Una verificación interna de imagen no sustituye esta prueba funcional.

Resultado esperado: una VM arranca desde el disco restaurado y conserva el marcador previo. Registra tamaño, firmware, herramienta y opciones, duración, resultados y límites. Si falla, el disco original permanece disponible como base de investigación. No conviertas su conservación en una copia independiente del host físico.

Una **instalación limpia** ejecuta la instalación prevista; una **preinstalación** prepara software/configuración antes de entregar; una **imagen** captura un estado para un uso definido. Distribuir imágenes a varios equipos exige identidad, controladores, licencia y preparación adecuadas. En Windows se requiere su procedimiento de generalización cuando corresponda; copiar un controlador de dominio no se trata como clonar un PC cualquiera.

Cifrado, arranque, sistemas de archivos, arquitectura y cambios de tamaño pueden imponer requisitos adicionales. Este taller usa un Linux de prácticas y destino no menor para aislar variables. No sirve como receta universal para cualquier disco o sistema cifrado.

Fuentes oficiales: guardar una imagen con Clonezilla y restaurarla. Procedimiento contrastado documentalmente; no se ha ejecutado Clonezilla en una VM del entorno editorial.

¿Lo has pillado?

1. ¿Una carpeta de copia en el mismo SSD cubre su avería física?

2. ¿Restaurar una instantánea revierte necesariamente una carpeta compartida del anfitrión?

3. ¿Una restauración que no muestra errores demuestra que el usuario puede trabajar?

Soluciones. 1) No: comparte el punto de fallo. 2) No: depende del alcance y normalmente esa carpeta no forma parte del disco del invitado. 3) No: hay que abrir datos, comprobar permisos y probar las tareas necesarias.

Bloque 4. Redes locales que puedes entender

21. Las piezas de la red y el mapa que las une

Al terminar: distinguirás funciones de tarjeta, switch, router y punto de acceso, y dibujarás un plano lógico. **Antes:** capítulo 08.

Una red no empieza en la pantalla de configuración IP. Empieza en unas necesidades: qué equipos deben comunicarse, con qué servicios, desde dónde y con qué disponibilidad. El diseño físico explica cables, ubicaciones y conexiones. El diseño lógico explica redes, direcciones, segmentos y circulación del tráfico.

Una función por vez

La **interfaz de red** conecta un equipo a un medio o enlace. Puede ser física o virtual. Un ordenador con Ethernet, wifi y varios adaptadores virtuales tiene varias interfaces: «la IP del ordenador» puede referirse a distintas direcciones según el camino.

Un **switch Ethernet** conmuta tramas dentro de una red de enlace. Aprende direcciones MAC de origen y puertos, y utiliza su tabla para decidir dónde enviar determinadas tramas. Si desconoce el destino, puede inundar la trama por los puertos pertinentes del mismo dominio de difusión, salvo el de entrada. No guarda una lista universal de todas las IP de Internet.

Un **router** encamina paquetes entre redes IP según sus rutas. Un **punto de acceso** permite que estaciones inalámbricas participen en una red. Un aparato doméstico puede reunir router, switch, punto de acceso, servidor DHCP y otras funciones. Que estén en la misma caja no las hace equivalentes.

MAC, IP y alcance

La dirección **MAC** se utiliza en comunicaciones de enlace como Ethernet. Una **IP** se utiliza para el encaminamiento a nivel de red. Las MAC no tienen por qué permanecer invariables: existen direcciones administradas localmente y mecanismos de aleatorización. No las utilices como prueba infalible de identidad de una persona.

Dentro de un enlace Ethernet, la trama lleva direcciones de origen y destino. Cuando el paquete pasa por un router, se construye una trama para el siguiente enlace. La IP de destino del paquete normalmente sigue identificando el destino final, salvo transformaciones como NAT. La MAC de destino del primer salto no tiene por qué ser la del servidor remoto.

Topología, segmentos y VLAN

Una topología física en estrella conecta equipos a un punto central, habitualmente un switch. Su ventaja es que el fallo de un cable de acceso no suele cortar todos los demás; el equipo central puede seguir siendo un punto de fallo importante.

Una **VLAN** separa lógicamente dominios de difusión en una infraestructura compatible. Un puerto de acceso suele transportar la VLAN asignada para un equipo; un enlace configurado como troncal puede transportar varias con etiquetado según su configuración. La comunicación entre VLAN requiere encaminamiento y políticas. Crear VLAN no garantiza por sí solo una política de seguridad correcta.

En Aula Norte separaremos, cuando el proyecto lo permita, administración, aula e invitados. La red de invitados necesita llegar a Internet sin acceso a las carpetas administrativas. Eso exige reglas además de nombres distintos para las redes wifi.

Práctica: inventario y plano

Dibuja tres equipos, una impresora, un switch y un router. Numera conexiones y asigna identificadores a dispositivos. Marca qué elemento permite compartir un enlace y cuál comunica redes distintas. Añade una versión física con ubicaciones y otra lógica con segmentos. No incluyas contraseñas en el plano.

Resultado esperado: otra persona puede seguir el camino equipo switch router y localizar el puerto correspondiente a la impresora. Para un laboratorio virtual, sustituye cables por conexiones virtuales e indica el modo de cada red.

SOS: dos cables para «tener más velocidad»

No conectes enlaces duplicados entre switches sin un diseño apropiado. Un bucle de capa de enlace puede producir tráfico excesivo y degradar la red. Las funciones de prevención de bucles y agregación requieren soporte y configuración compatibles. Añadir cables no duplica automáticamente el rendimiento.

¿Lo has pillado?

1. ¿Un punto de acceso es siempre el router de salida?

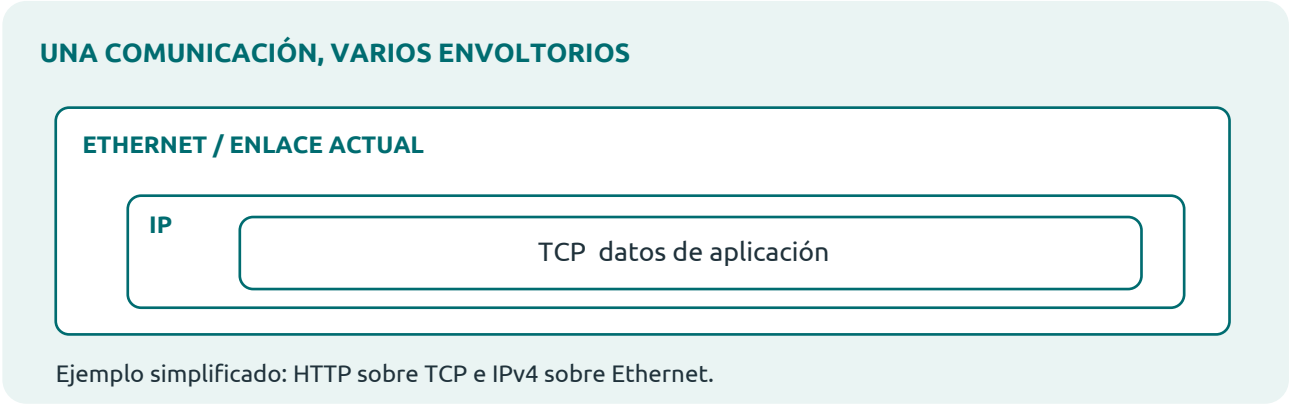
2. ¿Una MAC identifica siempre a la misma persona?

3. ¿Una VLAN permite comunicación con otra sin router o función de encaminamiento?

Soluciones. 1) No: conecta estaciones inalámbricas; el encaminamiento puede estar en otro dispositivo. 2) No: es un dato de interfaz y puede cambiar o suplantarse. 3) No en el funcionamiento IP ordinario entre subredes distintas: hace falta un camino de capa de red y reglas que lo permitan.

22. OSI y TCP/IP: modelos para localizar problemas

Al terminar: explicarás encapsulación y usarás las capas para ordenar pruebas. **Antes:** interfaces, switch y router.



Cada envoltorio sirve a una función concreta.

Un modelo divide una comunicación compleja en funciones. No es una obligación de que cada programa contenga siete piezas visibles. El modelo **OSI** utiliza siete capas; el modelo **TCP/IP** suele presentarse con cuatro, aunque hay materiales docentes que separan la parte física y muestran cinco.

Las siete funciones del modelo OSI

Física: señales y medios. **Enlace:** comunicación de tramas en un enlace. **Red:** direcciones y encaminamiento entre redes. **Transporte:** comunicación entre extremos mediante protocolos como TCP o UDP. **Sesión:** organización del diálogo. **Presentación:** representación de datos. **Aplicación:** funciones próximas a servicios usados por las aplicaciones.

En el modelo TCP/IP de cuatro capas se agrupan en acceso a red, Internet, transporte y aplicación. Las equivalencias ayudan a estudiar, pero no asignan siempre limpiamente cada tecnología a una única casilla. TLS, por ejemplo, se entiende mejor por su función que forzándolo a una etiqueta universal.

Encapsular: añadir información para el viaje

Imagina una petición HTTP enviada mediante TCP e IPv4 sobre Ethernet. Los datos de aplicación se entregan a TCP, que añade información de transporte. IP incorpora datos para llevar el paquete hacia el destino. Ethernet construye la trama para el enlace actual. El receptor interpreta y retira envoltorios hasta entregar los datos a la aplicación adecuada.

Se suele hablar de **segmento TCP**, **datagrama UDP**, **paquete IP** y **trama Ethernet**. La palabra paquete también se usa informalmente para otros conjuntos de datos: en un examen o diagnóstico conviene precisar el nivel.

TCP y UDP sin etiquetas engañosas

TCP ofrece un flujo de bytes ordenado y fiable mediante mecanismos como secuencia y retransmisión. No garantiza que la aplicación termine correctamente ni que una operación de negocio se haya completado. Si una conexión se interrumpe después de enviar un pedido, la aplicación aún debe saber cómo evitar duplicarlo al reintentar.

UDP proporciona datagramas sin esos mecanismos de entrega ordenada y retransmisión de TCP. Una aplicación puede construir funciones adicionales encima. No significa «siempre rápido» ni «solo para vídeo». La elección depende de requisitos y diseño.

MTU y tamaño

La **MTU** limita el tamaño que puede transportarse a cierto nivel en un enlace. Si parte del camino admite menos, los extremos o dispositivos deben tratar esa limitación mediante los mecanismos correspondientes. Añadir túneles puede reducir el espacio disponible para los datos. No cambies MTU porque una aplicación sea lenta sin evidencias de ese tipo de problema.

Ejemplo: el cable está conectado, la web no abre

El enlace físico puede estar activo, pero faltar configuración IP. La IP puede ser correcta, pero no existir una ruta. El camino puede funcionar y fallar DNS. El servidor puede responder a la red y tener detenido el servicio web. Las capas te ayudan a distinguir posibilidades; no garantizan una secuencia rígida válida para todos los casos.

Práctica: asigna observaciones a funciones

Relaciona cada síntoma con una primera hipótesis: conector roto, puerta de enlace incorrecta, nombre no resuelto, conexión TCP rechazada y contraseña rechazada por una aplicación. Escribe una prueba que ayude a cada caso.

Solución orientativa: inspección y sustitución controlada del enlace; revisar IP y rutas; consultar el nombre; verificar servicio y escucha; revisar identidad y autorización de la aplicación. La contraseña rechazada demuestra que al menos cierta comunicación con el servicio pudo haberse producido: no empieces sustituyendo cables sin otro indicio.

¿Lo has pillado?

1. ¿TCP garantiza que el usuario ha guardado el documento en el servidor?

2. ¿Cada trama Ethernet viaja intacta a través de todos los routers de Internet?

3. ¿OSI y TCP/IP son dos nombres del mismo protocolo?

Soluciones. 1) No: la confirmación funcional corresponde a la aplicación y al almacenamiento. 2) No: los enlaces utilizan sus propias tramas; un router vuelve a encapsular para el siguiente salto. 3) No: son modelos o marcos de funciones; TCP e IP son protocolos concretos dentro de una arquitectura.

23. IPv4: dirección, máscara y puerta de enlace

Al terminar: decidirás si dos direcciones pertenecen a la misma subred y describirás una configuración básica. **Antes:** binario del capítulo 06.

Una dirección IPv4 contiene 32 bits. Se escribe habitualmente como cuatro octetos decimales, cada uno entre 0 y 255: `192.168.10.25`. La dirección aislada no indica qué parte identifica la red. Para eso necesitas la **máscara** o longitud de prefijo.

La barra cuenta bits de red

`/24` significa que los primeros 24 bits forman el prefijo. Su máscara decimal es `255.255.255.0`. Quedan ocho bits para la parte de host. En una subred convencional, todos los bits de host a cero identifican la red y todos a uno su difusión o broadcast.

Así, `192.168.10.25/24` pertenece a `192.168.10.0/24`, con broadcast `192.168.10.255` y rango habitual de hosts de `.1` a `.254`. Esto no convierte automáticamente `.1` en router ni `.254` en servidor: son decisiones del diseño.

El cálculo general se obtiene mediante AND binario entre dirección y máscara. En un `/24` es sencillo verlo por octetos; en otros prefijos hay que observar los bits. Por eso no basta con aprender «las tres primeras cifras deben coincidir».

Puerta de enlace y DNS no son lo mismo

La **puerta de enlace predeterminada** es el siguiente salto utilizado cuando no hay una ruta más específica aplicable. En una configuración sencilla es la dirección del router en el enlace local. Debe ser alcanzable con esa configuración; no basta con escribir la dirección de cualquier router lejano.

El **servidor DNS** responde consultas de nombres. Puede estar en el router, en un servidor local o en otra red. Su función no se confunde con la puerta de enlace aunque el aparato doméstico ofrezca ambas bajo la misma dirección.

Ejemplo desarrollado

Aula Norte asigna a un cliente `192.168.10.25/24`, router `192.168.10.1` y servidor local `192.168.10.10`. Para llegar al servidor local, el cliente determina que comparte prefijo y busca el destino en su enlace. Para un destino fuera de esa red, consulta sus rutas y puede utilizar el router.

Si se configura por error `/16`, el cliente considerará locales más direcciones de las previstas. Podría intentar resolver por enlace un destino que realmente necesita un router. Una máscara incorrecta no siempre impide toda comunicación: puede producir fallos parciales difíciles de interpretar.

Direcciones privadas y otras especiales

Los bloques privados de RFC 1918 son `10.0.0.0/8`, `172.16.0.0/12` y `192.168.0.0/16`. El segundo abarca de 172.16 a 172.31, no todas las direcciones que empiezan por 172. No se encaminan como direcciones públicas globales de Internet, aunque pueden comunicarse a través de redes privadas conectadas adecuadamente.

El bloque `127.0.0.0/8` corresponde a loopback en IPv4; `127.0.0.1` es una dirección habitual de prueba local. `169.254.0.0/16` se utiliza para direccionamiento de enlace local bajo reglas específicas. Una dirección de ese bloque no demuestra una salida funcional a Internet y puede ser una pista si esperabas recibir DHCP.

Fuente de los bloques privados: RFC 1918, https://www.rfc-editor.org/rfc/rfc1918. Para los demás bloques especiales, consulta el registro oficial de IANA: https://www.iana.org/assignments/iana-ipv4-special-registry/.

Práctica en papel

Un equipo A usa `192.168.40.10/24`; B usa `192.168.40.200/24`; C usa `192.168.41.20/24`. Decide qué pares comparten subred. Después cambia únicamente la máscara de los tres a `/23` y repite.

Solución razonada: con `/24`, solo A y B comparten prefijo. Con `/23`, la máscara es `255.255.254.0`, y el bloque que empieza en 192.168.40.0 incluye los terceros octetos 40 y 41. Los tres pertenecen a esa subred si el enlace y el diseño también son adecuados. La coincidencia aritmética no conecta físicamente redes separadas.

SOS: dirección duplicada

Dos equipos con la misma dirección en el mismo ámbito pueden provocar conflictos e intermitencias. Revisa inventario, reservas y asignaciones. No elijas otra dirección al azar: podría estar ocupada o reservada. El proceso debe coordinarse con el plan de direccionamiento.

¿Lo has pillado?

1. ¿Una IP basta para calcular su red?

2. ¿Todas las direcciones 172 son privadas?

3. ¿La puerta de enlace tiene que acabar en .1?

Soluciones. 1) No: necesitas prefijo o máscara. 2) No: el bloque privado señalado va de 172.16 a 172.31. 3) No: es una convención frecuente, no una obligación del protocolo.

24. Subredes paso a paso, con cuentas que puedes comprobar

Al terminar: calcularás red, broadcast y rango de hosts, y repartirás un bloque con VLSM. **Antes:** binario, potencias de dos y capítulo 23.

UN /24 DIVIDIDO EN CUATRO /26



Ejemplo: último octeto de 192.168.50.0/24. Cada bloque: 64 direcciones.

Las fronteras del bloque deben respetarse al asignar subredes.

Dividir una red consiste en dedicar más bits al prefijo. Cada bit adicional divide por dos el tamaño del bloque. Para IPv4, un prefijo `/p` deja `32 − p` bits y contiene `2 elevado a (32 − p)` direcciones. En una subred convencional con broadcast se reservan red y broadcast, de modo que los hosts utilizables son el total menos dos.

La resta de dos no se aplica sin matices a todos los casos: los enlaces `/31` tienen reglas específicas y `/32` representa una dirección individual. En los ejercicios iniciales utilizaremos redes convencionales de `/24` a `/30`.

Método 1: mirar los bits

Convierte `192.168.10.77/26`. La máscara es `255.255.255.192`; el último octeto de máscara es `11000000`. El último octeto de la IP, 77, es `01001101`. AND conserva los bits comunes: `01000000`, que vale 64. La red es `192.168.10.64/26`.

Quedan seis bits de host. Si todos se ponen a uno, el último octeto es `01111111` = 127: ese es el broadcast. El rango habitual va de `.65` a `.126`, 62 hosts. El equipo `.77` está dentro de él.

Método 2: tamaño del salto

En el octeto donde la máscara deja de ser 255, resta su valor a 256. Para 192: 256 − 192 = 64. Las redes empiezan en 0, 64, 128 y 192. El 77 cae entre 64 y 127. Obtienes el mismo resultado que con bits.

Con `/27`, el último octeto de máscara es 224 y el salto es 32. Hay bloques 0-31, 32-63, 64-95 y así sucesivamente. No mezcles el salto con el número de hosts: un bloque de 32 direcciones ofrece normalmente 30 hosts.

Tabla de referencia que debes poder reconstruir

- `/24`: máscara 255.255.255.0; 256 direcciones; 254 hosts convencionales.
- `/25`: máscara 255.255.255.128; 128 direcciones; 126 hosts.
- `/26`: máscara 255.255.255.192; 64 direcciones; 62 hosts.
- `/27`: máscara 255.255.255.224; 32 direcciones; 30 hosts.
- `/28`: máscara 255.255.255.240; 16 direcciones; 14 hosts.
- `/29`: máscara 255.255.255.248; 8 direcciones; 6 hosts.
- `/30`: máscara 255.255.255.252; 4 direcciones; 2 hosts.

VLSM: ajustar tamaños distintos

Aula Norte dispone del bloque de laboratorio `192.168.50.0/24`. Necesita subredes para 50, 25 y 10 interfaces, contando ya las direcciones de router y otros equipos necesarios. Elige el bloque mínimo que admite cada cantidad: `/26` para 50, `/27` para 25 y `/28` para 10.

Ordena de mayor a menor y asigna respetando fronteras:

1. Aula: `192.168.50.0/26`; hosts `.1-.62`; broadcast `.63`.
2. Administración: `192.168.50.64/27`; hosts `.65-.94`; broadcast `.95`.
3. Servicios: `192.168.50.96/28`; hosts `.97-.110`; broadcast `.111`.

Quedan direcciones sin asignar. No puedes describir necesariamente todo el resto con un único prefijo: depende de sus fronteras. Si reservaras crecimiento, tendrías que comprobar si ampliar una subred invadiría otra ya ocupada.



Ojo con este error

La dirección del router también consume una dirección de host en estas subredes. Si te piden 30 ordenadores más un router, `/27` no alcanza: ofrece 30 hosts en total, y necesitas al menos 31.

Cuando la frontera cae en otro octeto

Para `172.20.9.140/23`, la máscara es `255.255.254.0`. El salto es dos en el tercer octeto. El 9 pertenece al bloque 8-9. La red es `172.20.8.0`, el broadcast `172.20.9.255` y los hosts van de `172.20.8.1` a `172.20.9.254`. Hay 512 direcciones y 510 hosts convencionales.

No calcules solo el último octeto: en ese prefijo el bloque abarca dos valores del tercero.

Vamos a probarlo

Calcula red, broadcast y hosts de los siguientes casos antes de mirar las soluciones:

1. `192.168.1.130/25`.
2. `192.168.1.130/27`.

3. `10.0.5.19/30`.

4. ¿Qué prefijo mínimo convencional necesitas para 60 ordenadores, una impresora y un router?

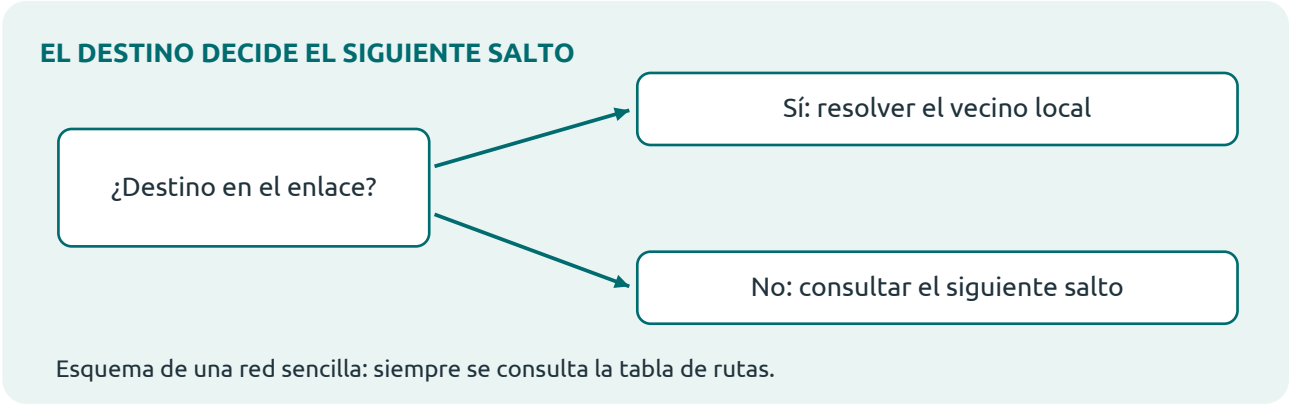
5. ¿Puede `192.168.50.80/27` ser una dirección de red escrita de forma canónica?

Soluciones razonadas. 1) Red `.128`, broadcast `.255`, hosts `.129-.254`. 2) Red `.128`, broadcast `.159`, hosts `.129-.158`. 3) Red `10.0.5.16`, broadcast `.19`, hosts `.17-.18`: la dirección del enunciado es broadcast y no se asigna como host convencional. 4) Necesitas 62 direcciones utilizables: `/26` ofrece exactamente 62; cualquier crecimiento exige reconsiderarlo. 5) No: pertenece al bloque `.64-.95`. La notación de red canónica sería `.64/27`.

Fuente para ampliar: CIDR, RFC 4632, https://www.rfc-editor.org/rfc/rfc4632. El aprendizaje de este capítulo se apoya en cálculos originales que puedes contrastar con los recursos del libro.

25. IPv6, vecinos y rutas: no todo se resuelve con una máscara

Al terminar: leerás una dirección IPv6, distinguirás ARP y NDP y seguirás una decisión de ruta.
Antes: dirección, enlace y subred.



Para un destino remoto se resuelve el vecino del siguiente salto.

IPv6 utiliza direcciones de 128 bits, representadas habitualmente mediante grupos hexadecimales separados por dos puntos. No es una dirección IPv4 más larga escrita con los mismos cuatro octetos. Su operación introduce diferencias que conviene estudiar expresamente.

Leer sin perderte en los ceros

`2001:0db8:0000:0000:0000:0000:0000:0010` puede abreviarse como `2001:db8::10`. Se pueden omitir ceros iniciales de cada grupo y comprimir una secuencia de grupos nulos mediante `::`, una sola vez en la dirección. Si lo usaras dos veces, sería ambiguo saber cuántos grupos faltan en cada lugar.



Ojo con este error

En los ejemplos utilizaremos `2001:db8::/32`, reservado para documentación. No es un prefijo para asignar a una red pública real. Un `/64` señala 64 bits de prefijo, habitual en muchas redes IPv6 con autoconfiguración, y no equivale a la lógica de «restar dos» de los ejercicios IPv4.

Alcance y autoconfiguración

Una interfaz puede tener varias direcciones IPv6 con diferentes alcances. Las de enlace local, del bloque `fe80::/10`, permiten funciones en el enlace y no se encaminan como direcciones globales. En algunas herramientas debes indicar además la interfaz o zona para evitar ambigüedad.

IPv6 no utiliza broadcast como IPv4; emplea multicast para funciones donde corresponde. Los anuncios de router pueden proporcionar información del prefijo y del router predeterminado.

SLAAC y DHCPv6 tienen funciones distintas y pueden combinarse según el diseño. No presupongas que DHCPv6 sustituye todos los anuncios de router.

Fuentes para ampliar: RFC 8200, https://www.rfc-editor.org/rfc/rfc8200; arquitectura de direcciones, RFC 4291, https://www.rfc-editor.org/rfc/rfc4291; representación textual, RFC 5952, https://www.rfc-editor.org/rfc/rfc5952.

ARP en IPv4 y NDP en IPv6

En Ethernet con IPv4, **ARP** permite averiguar la dirección de enlace asociada a una dirección IP del enlace local. Si el destino final está fuera, el equipo suele resolver la MAC del siguiente salto, no la del servidor de Internet.

IPv6 utiliza **Neighbor Discovery**, basado en ICMPv6, para funciones como resolución de vecinos y descubrimiento de routers. No es «ARP con direcciones largas». Bloquear indiscriminadamente ICMPv6 puede romper funciones necesarias.

ICMP e **ICMPv6** transportan mensajes de control y error, y algunas herramientas utilizan sus mensajes para comprobar alcance. Recibir respuesta a un ping no prueba que una aplicación funcione. No recibirla tampoco demuestra que el equipo esté apagado: puede existir filtrado.

Elegir la ruta más específica

Una tabla de rutas indica prefijo de destino, siguiente salto o enlace, interfaz y otros datos. Entre rutas aplicables, la longitud de prefijo es una decisión fundamental: se prefiere la coincidencia más específica; si hay alternativas de igual especificidad intervienen otras reglas y métricas del sistema.

Ejemplo: un equipo tiene una ruta a `10.20.0.0/16`, otra a `10.20.5.0/24` y una predeterminada. Para `10.20.5.30`, la `/24` es más específica. Para `10.20.8.30`, coincide la `/16`. Para un destino sin otra coincidencia se utiliza la predeterminada si existe.

Práctica de observación

En Windows consulta `ipconfig /all`, `route print` y `arp -a`. En Linux con iproute2, consulta `ip address`, `ip route`, `ip -6 route` e `ip neigh`. Identifica una interfaz, su dirección, una ruta conectada y la predeterminada si está configurada. No borres vecinos ni rutas para esta actividad.

Resultado esperado: una ficha que diferencie ruta y asociación de vecino. Oculta direcciones públicas, nombres y otros datos si compartes las capturas. La ausencia de IPv6 global no impide completar la parte de lectura conceptual.

¿Lo has pillado?

1. ¿Puedes escribir dos `::` en una dirección IPv6?
2. ¿Qué MAC busca el cliente para enviar a un servidor fuera del enlace en una red Ethernet IPv4 sencilla?
3. ¿Una ruta `/24` aplicable es menos específica que una predeterminada?

Soluciones. 1) No: resultaría ambiguo expandir los grupos omitidos. 2) La del siguiente salto local correspondiente, normalmente el router. 3) Es más específica y se prefiere para ese destino bajo el proceso ordinario de selección descrito.

26. Ethernet y wifi: el medio también importa

Al terminar: planificarás comprobaciones básicas de cableado y cobertura sin confundir categoría, velocidad y calidad real. **Antes:** enlaces, switch y punto de acceso.

Una conexión depende de todos sus elementos. En cobre intervienen cable, conectores, terminaciones, latiguillos, tomas, paneles y puertos. En radio intervienen banda, canal, distancia, obstáculos, interferencias y capacidades de los equipos.

Cableado estructurado

Un enlace de cableado estructurado organiza tomas y paneles de forma documentada. Etiquetar ambos extremos permite localizarlo. Un latiguillo mal identificado puede provocar que desconectes un servicio distinto del que intentabas reparar.

Las categorías describen características del cableado; la velocidad alcanzable depende de la norma Ethernet, la longitud y el conjunto del canal. No deduzcas una velocidad por el color de la cubierta o por la forma exterior del conector. La fibra utiliza otros medios y requiere compatibilidad de transceptores, tipo de fibra, conectores y distancia.

En terminaciones de par trenzado se usan esquemas como T568A y T568B. Debe respetarse el procedimiento y mantenerse la geometría de pares conforme a los requisitos del sistema. Un probador sencillo de continuidad puede detectar algunos fallos de hilos, pero no certifica todas las prestaciones de un enlace.

Velocidad negociada y transferencia real

Un puerto puede negociar una velocidad y funcionar a una tasa útil inferior. Influyen protocolos, almacenamiento, carga y otros tramos. Si un enlace que debería admitir más negocia a una velocidad baja, revisa capacidades de ambos puertos y el canal físico antes de atribuirlo a DNS.

La alimentación **PoE** puede suministrar energía a dispositivos compatibles. Comprueba norma, presupuesto de potencia, equipo suministrador y receptor. Que un cable transporte datos no significa que cualquier inyector de alimentación sea adecuado.

Wifi: SSID, banda y canal

El **SSID** identifica una red inalámbrica de forma visible, pero no es una garantía de identidad: puede repetirse. La autenticación y protección deben configurarse adecuadamente. Utiliza modos de seguridad actuales compatibles con los requisitos del entorno y evita prácticas heredadas inseguras.

La banda y el canal condicionan cobertura e interferencias. Los canales y potencias permitidos dependen del país y de la regulación vigente. No copies configuraciones de otra región ni supongas que ensanchar el canal siempre mejora: puede aumentar la ocupación y empeorar la convivencia.

Una señal fuerte no garantiza buen rendimiento. Puede haber muchos clientes, interferencias o una salida limitada. La itinerancia entre puntos de acceso depende del diseño y de decisiones de los dispositivos; poner el mismo nombre a dos redes no garantiza una transición sin cortes.

Práctica física o de simulación

Con un latiguillo y probador de formación, identifica extremos, revisa visualmente y registra el resultado del mapa de hilos. No intervengas en cableado activo de otros usuarios. Si no tienes material, dibuja una ficha de enlace con toma, panel, puerto y equipo, y analiza un caso de hilos cruzados o abiertos.

Para wifi, en una red propia observa ubicación, banda, intensidad y rendimiento de una tarea en dos lugares. Mantén equipo y tarea constantes y repite. No escanees ni captures tráfico de redes ajenas. La prueba sirve para comparar esas condiciones, no para certificar toda la cobertura del edificio.

Resultado esperado: una tabla de observaciones y una propuesta justificada: recolocar un punto de acceso, revisar un cable o investigar congestión. No modificar canales ni potencia sin registrar el estado inicial y comprobar la regulación aplicable.

SOS: funciona junto al router, falla en el aula

Compara ubicación, obstáculos y asociación a puntos de acceso. Después revisa si el problema es enlace, autenticación, configuración o salida. Un repetidor añadido sin estudio puede amplificar problemas o crear otros; primero necesitas datos sobre el tramo que falla.

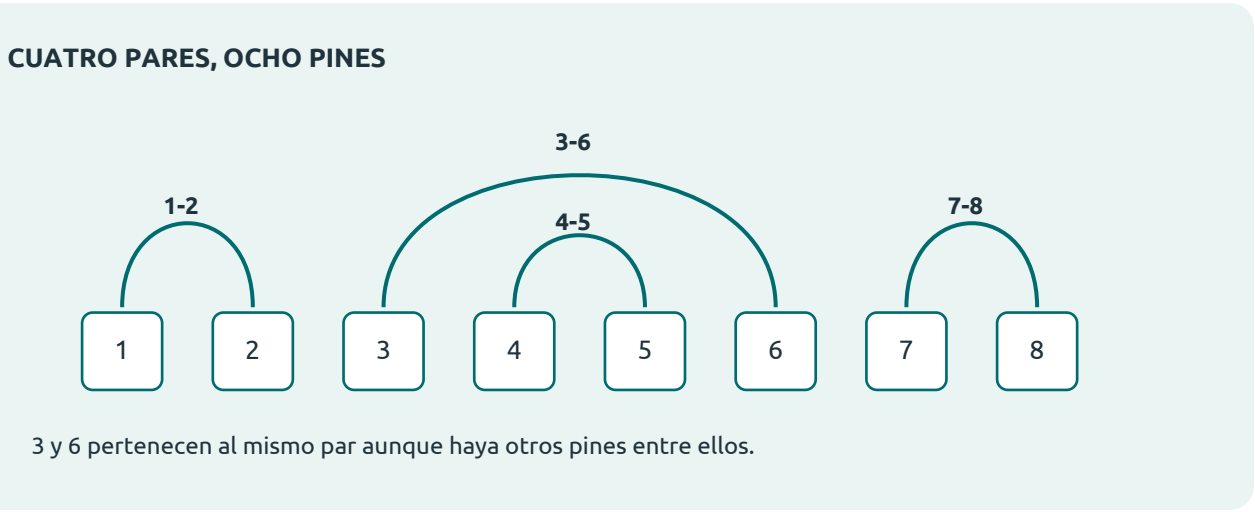
Taller de cableado: del plano a la identificación

Parte de un plano de aula ficticio. Sitúa rack o armario, panel, tomas, recorridos y equipos. Cuenta puntos, longitudes y latiguillos por tramo; no calcules solo la distancia en línea recta. Identifica ambos extremos con un código que aparezca también en el plano y el inventario.

El **enlace permanente** y el **canal completo** no tienen el mismo alcance de prueba: el canal incluye latiguillos. Respeta límites de longitud, radio de curvatura, tracción, separación y puesta a tierra que establezcan el diseño, la norma aplicable y los componentes. Una categoría impresa en la cubierta no certifica el canal terminado.

Antes de montar, revisa fijaciones, canalización, pasos, herramienta y protección del puesto. No perfores paredes ni trabajas en altura para esta primera práctica: utiliza un panel de entrenamiento. No conectes cableado en preparación a alimentación, PoE o equipos en servicio.

T568A y T568B sin adivinar los pares



Los pines contiguos no siempre forman un par: observa 3 y 6.

Esta tabla indica el conductor que corresponde a cada **número de pin**. Utiliza el dibujo y numeración del conector o herramienta del taller; mirar el conector desde el otro lado invierte visualmente el orden.

Pin	T568A	T568B
1	Blanco/verde	Blanco/naranja
2	Verde	Naranja
3	Blanco/naranja	Blanco/verde
4	Azul	Azul
5	Blanco/azul	Blanco/azul
6	Naranja	Verde
7	Blanco/marrón	Blanco/marrón
8	Marrón	Marrón

Los pares ocupan 1-2, 3-6, 4-5 y 7-8. No emparejes 3-4 por estar juntos en la lista. En un cable recto ambos extremos siguen el mismo esquema. El cruce A-B intercambia los pares usados por Ethernet clásico de dos pares; no lo presentes como diseño universal de cruce para cualquier interfaz. Muchas interfaces actuales incorporan Auto MDI-X.

Terminar y comprobar un latiguillo de prácticas

1. Selecciona cable, conectores y herramienta compatibles con categoría, conductor sólido o flexible y diámetro. Un conector cualquiera no sirve para todos los cables.
2. Prepara el extremo según su fabricante: retira solo la cubierta necesaria sin dañar aislamiento y conserva el trenzado hasta donde indique el sistema.

3. Ordena conductores por el esquema acordado, recorta uniformemente y comprueba su posición en la guía/conector. La cubierta debe quedar sujeta por el mecanismo previsto.
4. Engasta con la herramienta adecuada o termina el módulo de toma según su diseño. No mezcles instrucciones de un conector modular con las de una toma de impacto.
5. Inspecciona y utiliza el probador desconectado de equipos activos. Registra mapa de hilos y resultado; corrige únicamente el extremo o cable defectuoso identificado.
6. Etiqueta y prueba la tarea de red con equipos de laboratorio. La certificación del canal requiere el instrumento y el perfil de prueba adecuados.

Un comprobador sencillo puede detectar abiertos, cortos o cruces. Un **par dividido** puede conservar continuidad pin a pin y fallar eléctricamente porque los conductores no pertenecen al par trenzado correcto. El mapeo básico no demuestra prestaciones de frecuencia, diafonía o pérdida de retorno.

Fuentes de terminación y diagnóstico: Fluke Networks, T568A/T568B y FOA, mapa de hilos y pares divididos.

Taller de switch y punto de acceso

Utiliza equipos del aula con autorización, configuración inicial guardada y acceso administrativo previsto. Empieza por un único segmento. El switch enlaza equipos; el AP conecta la radio a la red; un router puede integrar DHCP y NAT. No actives un segundo servidor DHCP por confundir el modo AP con el modo router.

Para la práctica SMR-SERVICIOS puedes reservar `10.77.0.2` para gestión del switch y `.3` para el AP, fuera del rango DHCP `.100` a `.150`, siempre que no estén ocupadas. Configura máscara y acceso de gestión según el diseño. Si no hay router, no inventes puerta de enlace.

En un switch administrable identifica puertos de acceso, VLAN sin etiquetar, PVID y enlaces etiquetados según el fabricante. Primero conserva la conectividad de gestión; no cambies a la vez todos los puertos. En una ampliación con dos VLAN, prueba pertenencia y separación, y añade encaminamiento solo si el diseño lo autoriza. Un switch no administrable no ofrece esos controles.

En el AP configura nombre de red de laboratorio, país/región correctos, banda y canal acordes al entorno y dispositivos. Utiliza un modo mantenido, preferentemente WPA3-Personal si los clientes lo admiten; documenta cualquier compatibilidad con WPA2-AES. No uses WEP o TKIP para una red de trabajo. En 6 GHz se aplican requisitos que excluyen WPA2-Personal; no traslades un perfil antiguo sin revisarlos. Crea una contraseña de práctica propia, sin publicarla en capturas.

Cambia credenciales administrativas iniciales por el procedimiento del aula, actualiza desde el canal oficial y restringe la gestión. Si hay PoE, verifica estándar, potencia y compatibilidad del puerto y equipo; alimentación pasiva y PoE negociado no son intercambiables. Guarda la configuración de recuperación protegida.

Referencia de seguridad: HPE Aruba, WPA3-Personal y sus modos.

Prueba de aceptación de wifi

Conecta dos dispositivos de laboratorio, comprueba asociación, dirección, DNS y acceso a la tarea interna. Repite en varios lugares y registra señal, banda, canal, tasa negociada y resultado de la tarea. No conviertas barras de señal en una medida completa de calidad.

Prueba una credencial incorrecta y la separación de invitados si el diseño la ofrece. Un SSID diferente no demuestra aislamiento: intenta únicamente el acceso de prueba previsto y verifica la regla que debe impedirlo. Después restaura configuración y retira las redes de prueba de los clientes cuando termine la actividad.

Entrega plano, lista de puntos, mapa del cable, configuración sin secretos y pruebas positivas/negativas. Si no tienes instrumental o AP, trabaja con el material del docente y marca esas evidencias como análisis/simulación, no como montaje o cobertura medidos.

¿Lo has pillado?

1. ¿Un probador básico de continuidad equivale a certificación de categoría?

2. ¿La velocidad negociada garantiza igual tasa de descarga desde cualquier web?

3. ¿El mismo SSID garantiza que el punto de acceso es legítimo?

Soluciones. 1) No: la certificación comprueba prestaciones adicionales con instrumentos y criterios adecuados. 2) No: existen otros límites y sobrecargas. 3) No: el nombre puede copiarse y se necesita autenticación y validación adecuadas.

27. Diagnosticar conectividad: una prueba, una pregunta

Al terminar: separarás enlace, direccionamiento, rutas, nombres y servicio en una incidencia. **Antes:** capítulos 21-26. **Entorno:** equipos propios o laboratorio autorizado.

«No tengo Internet» puede significar que una única web no abre, que no funcionan los nombres o que no hay enlace. Empieza por la tarea, el alcance y el momento del fallo. Pregunta qué sí funciona y qué cambió. La información reduce pruebas innecesarias.

Paso 1: enlace y configuración

Comprueba adaptador, conexión física o asociación inalámbrica. Consulta la configuración de la interfaz realmente utilizada. Anota dirección, prefijo, puerta de enlace y servidores DNS. Si hay adaptadores virtuales o VPN, identifica qué rutas introducen.

En Windows usa `ipconfig /all`; en Linux, `ip address` y las herramientas de su gestor de red. Una IP de aspecto habitual no demuestra que sea correcta para ese segmento. Compara con el plan, no con la configuración de una red anterior.

Paso 2: camino y siguiente salto

Consulta rutas. Prueba un destino local conocido y autorizado cuando corresponda. En Windows, `ping -n 4 direccion` limita a cuatro solicitudes; en Linux suele utilizarse `ping -c 4 direccion`. Sustituye `direccion` por la dirección del laboratorio, sin copiar literalmente el término.

Un ping a loopback comprueba una parte de la pila local; no verifica el cable. Un ping al router aporta otra evidencia, pero puede estar filtrado. No conviertas una única respuesta o ausencia en diagnóstico definitivo.

Paso 3: nombres

Compara la consulta del nombre esperado con el dato correcto del laboratorio. En Windows, `Resolve-DnsName nombre` consulta DNS con opciones según el entorno. En Linux, herramientas como `resolvectl query nombre` o `getent hosts nombre` consultan mecanismos que no son idénticos entre sí. Indica cuál utilizaste y qué información esperabas.

Si una aplicación funciona por dirección pero no por nombre, DNS es una hipótesis importante, aunque intervengan otros detalles. En HTTPS, probar directamente por IP puede producir un error de nombre de certificado: no ignores ese error ni lo interpretes automáticamente como servicio caído.

Paso 4: servicio concreto

Un servidor puede responder a ping y no tener el servicio escuchando. En Windows, `Test-NetConnection -ComputerName nombre -Port 443` comprueba una conexión TCP al puerto indicado en un entorno adecuado. Una prueba positiva no valida contenido, certificado ni permisos de la aplicación. Si el servicio utiliza UDP, esa prueba TCP no comprueba el protocolo correcto.

En Linux puedes utilizar herramientas del servicio, como `curl` para una petición web si está instalado. No desactives la validación de certificados para hacer que una prueba parezca correcta: registra el motivo del fallo y corrige la confianza o el nombre según el diseño.

Paso 5: seguir el recorrido

Windows dispone de `tracert` y Linux puede utilizar `tracepath` o `traceroute` cuando están instalados. Las respuestas dependen de routers, filtros y de la modalidad de la herramienta. Un asterisco en un salto no demuestra que todo el tráfico se detenga allí: el destino puede seguir respondiendo.

Caso resuelto: solo falla la intranet por nombre

El cliente accede a una carpeta local del servidor y tiene una ruta coherente. La consulta de `intranet.aulanorte.test` devuelve una dirección antigua. El registro del laboratorio identifica una migración reciente. Se revisa el dato en el servidor DNS y la caché conforme al procedimiento, y después se repite la consulta y el acceso HTTPS con su nombre correcto.

La solución documenta qué registro cambió y por qué. Cambiar a un DNS público no sería adecuado para resolver un nombre interno que ese servidor externo desconoce.

Práctica: una tabla de diagnóstico

Prepara columnas «prueba», «pregunta», «resultado esperado», «observado» y «conclusión limitada». Completa cinco filas: enlace, configuración, ruta, nombre y servicio. Utiliza un destino de laboratorio conocido; no necesitas provocar un fallo real.

Resultado esperado: cada conclusión se ajusta a la prueba. «El puerto TCP responde» es válido; «la aplicación es totalmente segura y funciona para todos» excede la evidencia. Para recuperar la actividad basta con cerrar las herramientas: las consultas propuestas no cambian la configuración.

¿Lo has pillado?

1. ¿Responder a ping demuestra que HTTPS funciona?

2. ¿Un asterisco de traceroute prueba que ese router está averiado?

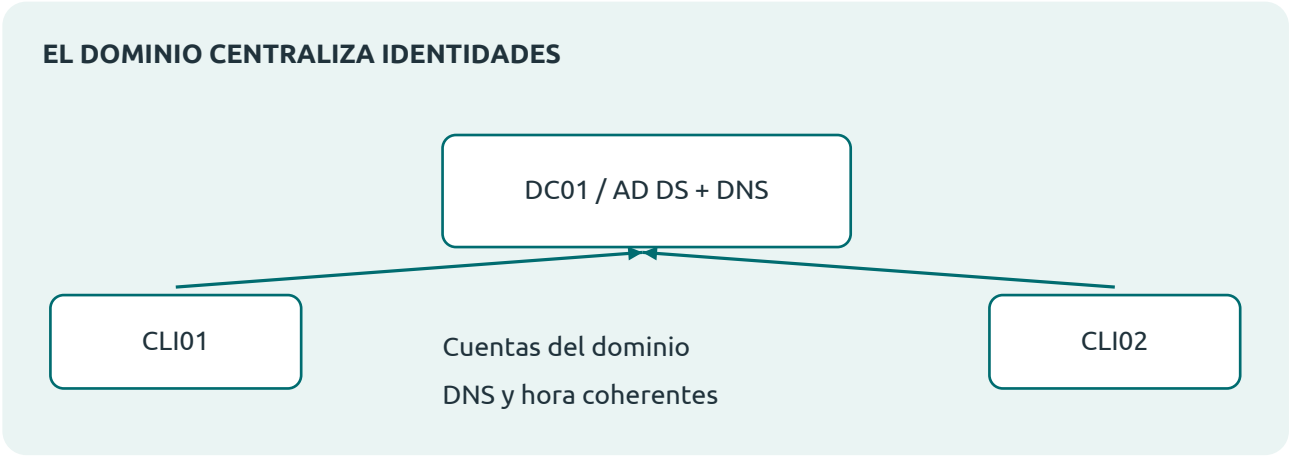
3. ¿Por qué anotar la interfaz y la hora?

Soluciones. 1) No: son protocolos y funciones diferentes. 2) No: puede no responder a esa prueba mientras sigue encaminando. 3) La configuración y el camino pueden cambiar; la evidencia debe poder relacionarse con el síntoma.

Bloque 5. Sistemas operativos en red

28. Del grupo de trabajo al dominio

Al terminar: distinguirás cuentas locales, dominio, directorio y controlador, y planificarás un dominio de laboratorio. **Antes:** usuarios, permisos, DNS y direccionamiento.



Un cliente debe poder localizar los servicios internos del dominio.

En un grupo de trabajo, cada equipo administra sus cuentas locales. Si necesitas cambiar el acceso de una persona en veinte máquinas, repetir la gestión en cada una resulta incómodo y propenso a errores. Un dominio permite centralizar identidades y administrar recursos mediante una infraestructura común.

Centralizar no significa que todos los archivos deban estar en el mismo servidor ni que desaparezcan las cuentas locales. Significa que existe una autoridad y unos servicios que los equipos utilizan para ciertas funciones de identidad y administración.

Directorio, dominio, bosque y controlador

Un **servicio de directorio** mantiene información organizada sobre objetos: usuarios, grupos, equipos y otros recursos. En Active Directory Domain Services, **AD DS**, un dominio constituye un ámbito de identidades y administración dentro de una estructura mayor. Un **bosque** contiene uno o varios dominios que comparten elementos de la infraestructura del directorio.

Un **controlador de dominio** presta servicios del dominio y mantiene una copia de los datos de directorio que le corresponden. En producción se diseña disponibilidad y recuperación: tener un solo controlador es un punto de fallo. En una práctica pequeña utilizaremos uno para aprender, sin presentarlo como arquitectura suficiente para cualquier empresa.

El dominio DNS y el dominio de identidad se relacionan, pero no son lo mismo que registrar una web. Comprar un nombre de Internet no crea Active Directory. Instalar AD DS tampoco publica automáticamente una página web.

Dos dependencias que no conviene saltarse

DNS: los clientes necesitan localizar servicios del dominio. Poner un DNS público como solución a una unión fallida puede impedir esa localización si desconoce los registros internos.

Hora: mecanismos de autenticación como Kerberos dependen de una sincronización adecuada. Comprueba reloj, zona horaria y origen de tiempo. Si dos equipos muestran horas distintas, determina si es una diferencia real o solo de presentación por zona horaria.

Preparación del laboratorio de dominio

Utiliza una red virtual interna identificada como `SMR-AD`. Prepara `DC01` con Windows Server 2025, edición y licencia válidas para el entorno, y `CLI01` con una edición de Windows 11 que admita unión a AD DS, como Pro. La edición Home no sirve para esta práctica de unión clásica. Instala actualizaciones y registra compilación y recursos asignados.

El controlador tendrá `10.77.0.10/24`. El cliente puede usar `10.77.0.100/24` estática durante este ejercicio y utilizará `10.77.0.10` como DNS. No configures una puerta de enlace ficticia: si el laboratorio no tiene router, no tiene salida a otras redes. Para actualizar sistemas, utiliza previamente un acceso controlado y retíralo antes de los experimentos de infraestructura.

El dominio de prácticas será `aulanorte.test`, con nombre corto `AULANORTE` cuando proceda. `.test` permite identificar el uso de laboratorio; no lo consideres un diseño de nombres para publicar servicios reales. En una organización se planifica el espacio de nombres, las delegaciones y su relación con los dominios que controla.

Práctica guiada: crear un dominio nuevo aislado

1. Comprueba nombre, dirección, DNS, hora y aislamiento de `DC01`. Guarda la base de recuperación del laboratorio antes de promoverlo.
2. En Administrador del servidor, añade el rol AD DS con las herramientas de administración. La instalación del rol no crea todavía el dominio.
3. Abre la acción de promoción y elige crear un bosque nuevo solo porque este laboratorio no tiene ninguno. Introduce `aulanorte.test` y revisa las opciones de DNS y catálogo global propuestas.
4. Define una contraseña de restauración de servicios de directorio y guárdala protegida para la práctica. No la publiques en capturas ni la confundas con la contraseña de un alumno.
5. Revisa nombres, ubicaciones y comprobaciones de requisitos. Lee advertencias en su contexto: no las ignores sistemáticamente ni concluyas que cualquier aviso es fatal.
6. Completa la promoción y el reinicio. Comprueba que existen el dominio, la zona DNS prevista y los servicios del controlador.
7. Desde `CLI01`, comprueba la resolución del dominio usando el DNS interno. Une el equipo al dominio mediante una cuenta autorizada para esa acción y reinicia cuando lo solicite.
8. Inicia una sesión de dominio con una cuenta de prueba creada para ello. Comprueba la identidad utilizada y la existencia del objeto de equipo en el directorio.

Resultado esperado: el cliente pertenece al dominio y una cuenta del dominio inicia sesión. Una sesión iniciada con una cuenta local del mismo nombre no demuestra ese resultado.

Recuperación: en este laboratorio desechable, puedes reconstruir ambos invitados desde la base anterior a la promoción. No apliques esa simplificación a controladores de producción: su recuperación requiere procedimientos propios de AD DS. Para sacar un cliente de un dominio, conserva antes una cuenta local administradora y acceso a los datos necesarios.

Fuente de procedimiento y opciones: Microsoft Learn, instalación de AD DS, https://learn.microsoft.com/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-.

SOS: «no se encuentra el dominio»



Truco de taller

Revisa DNS del cliente, resolución de registros de servicio, conectividad con el controlador y estado de sus servicios. No cambies cuentas y contraseñas antes de comprobar si el cliente puede localizar la infraestructura. Un ping correcto a la dirección del controlador no valida todos esos servicios.

¿Lo has pillado?

1. ¿Instalar el rol AD DS equivale a completar la promoción?

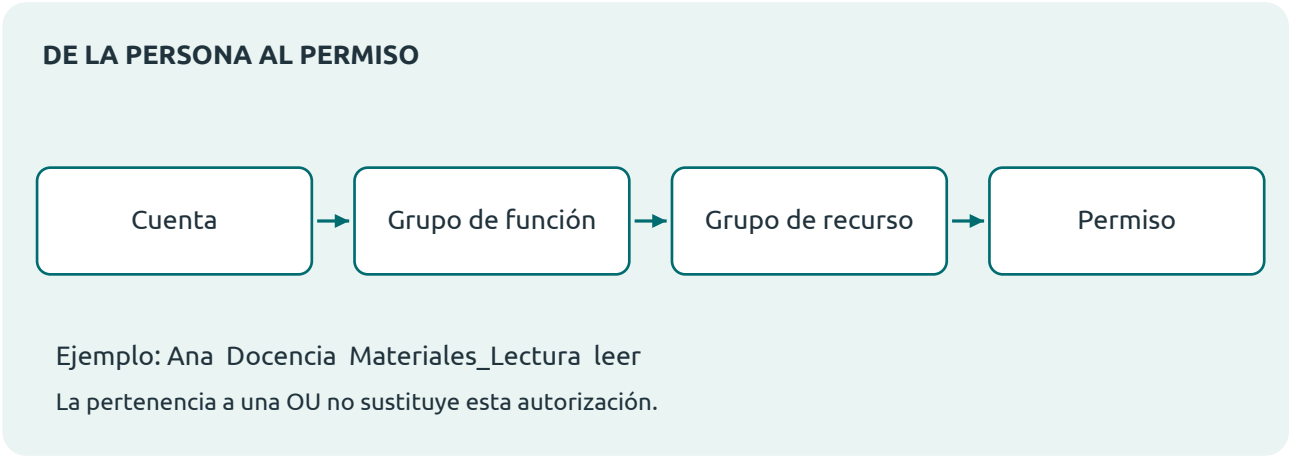
2. ¿Una cuenta local y otra de dominio con el mismo nombre son la misma identidad?

3. ¿Por qué el DNS público no sustituye automáticamente al interno?

Soluciones. 1) No: la promoción configura su papel en el dominio o bosque. 2) No: pertenecen a autoridades distintas y tienen identificadores diferentes. 3) Porque puede carecer de los registros internos necesarios para localizar servicios del dominio.

29. Organizar usuarios, grupos y políticas

Al terminar: diseñarás una estructura pequeña y comprobarás una política sin afectar a todo el dominio. **Antes:** capítulo 28 y cuentas locales.



Un diseño comprensible permite revisar quién accede a cada recurso.

Un directorio desordenado puede funcionar al principio y volverse difícil de mantener. El objetivo no es reproducir cada detalle del organigrama. Es facilitar administración, delegación y aplicación de reglas comprensibles.

Unidades organizativas y grupos

Una **unidad organizativa**, u OU, agrupa objetos dentro del dominio para fines administrativos, como delegar tareas y vincular políticas. Un **grupo** reúne identidades para asignar derechos u otros usos. Meter un usuario en una OU no lo incorpora automáticamente al grupo que permite abrir una carpeta.

Para Aula Norte crea una OU de laboratorio y, dentro, una estructura sencilla para personas y equipos. Prepara dos cuentas ficticias: `ana.docencia` y `luis.admin`. Crea grupos de seguridad que representen funciones, por ejemplo `GG_Docencia` y `GG_Administracion`. No añadas esas cuentas a grupos privilegiados para evitar mensajes de acceso.

Conceder acceso mediante grupos

Un patrón útil en un dominio pequeño es: cuentas grupos de función grupos del recurso permisos. Por ejemplo, `ana.docencia` pertenece a `GG_Docencia`; ese grupo se incorpora a `DL_Materiales_Lectura`; el último recibe lectura sobre Materiales.

Las siglas del patrón describen un diseño y sus ámbitos de grupo deben elegirse correctamente. No memorices una cadena sin comprender qué identidad termina autorizada y sobre qué recurso. Si solo existe un recurso pequeño, puede bastar un diseño más sencillo, siempre documentado.

Altas, cambios y bajas

Un alta requiere identidad, función, permisos mínimos, acceso inicial y explicación del uso. Un cambio de puesto exige retirar accesos que dejan de ser necesarios además de conceder los nuevos. Una baja debe contemplar deshabilitación, sesiones, datos, propiedad y retención conforme al procedimiento de la organización.

Deshabilitar una cuenta no garantiza que toda sesión ya iniciada termine inmediatamente en todos los servicios. Las aplicaciones y credenciales pueden tener sus propios mecanismos y tiempos. Verifica el alcance del cierre de acceso que necesitas.

Qué hace una GPO

Una **Group Policy Object**, o GPO, contiene configuraciones para usuarios o equipos. Su efecto depende de dónde se vincula, qué objetos quedan dentro del alcance, filtros, permisos y reglas de procesamiento. Una configuración de usuario y una de equipo no se aplican indistintamente al mismo objeto.

Como orientación, las políticas se procesan desde el ámbito local, sitio, dominio y OU, con reglas adicionales para herencia, vínculos y excepciones. Cuando hay conflicto, analiza la configuración concreta y el resultado; no uses «la última siempre gana» como explicación universal.

Fuente para ampliar: Microsoft Learn, procesamiento de políticas, https://learn.microsoft.com/windows-server/identity/ad-ds/manage/group-policy/group-policy-processing.

Práctica de política con alcance reducido

1. En el dominio de laboratorio, crea una OU llamada `Pruebas_GPO` y mueve únicamente un usuario ficticio a ella.
2. Crea una GPO identificable y vincúlala solo a esa OU. Anota valor inicial y objetivo antes de editarla.
3. Para observar un efecto sencillo, configura una directiva de usuario que impida temporalmente el acceso al Panel de control y Configuración, si la plantilla de tu versión la ofrece. No la vincules al dominio completo ni uses una cuenta administrativa como sujeto de prueba.
4. Inicia sesión con el usuario de prueba en el cliente y solicita actualización con `gpupdate /force` cuando corresponda. Algunas configuraciones requieren cerrar sesión o reiniciar; lee el aviso.
5. Comprueba el comportamiento y consulta `gpresult /r` en esa sesión. El informe de usuario y el de equipo tienen alcances y permisos diferentes.
6. Prueba con el otro usuario, fuera de la OU, y comprueba la diferencia esperada.
7. Deshabilita o retira el vínculo de la política de prueba, actualiza y verifica la recuperación. Revisa si la configuración utilizada revierte automáticamente o necesita una acción adicional.

Resultado esperado: puedes mostrar qué usuario recibe la política y por qué. Una captura del editor de GPO solo demuestra la configuración almacenada, no su aplicación en el cliente.

SOS: la política no aparece

Comprueba que el objeto correcto está en el ámbito, que la política está vinculada y activa, que tiene permiso para aplicarse y que el cliente alcanza DNS y controlador. Revisa resultado y eventos. Mover un usuario no altera la OU del equipo; confundir ambos explica muchos casos.

¿Lo has pillado?

1. ¿Una OU equivale a un grupo con acceso a carpetas?

2. ¿Por qué probar primero con una cuenta y OU de laboratorio?

3. ¿Conceder nuevos permisos basta cuando una persona cambia de función?

Soluciones. 1) No: organización administrativa y autorización a recursos son funciones distintas. 2) Permite comprobar el efecto y la retirada con un alcance limitado. 3) No: hay que revisar y retirar los anteriores que ya no procedan.

30. Carpetas e impresoras compartidas: permisos efectivos

Al terminar: separarás permiso local, permiso de compartición y la prueba real del usuario.
Antes: ACL, grupos y rutas.

POR RED, AMBOS CONTROLES DEBEN PERMITIR



Ejemplo sin denegaciones: cambio + lectura lectura por red

El acceso local no atraviesa necesariamente ambos controles.

Los permisos se comprueban desde la identidad y recorrido reales.

Una carpeta compartida expone un recurso a través de la red. La ruta `\\SRV01\Materiales` es una ruta UNC: identifica servidor y nombre del recurso. Ese nombre no tiene por qué coincidir con la ruta física del servidor, como `D:\Datos\Materiales`.



Consejo de David

El acceso depende de que el cliente llegue al servicio, se autentique y esté autorizado. Que el recurso aparezca en una lista no significa que pueda abrirse, y que no aparezca no demuestra que no exista.

Dos controles en Windows

En una carpeta compartida sobre NTFS intervienen permisos del recurso compartido y permisos del sistema de archivos. Para una operación por red deben permitirla ambos conjuntos, además de otros controles aplicables. Acceder localmente al servidor no atraviesa necesariamente el control de compartición, por lo que la prueba no equivale a la del cliente.

Ejemplo didáctico sin denegaciones explícitas: el recurso concede cambio, pero NTFS concede solo lectura. El usuario podrá leer, pero no modificar por esa ruta de red. Si NTFS concede modificación y el recurso solo lectura, el resultado por red sigue siendo lectura. En casos con múltiples grupos, denegaciones, herencia y derechos específicos, revisa las entradas y el acceso efectivo con más detalle.

Diseñar la carpeta de Aula Norte

Crea Materiales para que Docencia modifique y el alumnado lea. Crea Administración para su personal autorizado. Mantén permisos administrativos de servicio y recuperación necesarios, sin conceder control total indiscriminadamente a usuarios ordinarios.

Si una persona necesita entregar trabajos sin ver los de otros, una carpeta común con lectura y escritura para todos no resuelve el requisito. Necesitas diseñar subcarpetas, permisos o una aplicación de entrega que aplique ese comportamiento. «Puede subir archivos» no demuestra privacidad entre alumnos.

Práctica Windows: una matriz pequeña

En un servidor de archivos de laboratorio, prepara una carpeta de datos nueva, compártela como `Materiales` y utiliza grupos para asignar el acceso. Anota permisos del recurso y NTFS antes de probar. Crea un archivo ficticio desde la cuenta docente.

Desde el cliente, con la cuenta lectora, prueba listar, abrir, crear, modificar y borrar archivos ficticios. Repite con la cuenta docente. Registra cada operación como permitida o denegada, sin suponer que abrir un archivo prueba todas las demás.

Si cambias identidades, comprueba qué credenciales usa la conexión. Una sesión de red existente o credenciales guardadas pueden hacer que pruebes con otra cuenta. Cierra solo las conexiones de laboratorio conforme al procedimiento y vuelve a autenticarte; no borres todas las credenciales del equipo para resolver un caso aislado.

Resultado esperado: la matriz coincide con el diseño. Si no coincide, determina la identidad efectiva y el control que está denegando o concediendo. Para recuperar, retira el recurso de prueba y restaura las ACL registradas antes de eliminar los archivos ficticios.

Samba: compartir desde Linux con clientes Windows

Samba proporciona servicios compatibles con SMB. Un servidor de archivos Samba independiente puede tener cuentas locales para esta práctica. Integrarlo en un dominio requiere otro diseño de identidades; no basta con escribir el nombre del dominio en una opción de grupo de trabajo.

En un invitado Ubuntu preparado, instala Samba desde el repositorio oficial. Para un recurso de laboratorio con autenticación, crea el usuario local ficticio y la carpeta con permisos restringidos, y registra la cuenta en Samba. Los siguientes comandos requieren administración y crean recursos nuevos:

BASH

```
sudo adduser docente1
sudo install -d -o docente1 -g docente1 -m 0750 /srv/smr-materiales
sudo smbpasswd -a docente1
```

La contraseña se introduce en el diálogo correspondiente, nunca dentro de una línea compartida. Guarda copia de `/etc/samba/smb.conf` antes de añadir este recurso al final; el fragmento no reemplaza toda la configuración global:

```ini
[Materiales]
    path = /srv/smr-materiales
    browseable = yes
    guest ok = no
    read only = no
    valid users = docente1
```

Comprueba la sintaxis mediante `testparm` y aplica el cambio reiniciando `smbd` dentro de este laboratorio. Verifica estado, escucha y cortafuegos limitado al segmento de pruebas. Desde un cliente utiliza la ruta UNC del servidor y autentícate con `docente1`. Crea, abre y modifica únicamente un archivo ficticio.

Resultado esperado: ese usuario accede y una identidad no autorizada no accede. La cuenta de Samba no elimina los permisos del sistema de archivos. El fragmento es un ejemplo independiente, no configura la matriz completa de grupos del dominio.

Fuente de instalación y estructura: Ubuntu, servidor de archivos Samba, https://ubuntu.com/server/docs/how-to/samba/file-server/. Para autenticación y controles adicionales, consulta el manual de tu versión.

Impresoras compartidas

Distingue el dispositivo físico, su cola en el servidor y la conexión desde el cliente. Define quién puede imprimir y quién administrar trabajos o la impresora. Instala controladores compatibles mediante mecanismos autorizados; no rebajes controles de seguridad para evitar un aviso.

La prueba incluye un documento real desde la cuenta y aplicación afectadas. Si un alumno puede imprimir pero no administrar la cola, puede ser exactamente el resultado correcto. Documenta también cómo retirar una conexión antigua al cambiar de servidor.

¿Lo has pillado?

1. ¿Probar como administrador del servidor demuestra que el alumno accede desde el cliente?

2. ¿SMB y la carpeta física son lo mismo?

3. ¿`guest ok = no` concede por sí solo permiso de escritura en Linux?

Soluciones. 1) No: identidad y recorrido son diferentes. 2) No: el protocolo y recurso publicado apuntan a una ubicación. 3) No: impide ese acceso como invitado, pero la autorización y los permisos del sistema siguen importando.

31. Administrar servidores y conectar sistemas distintos

Al terminar: organizarás almacenamiento, acceso remoto, supervisión e integración sin mezclar identidades. **Antes:** servicios, cuentas y recursos compartidos.

Un servidor debe funcionar cuando nadie está mirando su escritorio. Eso exige un arranque previsible, servicios gestionados, almacenamiento supervisado, actualizaciones planificadas y recuperación documentada. Una prueba manual exitosa es solo el principio.

Discos, volúmenes, cuotas y disponibilidad

Identifica discos físicos o virtuales, particiones, sistemas de archivos y puntos de montaje. Si un servicio espera una carpeta en un volumen que no se montó, puede escribir en otro lugar o fallar. Comprueba ubicación real antes de investigar la aplicación.

Una **cuota** limita uso de almacenamiento según las funciones del sistema. El espacio total libre no impide que un usuario alcance su cuota. Registra ambos datos si una operación falla por falta de espacio.

RAID combina unidades conforme a una organización. RAID 0 distribuye datos y no proporciona redundancia frente al fallo de una unidad. RAID 1 replica y permite tolerar ciertos fallos dentro de su diseño. RAID 5 y 6 añaden paridad y tienen requisitos y límites propios. No elijas un nivel solo por capacidad: considera carga, reconstrucción, supervisión y fallos previstos.

La redundancia no sustituye una copia: puede reproducir un borrado o corrupción en el conjunto. Un disco extra no se convierte en protección útil si nadie recibe ni atiende las alertas.

Acceso remoto y cuentas de administración

Utiliza protocolos adecuados y limita quién puede llegar a ellos. Una cuenta de administración debe ser distinta de la cuenta usada para navegar y leer correo cuando el diseño lo permita. Registra acciones y conserva un camino de recuperación ante un bloqueo de acceso.

En Windows puedes emplear herramientas remotas compatibles con el rol y edición. En Linux, SSH proporciona una vía habitual. Instalar un servicio remoto no exige publicarlo en Internet. En el laboratorio se mantendrá en la red interna.

Integrar no es duplicar nombres de usuario

Para integrar identidades entre Windows y Linux debes definir quién es la autoridad y cómo se traducen identidades y permisos. AD DS utiliza distintos protocolos para funciones diferentes. Kerberos participa en autenticación; LDAP permite acceder al directorio bajo su configuración y controles. No son dos nombres de la misma función.

Herramientas como SSSD o Winbind tienen usos y requisitos específicos. Un equipo Linux que autentica usuarios del dominio y un servidor Samba miembro que comparte archivos no son

necesariamente el mismo procedimiento. Sigue una guía correspondiente al objetivo y versión, en lugar de combinar fragmentos de ambas.

Qué comprobar en una integración de laboratorio

El equipo debe resolver nombres y registros del dominio, tener hora coherente y alcanzar los servicios necesarios. La unión debe registrar correctamente la máquina. Después comprueba una cuenta autorizada, sus grupos y el acceso a un recurso. Si solo verificas una contraseña, todavía no has probado la autorización sobre archivos.

Ampliación guiada: en una copia del laboratorio AD, elige una guía oficial para unir un cliente Ubuntu al dominio. Documenta paquetes, proveedor de identidades, nombre de dominio y mecanismo de creación de carpetas personales. No ejecutes varias guías de integración sobre el mismo invitado sin volver al estado inicial.

Práctica: ficha de operación del servidor

1. Registra nombre, interfaces, direcciones, discos, volúmenes y funciones del servidor de prácticas.
2. Identifica una dependencia: volumen de datos, DNS, reloj u otro servicio.
3. Comprueba el estado de un servicio y su modo de inicio. Reinicia el invitado en una ventana de laboratorio, no el servicio de otra persona.
4. Tras arrancar, verifica almacenamiento, identidad y una operación desde el cliente.
5. Anota dónde revisar registros, cómo recibir avisos y qué datos hacen falta para reconstruir el servidor.

Resultado esperado: la operación se puede realizar después de reiniciar, sin ajustes manuales que nadie haya documentado. Si falla, compara con el estado anterior y revisa dependencias y arranque.

SOS: puedo iniciar sesión, pero no abrir la carpeta

La autenticación puede estar funcionando mientras falla la traducción de grupos, el permiso de recurso o el sistema de archivos. Comprueba identidad y grupos efectivos, ruta, servicio y autorización. Cambiar la contraseña no corrige automáticamente un mapeo incorrecto de identidades.

Taller de integración: iniciar sesión en Linux con una identidad de AD

Usa un Ubuntu de prácticas añadido a la red interna **SMR-AD**, separado del servidor BIND del otro laboratorio. Su DNS será el controlador `10.77.0.10`, con dominio `aulanorte.test`; la hora debe estar sincronizada. Conserva una cuenta local administradora y una base recuperable. Que existan dos usuarios de igual nombre en máquinas distintas no demuestra integración.

En Ubuntu mantenido, instala las herramientas de integración de sus repositorios. Para la referencia del taller se utilizan `realmd`, `adcli`, `sssd-ad` y `sssd-tools`; la detección indica

dependencias adicionales como NSS/PAM y herramientas comunes. Revisa los paquetes y la documentación de tu versión.

```bash
sudo apt install sssd-ad sssd-tools realmd adcli
realm discover aulanorte.test
```

La detección debe localizar AD mediante DNS y mostrar la infraestructura prevista. Si no ocurre, investiga nombres, reloj, conectividad y servicios antes de forzar la unión. Después utiliza una cuenta con permiso para unir este equipo; no escribas su contraseña dentro del comando:

```bash
sudo realm join -U cuenta.union aulanorte.test
realm list
id 'ana.docencia@aulanorte.test'
getent passwd 'ana.docencia@aulanorte.test'
```

`cuenta.union` representa la cuenta autorizada que hayas preparado; no es un usuario incorporado automáticamente. Comprueba identidad y grupos recuperados del dominio. La creación de carpeta personal al primer acceso requiere la configuración PAM adecuada; la documentación de Ubuntu utiliza `sudo pam-auth-update --enable mkhomedir` para habilitar el mecanismo cuando corresponda.

Define quién puede iniciar sesión. En una práctica pequeña puedes aplicar la política de acceso de realmd y permitir solo la cuenta de prueba con `sudo realm permit 'ana.docencia@aulanorte.test'`, comprobando el resultado con `realm list`. Registra la política inicial y verifica con otra cuenta de prueba que no hayas autorizado accidentalmente a todo el dominio.

Inicia una sesión real con esa identidad, comprueba directorio personal y grupos y realiza una tarea autorizada. Una respuesta de `getent` demuestra resolución de identidad; no acredita por sí sola un inicio de sesión ni acceso a una carpeta. Si falla, separa esas fases y revisa los registros pertinentes sin publicar datos de cuentas.

Recuperación: conserva acceso local; utiliza el procedimiento de salida de dominio de realmd y coordina la retirada del objeto de equipo si se requiere. En este laboratorio puedes reconstruir el invitado desde su base. No borres objetos ni credenciales compartidas de una infraestructura real.

SSSD para autenticación de un cliente no configura automáticamente un servidor Samba miembro. Si necesitas compartir archivos con identidades del dominio, el diseño de Samba, Winbind/identidades y permisos se prepara según su documentación específica. Tampoco implica que cualquier GPO de Windows se aplique íntegramente a Linux.

Fuentes: Ubuntu, SSSD con Active Directory y realmd en Ubuntu. Revisado documentalmente; no ejecutado contra un dominio en el entorno editorial.

RAID: capacidad, fallos y límites

RAID 0 reparte datos entre unidades y no aporta redundancia: perder una puede destruir el conjunto. **RAID 1** mantiene copias en espejo; para dos unidades iguales su capacidad útil aproximada es la de una. **RAID 5** distribuye datos y paridad: con n unidades iguales ofrece aproximadamente (n - 1) capacidades y tolera el fallo de una, bajo su diseño. **RAID 6** utiliza doble paridad y aproximadamente (n - 2), tolerando dos fallos de unidad.

RAID 10 combina reparto y espejos. No basta contar «dos discos averiados»: importa si afectan a miembros del mismo espejo. En todos los casos hay metadatos, condiciones de implementación y procesos de reconstrucción. Un conjunto degradado necesita atención y la reconstrucción añade carga y riesgo.

Ejemplo de cuatro unidades ficticias de 2 TB iguales: RAID 0 ofrece unos 8 TB sin redundancia; RAID 5, 6 TB; RAID 6, 4 TB; RAID 10 convencional, 4 TB. Son capacidades decimales simplificadas antes de formato/metadatos. Un espejo no protege de borrar accidentalmente un archivo porque la operación puede reflejarse en todos sus miembros.

Práctica RAID 1 en discos virtuales desechables

En una VM Linux dedicada, prepara **dos discos virtuales vacíos adicionales**, distintos del de sistema. Registra identificadores y capacidades con las herramientas de almacenamiento. Instala `mdadm` de los repositorios y conserva la base del laboratorio. Crear el conjunto escribe metadatos; formatearlo después destruye el contenido anterior de esos discos.

En la sintaxis siguiente, sustituye los marcadores por los dos dispositivos verificados. Los marcadores **no son comandos listos para pegar** y no se utilizan discos físicos del host:

```text
mdadm --create /dev/md0 --level=1 --raid-devices=2 DISCO_A DISCO_B
```

La ejecución requiere permisos administrativos en esa VM. Comprueba estado con `cat /proc/mdstat` y `sudo mdadm --detail /dev/md0`; espera la sincronización prevista. Crea después el sistema de archivos sobre **el dispositivo del conjunto**, móntalo en la carpeta de laboratorio y escribe un marcador. No formatees por separado uno de sus miembros.

Bajo la guía del taller, utiliza la opción de marcar como fallido **un miembro identificado**, observa estado degradado y verifica lectura del marcador. Retira/sustituye ese disco virtual según el procedimiento de mdadm, añade un miembro vacío compatible y observa reconstrucción y estado final. No declares recuperación al empezar la resincronización.

Aceptación: contenido conservado, estados documentados, sincronización completada y copia independiente prevista. La prueba simula un fallo lógico de miembro en una VM; no demuestra resistencia del host ni recuperación de una cabina real. Para retirar el laboratorio, desmonta, detén el conjunto y conserva solo los discos de práctica identificados según el plan.

Fuente: manual mdadm de Ubuntu 24.04. No se creó un RAID real en este entorno editorial.

Cuotas de carpeta y cuotas de usuario

Una cuota limita o vigila uso bajo un ámbito: usuario, carpeta o volumen según herramienta. Una cuota **blanda** puede informar sin bloquear; una **dura** impide superar el límite previsto. No confundas falta de espacio físico con haber alcanzado una cuota.

En un Windows Server de laboratorio, instala el servicio de rol FSRM si no existe. Abre su administración, crea una carpeta de prueba vacía y una cuota sobre **esa ruta**, con límite pequeño definido por el docente. Distingue cuota dura o blanda, umbrales y acciones; no configures correos reales en la primera prueba.

Copia archivos ficticios hasta acercarte al límite y luego intenta superarlo. Compara con otra carpeta fuera de esa cuota. Comprueba aviso o bloqueo según elección, y retira solamente la cuota de práctica al terminar. Una cuota de carpeta FSRM y una cuota por propietario de NTFS tienen ámbitos diferentes.

Fuente: Microsoft, crear una cuota FSRM. El recorrido se propone como práctica de Windows Server; no se ha ejecutado en la edición.

¿Lo has pillado?

1. ¿RAID 1 recupera por sí solo un documento borrado ayer?

2. ¿Tener espacio libre elimina la posibilidad de una cuota agotada?

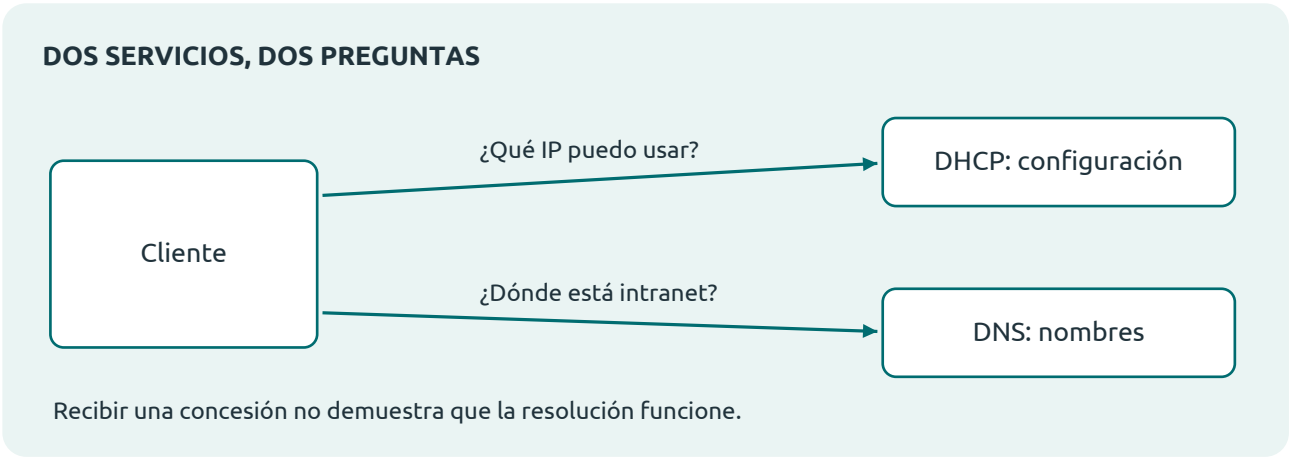
3. ¿Kerberos y LDAP tienen exactamente el mismo propósito?

Soluciones. 1) No: la eliminación puede reflejarse en la réplica; necesitas una copia o versión recuperable. 2) No: el límite puede ser de usuario o recurso. 3) No: participan en funciones diferentes de una infraestructura de identidades.

Bloque 6. Servicios en red

32. DHCP y DNS: configuración y nombres sin confundirlos

Al terminar: desplegarás un ejemplo de laboratorio de asignación IPv4 y resolución de nombres, y sabrás qué prueba corresponde a cada función. **Antes:** redes locales y administración Linux.



Asignación y resolución son funciones independientes.

DHCP entrega configuración a clientes. DNS responde consultas sobre nombres y otros datos. Un cliente puede recibir una dirección correctamente y no resolver la intranet, o resolver nombres y tener una puerta de enlace equivocada. Separar ambas funciones permite explicar el fallo.

Un laboratorio distinto al dominio



Ojo con este error

Este ejercicio utiliza una red virtual interna llamada `SMR-SERVICIOS`, separada de `SMR-AD`. No conectes ambos laboratorios ni dupliques la zona del dominio AD sobre servidores sin coordinar. Utiliza un invitado Ubuntu Server 24.04 LTS como referencia de estructura de paquetes y registra las versiones reales que instales. El servidor tendrá `10.77.0.20/24` fija; el cliente recibirá una dirección de `.100` a `.150`.

El nombre `enp0s8` de la plantilla es un ejemplo: sustitúyelo por la interfaz interna identificada en tu servidor. Instala paquetes y actualizaciones mediante acceso controlado y después deja la interfaz de DHCP únicamente en la red interna. No utilices puente a la red de casa, y desactiva el DHCP del hipervisor en esa red si lo hubiera. Para este ejercicio sin router no entregaremos una puerta de enlace inventada.

Qué sucede al pedir una configuración

En una asignación inicial típica de DHCPv4, el cliente descubre servidores, recibe ofertas, solicita una configuración y obtiene una confirmación. Se suele resumir como Discover, Offer, Request y Acknowledge, o DORA. No todo intercambio de renovación repite exactamente la misma secuencia inicial.

La **concesión** tiene un plazo. El cliente intenta renovar y, en ciertas condiciones, buscar confirmación de otros servidores. Una **reserva** asocia un identificador con una asignación prevista según el servidor. Una **exclusión** evita usar parte del rango dinámico. No confundas reserva con poner manualmente una IP en el cliente.

Los mensajes iniciales de difusión no atraviesan routers de la misma manera que una comunicación unicast ordinaria. Para atender otra subred puede requerirse un agente de retransmisión DHCP y una configuración coordinada. Un servidor instalado en cualquier punto no atiende automáticamente todos los segmentos.

Configuración mínima de Kea DHCPv4

En el invitado, instala `kea-dhcp4-server` desde el repositorio de Ubuntu. La distribución puede instalar y gestionar otros componentes; comprueba qué servicio estás configurando. Guarda una copia de `/etc/kea/kea-dhcp4.conf` antes de cambiarlo. En este invitado nuevo y desechable, la plantilla de recursos puede servir como configuración mínima:

JSON

```
{
  "Dhcp4": {
    "interfaces-config": { "interfaces": ["enp0s8"] },
    "lease-database": { "type": "memfile", "persist": true },
    "valid-lifetime": 3600,
    "renew-timer": 900,
    "rebind-timer": 1800,
    "subnet4": [
      {
        "id": 1,
        "subnet": "10.77.0.0/24",
        "pools": [ { "pool": "10.77.0.100 - 10.77.0.150" } ],
        "option-data": [
          { "name": "domain-name-servers", "data": "10.77.0.20" }
        ]
      }
    ]
  }
}
```

La interfaz limita dónde atiende. El bloque declara subred y rango de direcciones. Los temporizadores están expresados en segundos. La opción DNS apunta al servidor que configuraremos a continuación. No hemos configurado actualización dinámica de DNS: recibir una concesión no crea aquí un registro de nombre para cada cliente.

Valida antes de iniciar el servicio. La comprobación de sintaxis no demuestra que la interfaz exista ni que no haya otro DHCP:

```bash
sudo kea-dhcp4 -t /etc/kea/kea-dhcp4.conf
sudo systemctl restart kea-dhcp4-server
systemctl status kea-dhcp4-server
```

Consulta registros si falla y no continúes con el cliente hasta conocer el estado. Revisa también reglas del cortafuegos y que los mensajes DHCP puedan pasar por el enlace de laboratorio.

Fuente para opciones y servicio: Ubuntu, instalación de Kea, https://ubuntu.com/server/docs/how-to/networking/install-isc-kea/. La plantilla de este libro emplea un rango y opciones propios para una red aislada.

DNS: autoridad, consulta y caché

Un servidor **autoritativo** responde sobre zonas para las que es autoridad. Un **resolvedor recursivo** busca respuestas por cuenta del cliente conforme a su configuración y guarda información temporalmente. Un servidor puede cumplir ambos papeles, pero son funciones distintas. No expongas un resolvedor abierto a Internet para esta práctica.

Un registro **A** asocia un nombre con IPv4; **AAAA**, con IPv6. **CNAME** crea un alias bajo sus reglas. **MX** indica servidores de correo de un dominio, **NS** identifica servidores de nombres y **PTR** se utiliza en búsquedas inversas. El **TTL** influye en cuánto tiempo puede mantenerse una respuesta en caché.

Una **zona** es una porción administrada del espacio de nombres. Escribir `intranet` en el servidor web no crea un registro DNS. Los clientes necesitan consultar un servidor que conozca el nombre o disponer de otro mecanismo de resolución configurado.

Zona de laboratorio con BIND

Instala `bind9` y herramientas de consulta, como `bind9-dnsutils`, según los paquetes de la distribución. Guarda copia de sus archivos de configuración. Añade esta declaración a la configuración local de zonas, normalmente `/etc/bind/named.conf.local`:

```text
zone "aulanorte.test" {
    type primary;
    file "/etc/bind/db.aulanorte.test";
};
```

Crea el archivo de zona con contenido propio del laboratorio:

```text
$TTL 300
@ IN SOA ns1.aulanorte.test. hostmaster.aulanorte.test. (
  2026110501 3600 600 86400 300 )
@        IN NS ns1.aulanorte.test.
ns1      IN A 10.77.0.20
intranet IN A 10.77.0.20
archivos IN A 10.77.0.20
```

El punto final indica un nombre absoluto en el archivo de zona. El número de serie se incrementa al modificarla siguiendo un esquema coherente. La dirección del contacto en SOA tiene una representación especial: no es una contraseña ni una URL.

Comprueba configuración global y zona antes de aplicar:

```bash
sudo named-checkconf
sudo named-checkzone aulanorte.test /etc/bind/db.aulanorte.test
sudo systemctl restart bind9
```

En tu versión, confirma el nombre y alias de unidad del servicio. Limita la escucha, las consultas y cualquier recursión al ámbito previsto del laboratorio mediante las opciones de BIND y el cortafuegos. Que una zona sea correcta no define por sí solo toda esa política.

Fuente para estructura y comprobaciones: Ubuntu, DNS con BIND, https://ubuntu.com/server/docs/how-to/networking/install-dns/.

Verifica desde un cliente

Configura el cliente para obtener IPv4 automáticamente en la interfaz interna. En Windows, puedes renovar esa configuración con los mecanismos de la interfaz o `ipconfig /renew`; no liberes interfaces que sostienen una sesión remota. Comprueba concesión dentro de `.100-.150`, máscara `/24` y DNS `.20`. En Linux utiliza el gestor de red instalado para renovar y observar; no presupongas que `dhclient` esté disponible.

Desde un cliente que tenga `dig`, ejecuta `dig @10.77.0.20 intranet.aulanorte.test A`. Debe devolver `.20`. Después consulta mediante el resolvedor normal del cliente. La primera prueba demuestra que el servidor responde a una consulta explícita; la segunda comprueba el camino que utilizan sus aplicaciones.

Resultado esperado: el cliente obtiene configuración y resuelve el nombre interno. No esperes navegar por Internet: el diseño no ofrece router ni resolución pública. En el capítulo siguiente usaremos el nombre para acceder al servicio web.

Recuperación: detén el DHCP de prácticas antes de conectar el invitado a otra red. Restaura configuraciones guardadas o reconstruye el invitado. Conserva las concesiones y consultas como evidencias sin datos personales.

SOS: recibo dirección, pero no resuelvo

Comprueba qué servidor DNS recibió el cliente y consulta ese servidor explícitamente. Revisa zona cargada, interfaz de escucha y filtros. Una concesión que entrega `.20` no demuestra que BIND esté funcionando en `.20`. Si aparece una dirección de otro rango, investiga otro DHCP o una conexión virtual incorrecta.

Taller DNS: alias, correo, caché y una secundaria

Amplía la zona de prácticas con registros A para `correo` y `ftp` apuntando al servidor `.20`, y un registro MX de `aulanorte.test` hacia `correo.aulanorte.test.`. MX apunta a un nombre de servidor, no directamente a una dirección IP. Para un alias de prueba utiliza CNAME sobre un nombre que no tenga datos incompatibles. Incrementa el serial, valida y recarga según el capítulo.

Un resolvedor recursivo busca respuestas y puede conservarlas en caché; una zona autoritativa mantiene los datos que administra. Restringe recursión y acceso a caché a las redes autorizadas. No expongas un resolvedor abierto. Si el docente proporciona salida NAT controlada, consulta un dominio público documental y repite antes de caducar el TTL; observa caché y tiempos sin confundir esa prueba con la autoridad de tu zona interna.

Prepara una segunda VM BIND en `10.77.0.21` dentro de SMR-SERVICIOS. Para la zona, configura el primer servidor como primario y el segundo como secundario. Este obtiene los datos mediante transferencia; no edites su copia recibida como si fuera el origen.

En un primer montaje cerrado puedes restringir transferencias a `.21`; para autenticarlas utiliza **TSIG**, una clave compartida entre los servidores. Genera una clave del algoritmo admitido con `tsig-keygen`, guarda el archivo con permisos de lectura solo para el servicio y administración, y distribúyelo por el canal del laboratorio. TSIG autentica; no cifra todos los datos DNS.

En el primario, integra la clave y autoriza transferencia para ella en la zona. En el secundario, integra la misma clave, declara `type secondary`, especifica el primario y su clave y elige una ruta de copia que BIND pueda escribir. No publiques el secreto ni lo incluyas en el repositorio del ejercicio.

Esquema de la zona secundaria, con clave generada aparte:

```text
zone "aulanorte.test" {
    type secondary;
    primaries { 10.77.0.20 key aulanorte-transfer; };
    file "/var/cache/bind/db.aulanorte.test";
};
```

Valida configuración en ambos equipos. Comprueba SOA y un registro en cada servidor; modifica un dato ficticio en el primario, aumenta serial, valida/recarga y observa transferencia y coincidencia del serial. Una consulta AXFR sin la clave desde un cliente no autorizado debe

rechazarse si así has definido el control. Mantén la clave del lado servidor; no la copies a todos los clientes para probar.

Aceptación: ambos responden los datos previstos, la secundaria recibe cambios y el acceso de transferencia queda limitado. Documenta TTL, serial y registros depurados. Para recuperar, conserva la zona primaria y la configuración anterior; la secundaria no sustituye una copia de seguridad de todo el servicio.

Fuentes: BIND 9, configuración y zonas y seguridad y TSIG. La transferencia y caché son prácticas propuestas; no se ejecutaron servidores BIND en la edición.

¿Lo has pillado?

1. ¿La plantilla crea registros DNS de los clientes automáticamente?

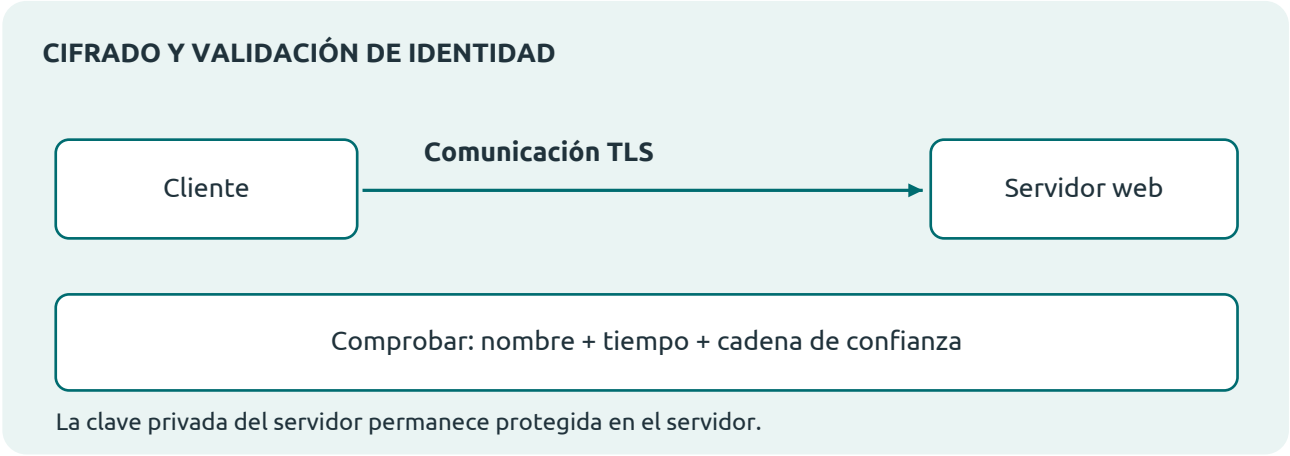
2. ¿Consultar con `dig @servidor` prueba por sí solo la configuración del resolvedor del sistema?

3. ¿Hay que anunciar un router inexistente para que DHCP funcione?

Soluciones. 1) No: no configura actualización dinámica. 2) No: selecciona explícitamente el servidor de esa consulta. 3) No: una red aislada puede funcionar sin ruta predeterminada.

33. Servidor web: del nombre a una respuesta verificable

Al terminar: publicarás una página estática de laboratorio y distinguirás HTTP, TLS, nombre y contenido. **Antes:** capítulo 32 y permisos de archivos.



Tener cifrado no basta si se ignora la identidad del extremo.

Un servidor web escucha peticiones y devuelve respuestas. El navegador interpreta recursos y construye una presentación. El DNS permite localizar una dirección; el servidor decide qué sitio y contenido corresponden a la petición. Un nombre bien resuelto no demuestra que el sitio correcto esté configurado.

Petición, método y estado



Ojo con este error

Una petición contiene información como método, destino y cabeceras. **GET** solicita una representación; **POST** envía contenido para ser procesado conforme a la aplicación. No asumas que usar POST cifra los datos: el transporte y la aplicación determinan su protección.

Las respuestas incluyen un estado. `200` suele indicar éxito de la petición; `301` o `302`, redirección; `403`, acceso rechazado; `404`, recurso no encontrado; y `500`, error interno. Interpretar el mensaje exige contexto. Un `404` demuestra que hubo una respuesta HTTP de algún servidor, pero puede ser el sitio equivocado.

Publicar una página estática con Apache

En el invitado Linux del laboratorio instala `apache2` desde el repositorio. Prepara `/srv/www/aulanorte` con permisos de lectura y recorrido adecuados para el servicio; no conviertas al proceso web en propietario con escritura de todo el árbol por comodidad.

Copia la página ficticia `index.html` incluida en recursos a esa carpeta mediante administración autorizada. Su texto distintivo es `AN-01`, útil para reconocer el sitio esperado. No publiques

copias de seguridad, claves, contraseñas o ficheros de configuración dentro del directorio servido.

Crea `/etc/apache2/sites-available/aulanorte.conf` con este ejemplo para la estructura de paquetes de Ubuntu:

APACHE

```
<VirtualHost *:80>
    ServerName intranet.aulanorte.test
    DocumentRoot /srv/www/aulanorte
    <Directory /srv/www/aulanorte>
        Options -Indexes
        AllowOverride None
        Require all granted
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/aulanorte-error.log
    CustomLog ${APACHE_LOG_DIR}/aulanorte-access.log combined
</VirtualHost>
```

`ServerName` selecciona el nombre del sitio. `DocumentRoot` indica el contenido. El bloque Directory permite el acceso a esa ubicación; `Options -Indexes` evita el listado automático de directorios bajo esa configuración. Permitir lectura HTTP no equivale a permitir escritura sobre los archivos del servidor.

Habilita el sitio con `sudo a2ensite aulanorte.conf`, comprueba mediante `sudo apache2ctl configtest` y, si el resultado es correcto, aplica con `sudo systemctl reload apache2`. Un error de sintaxis debe corregirse antes de recargar. Las herramientas y rutas son específicas del empaquetado; no las copies literalmente a otra distribución sin revisarlas.

Fuente para la selección de sitios por nombre: Apache HTTP Server 2.4, https://httpd.apache.org/docs/2.4/vhosts/examples.html. Este ejemplo usa rutas y contenido propios de la práctica.

Verificar sin confundir pruebas

Desde el cliente, consulta el DNS y abre `http://intranet.aulanorte.test`. Debes ver el texto `AN-01`. Si visitas solo la dirección IP, puede aparecer el sitio predeterminado y no el que querías probar.

Con `curl -I http://intranet.aulanorte.test` consultas cabeceras mediante una petición HEAD. Para comprobar el contenido, realiza una petición GET normal, como `curl http://intranet.aulanorte.test`, o usa el navegador. No declares correcto el contenido por obtener una cabecera de éxito.

Registra la petición en el log de acceso y revisa el log de error si no funciona. Que el archivo sea legible por un administrador no prueba que el proceso de Apache pueda recorrer su ruta y leerlo.

HTTPS y certificados

HTTPS combina HTTP con una comunicación protegida por TLS. El cliente debe comprobar, entre otros aspectos, nombre, validez temporal y confianza en el certificado. El certificado incluye una clave pública; la clave privada correspondiente debe mantenerse protegida.

Un certificado para otro nombre no se vuelve correcto porque el navegador permita avanzar. En el laboratorio `.test` se utilizan mecanismos de confianza internos o de prueba; no puedes tratarlo como un nombre público validable por cualquier autoridad pública.

Ampliación práctica: en un invitado aislado, configura un sitio TLS con un certificado que incluya `intranet.aulanorte.test` en su extensión de nombres alternativos. Utiliza una autoridad de laboratorio y distribuye su certificado de confianza únicamente a los clientes de prueba por un procedimiento controlado. No distribuyas su clave privada. Configura certificado y clave en el sitio TLS, habilita el módulo necesario, comprueba sintaxis y verifica desde el cliente sin desactivar validación.

Prueba además un nombre distinto: la validación debería rechazarlo si no está cubierto. Ese resultado es parte del aprendizaje. Al cerrar, retira la confianza de prueba del cliente y elimina las claves del laboratorio conforme al plan.

HTTPS paso a paso con confianza limitada a una prueba

En recursos encontrarás `crear-certificados-laboratorio.sh`. Lee el script antes de ejecutarlo. Con Bash y OpenSSL disponibles, pásale la ruta de un directorio nuevo: generará una autoridad efímera y un certificado de servidor de siete días. No modifica la confianza del equipo ni instala servicios. Sus claves privadas quedan en el directorio de salida con permisos restringidos; son material exclusivo del laboratorio.

Copia `servidor.crt` a `/etc/ssl/certs/aulanorte-servidor.crt` y `servidor.key` a `/etc/ssl/private/aulanorte-servidor.key` en el invitado servidor, con propietario y permisos adecuados: la clave privada debe quedar bajo control administrativo, por ejemplo root y modo 600. No la pongas en `/srv/www/aulanorte`. La clave de la autoridad, `ca.key`, no se copia al servidor web ni al cliente.

El archivo `aulanorte-apache-tls.conf` de recursos define el sitio del puerto 443 y esas rutas. Cópialo a `sites-available`, habilita SSL mediante `sudo a2enmod ssl` y el sitio con `sudo a2ensite aulanorte-apache-tls.conf`. Revisa que la configuración incluya escucha en 443 sin duplicarla y que permita solo los protocolos TLS previstos por el ejemplo y compatibles con tu versión. Comprueba con `sudo apache2ctl configtest`, recarga y verifica las reglas del cortafuegos interno.

Entrega únicamente `ca.crt` al cliente por una vía fiable. Para esta prueba puedes limitar la confianza a una invocación de curl, sin instalar la autoridad en todo el sistema:

```bash
curl --cacert ca.crt https://intranet.aulanorte.test
```

Ejecuta desde la carpeta del cliente que contiene `ca.crt`, con DNS de laboratorio funcional. Debe devolver el contenido AN-01 sin utilizar opciones que desactiven la validación. Si pruebas otra dirección o nombre no cubierto por el certificado, la validación debe fallar. Si falla con el nombre correcto, revisa reloj, certificado servido, cadena y archivo de confianza antes de modificar nada.

Cierre de la ampliación: deshabilita el sitio TLS de prueba si ya no se necesita y recarga tras comprobar sintaxis. Retira certificados y claves efímeros conforme al plan. Como `--cacert` solo afectó a esa invocación, no queda una autoridad añadida por este procedimiento al almacén global del cliente.

Fuentes: directivas TLS de Apache, https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html; generación de solicitudes y certificados con OpenSSL, https://docs.openssl.org/3.0/man1/openssl-req/. El script es un recurso didáctico propio, no una infraestructura de certificación para producción.

SOS: aparece otra web

Revisa nombre enviado, IP resuelta, puerto, configuración activa y orden del sitio predeterminado. Un virtual host no crea DNS. Un registro DNS tampoco activa el virtual host. Si una caché conserva un dato antiguo, identifica cuál y su alcance antes de vaciar todo sin necesidad.

¿Lo has pillado?

1. ¿HTTP 200 demuestra que has recibido el sitio deseado?

2. ¿POST cifra por sí mismo la información?

3. ¿El certificado público debe incluir la clave privada para que el cliente valide?

Soluciones. 1) No: comprueba nombre y contenido distintivo. 2) No: el método no sustituye TLS. 3) No: la clave privada no se entrega al cliente y debe protegerse.

34. Transferir archivos y administrar a distancia

Al terminar: distinguirás FTP, FTPS, SFTP, SSH y escritorio remoto, y verificarás una transferencia. **Antes:** servicios, usuarios, permisos y claves.

LA PRIVADA NO VIAJA AL SERVIDOR



Además: el cliente verifica la clave de host del servidor.

La autenticación no elimina los permisos de los archivos.

La clave pública autorizada y la clave de host cumplen papeles distintos.

Elegir una herramienta por su icono puede ocultar diferencias importantes. Dos programas capaces de copiar archivos pueden utilizar protocolos distintos y tener requisitos diferentes de cifrado, autenticación y cortafuegos.

Tres siglas que no son intercambiables

FTP utiliza un canal de control y conexiones de datos. En su forma tradicional sin TLS no protege credenciales y contenido frente a quien pueda observar el tráfico. Los modos activo y pasivo influyen en cómo se establece el canal de datos y en su paso por filtros o NAT.



Ojo con este error

FTPS añade protección TLS a FTP bajo sus modalidades. Sigue necesitando atender el diseño de canales y puertos. **SFTP** es un protocolo de transferencia asociado habitualmente a SSH. No es «FTP por el puerto 22» y no se configura con las mismas opciones de un servidor FTP.

Para las prácticas iniciales usaremos SFTP sobre SSH dentro del laboratorio. Conocer FTP permite interpretar temarios y sistemas heredados, pero no justifica enviar contraseñas reales sin protección.

SSH: identidad del servidor e identidad del usuario

SSH ofrece acceso remoto protegido y otras funciones. Antes de autenticar al usuario, el cliente debe verificar la identidad del servidor mediante su clave de host y el mecanismo de confianza utilizado. Aceptar una huella sin contrastarla es una decisión de confianza, no una comprobación realizada.

En el primer acceso de laboratorio, consulta la huella desde una vía fiable, por ejemplo la consola del invitado. Si después cambia, investiga si se reconstruyó el servidor o si hay otra causa. No borres la advertencia de `known_hosts` como respuesta automática.

La autenticación del usuario puede utilizar contraseña o claves, entre otros métodos. Una clave privada protegida permanece en el cliente correspondiente; la pública se incorpora al mecanismo autorizado del servidor. La frase de paso protege la clave privada almacenada, pero no concede por sí sola acceso al servidor.

Preparar el servicio en el invitado

En Ubuntu, instala `openssh-server` desde el repositorio y comprueba el estado del servicio correspondiente. Usa una cuenta ordinaria de laboratorio con permisos sobre su carpeta personal. Limita el acceso al segmento interno y registra la configuración antes de editarla.

En OpenSSH puedes comprobar la sintaxis del servidor con `sudo sshd -t`. Los archivos incluidos y valores efectivos pueden modificar el resultado: revisa la configuración de tu versión. Mantén abierta una vía de consola y una sesión válida al probar cambios de autenticación; no cierres el único acceso antes de comprobar el nuevo.

Práctica de transferencia por SFTP

Desde un cliente con OpenSSH, inicia `sftp docente1@10.77.0.20`, usando una cuenta existente del servidor. Verifica primero la clave de host por el procedimiento anterior. La contraseña, si se utiliza, se introduce cuando la herramienta la solicita, no dentro de la instrucción.

En la sesión SFTP:

```text
pwd
ls
lpwd
put entrega.txt
get entrega.txt recuperada.txt
bye
```

Antes de iniciar, crea `entrega.txt` en la carpeta local del cliente con un texto ficticio. `pwd` y `ls` se refieren al contexto remoto; `lpwd`, al local. `put` sube desde el cliente y `get` descarga. Confirma las rutas antes de sobrescribir un nombre existente.

Resultado esperado: existe el archivo remoto y la copia recuperada tiene el mismo contenido. Puedes comparar un hash criptográfico de original y recuperado para comprobar igualdad de bytes. Una transferencia anunciada como completa no verifica que el documento subido sea la versión que querías entregar.

Recuperación: conserva la evidencia y elimina únicamente los archivos ficticios de cliente y servidor tras confirmar sus rutas. Si cambiaste la configuración de acceso, restáurala mediante la consola y verifica de nuevo.

Fuente de herramientas y parámetros: manuales de OpenSSH, https://www.openssh.org/manual.html. Los manuales publicados pueden describir una versión más reciente que la instalada: consulta también la ayuda local.

Escritorio remoto

Un escritorio remoto transmite la interacción con una sesión gráfica. Requiere un servicio compatible, una edición que lo ofrezca, autorización y conectividad. Que Windows permita actuar como cliente no demuestra que esa edición acepte conexiones entrantes como servidor.

En una práctica Windows compatible, habilita el servicio solo en la red interna, autoriza una cuenta de prueba y conecta desde el cliente. Comprueba qué sesión se inicia, cómo se cierran las conexiones y qué sucede al desconectar frente a cerrar sesión. No publiques directamente ese acceso en Internet como parte del ejercicio.

SOS: autentico, pero no puedo subir

La autenticación puede ser correcta y faltar escritura o espacio, existir una cuota o estar mal elegida la ruta remota. Comprueba la identidad, el directorio actual y los permisos antes de cambiar la contraseña o desactivar controles.

Taller FTP/FTPS: control, datos y acceso anónimo limitado

Para estudiar FTP prepara otra VM aislada o una copia del servidor SMR-SERVICIOS, con `.20`, sin conexión puente a una red real. La referencia es **vsftpd 3.0.5 de Ubuntu 24.04**. Comprueba versión y opciones: no copies esta plantilla a un paquete anterior que desconozca los parámetros TLS.

FTP separa conexión de control y conexión de datos. En **pasivo**, el cliente abre la conexión de datos hacia un puerto anunciado por el servidor; en **activo**, el servidor conecta con el extremo indicado por el cliente. Por eso permitir únicamente TCP 21 puede dejarte autenticar sin listar ni descargar. Texto y binario también tienen semántica de transferencia; para comparar archivos exactos utiliza el modo binario apropiado.

Instala vsftpd en esa VM, prepara `/srv/ftp` con contenido ficticio legible y sin escritura para el usuario anónimo, y conserva la configuración previa. `recursos/servicios/ampliacion/vsftpd-lab.conf` limita clientes, tasa, puertos pasivos y acceso: anónimo de solo lectura, cuentas locales deshabilitadas y TLS requerido en autenticación/datos.

Genera el certificado de laboratorio con el script de esa carpeta en un destino nuevo. El certificado incluye `ftp.aulanorte.test`; la clave privada solo va al servidor, con permisos restrictivos. Copia certificado y clave a las rutas de la plantilla. El cliente recibe únicamente el certificado público de la CA por el mecanismo de confianza del aula.

Integra la configuración, verifica el arranque y revisa registros. Permite en el cortafuegos de laboratorio control 21 y datos pasivos 50000-50010 desde los clientes previstos. Para el ensayo activo estudia también el flujo de vuelta al cliente y su cortafuegos; no abras rangos indiscriminados en una red real.

Desde un cliente con curl compatible con FTPS explícito:

```bash
curl --ssl-reqd --cacert ca.crt ftp://ftp.aulanorte.test/
curl --ssl-reqd --cacert ca.crt \
  ftp://ftp.aulanorte.test/prueba.txt -o descarga.txt
```

Compara el archivo descargado con el original ficticio mediante hash o contenido. Después ensaya un cliente gráfico configurando FTP con TLS **explícito**, modo pasivo y validación de la CA/nombre. SFTP utiliza SSH y otro servicio; seleccionar SFTP no convierte esta conexión en FTPS.

Prueba que la subida anónima falle, que una conexión sin TLS se rechace y que un nombre de certificado incorrecto no se acepte. En una copia autorizada, cambia el cliente a modo activo y comprueba conexión de datos y reglas necesarias. No desactives validación de certificados para que desaparezca un error.

Resultado esperado: lectura autorizada y cifrada, integridad del archivo y rechazos previstos. Si se requiere gestionar usuarios con escritura, prepara cuentas/grupos, directorios y permisos mínimos en un ejercicio separado, como el SFTP de este capítulo; no amplíes escritura anónima. Recupera configuración o retira solo esta VM/certificados de prueba al cerrar.

Fuentes: vsftpd.conf de Ubuntu 24.04 y curl, uso de FTP/TLS. TLS 1.0/1.1 y SSL están deshabilitados en la plantilla; se permiten TLS 1.2/1.3 según soporte del paquete. No se ejecutó vsftpd en la edición.

Taller de acceso gráfico entre sistemas

El acceso gráfico necesita un servicio compatible y autorizado, identidad y consentimiento, además de conectividad. En un Windows de laboratorio que admita alojar Escritorio remoto, habilita el servicio desde su configuración, autoriza solo una cuenta de prueba y conserva NLA y controles del entorno. No confundas cliente RDP disponible con capacidad de alojar sesiones de cualquier edición.

Desde un cliente Linux con aplicación RDP autorizada, indica el nombre del equipo, verifica la identidad del servidor según el mecanismo del laboratorio y autentica sin guardar contraseñas en el ticket. Comprueba una tarea ficticia, cierre y fin de sesión. Prueba una cuenta no autorizada y registra su rechazo. No publiques 3389 en Internet para realizar este ejercicio.

Si la práctica utiliza un servidor gráfico Linux, sigue el procedimiento específico de esa distribución y entorno; X11, Wayland, VNC y RDP no son términos intercambiables. Documenta protocolo, servicio, cifrado y autorización elegidos. El taller se realiza en las máquinas del aula; la edición no acredita una sesión gráfica ejecutada.

¿Lo has pillado?

1. ¿FTPS y SFTP usan el mismo protocolo de transferencia?

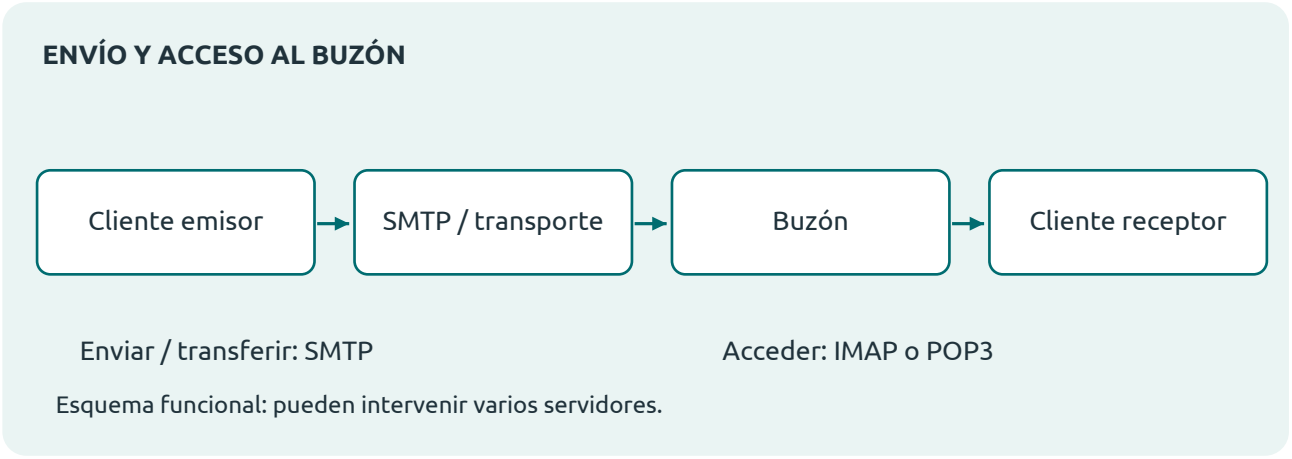
2. ¿La clave pública del usuario debe mantenerse secreta igual que la privada?

3. ¿Desconectar un escritorio remoto equivale siempre a cerrar sesión?

Soluciones. 1) No: FTPS protege FTP con TLS; SFTP usa su propio protocolo, normalmente sobre SSH. 2) No tienen el mismo papel: la privada es secreta; la pública se distribuye mediante el procedimiento apropiado. 3) No: una sesión puede seguir abierta según la plataforma y políticas.

35. Correo, proxy, NAT y encaminamiento

Al terminar: seguirás el recorrido de un mensaje y distinguirás varios servicios que suelen reunirse bajo «el servidor de Internet». **Antes:** DNS, rutas y transporte.



Aceptar, entregar y leer un mensaje son resultados diferentes.

No hace falta instalar todos los servicios posibles para entender una red. Sí necesitas saber qué función estás pidiendo y qué prueba la valida. Un proxy no es automáticamente un router y un servidor de correo no se identifica únicamente por poder abrir un puerto.

El recorrido de un correo

El cliente entrega un mensaje al servicio de envío autorizado. La infraestructura decide cómo transportarlo al dominio destinatario, donde se almacena o procesa. El destinatario accede mediante el servicio correspondiente. **SMTP** participa en envío y transferencia; **IMAP** permite gestionar correo en el servidor; **POP3** ofrece otro mecanismo de acceso con su comportamiento y configuración.

Los puertos habituales orientan, pero debes identificar protección TLS, autenticación y función. SMTP entre servidores no equivale al envío autenticado de un usuario. No conviertas un servidor en **relay abierto**, capaz de retransmitir indiscriminadamente mensajes ajenos: necesita políticas de destinatarios, redes y autenticación.

DNS aporta registros MX y otros datos relacionados. SPF, DKIM y DMARC contribuyen a políticas y comprobaciones de correo con funciones distintas; ninguno permite prometer que un mensaje es seguro por sí solo. Publicar correo real exige además identidad de dominio, reputación, protección, registros adecuados y mantenimiento. Aquí mantendremos mensajes ficticios dentro del laboratorio.

Práctica de análisis de correo

Utiliza un mensaje de prueba propio o un ejemplo ficticio con remitente, destinatario, fecha, asunto, `Message-ID` y varias líneas `Received`. Distingue dirección visible del remitente, datos de transporte y resultados de autenticación añadidos por infraestructura fiable. Las cabeceras pueden contener datos personales y no todas sus afirmaciones son igualmente confiables.

Dibuja cliente envío transporte buzón acceso. Sitúa SMTP e IMAP donde proceda. Si montas un servicio de correo de formación, configura aceptación solo para cuentas y dominio del laboratorio, sin publicación exterior, y prueba expresamente el rechazo de una retransmisión no autorizada.

Resultado esperado: explicas que recibir una respuesta SMTP de aceptación no prueba por sí solo que el destinatario haya leído el mensaje. Para verificar el caso hace falta observar entrega al buzón y acceso con la identidad prevista.

Referencias de protocolos de correo: SMTP, https://www.rfc-editor.org/rfc/rfc5321; IMAP 4rev2, https://www.rfc-editor.org/rfc/rfc9051.

Proxy directo e inverso

Un **proxy directo** actúa como intermediario para clientes que lo utilizan según la configuración. Puede aplicar controles y registrar tráfico dentro del alcance y obligaciones del entorno. Un **proxy inverso** recibe peticiones destinadas a servicios y las reenvía a servidores internos; puede centralizar funciones de entrada, reparto y TLS.

Un intermediario no tiene acceso automático al texto descifrado de cualquier HTTPS. La inspección TLS exige un diseño específico de confianza y tiene consecuencias técnicas y de privacidad. No instales certificados de inspección en equipos de otras personas para completar una práctica.

NAT y PAT

NAT transforma direcciones conforme a reglas. La traducción de puertos, frecuentemente llamada PAT o NAPT, permite distinguir comunicaciones de varios clientes que comparten una dirección de salida. NAT no sustituye el cortafuegos ni constituye una autorización de acceso por sí mismo.

En una salida doméstica típica, un cliente privado envía al router; este aplica traducción y mantiene estado para devolver respuestas. Un reenvío de puertos crea una regla para llegar a un servicio interno bajo condiciones concretas. Activarlo aumenta el alcance del servicio y no forma parte de este laboratorio aislado.

Encaminamiento: ida y vuelta

Dos redes requieren caminos apropiados y reglas en ambos sentidos. Un router con dos interfaces no encamina automáticamente en todos los sistemas: puede necesitar habilitar reenvío y políticas. Un cliente también necesita saber a qué siguiente salto enviar el tráfico remoto.

Para practicar, dibuja red A `10.77.10.0/24`, red B `10.77.20.0/24` y un router con `.1` en cada red. Un cliente A usa `.1` de A para llegar a B; el cliente B necesita un camino de regreso. Si un cortafuegos bloquea el tráfico, las rutas pueden ser correctas y la comunicación seguir fallando.

Caso resuelto: una aplicación solo falla al activar el proxy

Sin proxy, la intranet de laboratorio responde. Con el proxy configurado, el nombre interno no se resuelve desde el intermediario o la política rechaza la petición. Comprueba desde qué equipo se realiza la resolución y qué destinos quedan exceptuados conforme al diseño. No concluyas que el servidor web está caído porque el cliente muestra un error de proxy.

Taller de correo interno: SMTP, buzón y cliente

El laboratorio utiliza **Ubuntu 24.04, Postfix y Dovecot 2.3**, dos cuentas locales ficticias y dominio `aulanorte.test`. No tiene salida de correo a Internet. Dovecot 2.4 cambia parámetros: comprueba versión y utiliza su guía de migración si no tienes 2.3; esta plantilla no es intercambiable.

Prepara resolución de `correo.aulanorte.test` a `.20` y el MX de la zona. Instala `postfix` y `dovecot-imapd` desde los repositorios en una VM aislada. Si el asistente de Postfix pregunta por nombre de correo, indica el dominio del laboratorio. Crea `correoana` y `correoluis` con contraseñas de prueba propias y directorios personales; no reutilices cuentas o mensajes reales.

`recursos/servicios/ampliacion` contiene ajustes para `main.cf`, el servicio de presentación `submission` de `master.cf` y un fragmento para Dovecot 2.3. Conserva el resto de la configuración del paquete e integra los cambios sin duplicar servicios o parámetros contradictorios.

El diseño separa recepción SMTP 25 y presentación autenticada 587. La primera acepta destinos locales y rechaza relay externo desde clientes no autorizados. La segunda exige STARTTLS y autenticación mediante el socket de Dovecot. El buzón utiliza Maildir en el directorio del usuario; IMAPS 993 permite su lectura cifrada.

Genera el certificado con el script de ampliación y utiliza las rutas indicadas en ambos servicios. La clave queda en el servidor bajo control administrativo. En Dovecot 2.3, el prefijo < de `ssl_cert`/`ssl_key` indica leer el archivo. Mantén habilitado el backend de autenticación de cuentas locales del paquete y comprueba permisos del socket SASL para Postfix.

Añade a `/etc/aliases` un alias ficticio `docencia: correoana` y ejecuta la reconstrucción prevista, como `sudo newaliases`. No sustituyas los alias administrativos existentes sin revisarlos. Valida con `sudo postfix check`, revisa los ajustes efectivos con `postconf -n` y `doveconf -n` y reinicia/recarga según el servicio y el cambio.

Pruebas de envío, lectura y rechazo

En un cliente de laboratorio configura dos perfiles de correo: entrada `correo.aulanorte.test`, IMAP 993 con TLS; salida mismo nombre, SMTP 587 con STARTTLS y autenticación de la cuenta local. Verifica la CA y el nombre. Envía un mensaje ficticio de `correoana@aulanorte.test` a `correoluis@aulanorte.test`; comprueba entrega, lectura y respuesta. Prueba después el alias docencia y adjunto ficticio.

Para el rechazo de relay usa desde **otro cliente de la red**, sin autenticar, SMTP 25. Una sesión TLS de diagnóstico puede establecerse así:

```bash
openssl s_client -starttls smtp -connect correo.aulanorte.test:25 \
  -servername correo.aulanorte.test -CAfile ca.crt \
  -verify_hostname correo.aulanorte.test -verify_return_error -crlf
```

Dentro de la sesión, escribe EHLO con el nombre ficticio del cliente, MAIL FROM de una cuenta de laboratorio y RCPT TO hacia `nadie@example.invalid`. La petición de relay debe rechazarse antes de enviar datos. Termina con RSET/QUIT. No pruebes esa dirección desde el propio servidor confiable: cambiarías la condición de autorización.

Registra códigos, cola y eventos necesarios sin credenciales. Mensaje en cola, aceptación SMTP, entrega al buzón y lectura son resultados distintos. Si el destino local es aceptado pero el buzón no aparece, revisa entrega/Maildir, usuario y permisos; si IMAP falla, separa TLS, autenticación y ubicación.

Aceptación y recuperación: dos cuentas envían y leen, el alias llega al destinatario previsto, una credencial incorrecta y un relay no autorizado fallan. Conserva ajustes y datos ficticios para restaurar en una VM nueva; la copia debe incluir buzones y configuración pertinente. Este montaje no resuelve publicación real, reputación, DNS público o protección de un servicio de correo de Internet.

Fuentes: Ubuntu, Postfix, Dovecot 2.3, TLS, integración SASL con Postfix y cambios de 2.3 a 2.4. Plantillas contrastadas documentalmente; no se desplegó correo en el entorno editorial.

Taller de proxy explícito con control de acceso

Un proxy directo recibe peticiones del cliente para acceder a recursos; un proxy inverso representa servicios del lado servidor. El primero puede aplicar controles y caché de respuestas que lo permitan. HTTPS mediante CONNECT crea un túnel; no se convierte automáticamente en contenido visible o cacheable para el proxy.

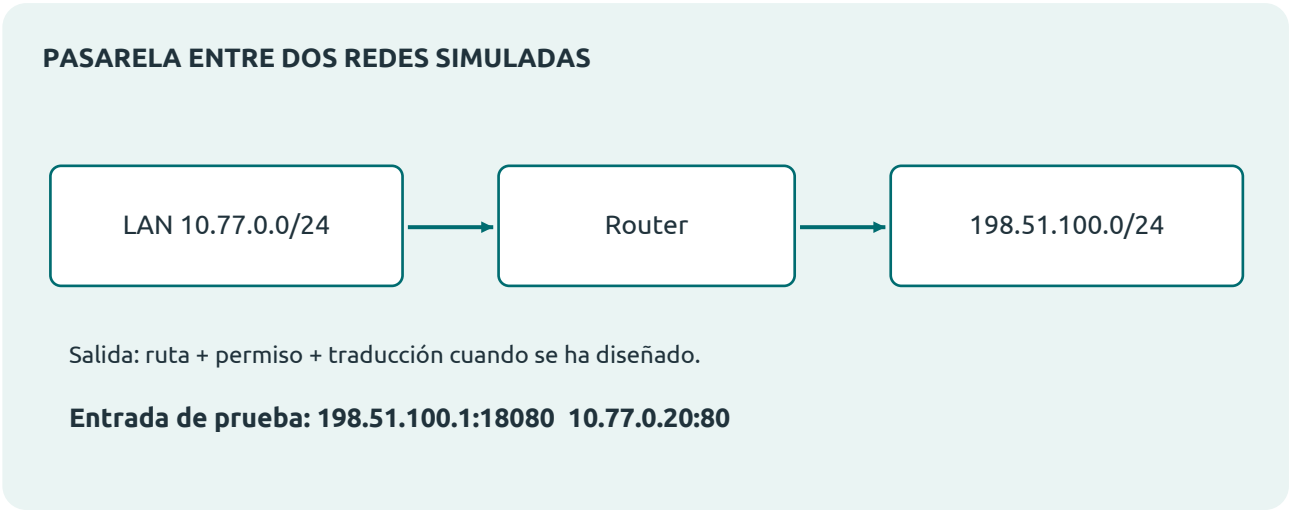
En una VM SMR-SERVICIOS instala Squid y conserva su configuración. La plantilla `squid-lab.conf` escucha 3128, limita origen/destino a la red de práctica y permite solo los puertos definidos. Integra el archivo del laboratorio, prepara el directorio de caché con el procedimiento del paquete y valida mediante `squid -k parse` antes de iniciar.

Configura un navegador de prueba con ese proxy y abre la intranet por su nombre. Comprueba registros y resultado. Una petición a otro puerto o destino fuera del alcance debe rechazarse. Retira después el proxy del cliente y explica por qué cambia el recorrido.

Para estudiar caché, usa un recurso HTTP ficticio preparado con controles de caché y repite la solicitud. Comprueba la evidencia del registro de Squid y las cabeceras del recurso; que la segunda carga sea rápida no demuestra un HIT. No interceptes TLS ni certificados de usuarios para esta práctica.

Fuente: Squid, ACL y orden de acceso. La plantilla es de laboratorio y no se ha ejecutado Squid en la edición.

Taller de pasarela: un exterior simulado



Las dos redes son internas al hipervisor; no hay publicación en Internet.

Prepara tres papeles en redes internas del hipervisor: cliente/servidor de LAN `10.77.0.0/24`, router con una interfaz en cada red, y equipo del exterior **simulado** `198.51.100.0/24`. Este último es espacio de documentación, no una red pública que debas publicar. No conectes estas interfaces mediante puente a una red real.

El router utiliza `10.77.0.1` y `198.51.100.1`; el servidor LAN, `.20`; el servidor exterior simulado, `198.51.100.10`. Los extremos usan la interfaz del router en su red como puerta de enlace. En la LAN conserva DNS interno y añade opción routers de DHCP solo cuando exista esta pasarela real.

En una VM-router nueva, identifica/adapta nombres de interfaz e instala nftables. Guarda su configuración y verifica que no estás mezclando otro gestor de reglas. El archivo `pasarela-lab.nft` crea tablas propias de filtrado/NAT sin vaciar reglas ajenas. Valídalo con `nft -c -f` bajo los permisos requeridos antes de aplicarlo una vez.

Activa reenvío IPv4 de forma controlada para el taller y registra el estado anterior; `sudo sysctl -w net.ipv4.ip_forward=1` cambia el valor en ejecución. La persistencia se configura aparte si el plan la requiere. El ejemplo no habilita encaminamiento IPv6; su política debe mantenerse coherente con el entorno.

Prueba HTTP desde LAN al servidor exterior simulado. El filtrado permite ese flujo y la regla de salida aplica masquerade: el extremo exterior ve el origen del router. Respuesta y estado de conexión permiten el retorno. No confundas esa traducción con el permiso de la cadena de reenvío.

Después, desde el exterior simulado solicita `http://198.51.100.1:18080`. La regla DNAT dirige la petición a `10.77.0.20:80`, y el filtrado permite exclusivamente ese flujo previsto. Comprueba contenido del servicio y retorno; un puerto diferente debe quedar bloqueado. No se modifica ningún router doméstico ni se publica el servicio en Internet.

Aceptación: acceso saliente, traducción observada, publicación simulada y prueba negativa, con direcciones y capturas ficticias. Para recuperar, retira solo las tablas del ejercicio y devuelve reenvío/rutas a su estado previo, o restaura la VM-router. No utilices `flush ruleset` como limpieza universal.

Fuentes: nftables, ejemplo de router y NAT. Configuración revisada, sin ejecución de una pasarela Linux en esta edición.

¿Lo has pillado?

1. ¿IMAP envía por sí solo correo entre dominios?

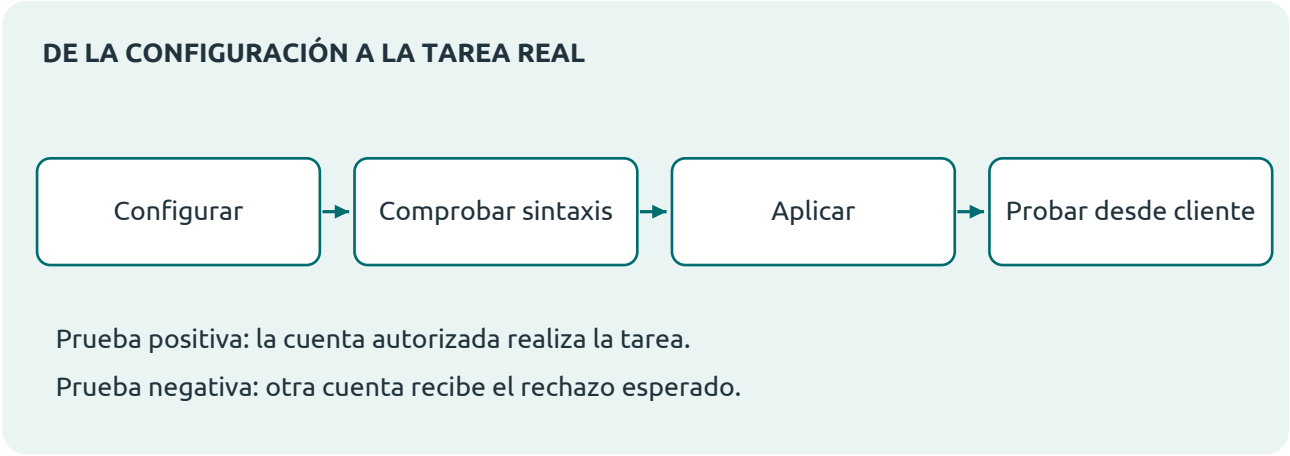
2. ¿NAT reemplaza todas las reglas del cortafuegos?

3. ¿Basta con una ruta de ida para garantizar la respuesta?

Soluciones. 1) No: tiene funciones de acceso y gestión del buzón; SMTP participa en transferencia. 2) No: traducción y filtrado cumplen funciones distintas. 3) No: se necesita camino de vuelta, políticas compatibles y servicios funcionando.

36. Un servicio no está terminado hasta probarlo desde el cliente

Al terminar: prepararás una comprobación completa, registrarás dependencias y diseñarás una prueba negativa. **Antes:** capítulos 28-35.



Un servicio se valida con operaciones concretas, no solo con un estado.

«El servicio aparece activo» es una observación útil. No demuestra que esté escuchando donde debe, que el cliente llegue, que el nombre sea correcto ni que la identidad tenga acceso. La aceptación debe describir una tarea que alguien pueda realizar.

Una cadena de verificaciones

Configuración: sintaxis, valores, archivos incluidos y permisos. **Proceso:** el programa arranca y conserva estado saludable. **Escucha:** dirección, interfaz, protocolo y puerto previstos. **Camino:** rutas y filtros permiten el tráfico requerido. **Nombre y confianza:** DNS y certificados corresponden al servicio. **Aplicación:** la operación funciona con la identidad adecuada. **Persistencia:** sigue funcionando tras un reinicio planificado y recupera su estado necesario.

En Linux, herramientas como `ss -lnt` muestran escuchas TCP y `ss -lnu`, UDP. Las opciones que revelan procesos pueden exigir permisos. Escuchar en `127.0.0.1` no ofrece el mismo alcance que escuchar en una interfaz interna o en todas. En Windows puedes consultar conexiones y escuchas mediante herramientas del sistema o cmdlets compatibles.

Pruebas positivas y negativas

Una prueba positiva confirma que un usuario autorizado puede leer Materiales. Una negativa comprueba que una cuenta no autorizada no entra en Administración. Ambas importan: permitir demasiado puede pasar inadvertido si solo pruebas con administradores.

El rechazo esperado debe interpretarse. Un usuario no puede leer una carpeta porque el servidor está apagado: eso no demuestra una política de autorización correcta. Debes comprobar también que el servicio funciona para una identidad que sí está autorizada.

Ejemplo de aceptación de la intranet

El cliente recibe configuración del rango correcto. Resuelve `intranet.aulanorte.test` hacia `.20`. Puede obtener `AN-01` por HTTP dentro del laboratorio. Si se ha completado la ampliación HTTPS, valida el certificado y accede usando el nombre correcto. Una petición de un recurso inexistente devuelve la respuesta prevista sin revelar información sensible.

Se comprueba el acceso en los registros y se repite después de un reinicio planificado. El expediente incluye versiones, configuración relevante, pruebas y recuperación. No se entrega la clave privada TLS como parte de una memoria pública.

Mantenimiento y cambios

Antes de un cambio registra el estado funcional. Guarda configuración y plan de reversión. Aplica durante una ventana adecuada, comprueba sintaxis y realiza pruebas de cliente. Si falla, decide si corregir o revertir conforme al riesgo y tiempo disponible. Una copia de configuración no es un plan de reversión si no sabes cómo restaurarla.

En servicios con datos, la reversión de un programa puede no deshacer cambios en esquemas o contenido. Antes de actualizar una aplicación con base de datos, revisa compatibilidad y copia coherente. No presupongas que una instantánea de una sola máquina cubre todas las dependencias distribuidas.

Práctica: expediente de servicio

Elige DNS, web o archivos del laboratorio y prepara una ficha con objetivo, dependencias, configuración, arranque, puertos, acceso permitido y denegado, registros, copia y recuperación. Ejecuta una prueba por cada punto que proceda y señala lo que no has podido probar.

Resultado esperado: otra persona puede verificar el servicio y entender el alcance de las evidencias. Si no dispones de máquinas para alguna prueba, diseña el caso en papel y márcalo como plan, no como ejecución.

SOS: funciona en el servidor, falla fuera

Comprueba la dirección de escucha y la ruta del cliente. Una prueba contra `localhost` puede haber usado otro sitio, otro puerto o una identidad con más privilegios. Repite con el nombre y recorrido reales del cliente, y compara registros de ambos intentos.

¿Lo has pillado?

1. ¿Qué demuestra un estado «activo» del servicio?

2. ¿Por qué un rechazo con el servidor apagado no valida permisos?

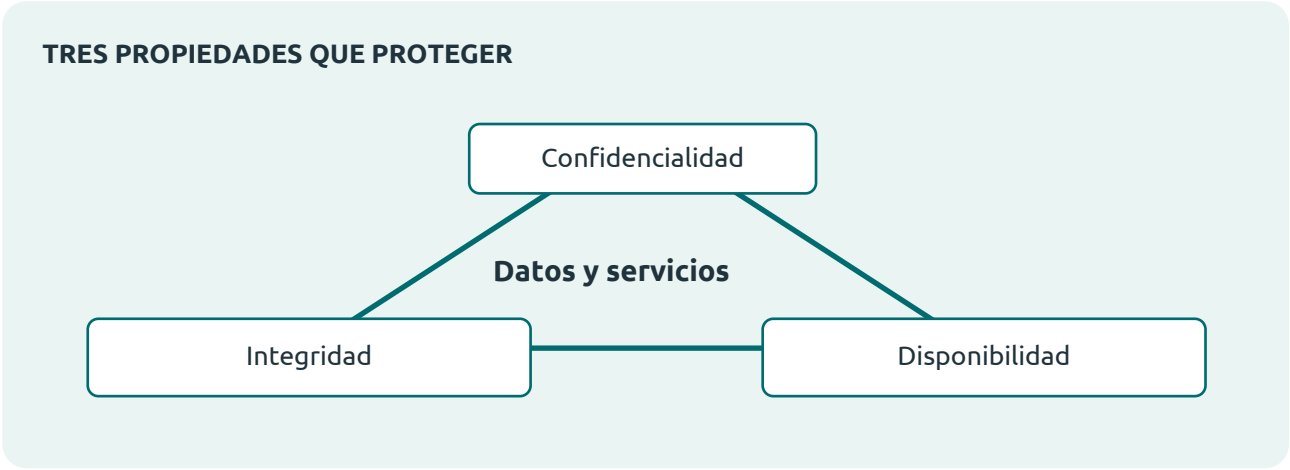
3. ¿Qué debe acompañar a una modificación de configuración?

Soluciones. 1) Solo una parte del estado del proceso gestionado, según la herramienta; faltan pruebas funcionales. 2) Porque no se ha ejercitado el control de autorización. 3) Motivo, estado previo, recuperación, comprobación y registro del resultado.

Bloque 7. Seguridad y recuperación

37. Entender el riesgo antes de comprar herramientas

Al terminar: construirás un análisis de riesgo pequeño y justificarás sus prioridades. **Antes:** equipos, redes, cuentas y servicios.



Una incidencia puede afectar a varias propiedades a la vez.

Proteger un sistema exige saber qué quieres conservar y frente a qué situaciones. Un antivirus no resuelve que cualquiera pueda entrar en el despacho y llevarse el equipo. Una puerta cerrada tampoco evita un borrado con una cuenta que tiene demasiados permisos.

La **confidencialidad** consiste en evitar accesos o revelaciones no autorizados. La **integridad** se refiere a conservar información y procesos frente a alteraciones indebidas. La **disponibilidad** permite utilizar los recursos cuando se necesitan. Una misma incidencia puede afectar a varias propiedades.

Activo, amenaza, vulnerabilidad e impacto

Un **activo** es algo que tiene valor para la actividad: documentos, identidades, equipos, servicios o conocimiento. Una **amenaza** es una causa potencial de daño. Una **vulnerabilidad** es una debilidad que puede contribuir a que el daño se produzca. El **impacto** describe las consecuencias.

En Aula Norte, las matrículas son un activo. Una cuenta comprometida es una situación de amenaza para sus datos. La reutilización de una contraseña y unos permisos excesivos son debilidades posibles. La exposición de información y la interrupción de la gestión son impactos diferentes que deben valorarse.

El **riesgo** relaciona posibilidades y consecuencias dentro de un contexto. No necesitas una cifra con muchos decimales para tomar una primera decisión útil. Sí necesitas explicar qué escenario estás valorando y qué pruebas apoyan tus estimaciones.

Un método sencillo y explícito

Para el ejercicio utilizaremos probabilidad e impacto con valores 1, 2 y 3. Su producto orienta el orden de revisión. Esta escala es una herramienta didáctica propia, no una certificación ni una medida objetiva universal. Dos riesgos con el mismo producto pueden requerir acciones distintas por sus consecuencias, obligaciones o facilidad de tratamiento.

Escenario A: borrado accidental de material docente sin copia recuperable. Probabilidad 2, impacto 3, resultado 6. Escenario B: caída breve de una impresora alternativa. Probabilidad 2, impacto 1, resultado 2. Si la impresora fuera la única forma de entregar documentación urgente, el impacto cambiaría.

Tratar y revisar

Puedes reducir el riesgo aplicando medidas, evitar la actividad que lo origina, compartir determinadas consecuencias mediante acuerdos adecuados o aceptar un riesgo de forma consciente por quien tiene autoridad. Aceptar no significa olvidarlo: documenta motivo, responsable y revisión.

El **riesgo residual** es el que queda después de las medidas. Una copia diaria probada reduce consecuencias del borrado, pero no garantiza recuperar cambios posteriores a la última copia. MFA reduce ciertos riesgos de acceso y no elimina una sesión ya robada ni un permiso mal asignado.

Seguridad física y entorno

Controla acceso a salas y armarios, sujeción y ubicación de equipos, condiciones ambientales y protección eléctrica adecuada. Un SAI puede aportar tiempo para mantener temporalmente cargas o apagar con orden dentro de su capacidad. No garantiza autonomía indefinida y necesita mantenimiento y pruebas.

Los cables deben disponerse sin crear riesgos y los soportes con datos deben gestionarse durante uso, traslado y retirada. Tirar una unidad a un contenedor ordinario sin un procedimiento de datos y residuos deja problemas técnicos y de organización sin resolver.

Práctica: mapa de riesgos de Aula Norte

Elige tres activos y un escenario concreto por cada uno. Registra amenaza, debilidad observada, consecuencia, probabilidad, impacto, medida, responsable y prueba. Utiliza solo datos ficticios.



Consejo de David

Ejemplo de prueba útil: «restaurar el documento en un destino separado y abrirlo» valida una parte de la recuperación. «Instalar una herramienta de copia» solo demuestra que has instalado software.

Resultado esperado: puedes explicar por qué atiendes primero un escenario y cómo sabrás si una medida sirve. Revisa las puntuaciones después de aplicar las medidas; no las bajes automáticamente para que la tabla parezca mejor.

¿Lo has pillado?

1. ¿Un equipo caro es siempre el activo más importante?

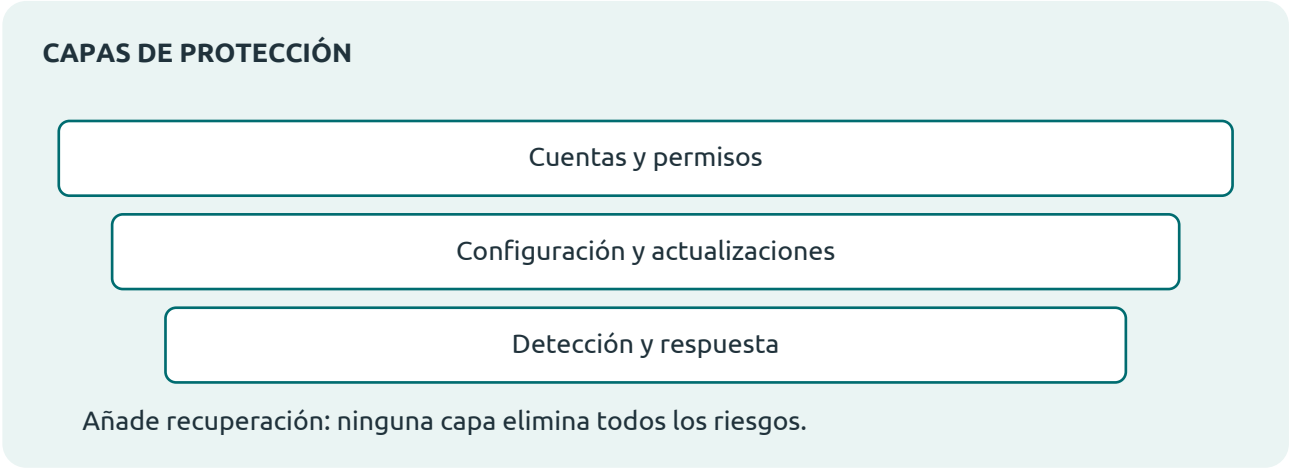
2. ¿Una cifra de riesgo demuestra por sí sola su exactitud?

3. ¿Qué diferencia hay entre instalar una medida y comprobarla?

Soluciones. 1) No: el valor depende también de datos, servicio y consecuencias. 2) No: depende del método, evidencia y contexto. 3) La instalación crea una capacidad; la prueba aporta evidencia de su efecto y sus límites.

38. Proteger equipos y cuentas con capas coherentes

Al terminar: prepararás una configuración base y un proceso de recuperación de acceso. **Antes:** cuentas, privilegios y mantenimiento.



Cada capa aborda riesgos distintos y necesita comprobación.

El **endurecimiento** consiste en reducir exposiciones y configurar protecciones según el uso. Se parte de un inventario y una base documentada, no de desactivar funciones al azar. Quitar un componente necesario sin conocer su dependencia puede causar una indisponibilidad.

Una base de equipo

Utiliza versiones mantenidas, actualizaciones por canales oficiales, aplicaciones necesarias y cuentas con privilegios adecuados. Retira servicios que no se necesitan después de comprobar su función. Configura bloqueo de sesión y protecciones del sistema, y revisa su estado en lugar de suponer que funcionan por tener un icono.

El software de protección puede detectar o bloquear amenazas dentro de su alcance. No convierte cualquier archivo descargado en seguro ni justifica desactivar actualizaciones. Las exclusiones deben tener un motivo concreto y revisarse; excluir una unidad entera para evitar un aviso puede dejar una exposición amplia.

Contraseñas y factores

Utiliza contraseñas largas, únicas y gestionadas con un mecanismo adecuado. Un gestor de contraseñas permite generar y guardar credenciales distintas; su acceso y recuperación también necesitan protección. No introduzcas contraseñas reales en comprobadores desconocidos ni en una memoria de prácticas.

MFA combina factores de categorías distintas, como conocimiento y posesión. Dos contraseñas no constituyen dos categorías. Los códigos temporales aportan protección, pero pueden ser engañados mediante phishing. Los mecanismos resistentes al phishing, como determinadas implementaciones de llaves de seguridad y passkeys, añaden propiedades diferentes: su funcionamiento y recuperación deben revisarse en el servicio elegido.

Referencia: NIST SP 800-63B-4, autenticadores, https://pages.nist.gov/800-63-4/sp800-63b/authenticators/. Sus requisitos describen un marco concreto; no son una afirmación de que cualquier web aplique esas reglas.

Los mecanismos **biométricos** utilizan rasgos como huella o cara según el dispositivo y diseño. Facilitan ciertos usos y necesitan evaluación de suplantación, accesibilidad, recuperación y tratamiento de datos. En sistemas como Windows Hello pueden servir para desbloquear una credencial vinculada al dispositivo; no son una contraseña que simplemente se envía al servidor. Una huella no se cambia como una clave si se expone su representación. Comprueba qué dato se guarda y dónde según el producto y la política. Microsoft, Windows Hello y Hello for Business.

Recuperación de acceso

Antes de activar un factor, revisa qué sucede si pierdes el dispositivo. Guarda códigos de recuperación en una ubicación protegida y separada cuando el servicio los ofrezca. Un pantallazo del código QR de enrolamiento puede contener un secreto que permite duplicar el factor: no lo publiques como evidencia.

Una cuenta de emergencia debe tener controles, custodia y revisión. Si cualquiera conoce su contraseña, no es una buena recuperación. Evita depender de una única persona o de un único dispositivo sin alternativa documentada.

Cifrado, hash y firma

El **cifrado** transforma datos para proteger su confidencialidad mediante claves. Un **hash** produce un resumen que permite, entre otros usos, comparar integridad; no se descifra como un documento cifrado. Una **firma digital** puede permitir comprobar integridad y relación con una clave firmante bajo una infraestructura y validación determinadas.

Un hash recibido junto a un archivo desde el mismo origen malicioso no acredita por sí solo legitimidad. Cifrar un disco tampoco protege todo cuando el usuario ya lo tiene desbloqueado y una aplicación autorizada lee los datos.

Práctica: una cuenta de laboratorio recuperable

En un servicio de pruebas que admita MFA, documenta opciones antes de activarlas. Prepara el mecanismo de recuperación, enrola el factor y prueba un inicio de sesión nuevo. Si no dispones de una cuenta adecuada, realiza el diseño en papel: no necesitas modificar tu cuenta principal para aprender el proceso.

Evidencia: describe el factor, la comprobación y dónde se custodia la recuperación sin incluir secretos. Revisa sesiones abiertas y cómo revocarlas conforme al servicio. Para retirar la práctica, utiliza el procedimiento oficial y verifica el acceso previsto.

SOS: recibo solicitudes MFA que no he iniciado

No las apruebes para detener los avisos. Accede al servicio por una vía conocida, revisa sesiones y sigue el procedimiento de incidente. Cambiar contraseña desde un enlace del propio mensaje puede llevar a una página falsa. Si afecta a una cuenta de organización, informa por el canal establecido.

Malware: reconocer la función y preparar la respuesta

Un **virus** necesita asociarse a otro contenido o programa para propagarse; un **gusano** puede propagarse entre sistemas aprovechando sus posibilidades de comunicación. Un **troyano** se presenta como algo útil o legítimo para inducir su ejecución. **Ransomware** describe una finalidad de extorsión que puede incluir cifrado y robo de datos. **Spyware** busca obtener información sin el conocimiento o autorización adecuados. Un **rootkit** intenta ocultar actividad o mantener acceso con mecanismos que dificultan detectarlo. Las categorías se solapan: un caso puede robar datos, propagarse y extorsionar.

El phishing es un engaño para conseguir una acción, credencial o información; no necesita instalar un virus. Un archivo comprimido con contraseña no se vuelve confiable por superar un filtro. Revisa procedencia, firma del editor cuando exista, canal de descarga y necesidad de ejecución. El capítulo 16 explica integridad; el hash publicado por el mismo origen comprometido tampoco resuelve toda la confianza.

Taller de protección, sin muestras maliciosas. En un invitado Windows compatible, abre Seguridad de Windows y consulta proveedor, actualización, historial y estado. Si Microsoft Defender Antivirus está activo, actualiza sus definiciones mediante el mecanismo oficial y analiza una carpeta nueva que contenga solo un texto ficticio. En PowerShell, `Start-MpScan -ScanType CustomScan -ScanPath C:\SMR-Prueba` inicia ese análisis cuando la carpeta existe y el proveedor y permisos lo permiten. Si hay otro antivirus activo, sigue su manual; no actives dos proveedores incompatibles ni retires el corporativo para hacer la práctica.

Registra versión del motor y definiciones, fecha, ruta y resultado sin publicar datos personales. La ausencia de detección en un texto inocuo demuestra que has podido ejecutar esa operación, no que el producto detecte todas las amenazas. Una prueba funcional de detección requiere un procedimiento de ensayo reconocido y autorizado por el centro. Este libro no distribuye malware ni exige descargarlo. No desactives la protección para obtener una captura más vistosa.

Si hubiera una detección: conserva el identificador del evento, consulta la acción aplicada y sigue el procedimiento del capítulo 41. Restaurar cualquier objeto de cuarentena para probar si «de verdad era peligroso» añade exposición y puede contradecir el plan de respuesta.

Referencia: Microsoft, Start-MpScan.

Taller de firma sobre un documento ficticio

Necesitas OpenSSL y una carpeta nueva de prácticas, sin archivos previos con estos nombres. Crea `acta.txt` con una frase ficticia. Genera una clave de ensayo y su parte pública:

BASH

```
umask 077
openssl genpkey -algorithm RSA \
  -pkeyopt rsa_keygen_bits:2048 -out firma.key
openssl pkey -in firma.key -pubout -out firma.pub
openssl dgst -sha256 -sign firma.key \
  -out acta.sig acta.txt
openssl dgst -sha256 -verify firma.pub \
  -signature acta.sig acta.txt
```

La verificación debe indicar éxito. Duplica el acta como `acta-cambiada.txt`, cambia una palabra y repite la última orden usando ese archivo y la firma original: debe fallar. Comparas contenido firmado y una clave pública concreta. No has acreditado por ello una identidad civil, una firma cualificada ni la validez jurídica de cualquier trámite.

La clave privada permite firmar y debe custodiarse. Esta clave sin contraseña sirve solo para el ensayo efímero, sin datos reales, y se retira al terminar. Entrega como evidencia el resultado positivo y el negativo, no la clave. Para certificados de servidor, nombre y confianza utiliza el taller TLS del capítulo 33; una conexión cifrada con un nombre incorrecto no supera esa prueba.

Fuente técnica: OpenSSL, operaciones de firma y verificación con dgst.

¿Lo has pillado?

1. ¿Dos contraseñas son necesariamente MFA?

2. ¿Un hash cifra el archivo de forma recuperable?

3. ¿Por qué no mostrar el QR de MFA en una práctica entregada?

Soluciones. 1) No: pertenecen a la misma categoría de conocimiento. 2) No: es otra función. 3) Porque puede contener el secreto de enrolamiento; la evidencia no debe permitir clonar el factor.

39. Cortafuegos, segmentación, wifi y VPN

Al terminar: expresarás reglas de acceso y comprobarás una política con pruebas positivas y negativas. **Antes:** puertos, rutas y servicios.

UNA REGLA EXPRESA UN FLUJO



Ejemplo: 10.77.0.0/24 TCP 443 del servidor

Permitir ese flujo no abre DNS, DHCP ni carpetas compartidas.

La conectividad y la autorización del recurso se verifican por separado.

Un **cortafuegos** permite o bloquea tráfico conforme a reglas y capacidades. Puede actuar en el equipo o entre redes. La regla debe indicar origen, destino, protocolo, puerto y sentido cuando proceda. «Permitir la aplicación» puede traducirse en varias comunicaciones distintas.

Diseñar la política antes del comando

En Aula Norte, administración necesita el servidor de archivos; invitados necesitan salida a Internet, pero no esa carpeta. El sistema de copias necesita comunicarse con su destino. Escribe esos flujos y rechaza los que no tengan una necesidad justificada según el diseño.

El orden de reglas y el tratamiento de conexiones establecidas dependen del producto. Una regla muy amplia puede hacer irrelevante una posterior más restrictiva. Revisa también IPv6: una política aplicada solo a IPv4 puede dejar otro camino sin controlar.

Ejercicio UFW en un invitado nuevo

Utiliza un invitado Ubuntu con UFW y acceso por consola, en `SMR-SERVICIOS`. La propuesta siguiente es para un ejercicio aislado y **no permite todos los servicios de los capítulos anteriores**. Antes de empezar, registra el estado de UFW y la configuración recuperable. No ejecutes esta secuencia en un servidor compartido ni desde tu única sesión remota.

BASH

```
sudo ufw status verbose
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow from 10.77.0.0/24 to any port 22 proto tcp
sudo ufw allow from 10.77.0.0/24 to any port 443 proto tcp
sudo ufw enable
sudo ufw status numbered
```

La política propuesta permite SSH y HTTPS desde la subred indicada, con salida permitida. No abre DNS, DHCP, SMB ni HTTP: si los necesitas, debes diseñar sus reglas específicas antes de aplicar el cortafuegos. El dominio AD requiere varios servicios y no debe recibir estas reglas mínimas como si fueran su política completa.

Comprueba HTTPS desde un cliente autorizado y revisa qué pasa con HTTP si existe un servicio escuchando en 80. Para interpretar un rechazo necesitas confirmar previamente que el servicio funciona; un puerto cerrado porque no hay proceso no prueba la regla de filtrado.

Recuperación: usa la consola para restaurar la base de UFW registrada o el invitado desechable. No cierres la consola hasta verificar el acceso. Si necesitas retirar una regla, identifícala de nuevo: los números pueden cambiar después de eliminar otras.

Fuente de sintaxis: Ubuntu, UFW, https://ubuntu.com/server/docs/how-to/security/firewalls/.

Segmentación y wifi

Separa funciones mediante redes y políticas apropiadas. Una VLAN de invitados debe tener controles de acceso entre segmentos; no basta con un SSID distinto. En redes inalámbricas, configura protección y autenticación adecuadas a los equipos, separa invitados y retira credenciales cuando dejen de corresponder.

No publiques la clave wifi de un entorno real en una captura. Las credenciales compartidas tienen consecuencias de revocación: si todas las personas usan una, retirar acceso a una puede requerir cambiarla para todas.

VPN: un túnel con un alcance definido

Una **VPN** proporciona una comunicación lógica protegida entre extremos según su tecnología. Puede unir redes o dar acceso remoto. No determina por sí sola qué debe poder hacer un usuario tras conectarse.

Un diseño distingue autenticación, claves, direcciones del túnel, rutas, DNS y reglas. En un túnel dividido viajan por la VPN ciertos destinos; en un túnel completo se dirige por ella un conjunto más amplio del tráfico conforme a configuración. Si una ruta o DNS quedan fuera del diseño, una aplicación puede no utilizar el camino que esperabas.

Práctica de diseño: dibuja un portátil remoto, una pasarela y un servidor interno. Indica qué red debe alcanzarse y qué destinos quedan excluidos. Define cómo revocar un dispositivo perdido y cómo comprobarías que una cuenta sin autorización no llega al servidor. Para desplegar, utiliza la guía oficial de la tecnología y versión elegidas en invitados separados; las claves privadas nunca se incorporan al plano ni a la entrega pública.

Taller: comprobar qué cambia al proteger una transmisión

Utiliza exclusivamente cliente y servidor del laboratorio interno `SMR-SERVICIOS`. Necesitas la intranet HTTP y HTTPS de los capítulos 32-33, Wireshark en el cliente y permiso de captura sobre esa interfaz. No selecciones la wifi física del anfitrión, una red de empresa ni tráfico de otras personas. Escribe alcance, duración y responsable de la práctica en el cuaderno.

1. Identifica la interfaz del cliente que tiene una dirección de `10.77.0.0/24`. Cierra aplicaciones innecesarias del invitado y desactiva la resolución automática de nombres en Wireshark si quieres evitar consultas adicionales durante el análisis.
2. Empieza una captura breve sobre esa interfaz. Desde ese cliente abre la página HTTP de laboratorio y solicita una URL ficticia como `http://intranet.aulanorte.test/?marca=SMR-ENSAYO`. No envíes contraseña ni datos reales.
3. Detén la captura. Aplica el filtro de visualización `http` y busca la petición, el nombre y la marca. Si el navegador cambia automáticamente a HTTPS, utiliza curl para solicitar expresamente HTTP; confirma esquema y puerto. Explica qué contenido queda expuesto en ese recorrido.
4. Inicia otra captura y solicita la versión HTTPS, confiando únicamente en la CA de prácticas conforme al capítulo 33. Filtra `tls` o `tcp.port == 443`. Relaciona extremos, puertos y tiempos; compara el acceso al contenido con el ensayo anterior sin aportar claves de descifrado a Wireshark.
5. La marca de la petición HTTPS no debería estar disponible como texto HTTP descifrado en esa captura ordinaria. Esto no hace invisibles todos los metadatos: direcciones, tamaños y tiempos pueden seguir siendo observables; DNS y ciertos datos de negociación dependen de los protocolos y opciones usados.
6. Guarda solo la captura mínima autorizada para la memoria. Identifica fecha, interfaz y filtro; el filtro de visualización oculta filas de la vista, pero no elimina esos paquetes del archivo guardado. Si necesitas retirar paquetes, exporta los seleccionados a otro archivo y verifica su contenido. Elimina el material conforme al plazo acordado.

Aceptación: explicas una observación y sus límites en cada recorrido. No encontrar una cadena no demuestra por sí solo cifrado correcto: comprueba también que capturaste la interfaz y sesión adecuadas, que hubo una petición nueva y que no se sirvió desde caché. Puedes añadir una marca ficticia distinta por ensayo.

En una red conmutada, el cliente observa lo que llega a su interfaz según el entorno. Activar modo promiscuo no garantiza recibir todo el tráfico del switch. Tampoco constituye autorización para interceptarlo. El cifrado autenticado, los controles de acceso físico, la segmentación y la administración del switch reducen riesgos distintos; un túnel VPN requiere además política de rutas, claves y acceso en ambos extremos.

Correo no deseado y engaños. Usa la función de notificar spam/phishing del servicio, limita exposición de direcciones y revisa filtros del servidor según el diseño. No abras adjuntos para comprobar una sospecha ni pulses «darme de baja» en cualquier mensaje fraudulento. En una prueba, compara mensajes ficticios legítimos y no deseados y documenta falsos positivos: bloquearlo todo impide también trabajar. Los bloqueadores de contenido y la reducción de rastreo deben respetar las aplicaciones y necesidades autorizadas.

Fuente: Wireshark, guía oficial de introducción y captura. Es un analizador; interpretar una captura necesita contexto.

¿Lo has pillado?

1. ¿Las reglas UFW del ejemplo permiten DNS y SMB?

2. ¿Una VPN concede automáticamente permisos de lectura en una carpeta?

3. ¿Un puerto que no responde demuestra por sí solo que el cortafuegos lo bloquea?

Soluciones. 1) No: son deliberadamente una política mínima para dos servicios TCP. 2) No: conectividad y autorización de la aplicación son controles distintos. 3) No: puede no existir escucha, fallar una ruta o intervenir otro filtro.

40. Copias que puedas restaurar

Al terminar: diseñarás una retención y recuperarás datos ficticios en un destino independiente.
Antes: capítulo 20 y almacenamiento.

COPIAR Y PROBAR LA RECUPERACIÓN



Comprobar contenido, permisos y tarea del usuario.

Una copia en el mismo disco comparte su fallo físico.

La independencia de fallos importa tanto como el número de copias.

La copia útil se define por lo que permite recuperar. Debe incluir datos y dependencias necesarios, tener una frecuencia adecuada y conservar versiones durante el periodo previsto. Una tarea que termina sin errores no demuestra por sí sola que el contenido es suficiente.

Completa, incremental y diferencial

Una **completa** recoge el conjunto seleccionado. Una **incremental** guarda cambios respecto al estado de referencia que utiliza la herramienta, habitualmente la copia anterior de la cadena. Una **diferencial** recoge cambios respecto a una completa de referencia. Para restaurar, identifica qué piezas exige el producto y comprueba que no falta ninguna.

Si haces una completa el domingo e incrementales diarias, recuperar el jueves puede requerir la completa y toda la cadena correspondiente. Con diferenciales respecto al domingo, puede bastar la completa y la diferencial del jueves. Las implementaciones pueden utilizar síntesis, deduplicación o formatos propios: consulta el procedimiento real.

Diversificar fallos y limitar modificaciones

La regla 3-2-1 propone tres copias contando el original, en dos tipos de soporte o medios y una fuera de la ubicación principal. Es una orientación para diversificar, no una garantía automática. Añade controles frente a borrado malicioso, como separación de credenciales, desconexión o inmutabilidad cuando el diseño lo requiera.

Referencia: INCIBE, guía de copias de seguridad, https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf. La práctica del libro utiliza datos originales y una restauración observable.



Ojo con este error

Una carpeta sincronizada puede propagar borrados y cambios. Si ofrece historial y recuperación, comprueba retención, permisos y límites; no presupongas que sincronización equivale a una copia protegida frente a todos los fallos.

RPO y RTO con un ejemplo

El **RPO** expresa la pérdida de datos tolerable medida en tiempo respecto a un punto de recuperación. El **RTO** fija un objetivo de tiempo para restablecer el servicio. Son objetivos del diseño, no tiempos que la herramienta garantiza solo por configurarlos.

Aula Norte admite perder como máximo dos horas de cambios y pretende recuperar en cuatro horas. Una única copia nocturna no satisface ese RPO durante toda la jornada. Copiar cada hora podría aproximarse al requisito si las copias son coherentes y recuperables. El RTO debe medirse incluyendo localizar medios, restaurar, verificar y devolver el servicio.

Retención, cifrado y pruebas

Decide cuántas versiones conservas y qué borrados deben poder recuperarse. Cifra copias cuando corresponda y separa la gestión de claves. Si una copia contiene datos de varias máquinas, verifica permisos y custodia también en el destino.

En bases de datos y aplicaciones activas, una copia simple de archivos puede ser incoherente. Utiliza mecanismos compatibles de exportación, instantánea o respaldo y documenta el orden de recuperación de dependencias.

Práctica reproducible con datos ficticios

El recurso `practica-restauracion.py` crea tres carpetas nuevas en un temporal: trabajo, copia y restaurado. Genera un documento inicial, calcula su SHA-256, hace una copia, cambia el documento de trabajo y restaura desde la copia sin sobrescribir el modificado. Ejecuta el script con Python 3 y lee sus resultados.

Resultado esperado: el restaurado coincide byte a byte con el inicial y difiere del trabajo modificado. También existe un informe de lo ocurrido. El ejercicio demuestra recuperación lógica y comparación de versiones; si las carpetas están en el mismo disco, no prueba protección ante su fallo físico.

Repite el diseño sobre un soporte independiente autorizado si dispones de él: anota cuánto tardas y verifica apertura y permisos. No simules un fallo desconectando una unidad mientras escribe ni borres documentos reales para aprender.

SOS: la copia «está», pero faltan datos

Comprueba selección, exclusiones, coherencia, versión y fecha. Un usuario puede haber guardado en una ubicación que no estaba incluida. Revisa también claves y formato. Trabaja sobre una copia de la evidencia cuando investigues y evita que una tarea automática sobrescriba la última versión buena.

¿Lo has pillado?

1. ¿Una copia diaria satisface siempre un RPO de dos horas?

2. ¿Qué puede perderse si falta una incremental intermedia?

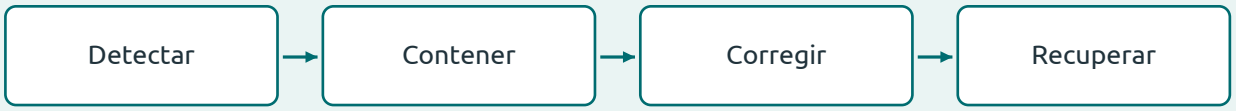
3. ¿Igualar hashes prueba también permisos y funcionamiento de una aplicación?

Soluciones. 1) No: la pérdida potencial entre copias puede superar ese periodo. 2) La recuperación de estados posteriores que dependan de esa pieza. 3) No: compara contenido bajo sus condiciones; permisos y aplicación necesitan pruebas adicionales.

41. Incidentes: actuar con orden y conservar evidencia

Al terminar: distinguirás alerta e incidente y prepararás un ejercicio de respuesta y recuperación. **Antes:** riesgo, registros y copias.

RESPUESTA CON EVIDENCIA



Registrar y comunicar durante todo el proceso.

Después: revisar causas, controles y lecciones aprendidas.

Conserva una cronología y distingue hechos de hipótesis.

Una alerta indica una condición que necesita revisión. Un incidente es un suceso que afecta o puede afectar de forma relevante a la seguridad o funcionamiento conforme a los criterios del entorno. El primer aviso no siempre explica la causa ni el alcance.

Preparación y canal de aviso

Antes del problema define responsables, contactos, prioridades, herramientas, permisos de actuación y datos mínimos del aviso. Si el correo corporativo está afectado, puede necesitarse otro canal previamente acordado. No envíes capturas con datos sensibles a un grupo abierto para pedir ayuda.

Registra hora, equipo, síntoma, usuarios afectados y acciones. Distingue lo visto de lo supuesto. «Hay archivos con nombres extraños» no equivale aún a «se han cifrado todos los servidores».

Contener sin improvisar

La contención intenta limitar daños. Puede incluir aislar un equipo, bloquear una cuenta o detener una propagación según el plan. No ejecutes una lista universal de apagados: algunas decisiones afectan a datos volátiles, continuidad y evidencia y deben seguir el procedimiento y responsables del entorno.

Si sospechas compromiso de una cuenta, considera sesiones, tokens y medios de recuperación además de la contraseña. Realiza cambios desde un equipo y canal adecuados. Si afecta a terceros o datos personales, escala por el canal establecido con rapidez.

Investigar, corregir y recuperar

La investigación busca alcance y origen mediante evidencias. Corregir puede exigir eliminar persistencia, parchear, reconstruir o ajustar controles. Recuperar implica volver desde un estado confiable y comprobar tareas y dependencias antes de reabrir el acceso.

Un análisis antivirus sin detecciones no demuestra que todo esté limpio. Restaurar archivos sobre un sistema aún comprometido puede volver a exponerlos. Después revisa qué permitió el caso y qué cambiará para detectarlo o limitarlo.

Simulacro sin malware real

Aula Norte detecta que la intranet presenta un texto no autorizado. El laboratorio ofrece copias ficticias de una página y registros preparados. No ejecutes programas maliciosos ni pruebes credenciales robadas.

1. Describe qué cambia y desde qué cliente se observa. Conserva la página alterada como evidencia de laboratorio.
2. Compara tiempos y registros preparados: un acceso administrativo aparece antes del cambio. Eso es una pista, no identifica automáticamente a la persona que actuó.
3. Propón contención proporcional: limitar el acceso administrativo afectado, conservar registros y mantener un canal de comunicación.
4. Verifica una copia buena, corrige la causa simulada y restaura en un destino controlado.
5. Comprueba contenido, permisos y acceso autorizado y no autorizado antes de dar el servicio por recuperado.
6. Redacta una cronología y una mejora concreta de prevención y detección.

Resultado esperado: el informe explica qué se sabe, qué queda incierto y qué evidencia apoya la recuperación. Una conclusión válida puede mantener una causa pendiente de investigación.

Continuidad de actividad

La recuperación técnica y la continuidad se relacionan. Mientras la intranet no está disponible, la academia puede necesitar un procedimiento alternativo de asistencia o materiales, con datos mínimos y custodia adecuada. El plan debe indicar cuándo volver al proceso normal y cómo incorporar lo registrado durante la interrupción sin duplicar o perder información.

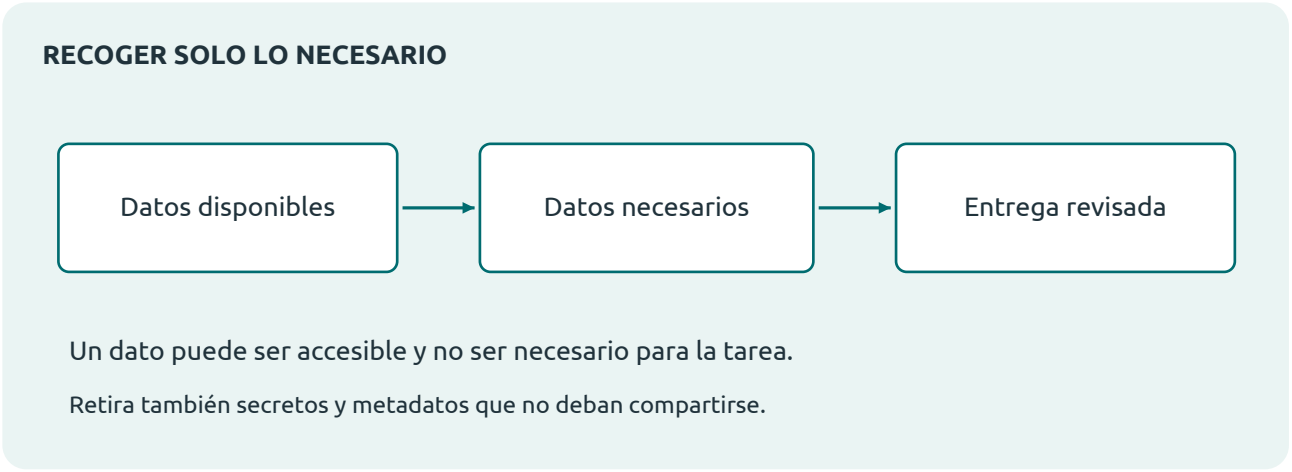
¿Lo has pillado?

1. ¿Una alerta basta para afirmar la causa?
2. ¿Cambiar una contraseña revoca necesariamente todas las sesiones en todos los servicios?
3. ¿Recuperar la página valida también la eliminación de la causa?

Soluciones. 1) No: exige investigación. 2) No: depende de los mecanismos y hay que verificar revocación. 3) No: contenido, causa y controles se comprueban por separado.

42. Privacidad y responsabilidad profesional

Al terminar: reconocerás datos que debes proteger y límites de una intervención técnica. **Antes:** cuentas, copias e incidentes. **Ámbito de referencia:** España y Unión Europea; consulta editorial: 5 de noviembre de 2026.



La evidencia debe permitir comprender sin revelar datos innecesarios.

Un técnico puede ver documentos, registros, nombres y conversaciones mientras trabaja. Tener capacidad técnica de acceso no significa tener autorización para leer, copiar o divulgar todo. Define la tarea, el alcance y los datos necesarios antes de intervenir.

Principios que se traducen en decisiones

En términos generales, el RGPD exige una finalidad y base jurídica adecuadas, minimización, conservación limitada y protección de los datos. El consentimiento es una posible base, no la única ni una solución universal. La responsabilidad del tratamiento y el papel del encargado deben identificarse conforme al caso.

Seudonimizar sustituye identificadores, pero puede seguir permitiendo relacionar datos con personas. No equivale automáticamente a anonimizar. Una captura sin nombre puede conservar correo, número de expediente u otros detalles identificables.

Fuente normativa: Reglamento (UE) 2016/679, especialmente artículos 4-6 y 32-34, https://www.boe.es/doue/2016/119/L00001-00088.pdf. Estas nociones orientan la práctica; las decisiones del tratamiento se encauzan mediante los responsables de la organización.

Ejemplo: reparar el correo de una persona

Necesitas comprobar un envío que falla. Puedes utilizar un mensaje ficticio dirigido a un buzón de pruebas autorizado. Abrir conversaciones personales para buscar un adjunto parecido añade datos que la tarea no requiere. Si hace falta acceder a un elemento real, sigue la autorización y el procedimiento establecidos y limita su copia y difusión.

Al entregar un parte, incluye el error y la acción útil; evita incorporar el cuerpo de mensajes o una lista completa de destinatarios sin necesidad. Guarda evidencias en un lugar autorizado con acceso y retención definidos.

Brechas de datos personales

Una brecha puede afectar a confidencialidad, integridad o disponibilidad; no requiere siempre un atacante externo. En el marco del RGPD, el responsable valora la notificación a la autoridad competente: se realiza sin dilación indebida y, cuando sea posible, dentro de las 72 horas desde que tenga constancia, salvo que sea improbable el riesgo para derechos y libertades. Si hay retraso, deben justificarse los motivos conforme al reglamento. El responsable debe documentar las brechas, se notifiquen o no.

El técnico debe avisar internamente con rapidez y aportar hechos; no esperar a tener un informe perfecto ni decidir por su cuenta que «no pasa nada». La comunicación a personas afectadas tiene sus propias condiciones, entre ellas el alto riesgo, y no debe confundirse con el plazo de notificación a la autoridad.

Fuente práctica: AEPD, notificación de brechas, https://www.aepd.es/preguntas-frecuentes/2-tus-obligaciones-como-responsable-del-tratamiento/11-brechas-de-datos-personales/FAQ-0233-a-quien-hay-que-notificar-las-brechas-de-datos-personales. Verifica el canal y la autoridad competente del caso.

Autorizaciones, licencias y límites de las pruebas

Para una intervención o evaluación técnica identifica equipos, acciones, horarios y responsable que autoriza. Una cuenta que permite acceder a una red no autoriza a probar vulnerabilidades de todos sus equipos. Utiliza datos sintéticos en el aprendizaje.

Respeta licencias de software, imágenes, fuentes y otros recursos. Gratis no implica permiso de redistribución o modificación. Conserva procedencia y condiciones cuando incorpores material a un trabajo. Al retirar un equipo, sigue el procedimiento de borrado o destrucción de datos y gestión del soporte; formatear rápidamente no demuestra borrado seguro.

Práctica: revisa una entrega antes de compartirla

Prepara una captura ficticia con nombre, dirección de correo de prueba, mensaje de error y una clave simulada claramente marcada como falsa. Crea una versión para la memoria que conserve el error y retire identificadores y secretos innecesarios. Revisa también metadatos del archivo y quién podrá abrir el enlace de entrega.

Resultado esperado: otra persona comprende el fallo sin recibir información que no necesita. Ocultar texto con un rectángulo en una capa editable no garantiza que el contenido subyacente haya desaparecido: verifica la exportación final y que no pueda recuperarse mediante selección o edición.

Web, derechos y normas de gestión

Servicios en línea. La LSSI española regula aspectos de los servicios de la sociedad de la información y del comercio electrónico. Según la actividad, entran en juego información del prestador, comunicaciones comerciales, contratación electrónica y reglas sobre almacenamiento o acceso a información en el terminal. No resuelvas todo copiando un aviso legal de otra web: identifica quién presta el servicio, qué ofrece y qué tecnologías utiliza.

En una tienda ficticia distingue tres tareas: identificar la información que debe ofrecer la actividad, configurar el proceso y verificar su comportamiento. Un banner que dice «aceptar» no prueba por sí solo que las tecnologías sujetas a consentimiento estén esperando ese consentimiento. Las excepciones y requisitos concretos se revisan con los responsables y la normativa aplicable. El RGPD y la LSSI tienen ámbitos relacionados y obligaciones diferentes.

Derechos de las personas. Ante una solicitud de acceso, rectificación, supresión u otro derecho, remite al canal del responsable, registra recepción y protege la identidad y los datos durante su gestión. La solicitud de acceso de una persona a sus datos no le concede una copia de la base completa con información ajena. El técnico localiza datos bajo instrucciones, limita la exportación y deja trazabilidad; no responde improvisando desde su correo personal.

Gestión de seguridad. ISO/IEC 27001 establece requisitos de un sistema de gestión de seguridad de la información. Se trabaja con alcance, riesgos, responsabilidades, controles, evidencia y mejora; comprar un antivirus no equivale a implantar ese sistema. Una certificación tiene un alcance y una entidad concreta: no la atribuyas automáticamente a todos sus productos o proveedores. El Esquema Nacional de Seguridad tiene su propio marco para los sistemas incluidos en su ámbito; no es intercambiable con una norma ISO.

Caso resuelto. Aula Norte quiere publicar fotografías del alumnado y enviar una promoción. Antes de tocar el CMS, separa las finalidades y pide al responsable que determine las condiciones aplicables. Configura los permisos y mecanismos aprobados, utiliza imágenes ficticias para el ensayo y prueba retirada, acceso y envío. No supongas que matricularse equivale a autorizar cualquier difusión o comunicación comercial.

Fuentes: LSSI, Ley 34/2002 e ISO/IEC 27001, además del RD 311/2022 sobre el ENS. Para protección de datos, las referencias RGPD y AEPD de este capítulo. Consulta normativa editorial: 5 de noviembre de 2026.

¿Lo has pillado?

1. ¿Poder abrir un archivo demuestra autorización para leerlo?

2. ¿Cambiar nombres por códigos garantiza anonimato?

3. ¿Todas las comunicaciones de brechas tienen exactamente el mismo destinatario y plazo?

Soluciones. 1) No: capacidad y autorización son distintas. 2) No: puede existir información adicional que permita identificar. 3) No: hay obligaciones y condiciones diferentes; avisa al responsable y aplica el procedimiento pertinente.

Caso de taller: devolver un portátil reparado

Has terminado de reparar un portátil de prácticas que contenía un perfil ficticio. Antes de devolverlo, revisa qué datos adicionales creaste durante el trabajo: copias temporales, capturas, exportaciones de registros y credenciales de prueba. La reparación puede haber terminado mientras esos archivos siguen en el escritorio o en un soporte auxiliar.

Preparación. Identifica qué evidencia necesita conservar la organización y dónde debe custodiarse. No decidas borrar toda la carpeta del usuario para dejar el equipo «limpio»: esa carpeta puede contener trabajo legítimo. Tampoco mantengas una copia personal del disco por si vuelven a llamarte.

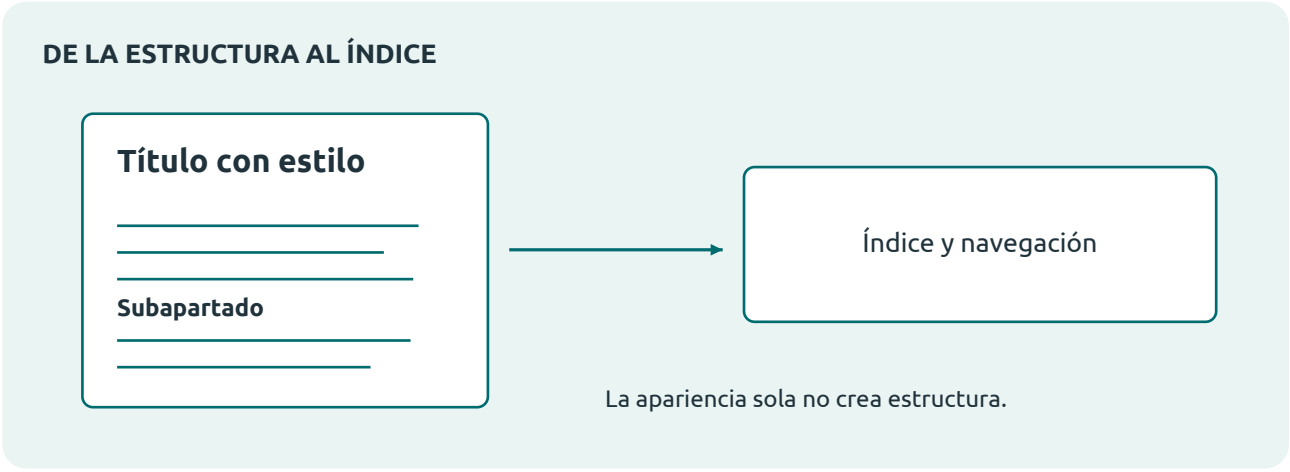
Comprobación. Entrega el resultado y las instrucciones necesarias sin adjuntar secretos. Si creaste una cuenta temporal, revisa con el responsable si debe retirarse y qué archivos dependen de ella. Si instalaste una herramienta de soporte, comprueba si debe permanecer y con qué permisos y configuración.

Cierre. Registra qué materiales se conservaron y cuáles se retiraron conforme al procedimiento. Revisa el soporte auxiliar utilizado. Una intervención bien documentada puede demostrar el trabajo mediante datos mínimos: no necesita exponer el contenido personal del equipo.

Bloque 8. Ofimática para trabajar y entregar bien

43. Documentos profesionales sin pelearte con el formato

Al terminar: prepararás una memoria con estructura, índice y referencias, y revisarás su PDF A4.
Antes: archivos, carpetas y formatos.



Los estilos crean estructura que puede alimentar un índice.

Una memoria técnica debe permitir entender qué hiciste, repetirlo y comprobar el resultado. El formato ayuda cuando hace visibles las relaciones entre ideas. Una palabra grande y en negrita puede parecer un título, pero si no tiene un estilo de encabezado la aplicación quizá no la reconozca como tal.

Contenido, estructura y presentación



Truco de taller

Un **estilo** reúne propiedades que se aplican de forma coherente. Utiliza estilos de título con niveles jerárquicos, cuerpo de texto, listas y pies de figura. Si cambias el estilo de todos los títulos, no necesitas corregir cada uno a mano.

Las **secciones** o funciones equivalentes permiten variar ciertos aspectos, como encabezados, columnas o numeración según la aplicación. Un salto de página empieza otra página; no equivale siempre a una nueva sección. Para colocar texto no pulses Intro veinte veces: al editar una frase anterior, ese espacio cambia de sitio.

Construir una memoria de Aula Norte

Empieza por objetivo y alcance. Describe entorno y versiones. Explica procedimiento con decisiones relevantes y termina con comprobaciones, incidencias y recuperación. Añade conclusiones que se apoyen en resultados: «el cliente pudo abrir el archivo con lectura» es más preciso que «todo perfecto».

Reserva títulos como «Objetivo», «Entorno», «Procedimiento», «Verificación» y «Recuperación». Una memoria corta no necesita diez niveles. Usa una tabla para comparar configuraciones y una lista numerada para una secuencia real.

Índices, figuras y referencias

Genera el índice a partir de estilos de encabezado. Al cambiar contenido, actualiza el índice y comprueba números y destinos. Un índice escrito a mano puede quedar desfasado al mover una imagen.

Añade un pie que explique qué demuestra cada figura. «Captura 7» aporta menos que «consulta DNS desde el cliente que devuelve la dirección del servidor». Usa referencias cruzadas cuando la aplicación las permita para no escribir números que después dejan de coincidir.

Cita la documentación que has utilizado y registra versión o fecha si importa. Una URL larga sin contexto no dice qué decisión respalda. Evita copiar párrafos de una guía para sustituir la explicación de tu procedimiento.

Tablas, imágenes y accesibilidad

Una tabla tiene encabezados claros y unidades. No la construyas con espacios. Repite la fila de cabecera cuando continúe en otra página y comprueba que no se cortan columnas al imprimir.

Inserta imágenes con resolución suficiente, proporciones conservadas y anclaje previsible. Una captura completa de un escritorio puede reducir el error a un texto ilegible: recorta solo la zona necesaria sin eliminar el contexto. Añade texto alternativo cuando el formato lo admita y evita depender exclusivamente del color para transmitir estados.

Combinación de correspondencia

Una combinación usa un documento modelo y una fuente de datos para generar documentos personalizados. Es útil para avisos o etiquetas de laboratorio. Identifica campos, evita duplicados y revisa una muestra antes de generar todo. Si los datos son personales, limita finalidad y acceso. No ejecutes envíos reales como parte de esta práctica.

Práctica paso a paso

1. En Writer o Word, crea un documento A4 con márgenes cómodos y estilos de título y cuerpo. No hagas portada: empieza por el objetivo del informe.
2. Escribe una memoria de una práctica anterior con cinco apartados y una tabla de configuración ficticia.

3. Inserta una figura explicativa propia con pie y referencia desde el texto. Añade una fuente utilizada, identificando el procedimiento que respalda.
4. Genera un índice automático. Cambia el orden de un apartado y actualízalo para comprobar que responde al contenido.
5. Añade números de página y exporta a PDF conservando enlaces y estructura cuando la herramienta lo permita.
6. Abre el PDF exportado, revisa todas sus páginas y prueba el índice. Comprueba que el texto se puede seleccionar y que imágenes y tablas son legibles a tamaño real.

Resultado esperado: memoria editable y PDF coherentes. Guarda el original editable antes de revisar el PDF: exportar no garantiza que puedas reconstruir todos los estilos a partir del resultado.

SOS: el índice no reconoce mis títulos

Comprueba estilos y niveles, no solo tamaño y negrita. Si la tabla se sale de la página, revisa anchura de columnas y área disponible antes de reducir toda la letra. Si queda una línea sola en otra página, ajusta las propiedades de párrafo y la estructura sin añadir espacios artificiales.

Taller: instalar y mantener una suite

La suite de referencia para esta práctica es LibreOffice, en una VM o equipo de aula autorizado. La licencia, sistema soportado, arquitectura y requisitos se comprueban antes de descargar. El procesador de textos, la hoja de cálculo, las presentaciones y la base de escritorio no incluyen necesariamente un cliente de correo: son componentes distintos.

En Windows, obtén el instalador desde la página oficial, verifica su procedencia y firma cuando corresponda y ejecuta el asistente con la cuenta/elevación autorizadas. Elige componentes e idioma, revisa asociaciones de archivos y completa. En Ubuntu mantenido, utiliza sus repositorios y el gestor de paquetes autorizado; comprueba si Base requiere un paquete adicional. No mezcles sin criterio instaladores de distintos canales.

1. Registra versión inicial, espacio, licencia y plan para conservar documentos y perfil. Usa una cuenta de prueba.
2. Instala la suite y los componentes que pide la práctica. Documenta opciones e incidencias.
3. Configura idioma, unidades, guardado y ubicación de pruebas. Crea un documento, una hoja y una presentación ficticios, guarda y vuelve a abrir.
4. Exporta un PDF y prueba un formato de intercambio. Revisa fuentes, saltos, fórmulas y elementos que no se conserven igual.
5. En una copia de laboratorio, aplica una actualización del mismo canal. Comprueba versión y las tareas anteriores.
6. Si falta una función, revisa componente, canal, perfil y documentación antes de reinstalar. Para retirar la aplicación, conserva los archivos y usa el mecanismo de desinstalación del sistema; no borres carpetas de programas a mano.

Resultado esperado: informe con versión, canal, componentes, pruebas antes/después e incidencia resuelta o escalada. Si la actualización falla, aplica la recuperación prevista para esa VM y conserva documentos. No prometas volver a una versión anterior manteniendo cualquier perfil sin probar compatibilidad.

Fuente: instalación oficial de LibreOffice. La instalación y actualización gráficas se proponen para el laboratorio del lector; no se han ejecutado en este entorno editorial.

Plantillas y macros que puedes explicar

Una **plantilla** conserva una estructura reutilizable sin sobrescribir cada vez el documento modelo. En Writer, prepara título, estilos, encabezado y campos de práctica; guárdala mediante la función de plantillas y crea dos documentos nuevos desde ella. Verifica que editar uno no cambia el otro ni el modelo.

Una **macro** automatiza acciones de la aplicación. LibreOffice permite grabar algunas operaciones en Writer y Calc; no graba cualquier acción o cuadro de diálogo. Activa la función de grabación si la versión la ofrece deshabilitada, registra una operación sencilla sobre un texto ficticio y guarda la macro en el documento de práctica.

Después lee el código generado, ejecuta sobre otra copia y comprueba el efecto. Si la grabación no recoge una acción, no concluyas que la automatización se ha realizado. Un script de LibreOffice Basic y uno de VBA de Microsoft Office no se pueden intercambiar sin revisar compatibilidad.

`recursos/ofimatica/macros-practica.bas` contiene ejemplos originales legibles para Writer, Calc y Base. El de Writer inserta una marca en el cursor. Crea un documento vacío, abre el organizador/editor de macros Basic, crea un módulo dentro de ese documento, copia solo el ejemplo que vas a estudiar y guarda en un formato que conserve su macro.

BASIC

```
Sub MarcaWriter
  Dim doc As Object
  doc = ThisComponent
  If Not doc.supportsService("com.sun.star.text.TextDocument") Then Exit Sub
  doc.Text.insertString(doc.CurrentController.ViewCursor, _
      "Práctica de SMR SOS", False)
End Sub
```

La macro actúa sobre el documento actual. Coloca el cursor en un lugar conocido, ejecútala una vez y comprueba la marca. Conserva la copia inicial para recuperar. No habilites macros de documentos desconocidos ni reduzcas globalmente la seguridad: trabaja con código propio revisado y el procedimiento de confianza del aula.

Fuentes: grabación de macros y seguridad de macros. Los ejemplos Basic se revisaron documentalmente; no se afirma ejecución en LibreOffice nativo.

¿Lo has pillado?

1. ¿Negrita y letra grande equivalen siempre a un encabezado estructurado?

2. ¿Actualizar el documento actualiza necesariamente un índice ya exportado a PDF?

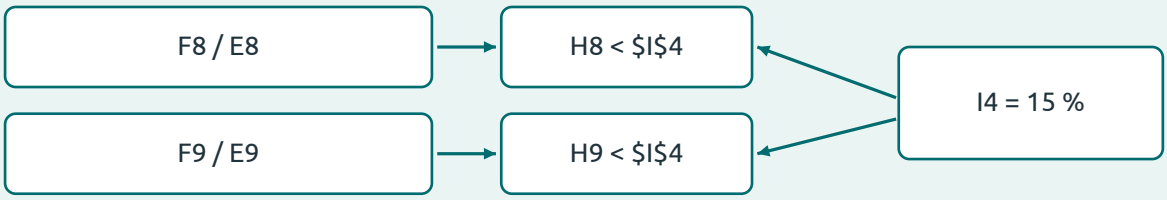
3. ¿Por qué conservar el archivo editable?

Soluciones. 1) No: utiliza el estilo y nivel adecuados. 2) No: debes actualizar y volver a exportar. 3) Porque contiene estructura y elementos de edición que el PDF puede no conservar de la misma manera.

44. Hojas de cálculo: fórmulas que puedes explicar

Al terminar: usarás referencias, condiciones, resúmenes y gráficos sobre un inventario ficticio.
Antes: unidades, archivos y operaciones aritméticas.

CADA FILA, UN UMBRAL COMPARTIDO



Las filas leen sus datos; todas consultan el umbral I4.

La fila cambia; la referencia al umbral permanece fija.

Una hoja de cálculo combina datos, fórmulas y presentación. La celda puede contener un número o una fórmula, y mostrar un formato distinto. Escribir `15 %` como texto no equivale siempre a almacenar el número `0,15` con formato porcentual. El separador decimal depende de la configuración.

El archivo `SMR-SOS-practica-inventario.xlsx` contiene un ejemplo resuelto con ocho equipos. Trabaja sobre una copia para conservar la base. Los datos son ficticios: no representan precios, equipos reales ni mediciones obtenidas en la academia.

Leer el inventario

Las columnas A-F contienen ID, equipo, zona, RAM, disco y espacio libre. G calcula espacio ocupado, H calcula porcentaje libre e I muestra estado. Las filas de datos van de 8 a 15. El umbral de alerta está en I4, inicialmente 15 %. Los resultados principales son ocho equipos, tres alertas y 3.456 GB de capacidad total declarada.

Una sola cifra de capacidad no mide rendimiento ni espacio disponible para todos los usuarios. Hemos elegido GB decimales de ejemplo y una alerta por porcentaje, no una regla universal de mantenimiento. El umbral es editable para explorar el caso.

Referencias relativas, absolutas y mixtas

`E8-F8` resta libre a capacidad de la misma fila. Al copiar hacia abajo, la referencia relativa cambia a `E9-F9`. `$I$4` conserva columna y fila al copiar: todas las filas comparan con un único umbral. `$I4` fija solo la columna e `I$4`, solo la fila.

El símbolo dólar no significa dinero en una referencia. Anclar todas las referencias tampoco es una solución: impediría que cada fila leyera sus propios datos.

Referencia: Microsoft, referencias relativas, absolutas y mixtas, https://support.microsoft.com/es-es/excel/switch-between-relative-absolute-and-mixed-references.

Porcentajes y condiciones

La operación básica de H8 es `F8/E8`. Con 80 GB libres de 512 GB, el resultado es 0,15625, que mostrado como porcentaje representa 15,625 %. El formato puede redondear la presentación sin cambiar el valor almacenado.

Una condición básica sería `SI(H8<$I$4;"Revisar";"Correcto")` en una interfaz que admita nombres españoles y punto y coma. Según aplicación y configuración pueden utilizarse nombres ingleses y otros separadores. El archivo XLSX guarda fórmulas con la representación que requiere ese formato; la interfaz puede mostrarlas traducidas.

El ejemplo resuelto añade controles: una capacidad ausente no se convierte en cero válido, el espacio libre no puede ser negativo ni superar la capacidad y un divisor cero no genera un porcentaje aparentemente correcto. Lee las comprobaciones de fuera hacia dentro y compara su estado con los datos de la fila.



Ojo con este error

Cero libre significa que no queda espacio en este ejemplo. Una celda vacía significa que falta el dato. Son estados distintos y deben producir mensajes distintos. `ESBLANCO` o `ISBLANK`, según el lenguaje de fórmulas, permite comprobar una celda realmente vacía; una fórmula que devuelve texto vacío no es necesariamente una celda sin contenido.

Sumar, contar y buscar

`SUMA` agrega valores; `PROMEDIO` calcula una media aritmética sobre los valores admitidos por la función. No sumes porcentajes para obtener un porcentaje global: el libre total se calcula como suma de libres dividida entre suma de capacidades, con datos completos y válidos.

Las funciones de condiciones múltiples, como `CONTAR.SI.CONJUNTO` y `SUMAR.SI.CONJUNTO`, permiten contar equipos o sumar capacidad que cumplen criterios. Mantén rangos alineados. Por ejemplo, sumar capacidad de Aula utiliza el rango de cantidades y el rango de zonas de las mismas filas.

Fuente para sintaxis de suma por criterios: ayuda de LibreOffice, https://help.libreoffice.org/latest/es/text/scalc/01/func_sumifs.html.

Para buscar una zona a partir de un ID puedes utilizar una búsqueda exacta mediante las funciones que admita tu versión. Define qué hacer si no existe el ID o aparece duplicado. Una primera coincidencia no suma todos los registros relacionados y puede ocultar un identificador mal gestionado.

Validación, filtro y gráfico

La validación restringe entradas como zona o cantidades. No la consideres una garantía absoluta: algunos pegados o procesos pueden introducir datos que requieren comprobación. El formato condicional destaca estados calculados, pero el color debe acompañarse de un texto comprensible.

Un filtro cambia qué filas ves; una suma ordinaria del rango puede seguir incluyendo filas ocultas. Para cálculos sobre lo visible necesitas la función y opciones adecuadas. No confundas el gráfico resumen de todas las zonas con el subconjunto que estás mirando tras filtrar.

El gráfico del archivo se alimenta de celdas con conteos por zona. Al cambiar la zona de un equipo, deben cambiar los conteos y sus barras. No dibujes una barra de altura fija para representar un resultado que quieres actualizar.

Práctica con resultados esperados

1. Cambia el espacio libre de AN01 a 0: porcentaje 0 %, estado Revisar y cuatro alertas.
2. Borra el dato libre de AN01: debe aparecer Falta dato y un dato pendiente, sin inventar un porcentaje. Restaura 80.
3. Cambia el umbral a 10 %: quedan dos alertas con estos datos. Vuelve al 15 %.
4. Introduce, en una copia, libre superior a la capacidad: debe advertirse un dato inválido. Restaura la base.
5. Cambia la zona de un equipo y comprueba el resumen y el gráfico; después revierte el cambio.
6. Añade una fila nueva y revisa fórmulas, validación y rangos. Algunas tablas se amplían automáticamente según la aplicación; no lo des por hecho. Los resúmenes del ejemplo utilizan un rango inicial acotado que debes ampliar para incluir el nuevo registro.

Resultado esperado: explicas cada cambio y conservas una copia final sin entradas inválidas. La práctica compara valores y fórmulas, no solo colores. Para imprimir, define el área, orientación y escala, y revisa la vista previa sin reducir el texto hasta hacerlo ilegible.

Taller de automatización en la hoja

Haz una copia del inventario y guárdala en el formato de trabajo de Calc que conserve el código. El ejemplo `MarcaCalc` del recurso crea una hoja llamada `Macro_practica` solo si no existe. Si ya existe, se detiene sin escribir; no utiliza la hoja de inventario ni cambia sus fórmulas.

Abre el editor Basic del documento de práctica, incorpora el ejemplo, léelo y ejecútalo. Debe aparecer la nueva hoja con una marca en A1. Ejecuta de nuevo: debe avisar que ya existe y conservar su contenido. Esa segunda prueba verifica un límite, no solo el camino de éxito.

Recupera usando la copia anterior o retirando exclusivamente la hoja que acabas de crear después de comprobar su nombre. Un libro con macros exige un formato apropiado y política de confianza; exportarlo a CSV no conserva hojas, formato ni código. Prueba también importar un CSV ficticio indicando separador, codificación y tipos para no perder ceros iniciales de identificadores.

Resultado esperado: dos ejecuciones, una creación y un rechazo sin cambio, con evidencia del inventario intacto. No se modificó el XLSX entregado para añadir macros ni se presenta este taller como ejecutado en Calc nativo por la edición.

¿Lo has pillado?

1. ¿Qué cambia al copiar `=F8/E8` una fila hacia abajo?

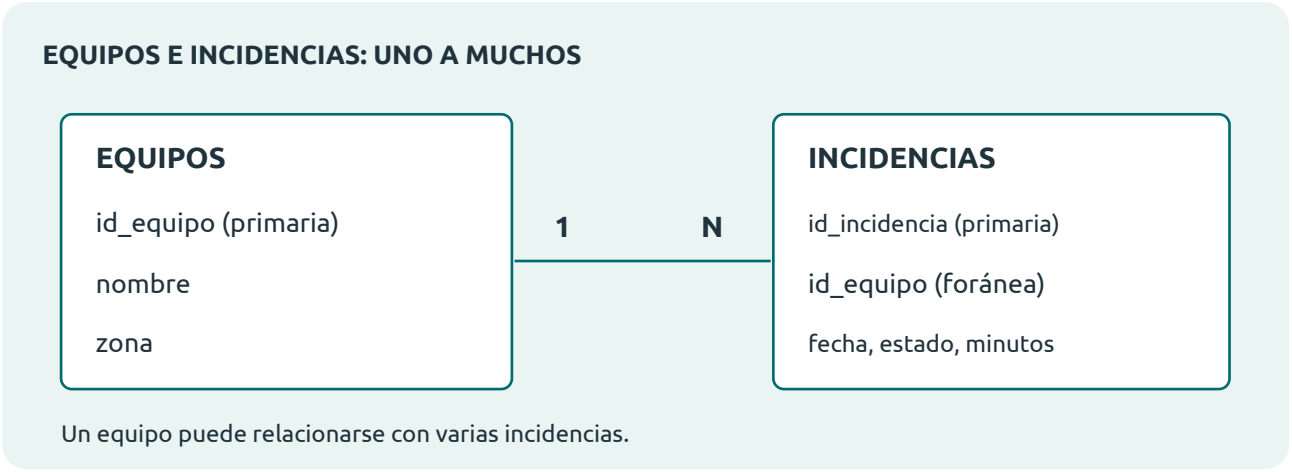
2. ¿El 15 % debe almacenarse como 15 si después se aplica formato porcentual?

3. ¿Filtrar Revisar hace que `SUMA(E8:E15)` sume solo lo visible?

Soluciones. 1) Normalmente pasa a `=F9/E9` por las referencias relativas. 2) No: el valor numérico correspondiente es 0,15. 3) No: una suma ordinaria incluye el rango conforme a su función; utiliza herramientas apropiadas si quieres excluir filas filtradas.

45. Bases de datos: relacionar sin repetirlo todo

Al terminar: diseñarás dos tablas, consultarás sus relaciones y planificarás formulario e informe.
Antes: datos tabulares y filtros.



Una clave relaciona registros, no posiciones de una lista.

Una base de datos organiza información y permite aplicar reglas y consultas. Una hoja de cálculo puede parecer una tabla, pero un sistema de bases de datos ofrece mecanismos distintos para relaciones, integridad y operaciones. Elegir depende de la necesidad, no de que una herramienta sea siempre superior.

Entidades, registros y claves

Una **tabla** representa un tipo de información. Una fila es un registro y una columna, un atributo. La **clave primaria** identifica cada registro. Una **clave foránea** relaciona un valor con una clave de otra tabla según las reglas definidas.

En Aula Norte tenemos equipos e incidencias. Un equipo puede tener varias incidencias; cada incidencia del ejemplo pertenece a un equipo. Es una relación uno a muchos. El nombre y zona del equipo se guardan en equipos, en lugar de repetirlos manualmente en cada incidencia.

Si una incidencia utiliza un ID inexistente, queremos que la base lo rechace. La **integridad referencial** evita ciertas relaciones incoherentes, pero no demuestra que el nombre escrito sea correcto ni que el equipo físico exista.

Un modelo pequeño

La tabla `equipos` contiene `id_equipo`, `nombre` y `zona`. La tabla `incidencias` contiene `id_incidencia`, `id_equipo`, `fecha`, `estado` y `minutos`. El tiempo es un número no negativo. El estado se restringe a Abierta, En curso o Cerrada.

En `aulanorte-incidencias.sql` de recursos encontrarás tres equipos y cuatro incidencias ficticias. Está preparado para SQLite 3 en una base nueva. No es una orden para ejecutar sobre una base que ya contiene trabajo: crear tablas con nombres existentes o mezclar esquemas puede fallar o alterar el entorno.

Consulta 1: filtrar

```sql
SELECT id_incidencia, id_equipo, estado
FROM incidencias
WHERE estado <> 'Cerrada'
ORDER BY id_incidencia;
```

La consulta devuelve las incidencias 2 y 3. `SELECT` elige columnas, `FROM` la tabla, `WHERE` filtra y `ORDER BY` ordena. No modifica registros. Las comillas simples delimitan los textos del ejemplo. La comparación con valores nulos tiene reglas distintas a las de texto ordinario; no supongas que `<>` selecciona automáticamente los nulos.

Consulta 2: unir información

```sql
SELECT i.id_incidencia, e.nombre, i.estado
FROM incidencias AS i
JOIN equipos AS e ON e.id_equipo = i.id_equipo
WHERE i.estado <> 'Cerrada'
ORDER BY i.id_incidencia;
```

Los alias `i` y `e` permiten identificar el origen de cada campo. La unión relaciona claves, no posiciones de filas. La incidencia 2 corresponde a PC aula 02 y la 3 a PC docencia. Si relacionaras por un nombre no único, podrías multiplicar resultados.

Consulta 3: agrupar

```sql
SELECT e.id_equipo, e.nombre, COUNT(i.id_incidencia) AS total
FROM equipos AS e
LEFT JOIN incidencias AS i ON i.id_equipo = e.id_equipo
GROUP BY e.id_equipo, e.nombre
ORDER BY e.id_equipo;
```

El resultado es AN01 con dos incidencias, AN02 con una y AN04 con una. La unión izquierda permite conservar un equipo aunque no tenga incidencias; por eso contamos el identificador de incidencia y no todas las filas indiscriminadamente. Para comprobarlo, añade un equipo ficticio sin incidencias en una copia y espera un conteo cero.

Diseñar en una base de escritorio

En Base o Access, crea un archivo nuevo y registra el motor que utiliza o al que se conecta. Un archivo de interfaz no contiene necesariamente todos los datos: puede depender de un servidor externo.

Crea las tablas en vista de diseño, elige tipos adecuados y establece la primaria. Para la relación, enlaza la clave de equipos con la foránea de incidencias y activa la integridad que soporte el

motor. No marques borrado en cascada por comodidad: decide si borrar un equipo debe eliminar su historial o si debe impedirse.

Introduce primero los equipos y después las incidencias. Si usas el script SQLite mediante una herramienta compatible, activa y comprueba las claves foráneas en esa conexión. La sintaxis de creación, fechas y funciones puede cambiar en el motor de Base o Access: adapta el diseño en lugar de pegar SQL de otro dialecto sin revisar.

Referencia: SQLite, soporte de claves foráneas, https://www.sqlite.org/foreignkeys.html. Los datos y consultas de este capítulo son originales del ejercicio.

Formularios e informes

Un **formulario** facilita introducir y consultar datos. Prepara uno para incidencias con una selección de equipo basada en su identificador y un nombre visible para la persona. Configura estados mediante opciones limitadas y comprueba que no admite un tiempo negativo. Que el formulario lo impida no sustituye las reglas del almacenamiento si otros programas pueden escribir.

Un **informe** presenta resultados para lectura o impresión. Crea uno basado en una consulta de incidencias abiertas, con título, fecha, encabezados y agrupación útil. Comprueba qué ocurre cuando no hay registros: debe comunicar ausencia de incidencias, no parecer un informe que falló al cargar.

Práctica completa

Crea la base nueva con los recursos, ejecuta las tres consultas y guarda resultados. Prueba, en una copia, un ID de equipo inexistente y un tiempo negativo: deben rechazarse bajo las reglas activas. Añade un equipo sin incidencias y comprueba el cero del resumen. Diseña después el formulario y un informe con los mismos datos en la herramienta de escritorio disponible.

Recuperación: conserva script y copia de la base antes de experimentar con cambios. Un archivo SQL de creación no sustituye una copia de datos posteriores. No ejecutes `DELETE`, `DROP` o `UPDATE` sin saber qué filas o estructura afectan.

Taller en Base: tablas, formulario e informe

Comprueba los componentes y runtimes opcionales del motor, asistentes e informes; algunas funciones de Base requieren Java según la versión y plataforma. Consulta los requisitos oficiales.

El archivo SQLite de recursos sirve para aprender y ejecutar SQL en SQLite. No se convierte en una base `.odb` por cambiar su extensión. Para practicar Base, crea una base nueva con su motor integrado disponible o una conexión compatible preparada por el docente; anota motor y versión porque tipos y sintaxis pueden variar.

1. Crea las tablas Equipos e Incidencias con los campos y claves del modelo. En la vista de diseño elige los tipos adecuados; para este primer ejercicio puedes introducir identificadores enteros explícitos.

2. Define la relación por identificador del equipo y el control de integridad previsto. Introduce dos equipos y dos incidencias ficticias. Comprueba que un identificador inexistente no se acepta si has activado esa integridad.

3. Con el asistente de consultas selecciona campos de ambas tablas, relaciona la clave y filtra incidencias abiertas. Comprueba el resultado contra los datos introducidos; no copies funciones específicas de SQLite si tu motor no las admite.

4. Usa el asistente de formularios para crear **Incidencias**. Incluye etiquetas claras y los campos necesarios. Añade una incidencia, modifica su estado y comprueba en la tabla que se guardó.

5. Crea un informe desde la consulta, agrupa por equipo si procede y revisa título, fecha, totales y páginas. Un informe es una presentación; no debe permitir saltarse reglas de las tablas.

6. Guarda y vuelve a abrir la base. Comprueba tablas, consulta, formulario e informe. Si utiliza un servidor externo, el archivo `.odb` puede guardar la conexión y otros objetos, sin contener todos los datos.

La macro `AbrirIncidenciasBase` del recurso abre un formulario llamado Incidencias si existe. Incorpórala en la biblioteca del documento Base y ejecútala con la base abierta y conexión preparada. Comprueba el nombre; el ejemplo avisa si falta y no crea registros. Puedes vincularla a un botón del formulario según las opciones de eventos de la aplicación.

Fuente de acceso al documento de Base: ThisDatabaseDocument, ayuda oficial. La prueba editorial ejecutada fue la del SQLite de recursos; este recorrido de interfaz y macro se propone como práctica del lector, sin afirmar ejecución nativa.

¿Lo has pillado?

1. ¿Una clave foránea válida demuestra que un dato es verdadero?

2. ¿Por qué unir por ID y no por orden de fila?

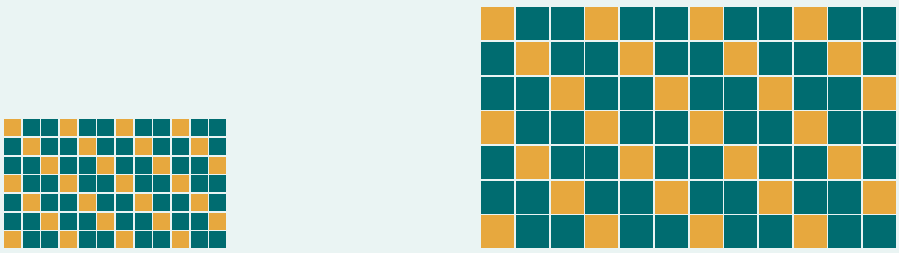
3. ¿Un formulario bonito garantiza integridad por otras vías de escritura?

Soluciones. 1) No: comprueba una relación definida, no toda la realidad. 2) El orden puede cambiar y no identifica una entidad. 3) No: hacen falta reglas y controles también en el sistema que almacena los datos.

46. Presentaciones, imagen y vídeo que ayudan a explicar

Al terminar: convertirás una práctica en una explicación visual breve y prepararás recursos con formato adecuado. **Antes:** documentos y resultados del inventario.

TAMAÑO, PÍXELES Y DENSIDAD



Misma cuadrícula

Más tamaño, menos densidad

El mismo número de píxeles ocupa más espacio con menor densidad.

Una presentación acompaña una explicación; no necesita reproducir cada párrafo de la memoria. Decide qué debe comprender la audiencia y qué evidencia permitirá sostenerlo. El tamaño de letra que se lee en tu portátil puede resultar insuficiente al proyectar.

De la memoria a cinco diapositivas

Para Aula Norte utiliza: problema, entorno, intervención, comprobación y siguiente paso. En «problema» concreta el fallo o necesidad. En «comprobación» muestra un resultado reconocible, como el gráfico de equipos por zona o una prueba de acceso, explicando sus límites.

Utiliza una plantilla y diseños coherentes. Alinea elementos, conserva márgenes y evita que cada diapositiva tenga una estructura diferente sin motivo. Las notas del presentador pueden recoger el detalle que explicarás oralmente.



Consejo de David

No uses animaciones para esconder falta de estructura. Si una transición o aparición ayuda a seguir el recorrido de una petición, úsala con moderación y comprueba que sigue entendiéndose en PDF o sin animación.

Imagen ráster y vector

Una imagen **ráster** contiene píxeles. Ampliarla mucho puede mostrar falta de detalle. Un **vector** describe formas que pueden escalar conservando sus bordes, aunque una ilustración vectorial puede incluir también imágenes ráster.

PNG es útil para capturas y gráficos con bordes y transparencia. JPEG suele ser adecuado para fotografías con compresión con pérdidas. SVG sirve para gráficos vectoriales compatibles. Elegir una extensión no crea detalle que el original no tenía.

Una imagen de 1.200 píxeles impresa a 10 cm de ancho aporta aproximadamente 305 píxeles por pulgada: 1.200 dividido entre 10/2,54. Si la extiendes a 20 cm, la densidad se reduce a la mitad. La cifra es una relación geométrica, no una garantía de que la captura contenga texto legible.

Recortar, redimensionar y exportar

Recortar elimina partes de la composición; redimensionar cambia sus dimensiones. Mantén proporciones para no deformar dispositivos ni letras. Conserva una copia del original y exporta una versión para el destino, sin sobrescribir la única fuente.

Si ocultas un dato sensible, verifica el archivo final y no solo una capa visible. El capítulo 42 explica por qué cubrir texto en un archivo editable puede dejarlo recuperable.

Vídeo y audio

El **contenedor** agrupa pistas y datos; el **códec** define su codificación. Un archivo MP4 puede contener combinaciones distintas que no todos los reproductores admiten. La resolución, frecuencia de fotogramas y tasa de bits influyen en calidad y tamaño, junto con el contenido y códec.

Para una demostración técnica, prioriza que se vea el detalle y se entienda el audio. Graba solo la ventana necesaria con cuentas y datos ficticios. Planifica guion, captura, recorte, subtítulos y exportación. No incluyas notificaciones, contraseñas o conversaciones ajenas por grabar todo el escritorio.

Práctica: explicar una restauración

Prepara cinco diapositivas que expliquen la práctica del capítulo 40. Incluye un diagrama del recorrido y una evidencia de que el archivo restaurado coincide con el inicial. Añade texto alternativo cuando proceda y verifica contraste sin depender solo del color.

Graba, si dispones de medios, un vídeo breve que muestre el procedimiento con narración o subtítulos. Reprodúcelo completo en otro reproductor o equipo compatible. Comprueba volumen, texto, formato y tamaño antes de entregar.

Resultado esperado: otra persona puede explicar objetivo, pasos y prueba final sin leer una pantalla saturada. Conserva el archivo editable y exporta PDF o vídeo según el destino. No prometas que las notas o animaciones se conservarán en todos los formatos.

Taller de imagen: conservar fuente y exportación

En `recursos/ofimatica/media` hay tres láminas originales en SVG y PNG. SVG conserva las formas y el texto como descripción vectorial; PNG es una representación de píxeles. Guarda una copia y compara tamaño, legibilidad al ampliar y finalidad de ambos.

En un editor de imagen autorizado importa una PNG, recorta un margen y exporta otra copia. Después redimensiona a la mitad manteniendo proporción y compara al mismo tamaño de pantalla. No cambies solo el número de ppp y esperes recuperar detalle perdido. Conserva la fuente para rehacer la exportación.

Añade un ajuste moderado de brillo/contraste a una captura propia con datos ficticios y comprueba que el texto siga legible. Si capturas desde escáner o cámara, registra resolución, iluminación, orientación y permisos. Para la práctica no se necesitan caras ni documentos personales.

Taller de vídeo: proyecto y archivo final

El recurso `ejemplo-12s.mp4` es una secuencia original de las tres láminas, sin audio. Abre una copia en Shotcut u otro editor autorizado, crea un proyecto con su carpeta de medios y comprueba resolución, frecuencia y duración. Un proyecto `.mlt` de Shotcut mantiene decisiones y referencias; no sustituye a todos los archivos fuente.

1. Importa el vídeo y llévalo a la línea de tiempo. Recorta un segundo al inicio y otro al final. Reproduce para revisar que no se haya perdido el mensaje importante.
2. Divide un fragmento, mueve el cursor y comprueba el corte. Añade un rótulo o subtítulo legible. No tapes información necesaria.
3. Si tienes una grabación de voz propia autorizada, añádela en otra pista, ajusta nivel y escucha sin saturación. El ejemplo entregado permanece sin audio para que esa parte sea una decisión de la práctica.
4. Exporta desde la línea de tiempo completa al formato previsto, por ejemplo MP4 con vídeo H.264 si tu herramienta lo ofrece. **MP4 es contenedor; H.264, códec.** La extensión no acredita qué codificación contiene.
5. Reproduce el archivo exportado en otro reproductor y comprueba imagen, texto, duración y audio si lo añadiste. Guarda proyecto, medios y exportación identificados.

Compara también una exportación a menor resolución o tasa y describe el cambio de tamaño y legibilidad. No existe una tasa única adecuada para cualquier vídeo. Para explicar una restauración real, sustituye las láminas por capturas ficticias autorizadas y un guion que muestre preparación, acción y comprobación.

Fuentes: guía de inicio de Shotcut y referencia de controles. La secuencia de muestra se generó y comprobó como archivo; la edición en Shotcut corresponde a la práctica, sin afirmar uso de esa interfaz en la edición.

Taller de presentación: patrón, vistas y proyección

Crea un patrón con tipografías, título, numeración y contraste coherentes. Utilízalo en cinco diapositivas del proyecto y cambia un elemento del patrón para comprobar qué se actualiza. Distingue vista de edición, clasificador para ordenar, notas del presentador y presentación a pantalla completa.

Ensaya con temporización y revisa proyección, proporción de pantalla, conexiones y sonido si lo usas. Una diapositiva que se lee en tu monitor puede ser ilegible desde el fondo del aula. Exporta PDF para consulta y conserva el proyecto editable; el PDF no reproduce necesariamente transiciones, vídeo o notas.

¿Lo has pillado?

1. ¿Cambiar una captura pequeña a PNG crea más detalle?

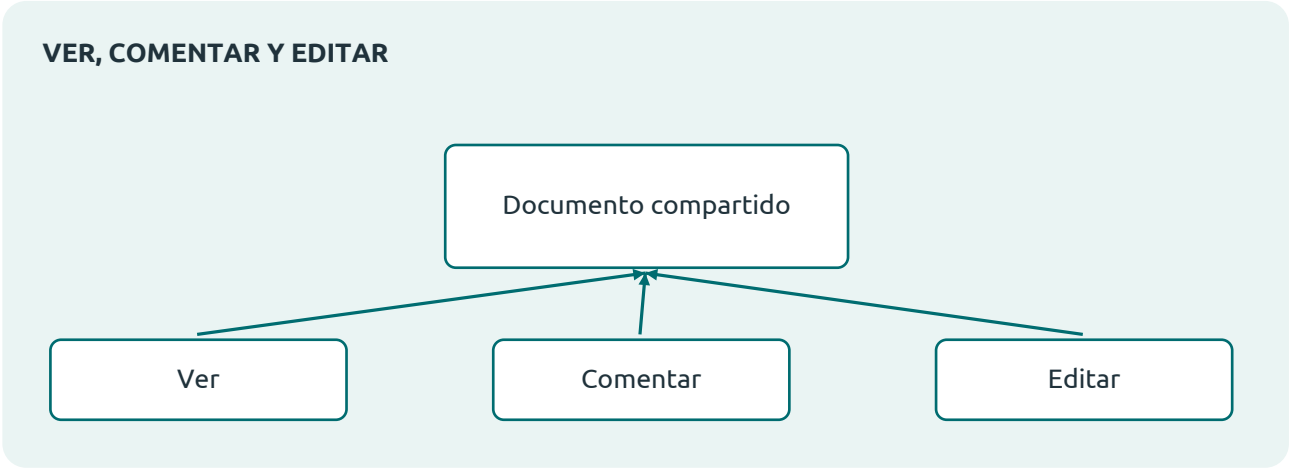
2. ¿MP4 identifica por sí solo el códec de todas sus pistas?

3. ¿Por qué comprobar la presentación en el destino?

Soluciones. 1) No: cambiar formato no reconstruye la información que falta. 2) No: es un contenedor. 3) Fuentes, proporciones, vídeo y funciones pueden variar entre equipos y formatos.

47. Correo, calendario y colaboración sin perder el control

Al terminar: organizarás comunicación y edición compartida con permisos y versiones claras.
Antes: correo del capítulo 35 y privacidad.



Cada persona debe recibir el permiso que necesita.

Las herramientas de colaboración reducen intercambios de copias cuando se utilizan con un procedimiento común. Si cada persona descarga un documento, lo modifica y lo vuelve a enviar con el mismo nombre, sigue existiendo un problema de versiones aunque el almacenamiento esté en la nube.

Mensajes que se puedan atender

El asunto identifica la tarea. El cuerpo indica contexto, acción necesaria y plazo si existe. Los adjuntos deben tener un nombre y versión reconocibles. Antes de enviar, comprueba destinatarios y si el contenido requiere un canal distinto.

Para y CC hacen visibles destinatarios según el servicio; CCO oculta su lista a otros destinatarios bajo el funcionamiento correspondiente. CCO no cifra el mensaje ni impide reenviar contenido. Un enlace de descarga puede ser revocable y limitar acceso; un adjunto ya entregado puede seguir en otras copias.

Organización y búsqueda

Utiliza carpetas o etiquetas con un criterio que puedas mantener. Las reglas automáticas pueden clasificar mensajes, pero una regla demasiado amplia puede esconder avisos importantes. Prueba con mensajes ficticios y revisa qué condiciones la activan.

Para buscar, combina remitente, asunto, fecha y adjuntos según las capacidades de la herramienta. No borres mensajes de forma masiva para solucionar un problema de espacio sin comprobar políticas, retención y copia.

Calendarios y zonas horarias

Una convocatoria necesita fecha, hora, zona, duración, participantes y objetivo. Un evento puede verse a otra hora local en un calendario de otra zona sin que represente otro instante. Diferencia una fecha de entrega sin hora de una reunión con inicio y fin.

Prueba una convocatoria ficticia sin enviar a otras personas: revisa cómo se muestra en dos zonas o configura el borrador y consulta su resumen. Cambiar la zona del equipo para arreglar una única invitación puede afectar otros registros.

Permisos de un documento compartido

Distingue ver, comentar y editar. Un enlace para «cualquiera que lo tenga» amplía el alcance respecto a una invitación nominal, según el servicio. Comprueba si permite descargar, reenviar, caducar o retirar acceso; no supongas capacidades que no están configuradas.

Prueba desde otra identidad de laboratorio. Una ventana donde tú sigues autenticado como propietario no demuestra lo que ve el destinatario. Revocar el enlace tampoco garantiza recuperar copias que alguien ya descargó.

Coautoría, historial y sincronización

La **coautoría** permite trabajo simultáneo bajo condiciones del formato y plataforma. El historial ayuda a recuperar estados, pero hay que conocer su retención y qué cambios incluye. La sincronización con un equipo desconectado puede crear conflictos al reconectar.

Elige una versión de referencia y un procedimiento para resolver cambios. Comparar versiones y aceptar o rechazar revisiones son acciones diferentes de sustituir todo el documento por la copia más reciente que alguien encontró.

Práctica: una entrega en equipo

Con documentos ficticios y cuentas de laboratorio propias o autorizadas, define quién edita y quién comenta. Crea una revisión identificable, deja una observación y resuélvela mediante un cambio comprobable. Consulta el historial y recupera una copia anterior sin sobrescribir la única versión vigente.

Después revisa el enlace desde una identidad sin autorización. Debe mostrar el comportamiento previsto por la política. Retira el permiso de prueba y verifica su efecto mediante una sesión nueva. No envíes invitaciones reales ni cambies documentos compartidos de otras personas para completar el ejercicio.

Resultado esperado: se sabe cuál es la entrega vigente, quién puede actuar y qué parte del historial se ha probado. Si no tienes plataforma disponible, documenta el flujo y utiliza control de cambios y archivos separados de forma explícita; marca la actividad como simulación.

SOS: «no veo los cambios»

Comprueba archivo, ubicación, identidad, conexión y estado de sincronización. Dos documentos con el mismo nombre en ubicaciones distintas no son la misma copia. Revisa si alguien está editando una descarga local en lugar del documento compartido.

Taller de cliente, libreta y sincronización

En una cuenta ficticia del servidor del capítulo 35, configura un cliente autorizado con nombre de cuenta, dirección, usuario de autenticación y servidores de entrada/salida. IMAP 993 con TLS y SMTP 587 con STARTTLS son los valores del laboratorio, no un descubrimiento automático válido para cualquier proveedor. Comprueba certificado, envío, lectura, carpeta de enviados y adjunto.

Crea dos contactos ficticios en una libreta, exporta una copia en el formato admitido y vuelve a importarla en una libreta vacía de prueba. Compara nombres, direcciones, campos y duplicados. Un archivo vCard conserva ciertos datos de contacto; no es la misma operación que sincronizar una libreta de manera continua.

Si utilizas la plataforma del taller web, **CalDAV** permite sincronizar calendarios y **CardDAV**, contactos, con clientes que los admitan. Cada sistema móvil o de escritorio requiere su aplicación y configuración compatible; no todos los calendarios incorporados ofrecen los mismos protocolos.

En un cliente de prácticas compatible añade cuenta, URL HTTPS de la plataforma e identidad/autenticación correspondientes. Si requiere contraseña de aplicación, créala y guárdala como un secreto revocable; no la pegues en el informe. Verifica confianza del certificado y alcance.

Crea una cita en el navegador y comprueba que aparece en el cliente; cambia su hora desde el cliente y revisa la web. Haz una prueba similar con un contacto cuando uses CardDAV. Revisa zona horaria y diferencia entre calendario personal y compartido. Si solo importaste un archivo una vez, no declares sincronización bidireccional.

Recuperación: retira la cuenta de prueba y revoca su credencial de aplicación según el procedimiento, conservando antes la información ficticia necesaria. No elimines un calendario compartido real para reiniciar un ejercicio.

Referencia de configuración y límites: manual de sincronización de Nextcloud, por ejemplo CalDAV/CardDAV en macOS. El ensayo debe realizarse en los clientes del lector; no se sincronizó un dispositivo personal en la edición.

¿Lo has pillado?

1. ¿CCO protege todo el contenido frente a los destinatarios?

2. ¿Retirar un enlace elimina necesariamente las descargas anteriores?

3. ¿Una versión más reciente por fecha es siempre la correcta?

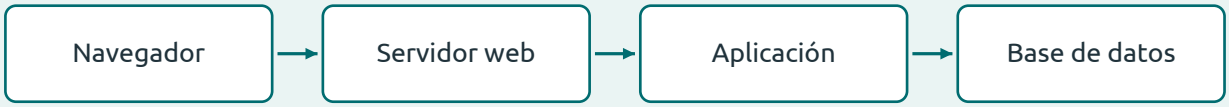
Soluciones. 1) No: afecta a visibilidad de direcciones, no a toda la información. 2) No: el acceso remoto y las copias ya obtenidas son cuestiones distintas. 3) No: puede contener un cambio erróneo o pertenecer a otra rama de trabajo; revisa contenido y procedimiento de aprobación.

Bloque 9. Aplicaciones web

48. Qué ocurre detrás de una página

Al terminar: separarás navegador, servidor web, aplicación y datos, y explicarás sesión y almacenamiento. **Antes:** HTTP/HTTPS, DNS y bases de datos.

PAPELES DENTRO DE UNA APLICACIÓN



Petición → procesamiento → respuesta; puede haber varios recursos.

Algunos sitios son estáticos y no necesitan aplicación ni base de datos.

Una respuesta visible no demuestra que se haya guardado una operación.

Una página puede ser un archivo estático o el resultado de una aplicación que consulta datos, aplica reglas y genera una respuesta. Que ambas se vean en un navegador no significa que necesiten la misma infraestructura.

Cliente, servidor web y aplicación

El **cliente web** solicita recursos e interpreta contenido. El **servidor web** recibe peticiones y ofrece respuestas o las dirige al componente que debe procesarlas. La **aplicación** aplica funciones: identificar usuarios, buscar incidencias o publicar contenidos. La **base de datos** conserva información organizada cuando forma parte del diseño.



Ojo con este error

Estos papeles pueden estar en una máquina o repartidos. El navegador también ejecuta código del lado cliente, pero eso no le concede autoridad para decidir permisos en el servidor. Si una validación solo existe en JavaScript del navegador, otra forma de petición puede saltársela.

Recursos y rutas

Un documento HTML puede referenciar CSS, imágenes y scripts. El navegador solicita esos recursos usando sus URL. Una página que aparece sin estilos puede tener el HTML correcto y fallar la ruta de su CSS.

Una URL distingue esquema, autoridad o servidor, ruta y otros componentes como consulta y fragmento. El fragmento que identifica un lugar del documento no se envía al servidor como

parte ordinaria de la petición HTTP. Un parámetro de consulta no debe utilizarse para transportar contraseñas reales: puede quedar en historiales y registros.

Sesiones, cookies y autorización

HTTP no convierte automáticamente varias peticiones en la misma sesión de usuario. Las aplicaciones utilizan mecanismos como identificadores de sesión, cookies o tokens bajo su diseño. Una cookie es un dato que el navegador gestiona según sus reglas; no es por sí misma una prueba suficiente de seguridad.

La aplicación debe comprobar identidad y autorización para cada operación que lo requiera. Ocultar un botón de borrar no impide que alguien intente solicitar esa operación. Cerrar una ventana tampoco garantiza que una sesión del servidor se haya revocado.

Frontend, backend y almacenamiento

Frontend describe la parte de interacción que utiliza la persona, normalmente en el navegador. **Backend** agrupa procesamiento y servicios del lado servidor. No hace falta escribir un backend completo para administrar una aplicación, pero sí conocer sus dependencias.

Una aplicación puede almacenar ficheros fuera de la base de datos. Copiar únicamente el SQL puede dejar registros que apuntan a imágenes inexistentes. Copiar solo el directorio web puede perder cuentas, entradas o configuraciones que estaban en la base.

Ejemplo: «el formulario dice enviado»

Un script puede cambiar un texto en pantalla sin enviar nada. Para demostrar una entrega necesitas comprobar la petición, la respuesta de la aplicación y el estado persistido o resultado previsto. Un `200` de una página distinta o un mensaje dibujado localmente no acredita que el servidor haya guardado la incidencia.

La práctica HTML del siguiente capítulo es deliberadamente local: muestra una descripción y dice expresamente que no envía ni almacena incidencias. Su objetivo es aprender estructura e interacción, no fingir un servicio operativo.

Práctica: inspecciona un recurso propio

Abre la página de recursos del capítulo 49 con las herramientas de desarrollo de tu navegador. Identifica documento, CSS, script e imagen. Comprueba sus rutas y la consola. Si trabajas mediante archivo local, habrá diferencias respecto a servirlo por HTTP; registra cuál estás utilizando.

Dibuja después qué añadirías para guardar una incidencia: servidor que valide, autorización apropiada, almacenamiento y una respuesta verificable. No utilices datos personales ni una web ajena para experimentar.

Resultado esperado: puedes explicar qué hace realmente la página y qué no has implementado. Para recuperar, vuelve a los archivos originales si modificaste una ruta o recurso de la copia.

¿Lo has pillado?

1. ¿Un mensaje de éxito en pantalla demuestra almacenamiento en servidor?

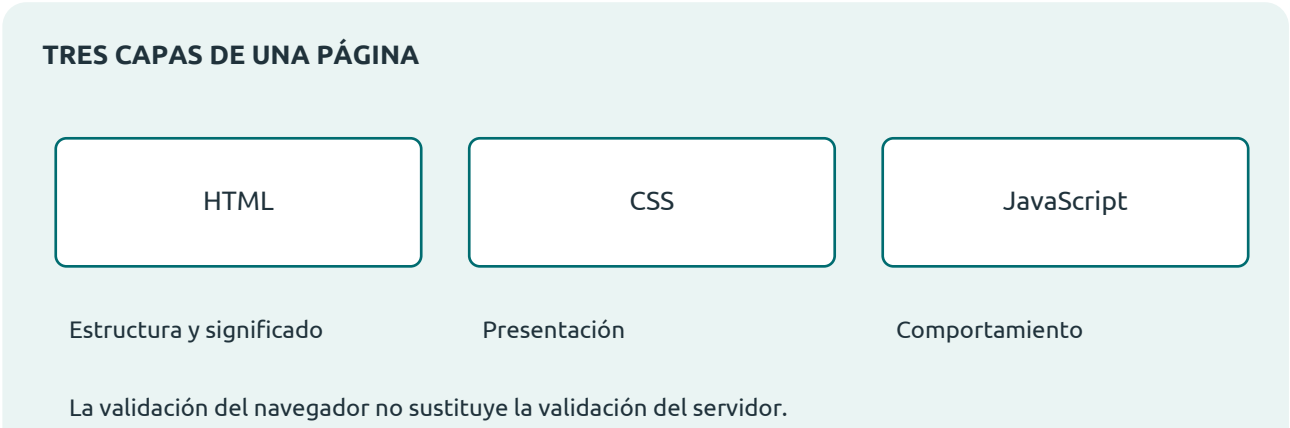
2. ¿Un control oculto en el navegador sustituye la autorización del backend?

3. ¿La base de datos contiene necesariamente todos los archivos subidos?

Soluciones. 1) No: hace falta comprobar la operación real. 2) No: el servidor debe aplicar su control. 3) No: depende del diseño; los ficheros pueden estar en otro almacenamiento.

49. HTML y CSS para comprender y modificar

Al terminar: editarás una página accesible de prácticas y comprobarás su funcionamiento en distintas anchuras. **Antes:** archivos, rutas y capítulo 48.



Estructura, presentación y comportamiento cumplen funciones diferentes.

HTML describe estructura y significado. CSS define presentación. JavaScript puede añadir comportamiento. Las tres tecnologías se relacionan, pero una página sencilla puede existir sin JavaScript y una regla CSS no sustituye una estructura semántica.

Una estructura mínima

El recurso `practica-html` contiene `index.html`, `estilos.css`, `practica.js` y las ilustraciones `red.svg` y `red-movil.svg`. Mantén esos nombres y ubicaciones para que las referencias relativas funcionen. Copia la carpeta completa a tu espacio de prácticas y abre su documento principal.

HTML

```
<!doctype html>
<html lang="es">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>Práctica de Aula Norte</title>
  <link rel="stylesheet" href="estilos.css">
</head>
<body>
  <main>
    <h1>Práctica de Aula Norte</h1>
    <p>Una tarea, una explicación y una comprobación.</p>
  </main>
</body>
</html>
```

Este fragmento explica la base; el archivo completo del recurso incluye más secciones y el formulario. `lang` declara el idioma, `charset` la codificación y `viewport` ayuda a representar el

contenido en dispositivos móviles. El título de la pestaña y el encabezado visible cumplen papeles distintos.

Elementos y atributos

Un elemento puede tener etiqueta de apertura, contenido y cierre; otros, como `img` o `input`, tienen reglas propias y no llevan un cierre equivalente. Los atributos proporcionan datos, como la ruta `src` de una imagen o el destino `href` de un enlace.

Utiliza encabezados jerárquicos, párrafos, listas y regiones según su significado. Una imagen informativa necesita una alternativa textual adecuada. Una imagen decorativa puede requerir una alternativa vacía según el contexto. No conviertas todo en imágenes de texto: dificulta lectura, selección y adaptación.

Formularios: etiqueta y control deben estar relacionados

HTML

```
<label for="equipo">Identificador del equipo</label>
<input id="equipo" name="equipo" required
       pattern="AN[0-9]{2}" placeholder="AN01">
```

`for` debe coincidir con el `id` del control. El `name` participa en la identificación del dato cuando se utiliza un envío de formulario. El placeholder es una pista temporal, no sustituye la etiqueta. El patrón de este ejemplo acepta AN seguido de dos cifras; no valida la existencia del equipo en una base de datos.

`required`, tipos de campo y otras restricciones ayudan a evitar determinados errores de entrada en el navegador. El servidor debe realizar su propia validación cuando exista procesamiento remoto.

Fuente de estructura de formularios: estándar HTML de WHATWG, https://html.spec.whatwg.org/multipage/forms.html.

CSS: selector, propiedad y valor

CSS

```
* { box-sizing: border-box; }
body { max-width: 56rem; margin: 0 auto; padding: 1.5rem; }
h1, h2 { color: #006c70; }
section { padding: 1.5rem; border: 1px solid #cadada; }
```

El selector elige elementos; las declaraciones entre llaves asignan propiedades. `padding` separa contenido y borde. `margin` afecta al espacio exterior. `border-box` cambia cómo se integra borde y relleno en el tamaño declarado. Aprende el modelo de caja antes de añadir anchuras al azar.

La cascada y la especificidad influyen en qué regla termina aplicándose. Si un color no cambia, inspecciona el estilo calculado y las reglas que lo anulan. Añadir `!important` indiscriminadamente puede ocultar el problema y dificultar mantenimiento.

Diseño adaptable y foco

Una anchura máxima y espacios proporcionales ayudan a que la lectura se adapte. Las consultas de medios permiten cambiar determinadas reglas según las condiciones. No necesitas inventar una página distinta para cada pantalla.

Comprueba navegación con teclado y foco visible. En la práctica puedes saltar al contenido y llegar a los controles sin ratón. El mensaje de resultado utiliza una región de estado. Que una página tenga atributos de accesibilidad no certifica que sea accesible: hacen falta pruebas y revisión del contexto.

Qué hace el JavaScript de la práctica

El script intercepta el envío, revisa restricciones y muestra una descripción mediante texto, sin guardarla ni transmitirla. No utiliza `innerHTML` para insertar el síntoma introducido. Limpiar el formulario retira el mensaje. Cerrar la página pierde el estado de la práctica.

Vamos a probarlo

1. Abre la carpeta original y comprueba que se ven estilos e ilustración. Haz una copia de trabajo.
2. Cambia un encabezado y el color de una sección mediante CSS. Comprueba qué regla lo afecta.
3. Intenta comprobar una descripción con campos vacíos: el formulario debe impedirlo.
4. Introduce `AN01`, un síntoma ficticio de al menos doce caracteres útiles y un alcance. El mensaje debe aclarar que no se ha enviado nada.
5. Prueba un ID incompatible con el patrón y después corrígelo. Repite con teclado y en anchura estrecha.
6. Renombra temporalmente la hoja CSS en la copia y observa el efecto. Restaura el nombre o la referencia; explica por qué el contenido seguía existiendo.
7. Revisa la impresión y el tamaño del contenido sin convertirlo todo en letra minúscula.

Resultado esperado: identificas estructura, presentación y comportamiento, y puedes recuperar los archivos. Si publicas la copia en el servidor interno del capítulo 33, comprueba además respuestas HTTP y rutas; abrir el archivo local no verifica ese despliegue.

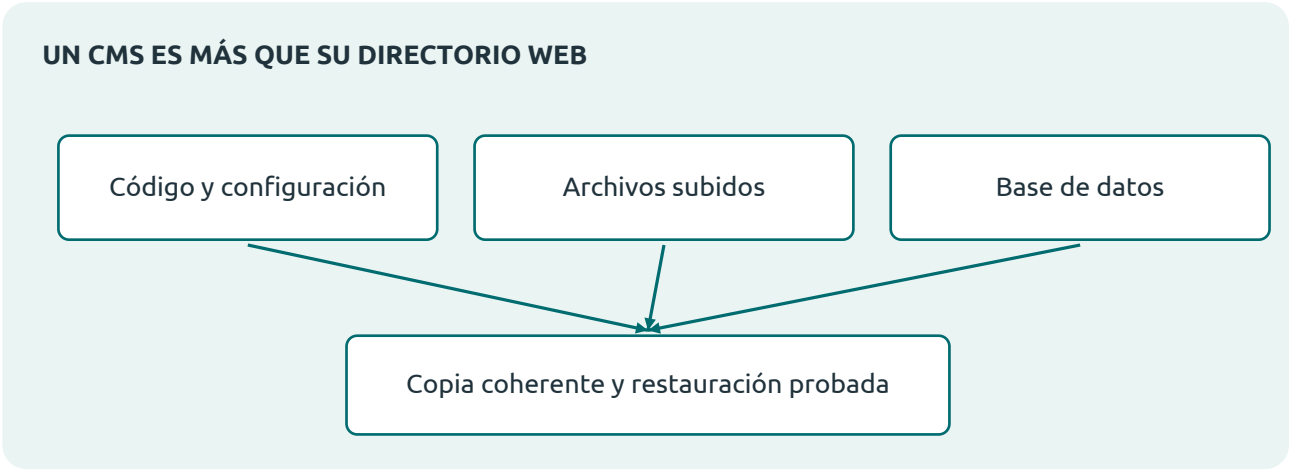
¿Lo has pillado?

1. ¿`placeholder` sustituye una etiqueta?
2. ¿Un ID que cumple el patrón existe necesariamente en el inventario?
3. ¿Cambiar la ruta del CSS destruye el contenido HTML?

Soluciones. 1) No: desaparece o cumple otra función y debe existir una etiqueta adecuada. 2) No: solo cumple el formato. 3) No: puede impedir la carga de estilos mientras el documento permanece.

50. Instalar y administrar un CMS

Al terminar: prepararás un CMS de laboratorio, sus funciones de usuario y una prueba de recuperación. **Antes:** servidor web, PHP o entorno correspondiente, bases de datos y copias.



La recuperación necesita las piezas que utiliza esa instalación.

Un **gestor de contenidos**, o CMS, permite crear y organizar contenido mediante una aplicación. Un **tema** define parte de la presentación; una **extensión** o plugin añade funciones. Instalar muchas extensiones no equivale a una solución mejor: cada una introduce dependencias y mantenimiento.

Utilizaremos WordPress como ejemplo de CMS, sin confundir el software descargable con servicios alojados que pueden tener condiciones y opciones distintas. La práctica se desarrolla en un invitado nuevo y una red interna, sin publicación externa.

Preparar una ficha de compatibilidad

Anota versión exacta de WordPress, PHP, base de datos y servidor web. En la consulta editorial del 5 de noviembre de 2026, WordPress recomienda PHP 8.3 o superior, MariaDB 10.11 o superior o MySQL 8.0 o superior, y HTTPS. Comprueba la tabla oficial de la versión antes de instalar: versiones antiguas que todavía ejecutan el programa pueden haber perdido soporte.

Fuente de requisitos: https://wordpress.org/about/requirements/. No utilices estas cifras para afirmar compatibilidad futura sin revisar la aplicación y sus extensiones.

Preparar las dependencias

Configura un servidor web que ejecute PHP con las extensiones requeridas por la versión. Comprueba la conexión con una base dedicada y una cuenta de base de datos con permisos sobre ella. Esa cuenta no debe ser el administrador general del motor por comodidad.



Ojo con este error

En un laboratorio local, el servidor de base de datos puede estar en la misma máquina; si no lo está, necesitas camino, escucha y autorización adecuados. `localhost` se interpreta desde el contexto donde se ejecuta la aplicación y puede utilizar mecanismos distintos según el cliente. No lo copies a una arquitectura de dos máquinas esperando que apunte a la otra.

Prepara el nombre `cms.aulanorte.test` en tu DNS interno y el sitio web correspondiente. No reutilices la raíz del sitio estático si quieres conservarlo. Define propietario y permisos para que el servicio lea código y pueda escribir solo donde la operación lo requiera.

Instalación guiada

1. Descarga el paquete oficial y registra versión y procedencia. Descomprímelo en un destino de laboratorio identificado.
2. Crea la base y el usuario de aplicación mediante la herramienta del motor. Guarda la credencial protegida y no la incluyas en capturas.
3. Sitúa el código en el directorio configurado para el CMS. Comprueba las dependencias de PHP antes de iniciar el instalador; un archivo PHP no debería ofrecerse como texto descargable.
4. Abre la URL interna y completa idioma, conexión a la base y parámetros solicitados. Identifica host, nombre de base, usuario y prefijo de tablas. El prefijo no sustituye una política de permisos.
5. Crea una cuenta de administración de laboratorio con nombre y contraseña propios. Revisa título del sitio, URL y opciones de visibilidad. Una preferencia para buscadores no es un control de acceso.
6. Accede al panel, crea una página ficticia y comprueba el resultado desde otra sesión sin administración.
7. Configura HTTPS del laboratorio y verifica enlaces, autenticación y certificado; no aceptes errores para aparentar que la prueba funciona.

Fuente del procedimiento de instalación: manual oficial de WordPress, https://developer.wordpress.org/advanced-administration/before-install/howto-install/. Registra las pantallas y pasos de tu versión; las etiquetas de interfaz pueden cambiar.

Contenidos y funciones de usuario

Distingue páginas de contenido estable y entradas organizadas cronológicamente según el CMS. Utiliza categorías, etiquetas, menús o navegación de forma coherente con el sitio. La biblioteca de medios no es un lugar para guardar archivos privados sin revisar cómo se publican.

Crea una cuenta editorial ficticia con un rol limitado. Prueba qué puede crear, revisar y publicar. En WordPress, roles como Administrador, Editor, Autor, Colaborador y Suscriptor tienen capacidades diferentes y pueden modificarse mediante configuración o extensiones. No concedas administración a todo el equipo que escribe noticias.

Temas y extensiones

Elige una necesidad concreta antes de instalar. Revisa procedencia, compatibilidad y mantenimiento. Prueba en una copia, activa y verifica la función y su retirada. Dos extensiones que alteran la misma parte pueden crear conflictos. Desactivar no equivale siempre a desinstalar ni a borrar sus datos.

No cambies directamente archivos de un tema para una modificación que desaparecerá en su siguiente actualización. Identifica los mecanismos de personalización apropiados de la plataforma. Conserva una base recuperable antes de experimentar.

Actualizar y restaurar

Haz una copia coherente de base, archivos relevantes y configuración. Ensaya la actualización en un clon aislado con las mismas dependencias. Comprueba portada interna del sitio, contenido, acceso por roles, medios y función ampliada. La copia debe poder restaurarse, no limitarse a existir.

El recurso de exportar contenido del CMS puede ser útil para transferir entradas, pero no necesariamente conserva toda la instalación, extensiones, ficheros y configuración. Define si necesitas exportación de contenido, copia completa o migración.

Fuente sobre alcance de copias:
https://developer.wordpress.org/advanced-administration/security/backup/.

Práctica de aceptación

Entrega una ficha con versiones, URL interna, dependencias y cuentas descritas sin contraseñas. Incluye una página, una entrada, un recurso multimedia propio, navegación y un usuario limitado. Prueba publicación autorizada y rechazo de una operación administrativa desde ese usuario.

Restaura la copia en otro invitado o destino preparado, sin enviar correos ni contactar servicios reales. Comprueba nombres, medios y roles. Para retirar el laboratorio, conserva evidencias y elimina sus credenciales y datos según el plan.

SOS: error de conexión con la base

Comprueba nombre del motor y base, dirección, credencial y permisos. La web puede estar atendiendo HTTP y fallar únicamente la conexión de aplicación. No cambies a una cuenta superadministradora para ocultar una concesión de permisos incorrecta.

¿Lo has pillado?

1. ¿Ocultar el sitio a buscadores impide que alguien con la URL acceda?

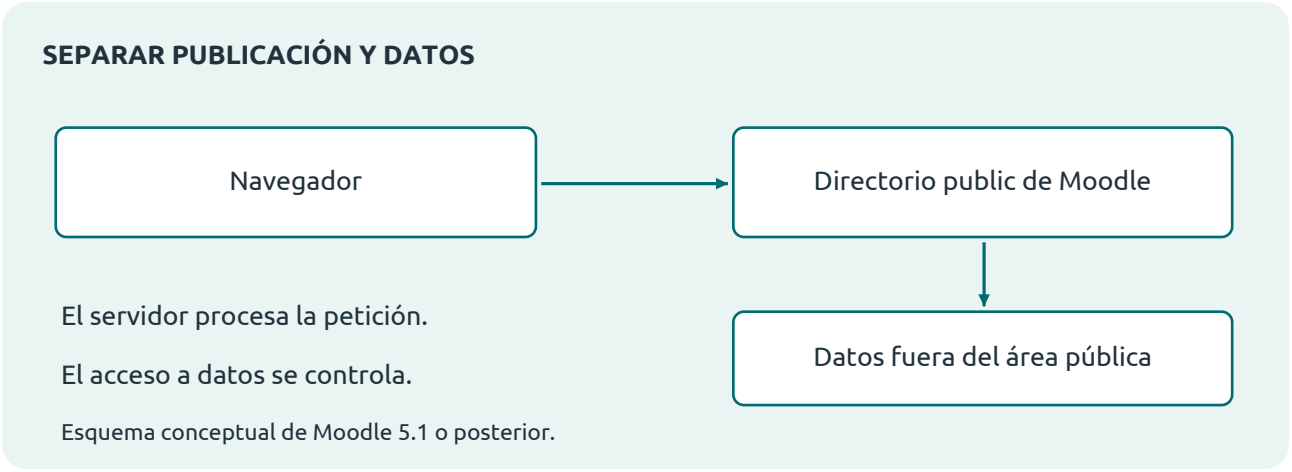
2. ¿Un tema y una extensión cumplen necesariamente la misma función?

3. ¿Exportar entradas demuestra una copia completa del CMS?

Soluciones. 1) No: necesitas un control de acceso real si el contenido es privado. 2) No: sus papeles principales son distintos, aunque ciertas funciones puedan solaparse. 3) No: revisa qué incluye y qué queda fuera.

51. Plataformas colaborativas y de aprendizaje

Al terminar: administrarás un curso de prueba con roles, entrega y restauración, y distinguirás copia de curso y de sitio. **Antes:** CMS, identidades y copias.



El directorio público no debe exponer datos privados de la plataforma.

Una plataforma de aprendizaje, o **LMS**, organiza cursos, participantes, actividades y evaluación. Una plataforma colaborativa puede añadir documentos compartidos, foros, calendarios o trabajo en grupo. Ambas necesitan mantenimiento técnico y reglas de uso; instalar no resuelve cómo se matricula o retira a una persona.

Utilizaremos Moodle como referencia. La documentación consultada corresponde a la rama 5.3. Antes de practicar identifica una versión mantenida, sus requisitos exactos de PHP, base de datos, extensiones y servidor. No mezcles instrucciones de ramas distintas: los cambios de estructura pueden afectar al despliegue.

Separar código, datos y configuración

El servidor debe poder ejecutar el código y acceder a una base dedicada y al almacenamiento de archivos de la plataforma. El directorio de datos no se publica como una carpeta web de descarga libre. Su ubicación, permisos y copia se planifican expresamente.

Desde Moodle 5.1, la estructura incorpora un directorio `public` para los archivos accesibles por web. La raíz que sirve el servidor debe configurarse según las instrucciones de la rama, en lugar de exponer todo el árbol de código como hacían ciertas guías anteriores. Esto no elimina la necesidad de proteger datos, claves y configuración.

Fuente de instalación y estructura: MoodleDocs, https://docs.moodle.org/503/en/Installing_Moodle. Consulta también las notas de versión enlazadas allí para los requisitos numéricos actualizados.

Recorrido de instalación de laboratorio

1. Prepara otro invitado o un entorno aislado separado del CMS anterior. Registra recursos, versión y dependencias antes de instalar.

2. Define un nombre interno, una base y una cuenta de aplicación específicas. Configura el directorio de datos fuera del alcance público.
3. Descarga código oficial y sitúalo según la estructura de la rama. Configura la raíz pública y los requisitos de ejecución del servidor y PHP.
4. Completa el instalador web o de consola siguiendo su guía. Revisa las comprobaciones de entorno y conserva la configuración sin secretos en la memoria.
5. Define una cuenta administrativa y crea la configuración mínima del sitio. Configura tareas programadas mediante el mecanismo oficial y comprueba su ejecución: ciertas operaciones se procesan en segundo plano.
6. Activa HTTPS del laboratorio y verifica nombre y confianza. Limita acceso a la red interna y revisa la política de correo para no enviar notificaciones a personas reales.
7. Crea cuentas ficticias para administración, docencia y alumnado, y comprueba sus distintos alcances.

Curso, matrícula y rol

Un usuario existente no está necesariamente matriculado en un curso. El **método de matriculación** determina cómo entra y con qué rol en el contexto correspondiente. Ser docente en un curso no implica administrar todo el sitio.

Crea el curso «Introducción al diagnóstico», una sección y un recurso de lectura original. Añade una tarea que solicite un parte ficticio de intervención. Define fecha de entrega, condiciones, formatos admitidos y evaluación de forma comprensible. Revisa zona horaria y acceso antes de abrir el curso a las cuentas de prueba.

Prueba de ciclo completo

Entra como alumno, abre el recurso, entrega un archivo ficticio y comprueba confirmación y estado. Desde docencia revisa, evalúa y devuelve una observación. Vuelve a alumno y comprueba qué puede ver. Si hay grupos, prueba que el aislamiento corresponda al diseño.

No compruebes toda la experiencia solo con una cuenta administradora: sus permisos pueden ocultar errores de matrícula, visibilidad o fechas. El rol simulado de la plataforma puede ayudar, pero una identidad de prueba independiente aporta otra verificación.

Copia de curso frente a copia del sitio

Una **copia de curso** puede recoger contenido y, según opciones y permisos, datos de participantes. Su alcance debe revisarse al crear y restaurar el archivo. Para compartir una actividad entre docentes no necesitas necesariamente incluir trabajos ni datos del alumnado.

Una **copia de sitio** requiere además los componentes necesarios para reconstruir la instalación, como base, código, configuración y almacenamiento de datos. Recuperar un curso en un sitio ya operativo no demuestra que puedas reconstruir el sitio tras perder el servidor.

Fuentes de los dos alcances: https://docs.moodle.org/503/en/Course_backup y https://docs.moodle.org/503/en/Site_backup.

Práctica de restauración

Genera una copia del curso ficticio y restáurala como otro curso de prueba, revisando nombres, participantes, archivos y fechas. Evita duplicar notificaciones reales. Comprueba como alumno y docente el resultado. Anota qué no se incluyó: dejarlo fuera puede ser una decisión correcta si corresponde al objetivo.

Después prepara en papel el plan de recuperación del sitio: piezas, orden, credenciales custodiadas, pruebas y tiempo. Si lo ejecutas en otro invitado, registra evidencia real; no presentes el plan como despliegue realizado.

SOS: las entregas no se procesan

Revisa estado de la actividad, límites, permisos, espacio y tareas programadas. Que la página principal abra no demuestra que cron esté funcionando. Consulta los registros adecuados y el estado de tareas antes de aumentar privilegios o reinstalar.

¿Lo has pillado?

1. ¿Una cuenta creada ya está matriculada en todos los cursos?

2. ¿La copia de un curso reemplaza la copia de datos y base del sitio?

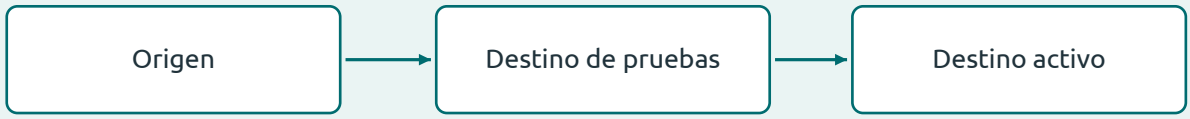
3. ¿Por qué importa la raíz `public` al seguir una guía antigua?

Soluciones. 1) No: depende de matriculación y contexto. 2) No: sus objetivos y componentes son distintos. 3) Porque la estructura de publicación ha cambiado y exponer una raíz incorrecta puede causar fallos y revelar componentes que no deben servirse.

52. Publicar, migrar y mantener colaboración web

Al terminar: elaborarás un plan de publicación o migración con pruebas y reversión. **Antes:** servidor web, DNS, TLS, aplicaciones y copias.

MIGRAR CON CONTROL DE LAS ESCRITURAS



Preparar y probar limitar cambios sincronizar conmutar.

Verificar la tarea y definir qué hacer con los datos si hay reversión.

Se controla dónde se escribe antes de cambiar el servicio de destino.

Publicar significa hacer accesible un servicio bajo un alcance decidido. En el libro practicarás primero en una red interna. Contratar un alojamiento, registrar un dominio o cambiar un DNS público son acciones reales adicionales que requieren su propia decisión y coordinación; no son necesarias para completar los ejercicios locales.

Dominio, DNS, alojamiento y aplicación



Consejo de David

El **dominio** identifica un espacio de nombres. El **DNS** relaciona nombres con información. El **alojamiento** aporta recursos y funciones bajo unas condiciones. La **aplicación** utiliza un entorno y sus datos. Que un proveedor gestione varios de esos elementos no los convierte en uno solo.

Compara requisitos técnicos, acceso a copias, límites de recursos, actualizaciones, exportación y recuperación. Un plan que permite subir HTML no ofrece necesariamente PHP, una base, tareas programadas o las versiones exigidas por Moodle.

Entorno de pruebas y producción

Un entorno de pruebas permite ensayar con datos ficticios o adecuadamente preparados. Debe evitar acciones reales involuntarias: correos, integraciones de pago, indexación o sincronización con otros sistemas. Copiar producción sin revisar esos enlaces puede tener efectos fuera del clon.

Registra diferencias entre entornos. Una función puede ir bien en pruebas y fallar en producción por versión, permisos, tamaño, memoria o configuración de proxy. La semejanza debe verificarse en los aspectos que necesita la aplicación.

Plan de migración

1. Inventaría código, base, archivos subidos, configuración, extensiones, tareas e integraciones. Identifica versiones y compatibilidad del destino.
2. Obtén una copia coherente y verifica una restauración de ensayo. Planifica si necesitas una pausa de escrituras para evitar perder cambios durante el traslado.
3. Prepara destino, certificados, permisos y acceso sin modificar todavía la entrada que usan los clientes.
4. Restaura piezas en el orden adecuado. Ajusta URL, rutas y configuración mediante mecanismos compatibles con la aplicación; un reemplazo de texto indiscriminado puede dañar datos estructurados o serializados.
5. Comprueba con el nombre esperado y una resolución de pruebas controlada: autenticación, contenido, medios, escritura, correo desactivado o dirigido al buzón de laboratorio, tareas y permisos.
6. Si se realiza un cambio de entrada, coordina DNS y cachés. El TTL orienta retención de respuestas, pero no garantiza que todos los usuarios cambien al mismo segundo.
7. Supervisa y conserva un plan de reversión. Decide qué hacer con las escrituras posteriores al cambio: volver al servidor antiguo sin conciliarlas puede perder información.

Lo que debes entregar

El plan indica responsable, ventana, pasos, criterio de éxito, criterio para revertir y datos que deben conservarse. La validación utiliza un cliente distinto del administrador y contiene pruebas negativas de acceso cuando corresponda.

Una migración no termina al mostrar la página inicial. Prueba una imagen subida, un enlace interno, una operación autenticada y la recuperación de la copia. Comprueba que el antiguo entorno deja de procesar tareas que ahora correspondan al nuevo para no duplicar acciones.

Caso de práctica: traslado interno de la intranet

Copia el sitio estático de un invitado a otro y conserva el anterior. Prepara nombre y acceso del destino en el laboratorio. Comprueba HTML, CSS e imagen, registra el contenido distintivo y verifica que las rutas relativas funcionan. Simula el cambio solo en el ámbito de laboratorio y revierte mediante la configuración registrada.

Para el CMS, añade base, medios y configuración a la ficha. Describe qué no necesita el sitio estático y por qué. Esa comparación te ayuda a evitar la falsa regla «migrar una web es copiar una carpeta».

SOS: la web abre, pero faltan imágenes

Revisa rutas, archivos subidos, permisos, URL almacenadas y referencias a la ubicación anterior. Distingue una respuesta 404, una denegación y un bloqueo por contenido mixto. No cambies todos los permisos a escritura global para resolver cualquier imagen ausente.

Taller de archivos web: instalar una nube de laboratorio

Un gestor de archivos web permite operar sobre documentos mediante navegador, con cuentas, permisos y funciones propias. No equivale a exponer una carpeta del servidor mediante un listado HTTP. Para esta práctica utilizaremos **Nextcloud** en una VM Linux de laboratorio, dos usuarios de prueba y un administrador separado.

Antes de instalar completa una ficha: rama mantenida elegida, sistema, arquitectura, servidor web, PHP del servidor y de consola, extensiones, base de datos, memoria y espacio. La documentación consultada admite Ubuntu 24.04 y PHP 8.3, entre otras combinaciones; vuelve a comprobar la tabla de la rama que descargues. No mezcles dependencias de versiones diferentes.

Para dos cuentas y aprendizaje puedes utilizar SQLite si la rama lo admite, como instalación mínima de pruebas. Para un servicio con mayor carga se diseña otro motor y dimensionado. El mínimo de memoria por proceso de la aplicación no representa toda la RAM necesaria para servidor, base y edición de documentos.

Requisitos: tabla oficial de Nextcloud. Registra la versión real instalada; esta práctica no obliga a contratar almacenamiento o utilizar datos reales.

Preparar servidor, datos e instalación

1. Configura en SMR-SERVICIOS `nube.aulanorte.test` hacia la dirección del servidor de pruebas. Prepara el sitio web HTTPS, PHP y extensiones indicadas por el instalador. Comprueba lectura de PHP en el servidor y evita dejar una página de diagnóstico accesible después.
2. Descarga el paquete oficial de la rama elegida y verifica su procedencia/integridad. Descomprime en un directorio propio, por ejemplo `/srv/www/nextcloud`, separado del CMS y LMS.
3. Prepara datos en `/srv/nextcloud-data`, fuera del directorio publicado, con propietario y permisos del servicio según la guía. No uses permisos 777 para resolver cualquier error.
4. Configura el sitio y nombre, y certificado de laboratorio válido para nube. El script de ampliación de servicios incluye ese nombre. Distribuye solo la CA pública a clientes de prueba; conserva la clave privada en el servidor.
5. Abre el asistente desde un cliente, crea el administrador, indica directorio de datos y selecciona SQLite para este ensayo mínimo, o la base/usuario dedicados si has preparado MariaDB u otro motor admitido. Completa y registra avisos.
6. Revisa dominios de confianza, HTTPS y estado de seguridad. No aceptes cualquier nombre ni desactives validaciones para ocultar una mala configuración.

7. Configura los trabajos en segundo plano según la guía: el método cron ejecuta `cron.php` con la cuenta del servicio y PHP compatible. Comprueba una ejecución y la información de última tarea; no depende solo de que alguien abra la web.

Fuentes: instalación en Linux y tareas de fondo. Este es un recorrido de laboratorio revisado documentalmente; no se desplegó Nextcloud en la edición.

Cuentas, carpetas, metadatos y pruebas de integridad

Crea `docencia` y `alumnado` como usuarios de la aplicación, con contraseñas propias y cuotas de prueba. No los conviertas en administradores para compartir una carpeta. Crea Materiales, sube un texto ficticio y un archivo README con instrucciones de uso, clasifica mediante etiquetas disponibles y comprueba búsqueda por nombre/metadatos. Buscar un archivo por nombre no demuestra indexación de todo su contenido ni OCR.

Comparte Materiales con lectura para alumnado y la capacidad de edición prevista para docencia. Desde dos sesiones o perfiles de navegador separados, comprueba descarga y rechazo de modificación. Prueba después un recurso específico con colaboración autorizada. Revisa herencia y posibilidad de volver a compartir: no deduzcas permisos solo por ver el nombre de una carpeta.

Descarga el archivo y compara su hash o contenido con el original. En una copia modifica una frase, comprueba versión disponible y prueba recuperación si has habilitado esa función. Papelera y versiones ayudan, pero su conservación depende de configuración/recursos y no sustituyen una copia independiente.

Resultado esperado: usuarios diferenciados, operaciones permitidas/denegadas, organización documentada e integridad comprobada. Retira recursos compartidos temporales y registra cambios. No entregues capturas con contraseñas ni contenido de terceros.

Instalar edición ofimática colaborativa

Nextcloud Office necesita el conector de la aplicación y un servicio Collabora Online. Para un laboratorio pequeño se puede utilizar **Built-in CODE Server**, con sus requisitos y límites. Una nube que permite descargar un `.docx` no acredita edición colaborativa en el navegador.

Desde la administración instala/activa Nextcloud Office y el servidor CODE compatible con arquitectura. La documentación diferencia `richdocumentscode` para x86-64 y `richdocumentscode_arm64` para ARM64, y exige un Linux compatible y recursos adicionales. Comprueba versión, dependencias y espacio temporal; no instales el paquete de otra arquitectura.

En la configuración de Office elige el servidor integrado y comprueba el estado de conexión. Si la aplicación necesita resolver su propio nombre o validar certificados, configura DNS y confianza en la VM y sus servicios. No sustituyas ese trabajo por desactivar TLS. La edición integrada tiene límites de rendimiento y escalado; un despliegue mayor necesita diseño específico.

Crea un documento con dos párrafos y una hoja de cálculo sencilla. Abre el documento simultáneamente con las dos cuentas autorizadas, añade una modificación distinta desde cada una, guarda/cierra y vuelve a abrir para verificar ambas. Después prueba una cuenta con solo lectura y exporta una copia a un formato de intercambio.

Aceptación: edición simultánea, persistencia, permisos y exportación. Si solo funciona previsualizar o descargar, la prueba de edición está pendiente. Documenta incidencias y recuperación del recurso; no afirmes compatibilidad perfecta de macros, fuentes o formatos por haber abierto un archivo.

Fuentes: instalación de Nextcloud Office y servidor CODE integrado.

Instalar y utilizar un calendario web

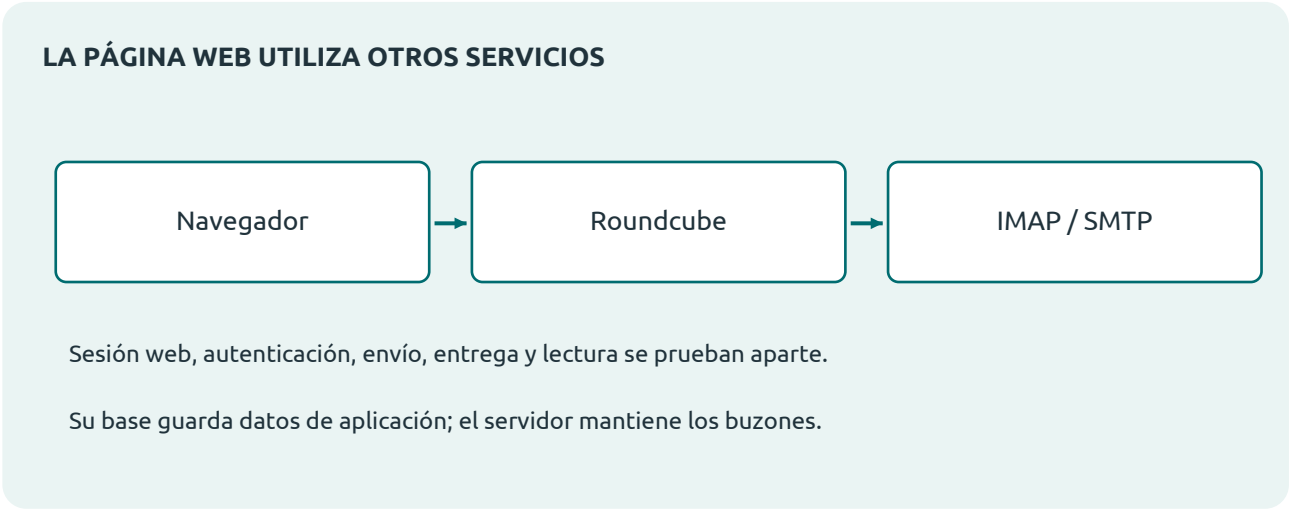
En la administración instala o habilita Calendar compatible con la versión. Crea un calendario de prueba, revisa zona horaria y añade una cita ficticia con hora, duración y recordatorio. Compártelo con otra cuenta interna primero en lectura y luego con la edición que corresponda.

Comprueba desde esa cuenta si ve, modifica o no puede cambiar la cita según el permiso. Exporta/importa un calendario de prueba mediante el formato admitido y revisa duplicados, horas y recurrencias. La suscripción a un enlace y la importación de una copia no tienen el mismo comportamiento ante cambios posteriores.

No envíes invitaciones a direcciones reales para probarlo. Si configuras avisos por correo, utiliza exclusivamente el servidor interno y cuentas ficticias del taller anterior. Una cita visible no demuestra entrega de un aviso; comprueba cada resultado por separado.

Fuente: manual oficial de Calendar.

Instalar acceso web al correo: Roundcube



Roundcube es cliente de los servicios de correo y no sustituye al buzón.

Roundcube es un cliente web: utiliza IMAP y SMTP y guarda configuración/otros datos de aplicación, pero no crea automáticamente los buzones del servidor. Prepara primero el servicio del capítulo 35 y verifica sus cuentas, TLS, envío y lectura desde un cliente.

En otra instalación web de laboratorio, descarga una release oficial completa de Roundcube compatible con PHP y su base. Prepara base y usuario dedicados o el backend de pruebas admitido, y aplica el esquema que corresponda a esa release. La distribución completa incluye dependencias que un archivo de código fuente puede no traer.

Configura HTTPS y la raíz pública que indique la versión. La documentación de las ramas nuevas consultada utiliza `public_html` y `installer.php`; no publiques por costumbre todo el árbol con configuración y datos. Ejecuta el instalador restringido al laboratorio, comprueba requisitos, conexión a base y directorios de temporales/registros. Genera las claves de aplicación que solicite, guarda la configuración protegida y deshabilita/retira el instalador según la guía.

Configura IMAP con TLS en 993 y SMTP con STARTTLS en 587 hacia `correo.aulanorte.test`. El fragmento `roundcube-conexiones.php` de recursos muestra esas conexiones y reutiliza la identidad de la sesión para SMTP; no contiene la configuración completa, base ni claves. PHP debe confiar en la CA del laboratorio y verificar el nombre; no se acepta desactivar la validación.

Accede con `correoana`, usuario local del servidor del taller, configura su identidad de correo ficticia y envía a `correoluis@aulanorte.test`. Comprueba lectura y respuesta, carpeta de enviados, adjunto y cierre de sesión. Una contraseña incorrecta debe fallar. La cuenta de Nextcloud es otra identidad: no se integra automáticamente por tener el mismo nombre.

En un servicio real se diseña también control de remitentes, sesiones, actualizaciones y protección del acceso. La primera conexión satisfactoria no acredita todos esos controles. Si faltan mensajes, separa cliente web, SMTP, entrega, IMAP y permisos antes de borrar o reinstalar.

Fuentes: instalación de Roundcube y conexiones y cuentas. Recorrido contrastado, no ejecutado en el entorno editorial.

Copia y restauración de las aplicaciones de colaboración

Define qué vas a recuperar: archivos, versiones, cuentas, permisos, documentos y calendarios. Una descarga de la carpeta Materiales no contiene necesariamente base, configuración y datos de las aplicaciones.

En Nextcloud conserva configuración, datos, base y personalizaciones pertinentes, junto con código/versión y extensiones necesarias para reconstruir. Coordina mantenimiento y tareas para una copia coherente; con SQLite también debes conservar su base y evitar copiarla a mitad de una escritura. Restaura en otra VM aislada, con nombre/confianza de prueba controlados, y repite permisos, descarga, calendario y documento colaborativo.

En Roundcube conserva base, configuración y personalizaciones, y recuerda que los mensajes pertenecen al servicio IMAP y su plan de copia. Restaurar únicamente Roundcube no reconstruye los buzones perdidos del servidor.

Fuente de alcance: copias de Nextcloud. Entrega un expediente con versiones y pruebas realizadas; distingue las que aún no has podido ejecutar. La edición no presenta una restauración de estas plataformas como realizada.

¿Lo has pillado?

1. ¿Registrar un dominio instala el CMS?

2. ¿Revertir al servidor antiguo recupera automáticamente las escrituras hechas en el nuevo?

3. ¿La prueba de portada valida toda una migración?

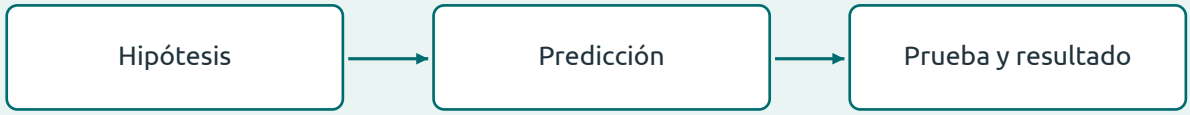
Soluciones. 1) No: son componentes distintos. 2) No: hay que planificar su conciliación o recuperación. 3) No: faltan datos, medios, roles, tareas y otras operaciones relevantes.

Bloque 10. Resolver problemas y trabajar con otras personas

53. Diagnosticar sin ir dando palos de ciego

Al terminar: construirás hipótesis comprobables, elegirás pruebas útiles y verificarás una reparación. **Antes:** los capítulos de hardware, sistemas, redes y servicios.

DE UNA IDEA A UNA PRUEBA



¿Qué resultado me haría descartar esta explicación?

Registrar también las pruebas que no confirman la primera idea.

Una prueba útil puede contradecir la explicación propuesta.

Un diagnóstico es una explicación que encaja con las evidencias y permite decidir qué hacer. Adivinar una pieza y cambiarla puede acertar una vez; un método permite aprender del resultado incluso cuando la primera hipótesis falla.

Del aviso a una descripción útil

«El ordenador va mal» es un punto de partida. Pregunta qué tarea intentaba realizar la persona, qué ocurrió, qué esperaba y desde cuándo sucede. Pide el mensaje exacto, el equipo, la aplicación y la hora aproximada. Distingue el comportamiento observado de la interpretación: «no carga la página de inventario» es un hecho; «se ha roto Internet» es una hipótesis.

Determina el **alcance**. ¿Una persona, un equipo, un aula o todos los usuarios? ¿Una aplicación o varias? ¿Afecta a cable y wifi? ¿Se reproduce con un documento vacío? Esta información permite elegir la primera rama del diagnóstico, pero no demuestra por sí sola una causa.

Pregunta también por cambios recientes. Una actualización próxima al fallo merece investigarse; la cercanía temporal no basta para culparla. Puede coincidir con una contraseña caducada, falta de espacio o una avería independiente.

Construye una línea de base

La **línea de base** describe cómo se comporta un sistema cuando funciona de manera aceptable. Incluye versiones, configuración, tiempos y pruebas concretas. «Antes iba rápido» aporta menos que «ayer el mismo informe de prueba tardó ocho segundos en el mismo equipo».

Compara casos parecidos: misma tarea, datos equivalentes, permisos adecuados y condiciones conocidas. Si cambias a la vez usuario, equipo y red y todo funciona, has encontrado un caso sano, pero aún no has aislado qué diferencia explica el fallo.

Una hipótesis debe arriesgarse a ser falsa

Formula una explicación con una predicción: «si el problema es exclusivamente la resolución del nombre interno, el servidor responderá por la dirección y protocolo conocidos, pero la consulta DNS del nombre fallará desde este cliente». El resultado permitirá mantener, matizar o descartar la hipótesis.

En HTTPS, sustituir un nombre por una IP puede cambiar certificado, servidor virtual y comportamiento. Por eso una prueba de dirección no es automáticamente equivalente a la petición original. El capítulo 33 explica cómo separar esas capas. No conviertas un error de certificado causado por tu prueba en una segunda avería imaginaria.

Elige pruebas según información obtenida, impacto y coste. Leer un registro o comprobar alcance suele ser preferible a reinstalar. Una prueba también puede modificar el estado: reiniciar borra algunos indicios y desconecta usuarios. Guarda primero la evidencia necesaria y planifica la intervención.

Cambia una variable y registra

Para cada paso escribe: hora, prueba, resultado esperado, resultado real y conclusión. «He probado cosas» no permite reconstruir nada. «10:14: consulta al DNS configurado devuelve NXDOMAIN para el nombre del laboratorio; otro cliente consulta un DNS diferente y obtiene la dirección correcta» sí orienta la investigación.



Ojo con este error

Que dos síntomas desaparezcan tras reiniciar no demuestra una causa común. El reinicio puede eliminar estados temporales distintos. Si solo puedes aplicar esa recuperación, documenta que la causa sigue pendiente y qué señales recogerás si se repite.

Si haces varios cambios inevitables en una ventana autorizada, registra cada uno y sus dependencias. El método no exige fingir que todas las intervenciones pueden aislarse perfectamente; exige conservar suficiente información para interpretar el resultado.

Caso resuelto: solo falla el portal interno

Aula Norte comunica: AN03 no abre `inventario.aulanorte.test`. Desde ese equipo sí se abre una página de prueba externa. Los otros equipos abren el portal interno. El nombre y la dirección de laboratorio ya están documentados en su inventario ficticio.

1. Se registra hora, mensaje del navegador y tarea. No se incluyen contraseñas ni capturas con datos de otras personas.

2. Se consulta la configuración de red del cliente. Tiene dirección de su red y un servidor DNS público configurado manualmente.
3. Se pregunta el nombre interno a ese DNS. La respuesta no lo resuelve. Se compara con el DNS interno documentado, que sí responde.
4. Se comprueba por qué AN03 usa un DNS distinto. El ejercicio asume un cambio manual anterior; en una instalación real habría que confirmar política, DHCP y administración.
5. Se recupera la configuración prevista mediante el procedimiento autorizado. No se añade al azar una entrada permanente en `hosts` para ocultar la causa.
6. Se repite la consulta y la tarea del navegador usando el nombre original. Se comprueba además navegación externa y persistencia de la configuración según su diseño.

Conclusión razonada: la configuración DNS observada explica la diferencia entre el nombre interno y las páginas externas. La comprobación final debe demostrar la tarea, no solo que un comando devuelve una dirección.

Causa, desencadenante y consecuencias

La **causa** explica el fallo; el **desencadenante** es el hecho que lo hace aparecer; las **consecuencias** son sus efectos. Un volumen lleno puede impedir que una aplicación escriba. La tarea nocturna que lo llenó es parte de la explicación; la falta de vigilancia o retención puede explicar por qué se repite.

«Liberar 2 GB» recupera servicio. Corregir la política de registros y verificar que no se pierde información necesaria aborda la repetición. No siempre podrás resolverlo todo en una intervención; separa recuperación inmediata y trabajo pendiente con responsable.

Práctica: expediente de diagnóstico

Trabaja con el caso ficticio anterior o con una copia de laboratorio. Usa la plantilla de `recursos/soporte/expediente-diagnostico.md`. Completa síntoma, alcance, tres hipótesis y una prueba para cada una. Debe existir al menos un resultado que te obligaría a descartar cada explicación.

Después recibe esta evidencia adicional: «AN03 resuelve ahora el nombre correcto, pero el portal devuelve acceso denegado únicamente para una cuenta». Actualiza el expediente. No mantengas una explicación DNS para un problema de autorización que las pruebas ya han separado.

Resultado esperado: distingues las dos incidencias o dos fases del caso y propones revisar identidad, rol y recurso en la segunda. Recuperación: conserva el expediente como ejercicio; no modifiques cuentas o DNS de un centro real.

¿Lo has pillado?

1. ¿Una coincidencia entre actualización y fallo prueba causalidad?

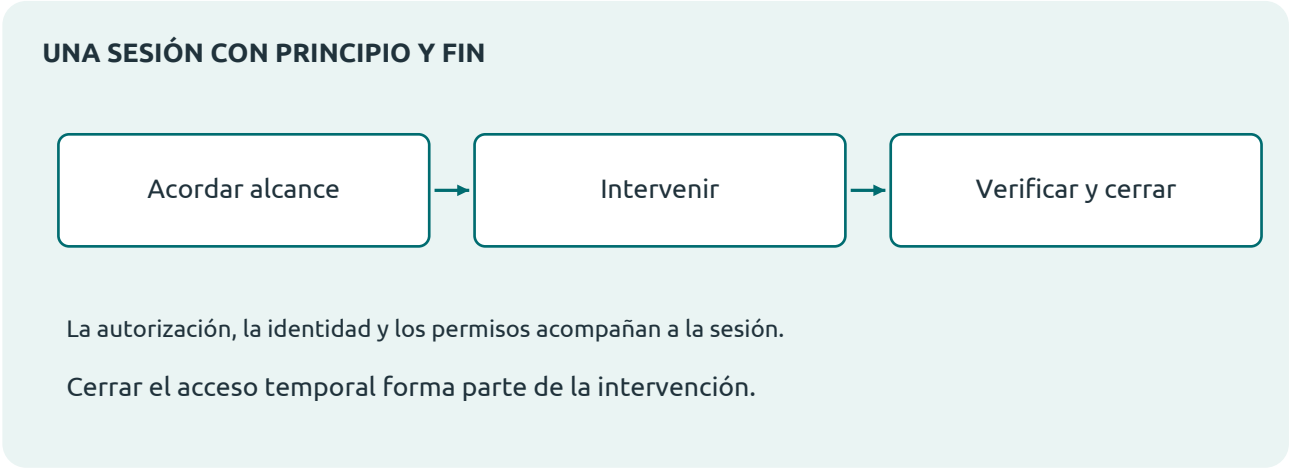
2. ¿Una reparación termina cuando el proceso aparece activo?

3. ¿Qué anotas si un reinicio recupera el servicio sin explicar la causa?

Soluciones. 1) No; genera una hipótesis que hay que contrastar. 2) No; se verifica la operación original y efectos relevantes. 3) El estado anterior, la acción, el resultado y que la causa permanece sin determinar, con seguimiento si procede.

54. Atender a una persona también es trabajo técnico

Al terminar: recogerás información con claridad, explicarás una intervención y organizarás una sesión de soporte remoto. **Antes:** permisos, privacidad y método de diagnóstico.



La persona y el soporte acuerdan el alcance de la intervención.

La persona que pide ayuda no tiene por qué conocer nuestros términos. Su trabajo consiste en realizar una tarea; el nuestro es comprender el bloqueo y ayudarle sin convertir la conversación en un examen de informática.

Preguntas que ayudan

Empieza por una pregunta abierta: «¿Qué estabas intentando hacer?». Después concreta: «¿Aparece el mensaje al abrir el archivo o al guardarlo?». Evita cinco preguntas seguidas: es fácil obtener respuesta solo a la última.

Reformula antes de actuar: «El archivo abre, pero no puedes guardar cambios en la carpeta compartida; en tu escritorio sí. Vamos a comprobar permisos y conexión a esa carpeta». La persona puede corregir una interpretación errónea antes de que pierdas tiempo.

No prometas una causa que no has comprobado ni una hora de reparación sin base. Sí puedes comprometer una siguiente actualización: «Voy a comprobar el alcance y te informo en quince minutos». Si no has resuelto entonces, comunica lo que sabes y el siguiente paso.

Explica impacto y alternativas

«Tengo que reiniciar» necesita contexto: qué equipo, qué trabajos se interrumpen, si se han guardado los documentos y qué alternativa temporal existe. Ajusta la intervención a la actividad y al procedimiento del centro o empresa.

Un **workaround** o solución temporal permite continuar mientras se corrige la causa. Debe ser comprensible, limitada y aceptada. No conviertas en alternativa habitual compartir cuentas, desactivar protecciones o enviar documentos a una cuenta personal.

Una explicación final útil tiene tres partes: qué se observó, qué cambió y qué debe hacer la persona si vuelve a pasar. Evita mensajes culpabilizadores como «lo has tocado otra vez». Describe estados y medidas verificables.

Escalar sin abandonar

Escalar significa transferir el caso o solicitar una capacidad que falta: permisos, conocimiento especializado, proveedor o decisión de negocio. No es un fracaso. Un escalado útil incluye impacto, alcance, cronología, evidencias depuradas, hipótesis, pruebas y cambios realizados.

Identifica quién sigue siendo responsable de comunicar con la persona usuaria. Si tres equipos técnicos se pasan un aviso sin responsable visible, la comunicación se rompe aunque todos estén trabajando.

Distingue **urgencia** de **impacto**. Una sola persona bloqueada puede tener una tarea crítica con vencimiento inmediato. Cincuenta equipos de un aula vacía pueden tener un impacto potencial importante pero una urgencia distinta. Usa la política acordada, no solo la cantidad de mensajes recibidos.

Una sesión remota de principio a fin

Utiliza una herramienta aprobada y comprueba quién solicita la ayuda y qué equipo se va a controlar. La autorización debe ajustarse a la política y al alcance: permitir ver una pantalla no implica autorizar cualquier cambio administrativo.

1. Antes: explica objetivo, duración aproximada, necesidad de guardar trabajo y posibilidad de detener la sesión. Pide cerrar o proteger contenido ajeno a la tarea.
2. Conexión: confirma equipo y persona por el procedimiento previsto. Usa las opciones de consentimiento e identificación de la herramienta.
3. Intervención: explica acciones relevantes. La persona introduce sus credenciales en el mecanismo adecuado; no te dicta la contraseña ni la pega en el chat del ticket.
4. Elevación: si hace falta más permiso, usa una cuenta o flujo autorizado. No habilites acceso permanente para simplificar una sesión puntual.
5. Verificación: pide realizar la tarea original y comprueba los efectos necesarios. No basta con mover el ratón y ver el escritorio.
6. Cierre: termina el control, comprueba el cierre de la conexión y registra la intervención. Retira accesos temporales conforme al procedimiento.

No grabes por defecto ni copies todo el escritorio como evidencia. Si una grabación está justificada y permitida, debe tener finalidad, información, acceso y conservación definidos. Los avisos legales dependen del contexto; el capítulo 42 explica por qué un consentimiento improvisado no resuelve todas las obligaciones.

Cuando alguien está frustrado

Reconoce el bloqueo de forma concreta: «Entiendo que no poder entregar el informe te impide cerrar el trabajo». Después explica lo que puedes hacer. Mantén límites respetuosos ante insultos o exigencias fuera de autorización; pide apoyo según el protocolo.

Evita atribuir una acción a una persona solo por el nombre de una cuenta en un registro. Las cuentas compartidas, sesiones abiertas o errores de reloj complican esa interpretación. Tu ticket debe registrar hechos y límites de la evidencia.

Práctica: dos personas y un guion

Una persona representa a quien necesita guardar un informe; otra, al soporte. No se conecta ningún equipo real. El usuario conoce este dato que solo revela si se pregunta: puede guardar en una carpeta distinta y el problema empezó al cambiar de departamento.

Recoge información, confirma el resumen, propone una prueba y explica cuándo escalarías a quien administra permisos. Redacta una respuesta inicial, una actualización sin resolución y una comunicación de cierre. Intercambiad papeles.

Resultado esperado: no prometes recuperar permisos que no te corresponde otorgar; compruebas la necesidad de acceso con su responsable y propones una alternativa autorizada si existe. Las tres comunicaciones contienen una acción o siguiente paso claros.

¿Lo has pillado?

1. ¿Puedes pedir una contraseña para acelerar la sesión?

2. ¿Escalar significa cerrar el aviso como resuelto?

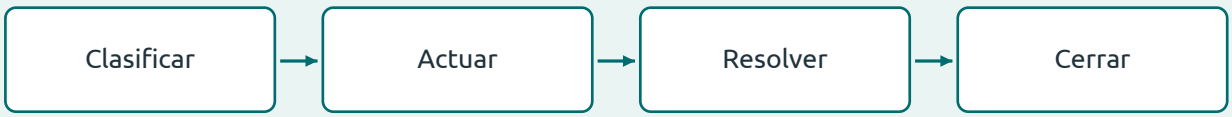
3. ¿Qué debe comprobar la persona al finalizar?

Soluciones. 1) No; usa el mecanismo autorizado de identificación o elevación. 2) No; se mantiene seguimiento y estado correcto. 3) La tarea por la que pidió ayuda, además de los efectos relevantes de la intervención y el fin del acceso remoto.

55. Tickets, inventarios y documentación que sirven mañana

Al terminar: registrarás trabajo trazable y crearás un procedimiento que otra persona pueda seguir. **Antes:** ofimática, diagnóstico y soporte.

DEL AVISO AL CIERRE VERIFICADO



En cada transición: responsable, evidencia y siguiente paso.

Pendiente requiere un motivo y una fecha de revisión.

Un estado necesita información suficiente para decidir el siguiente paso.

La documentación tiene un usuario: quien debe actuar después. Puede ser tu compañero, la persona afectada o tú mismo dentro de tres meses. Debe permitir decidir y reproducir sin depender de recuerdos.

Un ticket no es una novela ni una palabra

Un ticket identifica una petición o incidencia y permite seguirla. Campos básicos: identificador, apertura, activo o servicio afectado, descripción, impacto, prioridad justificada, responsable, estado, actuaciones y criterio de cierre. Añade fechas y zona horaria cuando el entorno lo requiera.

Un posible ciclo es **nuevo, clasificado, en curso, pendiente, resuelto y cerrado**. Es un ejemplo de organización, no un estándar obligatorio. «Pendiente» necesita motivo, responsable externo si existe y siguiente revisión. «Resuelto» puede esperar confirmación; «cerrado» responde al criterio acordado de aceptación.



Truco de taller

Evita un ticket gigante que mezcle una avería, una compra y tres permisos. Vincula los casos relacionados. Distingue incidencia (interrupción o degradación), solicitud (petición de servicio), problema (investigación de causas) y cambio (modificación controlada). Una organización puede usar otras categorías, pero debe explicarlas.

Prioridad con criterio explícito

Para el ejercicio de Aula Norte acordamos una matriz sencilla: impacto alto si bloquea la actividad esencial de un grupo, medio si afecta a una parte con alternativa y bajo si el efecto es limitado; urgencia alta si necesita recuperación inmediata para esa actividad, media si admite una ventana próxima y baja si puede planificarse.

Combinaremos alto/alto como P1, alto/medio o medio/alto como P2, bajo/bajo como P4 y el resto como P3. Es una **regla ficticia del ejercicio**, no un compromiso de respuesta profesional. No inventes un SLA de diez minutos porque un libro lo muestre. Un SLA es un acuerdo de nivel de servicio con alcance, condiciones y medición.

Si cambia la situación, revisa la prioridad y registra el motivo. Una alternativa temporal puede reducir la urgencia sin borrar la causa pendiente. Una pérdida de datos o indicio de seguridad puede activar un protocolo específico que prevalezca sobre la cola ordinaria.

Inventario: identidad, estado y relaciones

El inventario explica qué tienes y dónde se usa. Conviene separar identificador interno estable, número de serie, modelo, ubicación, responsable funcional, sistema/versión, estado, garantía y relaciones necesarias. No uses la dirección IP como identificador permanente: puede cambiar o compartirse según la arquitectura.

Registra también software y licencias cuando forme parte del alcance, con acceso restringido a la evidencia apropiada. No guardes contraseñas en la ficha del equipo. Evita que el inventario se convierta en un archivo de datos personales sin finalidad.

El inventario de la práctica ofimática es una introducción. Para un servicio real necesitas controlar altas, bajas, cambios y revisiones. Un equipo retirado debe seguir el proceso de borrado, reutilización o gestión de residuos que corresponda, con evidencia y responsables.

Diagramas que no obligan a adivinar

Un diagrama físico indica equipos, conexiones, puertos o ubicación. Uno lógico representa subredes, servicios, VLAN, rutas o dependencias. Puedes combinar ambos si la leyenda lo deja claro, pero no dibujes una línea sin explicar si es cable, comunicación o relación.

Incluye título, alcance, fecha, versión y leyenda. Usa símbolos y texto legibles al imprimir. La existencia de una línea entre dos equipos no demuestra que un flujo esté permitido por cortafuegos y aplicación.

Ejemplo: un portal depende de DNS, web, aplicación y base de datos. Su diagrama lógico puede mostrar esas relaciones aunque varios papeles estén en la misma VM. El esquema físico indicará en qué host se aloja y qué conexión utiliza. Ambos responden preguntas diferentes.

Un procedimiento ejecutable por otra persona

Un buen procedimiento indica objetivo, requisitos, permisos, alcance, preparación, pasos, criterios de éxito, recuperación y evidencias. Incluye versión y revisión. «Instala todo y comprueba» no basta: especifica qué observarás y cómo reconocerás un fallo.

No incluyas una contraseña de ejemplo que termine copiada en producción. Usa marcadores claramente explicados o un mecanismo de secretos. Para un paso destructivo, la identificación inequívoca del recurso y el respaldo previo deben formar parte del procedimiento, no quedar escondidos en una nota posterior.

La **reversión** devuelve el cambio a un estado anterior viable; la **restauración** recupera datos o sistema desde una copia. Pueden intervenir juntas. Si el sistema nuevo ha recibido datos, volver al antiguo puede perderlos: el capítulo 52 explica por qué una migración necesita controlar escrituras.

Caso: ticket mal cerrado

Ticket inicial: «AN03 no guarda. Arreglado». Faltan tarea, destino, causa, intervención y prueba. Una versión útil diría: «AN03 abre el informe, pero la cuenta de prueba no puede guardar en la carpeta del departamento nuevo. Se verifica acceso solicitado con su responsable; administración incorpora la cuenta al grupo aprobado. Tras renovar la sesión según el sistema, la cuenta guarda y vuelve a abrir un documento ficticio en la carpeta. Se comprueba que sigue sin acceder al recurso de otro departamento».

Esta descripción separa solicitud de permiso, aplicación por el responsable y pruebas positiva y negativa. No publica usuarios reales ni el contenido del informe. Si la causa era distinta, el ticket debe reflejar esa evidencia en lugar de copiar esta solución.

Práctica: un compañero debe poder continuar

Usa `recursos/soporte/ticket.md` y `procedimiento.md`. Crea un ticket para el caso DNS del capítulo 53, enlázalo al activo ficticio AN03 y redacta un procedimiento para comprobar la resolución del nombre del laboratorio. Incluye requisitos y una rama para «respuesta correcta, pero la tarea sigue fallando».

Entrega los documentos a otra persona sin explicaciones orales. Pídele que marque cada punto que admite dos interpretaciones. Corrige y añade versión. Si no hay compañero, repasa al día siguiente haciendo solo lo que está escrito.

Resultado esperado: el procedimiento distingue consulta DNS de acceso a la aplicación; el ticket registra evidencia, estado y criterio de cierre. No se aplican cambios reales. Conserva ambas versiones para explicar qué mejoró.

¿Lo has pillado?

1. ¿Qué falta en un estado «pendiente» sin comentario?

2. ¿La IP es una buena identidad permanente del activo?

3. ¿Cómo compruebas que un cambio de permisos no ha dado demasiado acceso?

Soluciones. 1) Motivo, responsable y siguiente revisión, entre otros datos del proceso. 2) No: puede cambiar; usa un identificador estable y relaciona direcciones cuando proceda. 3) Con la operación autorizada y una prueba negativa relevante desde identidades de laboratorio, además de revisar la configuración.

Bloque 11. Inglés, empleabilidad y un trabajo sostenible

56. Inglés profesional para desenvolverte en informática

Al terminar: comprenderás instrucciones sencillas, describirás un fallo, pedirás aclaraciones y escribirás una comunicación técnica breve. **Antes:** vocabulario básico de equipos, redes y soporte.



Comprender también incluye pedir una aclaración antes de actuar.

No necesitas sonar como una película. Necesitas entender qué debes hacer, confirmar lo que no está claro y explicar un resultado. Es mejor una frase corta correcta que un párrafo que no sabes defender en una conversación.

Unidad A. Vocabulario con una tarea detrás

Aprende cada palabra dentro de una situación. **Device** es dispositivo; **equipment** suele ser un nombre no contable: decimos *some equipment*, no *three equipments*. Para contar, utiliza *three devices* o *three pieces of equipment*.

- **Power supply:** fuente de alimentación. *Check the power supply* pide comprobarla; no autoriza abrirla.
- **Motherboard, memory, storage:** placa base, memoria y almacenamiento. *Memory* y *storage* no son intercambiables.
- **Drive, folder, file, path:** unidad, carpeta, archivo y ruta. *Save the file in this folder* indica un destino.
- **Wired, wireless, network, gateway:** por cable, inalámbrico, red y puerta de enlace.
- **Username, password, account, permission:** nombre de usuario, contraseña, cuenta y permiso.

- **Backup, restore, update, upgrade:** copia, restaurar, actualizar y pasar a una versión o nivel superior según el contexto.
- **Issue, error message, log, workaround:** incidencia o problema, mensaje de error, registro y solución temporal.
- **Available, required, optional, supported:** disponible, obligatorio, opcional y con soporte o compatible según la frase.



Ojo con este error

actually suele significar «en realidad»; *currently*, «actualmente». *Library* es biblioteca o librería de software; no es una tienda de libros. *Eventually* suele indicar «finalmente» o «con el tiempo». Lee el contexto antes de elegir traducción.

Crea tarjetas con término, ejemplo y una pregunta. Para *restore*: *Can you restore the test file?* y «¿se pide crear una copia o recuperarla?». La respuesta es recuperarla. Pronunciar y usar el ejemplo ayuda más que copiar veinte veces la traducción.

Unidad B. La gramática que necesitas para una intervención

El **imperativo** sirve para instrucciones: *Open the settings. Select the test account. Do not delete the original file.* La forma negativa con *do not* es importante: omitir *not* cambia la acción.

El **presente** describe estados o hábitos: *The server is online. The printer does not respond.* Para una situación en curso: *The application is installing an update.* El **pasado** explica lo que ocurrió: *The service stopped at nine. I restarted the test application.*

Usa preguntas que puedas comprobar: *Does the problem affect other users? When did it start? Can you open another file?* Con *did*, el verbo principal vuelve a su forma base: *Did you restart it?*, no *Did you restarted it?*

Can expresa capacidad o posibilidad y puede usarse para pedir algo. **Could you…?** suele formular una petición más cortés. **Must** o **must not** expresan obligación o prohibición según el texto; **should** suele recomendar. No rebajes *must not disconnect* a «sería mejor no desconectar».

There is introduce un elemento singular; **there are**, varios: *There is an error message. There are two network adapters.* Para describir una prueba, conecta condición y resultado: *If the name cannot be resolved, check the configured DNS server.* Debes saber qué entorno autoriza esa comprobación.

Prueba estas equivalencias: «el equipo tiene dos unidades» es *The computer has two drives.* «No puedo guardar» es *I cannot save the file.* «Pude abrirlo ayer» es *I could open it yesterday.* La última frase informa de una diferencia temporal; aún no explica la causa.

Unidad C. Leer documentación sin traducir cada palabra

Primero identifica objetivo, requisitos, advertencias, pasos y resultado. Busca negaciones, condiciones y nombres de parámetros. Un número de versión, una ruta o una opción debe leerse con precisión aunque entiendas la idea general.

Texto original de práctica, referido solo al laboratorio ficticio:

Before you start, make a copy of the practice folder. Keep the original files unchanged. Open the copied folder and select the test document. This exercise does not require administrator privileges.

Save the document as report-test.txt. Add one sentence and save it again. Close the editor, reopen the file and check that the new sentence is present. A success message alone is not enough: you must check the saved content.

If you cannot save the file, record the exact error message and the destination path. Try a new, empty document in your own practice folder. Do not change permissions on a shared folder. Ask the person responsible for the lab if the problem continues.

When you finish, write down what you tested and what happened. You may remove your own practice copy after checking its location. Do not delete the original folder.

Contesta sin mirar soluciones: ¿se necesitan privilegios de administrador?, ¿qué nombre tendrá el archivo?, ¿qué prueba demuestra que se guardó?, ¿qué permisos no debes cambiar?, ¿qué puedes retirar al terminar?

Solución razonada: no se necesitan privilegios; el archivo es `report-test.txt`; hay que cerrar, volver a abrir y ver la frase; no se cambian permisos de la carpeta compartida; solo se retira la copia propia tras comprobar la ubicación. La instrucción de no borrar la carpeta original sigue vigente.

Unidad D. Hablar, deletrear y confirmar

Si no entiendes, utiliza una petición concreta: *Could you repeat that, please? Could you speak more slowly? Could you spell the file name? Do you mean the local folder or the shared folder?* Estas preguntas previenen errores y son parte de trabajar bien.

Para nombres, diferencia **dot** (punto), **slash** (barra /), **backslash** (barra inversa), **hyphen** (guion) y **underscore** (guion bajo). Una URL ficticia puede usar el dominio reservado del laboratorio; no practiques dictando direcciones internas reales a un servicio público.

Cuando escuches una cantidad, repítela: *Did you say thirteen or thirty?* Para AN03, puedes decir *A, N, zero, three* y pedir confirmación. Usa el alfabeto de deletreo que acuerde el entorno, especialmente si una letra resulta ambigua.

Ensaya este diálogo por parejas. No hace falta conectar un equipo:

- **User:** *I can open the report, but I cannot save it.*

- **Support:** *Does this happen in every folder?*

- **User:** *No. I can save a file in my practice folder.*

- **Support:** *What is the exact error message?*

- **User:** *It says "Access denied".*

- **Support:** *Thank you. I will check the request with the person responsible for access. Please do not share your password.*

La última frase no promete conceder acceso: comunica un siguiente paso. Después intercambiad los papeles y cambiad el síntoma manteniendo la claridad.

Unidad E. Comprensión oral con una lectura de otra persona

Usa `recursos/ingles/guion-escucha.md`. Pide a un compañero o docente que lea el texto dos veces sin mostrarlo. La primera escucha sirve para la idea general; la segunda, para detalles. Si estudias solo, puedes usar una función de lectura en voz alta disponible en tu equipo. El recurso entregado es texto, no una grabación.

Antes de escuchar, prepara estas preguntas: ¿qué equipo falla?, ¿desde cuándo?, ¿qué tarea sí funciona?, ¿qué muestra el error?, ¿a qué hora se pide la siguiente actualización?

No interrumpas cada palabra desconocida. Anota lo que crees haber entendido y después pide una aclaración específica. El objetivo no es adivinar: es identificar qué información falta para actuar sin equivocarse.

Solución: equipo AN03; desde las nueve; puede guardar en su carpeta de práctica; aparece *Access denied* en la carpeta compartida; se solicita una actualización a las diez y media. Si has confundido *nine* y *nineteen* o *ten thirty* y *ten thirteen*, solicita repetir o confirmar la hora.

Unidad F. Escribir un correo y un ticket

Una comunicación breve puede seguir este orden: asunto concreto, tarea y alcance, hechos observados, pruebas realizadas y siguiente paso. Separa hechos de suposiciones. No adjuntes contraseñas, datos personales ni un registro completo si basta un fragmento depurado.

Ejemplo original:

Subject: AN03 - Unable to save to the shared folder

Hello,

AN03 can open the test report, but the test account cannot save changes to the shared folder. Saving a new document in the local practice folder works. The error message is "Access denied".

No permissions have been changed. Could you confirm whether this test account should have write access? I will update the ticket after the access review.

Thank you.

Fíjate en *could you confirm*: se pide una decisión, no se ordena abrir permisos indiscriminadamente. *No permissions have been changed* comunica que todavía no se ha aplicado ese cambio; no significa que los permisos sean necesariamente correctos.

Práctica: redacta entre 70 y 100 palabras sobre un fallo ficticio de impresión. Incluye equipo, alcance, dos comprobaciones y una petición. Después reduce el texto a un ticket de cinco frases sin perder información necesaria.

Unidad G. Presentarte y preparar una entrevista

Prepara una presentación de treinta segundos: quién eres, qué estudias, un proyecto pequeño y qué aprendiste. Ejemplo: *I am studying computer systems and networks. In my practice lab, I configured a small network and documented the tests. I am learning to diagnose problems step by step.*

Si solo realizaste un laboratorio, dilo. Evita *I managed a company network* para una práctica de dos VM. Cuando te pregunten algo que no sabes, puedes responder: *I have not used that tool yet. I would check the documentation and test it in a lab first.* Después explica un ejemplo real de tu forma de aprender.

Práctica final y autoevaluación

Trabaja con la carpeta ficticia del texto de lectura. Lee las instrucciones, ejecuta solo las acciones autorizadas sobre tu copia, explica en voz alta una comprobación y redacta el resultado en inglés. Usa las plantillas de soporte para separar prueba, resultado y pendiente.

Valora cuatro dimensiones de 0 a 2: comprensión de instrucciones; precisión de datos; interacción y aclaraciones; claridad del mensaje escrito. Cero indica que falta o impide la tarea; uno, que se entiende con ayuda; dos, que permite actuar con claridad. Una negación mal entendida obliga a repetir esa parte aunque la suma sea alta.

Convenciones de comunicación sin estereotipos

Adapta saludo, tratamiento y grado de detalle a la persona, organización y canal. No deduzcas preferencias de cortesía por nacionalidad. Puedes pedir cómo prefiere que te dirijas a ella y confirmar el significado de una expresión.

Fechas como 03/04 pueden resultar ambiguas; escribe el mes o confirma el formato. En una reunión internacional añade zona horaria y revisa la convocatoria. Una petición como *Could you confirm the date and time zone?* evita una suposición.

En soporte oral no interrumpas continuamente y confirma datos clave. En mensajes, utiliza asunto claro y una petición concreta. Si hay un malentendido, reformula: *Let me check that I understood correctly*. La corrección profesional también incluye reconocer lo que todavía no has entendido.

¿Lo has pillado?

1. Traduce *Do not disconnect the device during the update*.

2. Corrige *Did you restarted the computer?*

3. ¿Cómo pides que te deletreen el nombre?

4. ¿Qué diferencia hay entre *backup* y *restore*?

Soluciones. 1) No desconectes el dispositivo durante la actualización. 2) *Did you restart the computer?* 3) *Could you spell the name, please?* 4) La copia conserva datos para recuperarlos; restaurar es realizar la recuperación. Debes interpretar también si una palabra actúa como nombre o verbo en su frase.

57. Empleabilidad: aprender un oficio y construir tu camino

Al terminar: reconocerás riesgos, interpretarás documentación laboral básica, prepararás una candidatura y justificarás un pequeño proyecto de servicio. **Antes:** soporte, documentación y hábitos de laboratorio.



La candidatura y el proyecto se apoyan en competencias demostrables.

Este capítulo contiene dos unidades: **IPE I**, sobre incorporación segura al trabajo, relaciones laborales y desarrollo personal; e **IPE II**, sobre búsqueda de empleo, trabajo en equipo, innovación y emprendimiento. Están relacionadas, pero cada una tiene sus prácticas y evidencias.

IPE I. Conoce el sector sin inventar experiencia

SMR puede llevarte a funciones de soporte, instalación, mantenimiento, operaciones o atención técnica, con distinto grado de autonomía. El nombre de un puesto no define por completo sus tareas. Lee responsabilidades, entorno, horarios, desplazamientos, herramientas y a quién se escala.

Construye un mapa con tres puestos que te interesen. Para cada uno, separa requisitos imprescindibles, conocimientos valorados y habilidades que puedes demostrar. Una práctica bien documentada de red local es evidencia de aprendizaje; no equivale a haber administrado una red empresarial.

Haz un balance personal: qué sabes explicar, qué sabes ejecutar con ayuda y qué sabes repetir sin guía. Añade una evidencia a cada afirmación. «Soy bueno con redes» resulta menos útil que un esquema propio, una configuración de laboratorio y pruebas que puedas defender.

IPE I. Peligro, riesgo y medidas preventivas

Un **peligro** es una fuente o situación capaz de causar daño; el **riesgo** considera la posibilidad y gravedad de ese daño en unas condiciones. Un cable en una zona de paso puede producir una caída; importa dónde está, quién pasa y cómo se organiza el espacio.

La prevención debe integrarse en la organización. La Ley de Prevención de Riesgos Laborales establece protección, información y formación, evaluación y medidas preventivas. No basta con entregar guantes o un cartel. Ante riesgo grave e inminente existen medidas y derechos específicos; informa y sigue el procedimiento de emergencia del entorno.

Fuente normativa, España, consultada el 5 de noviembre de 2026: Ley 31/1995, en particular artículos 14 a 21. https://www.boe.es/buscar/act.php?id=BOE-A-1995-24292

En un puesto informático revisa al menos: alimentación y cables; orden y circulación; cargas y posturas; pantallas e iluminación; ruido o temperatura si afectan; organización de tareas y factores psicosociales. La valoración profesional determina medidas y prioridades: esta lista de aprendizaje no sustituye la evaluación del puesto.

IPE I. Electricidad, equipos y manipulación

No intervengas en instalaciones eléctricas ni abras una fuente o un SAI por haber estudiado informática. Identifica el alcance de tu formación, autorización y procedimiento. Un equipo apagado puede mantener energía o tener alimentación desde más de una fuente. Una pulsera antiestática protege componentes frente a descargas; no es protección personal contra un choque eléctrico.

En el laboratorio, la preparación y desconexión siguen el manual y las instrucciones del docente. Si ves cable dañado, calentamiento anormal, líquido o batería hinchada, detén la actividad y comunícalo. No intentes comprobar un daño tocando partes ni reutilices una batería deformada.

Fuente técnica: INSST, Riesgo eléctrico. Su aplicación depende del trabajo y del personal autorizado. https://www.insst.es/materias/riesgos/seguridad-en-el-trabajo/riesgo-electrico

Para mover un equipo, comprueba peso, recorrido, agarre y necesidad de ayuda o medios. No conviertas una cifra de peso genérica en permiso para levantar cualquier carga. Antes de transportar una torre, organiza sus cables y evita sujetarla por piezas no diseñadas como asa.

IPE I. Pantalla, postura y organización

Ajusta el puesto para leer sin reflejos molestos, apoyar el cuerpo y utilizar teclado y ratón sin posturas forzadas. La pantalla, la mesa, el asiento y los accesorios deben formar un conjunto adecuado a la persona y la tarea.

Alterna tareas y organiza pausas según la evaluación y actividad. No hay una única postura inmóvil perfecta ni una duración de pausa universal que sirva para cualquier puesto. Un portátil usado durante periodos prolongados puede necesitar accesorios para adaptar pantalla y entrada de datos.

La presión continua, las interrupciones y las instrucciones contradictorias también requieren organización preventiva. Comunicar cargas excesivas y acordar prioridades es parte del trabajo.

Fuente: INSST, guía técnica de equipos con pantallas de visualización, edición consultada en 2026. https://www.insst.es/documentacion/catalogo-de-publicaciones/guia-tecnica-para-la-evaluacion-y-prevencion-de-los-riesgos-relativos-a-la-utilizacion-de-equipos-con-pantallas-de-visualizacion

IPE I. Emergencias: actuar dentro de tu preparación

Conoce salidas, señalización, punto de reunión, responsables y mecanismo de aviso del centro. No bloquees recorridos ni improvises una salida distinta porque es más corta. En un simulacro se aprende a seguir el plan sin exponerse.

La conducta **PAS** recuerda proteger, avisar o alertar, y socorrer. Evita convertirte en otra víctima; activa los recursos de emergencia y sigue las indicaciones. En España, el número general de emergencias es **112**. Describe ubicación y situación con claridad. La ayuda concreta depende del estado y de tu formación; aprende primeros auxilios con práctica supervisada.

Fuente: INSST, NTP 1062, soporte vital básico en el adulto. Esta lectura introduce organización de la respuesta; no certifica formación sanitaria ni sustituye entrenamiento actualizado. https://www.insst.es/documentacion/colecciones-tecnicas/ntp-notas-tecnicas-de-prevencion/30-serie-ntp-numeros-1031-a-1065-ano-2015/ntp-1.062-primeros-auxilios-soporte-vital-basico-en-el-adulto

IPE I. Contrato, convenio y condiciones

Antes de comparar ofertas, identifica empleador, función, lugar, jornada, horario, retribución anual y modalidad contractual. El **convenio colectivo** puede regular condiciones relevantes para el ámbito aplicable; no lo elijas solo por el nombre que parezca más informático.

El Estatuto de los Trabajadores regula materias como derechos, contrato, jornada, salario, vacaciones y extinción. Las vacaciones anuales retribuidas tienen un mínimo legal de treinta días naturales; no lo confundas con treinta días laborables. El convenio y el contrato pueden mejorar condiciones dentro del marco aplicable.

Una discrepancia sobre jornada, categoría o salario necesita contrastar documentos y normativa, no una respuesta universal de un manual. Guarda tu documentación y utiliza orientación laboral, representación de las personas trabajadoras u otros canales profesionales adecuados.

Fuente normativa, España, consulta de 5 de noviembre de 2026: Estatuto de los Trabajadores, especialmente artículos 3, 4, 8, 26, 34 y 38.
https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

El SEPE organiza su guía en contratos indefinidos, temporales y las modalidades formativas en alternancia y para obtener práctica profesional. «Temporal» no significa que se pueda utilizar sin causa o requisitos. La formación en empresa de un ciclo y un contrato formativo no son automáticamente la misma situación.

Fuente para comprobar modalidades y condiciones actuales: Guía de contratos del SEPE. https://sepe.es/HomeSepe/que-es-el-sepe/comunicacion-institucional/publicaciones/publicaciones-oficiales/listado-pub-empleo/guia-contratos.html

IPE I. Comprender una nómina sin aprender porcentajes de memoria

Identifica periodo, empresa, persona trabajadora, conceptos devengados, deducciones y líquido a percibir. El recibo incluye información sobre cotización; la aportación empresarial no se debe confundir con una deducción adicional del líquido de la persona.

Ejemplo exclusivamente aritmético: devengos ficticios de 1.650 euros y deducciones ficticias totales de 220 euros dejan 1.430 euros líquidos. Los 220 no se calculan con tipos reales: sirven para comprender la resta. Bases, tipos y retenciones dependen de conceptos, situación y reglas vigentes.

Referencia del modelo: Orden ESS/2098/2014, anexo del recibo individual de salarios. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-11637

Para comparar ofertas ficticias, una retribución anual de 21.000 euros distribuida en catorce pagos iguales daría 1.500 por pago antes de las deducciones pertinentes. En doce pagos iguales serían 1.750. El anual coincide; no implica que todo contrato pueda distribuirse de cualquier forma. Comprueba las condiciones reales de pagas y conceptos.

El informe de vida laboral y el de bases de cotización aportan información diferente. En los servicios oficiales de la Seguridad Social puedes consultar periodos y bases según el informe. No publiques un informe real como muestra de portfolio.

Fuente: Seguridad Social, información sobre vida laboral y bases en Import@ss. https://www.seg-social.es/wps/portal/wss/internet/HerramientasWeb/755269e7-0449-4643-83d2-cf2b4fde1110/vlbc1

IPE I. Tu plan de aprendizaje y tu identidad digital

Un **entorno personal de aprendizaje** reúne fuentes, herramientas, personas y hábitos para aprender. Para SMR puede incluir documentación oficial, cuaderno de laboratorio, grupo de estudio y una carpeta de evidencias revisadas. Seguir muchas cuentas sin practicar no garantiza aprendizaje.

Define un objetivo observable: «en cuatro semanas resolveré y explicaré tres casos de direccionamiento de mi laboratorio». Divide sesiones, identifica ayudas, reserva tiempo para repetir sin guía y revisa resultados. Anota también descansos y dificultades: un plan imposible de cumplir no se arregla culpándote.

Tu **identidad digital profesional** se construye con lo que publicas y cómo lo explicas. Comparte datos ficticios o autorizados, respeta licencias y distingue aportación propia, ayuda recibida y contenido generado. Un repositorio limpio con un proyecto comprensible vale más como evidencia que diez capturas sin contexto.

IPE I. Organización preventiva y protección social

La prevención necesita una organización adecuada al tamaño, actividad y condiciones de la empresa: puede apoyarse en las modalidades previstas legalmente, como servicio propio o ajeno, personas designadas o asunción por el empresario cuando concurran sus requisitos. No se elige solo por ser la opción más barata. La representación preventiva de las personas trabajadoras y los órganos de participación tienen funciones propias; el responsable de informática no los sustituye por saber configurar equipos.

La **vigilancia de la salud** se relaciona con los riesgos del trabajo y tiene reglas de consentimiento, excepciones, confidencialidad y acceso a resultados. La empresa recibe las

conclusiones que procedan sobre aptitud o medidas, sin convertir la historia clínica en un archivo del departamento técnico. No incluyas datos de salud de compañeros en la ficha de riesgos. Revisa el artículo 22 de la Ley 31/1995 y el procedimiento del servicio preventivo.

El plan de emergencia identifica medios, responsables, formación y actuación. Localiza botiquín, revisión de material y persona responsable según el plan; no presupongas que cualquier producto disponible debe aplicarse. Ante un accidente, protege y alerta y sigue indicaciones dentro de tu formación. Las técnicas concretas de primeros auxilios necesitan demostración y entrenamiento supervisados.

La **Seguridad Social** organiza protección ante situaciones como incapacidad temporal, nacimiento y cuidado de menor, jubilación u otras contingencias conforme a sus reglas. El desempleo tiene requisitos y gestión específicos. No todas las prestaciones nacen automáticamente por dejar de trabajar ni toda suspensión del contrato supone extinción. Compara cuatro supuestos ficticios: baja temporal, permiso con suspensión, finalización de contrato y despido; identifica qué relación continúa, qué documentos faltan y qué organismo oficial permite comprobar prestaciones y plazos. No calcules derechos con porcentajes recordados de otro año.

Si cambia horario, función o lugar de prestación, contrasta contrato, convenio, comunicación y normativa antes de concluir qué derechos se aplican. Representación laboral, orientación sindical, servicios de conciliación y asesoramiento profesional pueden ser vías según el asunto. El plazo y procedimiento dependen de la reclamación; guarda fechas y documentos y consulta pronto, sin publicar el expediente.

Práctica ampliada: añade al mapa de riesgos quién evalúa, quién forma, quién mantiene el botiquín y cómo participa la plantilla. En la comparación de ofertas separa salario, cotización y prestaciones. Respuesta orientativa: un antivirus no sustituye evaluación preventiva; una mayor cuota en una nómina no permite deducir por sí sola todas las prestaciones futuras. Fuentes de consulta: Ley 31/1995, Estatuto de los Trabajadores, Seguridad Social y SEPE ya enlazados en esta unidad.

IPE I. Práctica y soluciones

Prepara tres entregas: mapa de un puesto; ficha de cinco riesgos de un aula ficticia con medidas y responsables; comparación de dos ofertas inventadas. Usa `recursos/empleabilidad/plan-personal.md` y `ficha-riesgos.md`.

Caso: una oferta indica 21.000 euros anuales en catorce pagos iguales y otra 20.400 en doce. ¿Cuál tiene mayor anual? La primera. ¿Cuál tiene mayor pago ordinario bruto en el supuesto simplificado? La segunda: 1.700 frente a 1.500. No concluyas cuál te conviene sin estudiar jornada, condiciones, funciones y otros datos.

Caso preventivo: el paso de emergencia tiene cajas de monitores. La respuesta es comunicar y corregir la obstrucción mediante la organización prevista, sin trasladarla a otro recorrido. No basta una advertencia para que la gente pase «con cuidado».

Evaluación: cada riesgo debe tener una situación concreta, daño posible y medida coherente; cada competencia del mapa necesita evidencia o un plan para adquirirla. No se solicita visitar zonas peligrosas ni intervenir sobre alimentación eléctrica.

IPE II. Buscar empleo con evidencias

Selecciona una oferta y adapta tu candidatura a sus tareas. El currículum debe permitir encontrar formación, conocimientos, proyectos y experiencias relevantes. Usa un formato claro, fechas coherentes y afirmaciones que puedas explicar. No añadas una tecnología solo porque el anuncio la menciona.

Presenta un proyecto con contexto, tu papel, decisiones, pruebas y resultado. Ejemplo: «Diseñé en laboratorio una red de dos subredes; documenté direccionamiento y verifiqué acceso permitido y denegado». Si no configuraste VLAN o cortafuegos, no los añadas a la frase.

Organiza una tabla de candidaturas con empresa, puesto, fecha, adaptación realizada, estado y siguiente acción. Protege la información de contacto y elimina duplicados. Desconfía de peticiones de pagar para participar o de entregar credenciales; contrasta identidad y canal antes de facilitar documentación.

IPE II. Entrevista y prueba técnica

Ensaya respuestas con situación, tarea, acción y resultado. No hace falta una experiencia laboral para practicar: puedes explicar un error de laboratorio y cómo lo aislaste. «No sabía la causa; comparé configuración y consulta, encontré el DNS incorrecto y repetí la tarea» demuestra un método.

Si te proponen una herramienta desconocida, reconoce el límite y explica cómo aprenderías. En una prueba, confirma alcance, recursos y tiempo. Formula preguntas cuando falten datos. Un cambio agresivo sin comprender el sistema rara vez demuestra buen criterio.

Después revisa dos cosas: qué pudiste demostrar y qué quedó poco claro. Ajusta el plan de aprendizaje. El rechazo de una candidatura no prueba que no sirvas para el oficio; aporta información parcial sobre ese proceso.

IPE II. Trabajar en equipo y gestionar un conflicto

Acordad objetivo, reparto, entregas y mecanismo para pedir ayuda. Las tareas deben tener responsable y criterio de aceptación. «Todos hacemos la red» suele dejar huecos; «una persona propone direccionamiento y otra lo revisa con los requisitos» permite coordinar y comprobar.

Da una devolución basada en hechos: «El procedimiento no indica qué cuenta se utiliza; no he podido repetir la prueba». Añade una propuesta concreta. Evita confundir una crítica al trabajo con un juicio sobre la persona.

Si dos compañeros quieren soluciones distintas, escribid requisitos, opciones, evidencia y costes. Podéis hacer una prueba corta con criterios acordados. Si falta una decisión de autoridad o hay un conflicto que no se resuelve, escaladlo de forma respetuosa. No escondáis errores por miedo a perder una discusión.

La gestión emocional incluye reconocer frustración, parar cuando el razonamiento se bloquea y pedir apoyo. La inclusión requiere que todas las personas puedan contribuir: documentación legible, turnos, herramientas accesibles y reparto que no deje siempre a la misma persona sin practicar.

IPE II. De una necesidad a una propuesta de valor

Emprender puede ser crear una empresa, impulsar una mejora dentro de una organización o desarrollar una iniciativa social. No toda mejora exige una aplicación nueva. Empieza por comprender quién tiene el problema, qué hace hoy y qué coste o dificultad le supone.

Caso ficticio: tres asociaciones necesitan mantener pequeños equipos y entender sus copias. Una propuesta podría ser un servicio de revisión y formación con alcance claro. Antes de invertir, entrevista con preguntas sobre tareas reales: «¿cuándo comprobasteis la última restauración?» aporta más que «¿os gustaría mi servicio?».

Escribe hipótesis y una forma de contrastarlas. «Pagarían por una revisión trimestral» sigue siendo una hipótesis aunque tres personas digan que suena bien. Un piloto limitado y autorizado puede aportar evidencia sobre necesidad, esfuerzo y satisfacción. No prometas recuperación de datos sin conocer el entorno.

La **propuesta de valor** explica a quién ayudas, qué problema resuelves y qué resultado esperas ofrecer. «Soporte con IA» describe una herramienta; «ayudar a que el responsable pueda comprobar su copia y saber a quién avisar si falla» describe un resultado comprensible.

IPE II. Modelo, organización e innovación

Describe clientes o beneficiarios, actividades, recursos, socios, canales, costes e ingresos o financiación. Considera también seguridad, privacidad, accesibilidad y sostenibilidad. Si solo funciona gracias a trabajo no remunerado ilimitado, el modelo necesita revisión.

Podéis estudiar trabajo autónomo, sociedades y fórmulas de economía social como cooperativas. Diferéncialas por organización, responsabilidades y finalidad con asesoramiento y fuentes actuales antes de elegir. El ejercicio no implica darse de alta, firmar contratos ni realizar trámites reales.

La innovación puede mejorar un proceso existente: una lista de comprobación que reduce olvidos, una guía accesible o un registro de intervenciones. Mide si mejora el resultado. Una herramienta novedosa que añade costes y no resuelve el problema no es una mejora demostrada.

Recurso oficial para profundizar en el proyecto empresarial: Plan de Empresa de la DGEIPYME, con análisis de viabilidad técnica, económica y financiera. https://planempresa.ipyme.org/Home

IPE II. Números de un servicio ficticio

Para aprender, supongamos costes fijos de 240 euros al mes, un precio de 60 euros por revisión y costes variables de 20 por revisión. Las cifras son inventadas y excluyen impuestos y otras obligaciones; no son una recomendación de precios.

Cada revisión aporta 40 euros a cubrir costes fijos: 60 menos 20. Seis revisiones cubren 240. Con cinco, ingresos 300 y costes 340: resultado de menos 40. Con ocho, ingresos 480 y costes 400: resultado de 80 en este modelo simplificado.

Revisa el tiempo: si cada revisión ocupa dos horas, ocho requieren al menos dieciséis horas técnicas, más desplazamientos, preparación, administración y atención. Si no incluyes tu trabajo y demás costes pertinentes, el resultado no representa la viabilidad real.

Distingue **resultado** de **tesorería**. Puedes haber prestado un servicio que aún no te han pagado mientras debes abonar gastos. El presupuesto debe indicar alcance, entregas, supuestos, plazos y exclusiones comprensibles. No anuncies garantías que no puedes cumplir.

IPE II. Proyecto breve y evaluación

En parejas, diseñad una propuesta ficticia de mantenimiento para Aula Norte. Preparad necesidad, beneficiarios, entrevista simulada, alcance, recursos, calendario, reparto, riesgos, presupuesto simplificado y prueba de aceptación. Incluid una mejora ambiental y una de accesibilidad que se puedan comprobar.

Usad `recursos/empleabilidad/proyecto-servicio.md`. Ensayad una exposición de tres minutos y una pregunta difícil: «¿qué ocurre si no podéis restaurar una copia?». La respuesta debe reconocer límites, comunicar, conservar evidencia y aplicar el escalado previsto; no prometer éxito absoluto.

Evaluad de 0 a 2: necesidad y evidencia; coherencia técnica; organización inclusiva; números y supuestos; pruebas y comunicación. Cada punto sin demostrar se convierte en una acción de mejora con responsable. No hay actividad comercial real ni recogida de datos de posibles clientes.

IPE II. Validar, comunicar y financiar una mejora

Una entrevista de problema explora hechos pasados: tarea, frecuencia, dificultad y alternativas. Evita recoger datos personales innecesarios. Para el ensayo, interpreta con un compañero a una asociación ficticia que pierde documentos; separa lo dicho por ese personaje de evidencia de una organización real. Construye un prototipo de ficha de copia y observa si puede seguirlo. Si pide ayuda en el paso de restauración, corrige el diseño antes de prometer el servicio.

El **pensamiento de diseño** organiza comprensión de personas, definición del problema, generación de opciones, prototipo y prueba. Las etapas pueden repetirse. Una metodología ágil permite revisar incrementos y prioridades con devolución frecuente; no significa trabajar sin documentación o contrato. Un tablero sencillo puede usar pendiente, en curso y comprobado, con un límite de tareas simultáneas acordado.

El marketing explica valor y facilita una decisión informada. Prepara una página ficticia con destinatario, alcance, exclusiones, precio de ejemplo y canal de consulta, y pide a otra persona que resuma qué compraría. Si cree que garantizas recuperar cualquier disco, el mensaje debe corregirse. Mide comprensión y solicitudes pertinentes, no solo clics. No publiques la campaña ni contactes asociaciones reales para este ejercicio.

Una iniciativa social añade efectos y participación, además de ingresos. Para una propuesta de reutilización informática, analiza quién recibe equipos útiles, quién mantiene soporte y qué ocurre con los datos. Un **balance social** reúne información sobre impactos y prácticas sociales según un método identificado. La Economía del Bien Común es un enfoque que valora la contribución social de la actividad; la economía circular se centra en mantener valor de recursos y reducir residuos. Ninguna etiqueta acredita por sí sola resultados.

Las opciones de financiación pueden incluir recursos propios, aportaciones acordadas, crédito, subvenciones o financiación colectiva, con requisitos, coste, riesgo y compromisos distintos. En el proyecto ficticio compara dos opciones sin contratar: quién decide, qué devolución o contraprestación exige, qué ocurre si faltan ingresos y qué condiciones éticas o ambientales se valoran. Una convocatoria de ayudas necesita verificación de bases vigentes; no se presenta como ingreso seguro.

Entrega: hipótesis inicial, guion de entrevista, observación del prototipo, cambio introducido, mensaje de oferta y comparación de financiación. Usa el presupuesto y fases del capítulo 64 para justificar viabilidad. Conserva la diferencia entre una respuesta simulada, una intención y una contratación real.

¿Lo has pillado?

1. ¿Un salario mensual mayor implica un salario anual mayor?

2. ¿Una pulsera antiestática permite manipular alimentación eléctrica sin riesgo?

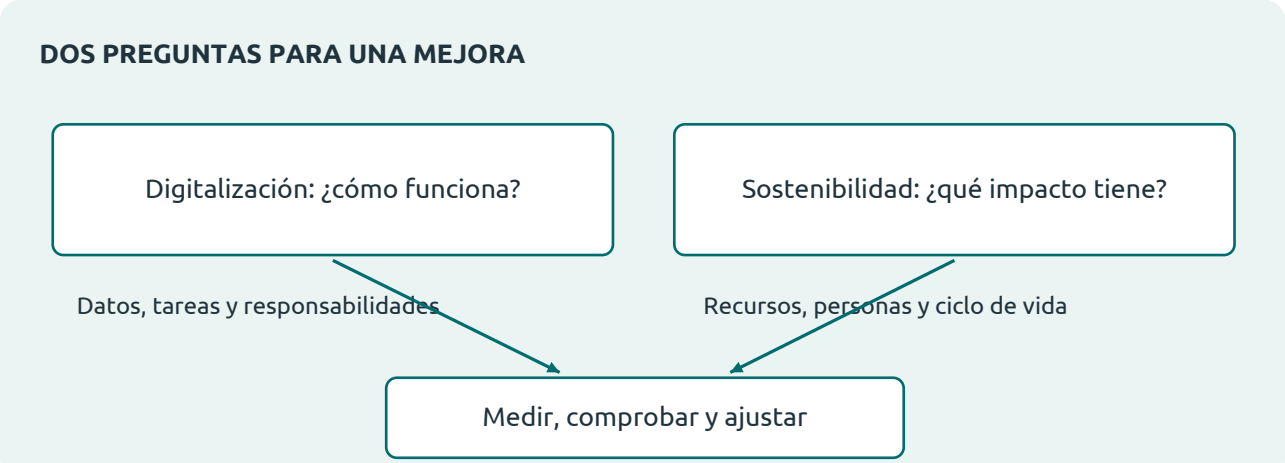
3. ¿Qué diferencia hay entre una idea atractiva y una necesidad validada?

4. Con los datos del servicio, ¿cuántas revisiones cubren los costes fijos?

Soluciones. 1) No; hay que comparar anual, pagas y condiciones. 2) No; su función es otra y se requiere el procedimiento y preparación adecuados. 3) La validación aporta evidencias sobre problema, beneficiarios y solución; una impresión favorable no basta. 4) Seis, en el modelo simplificado; no acredita viabilidad completa.

58. Digitalización y sostenibilidad con resultados comprobables

Al terminar: describirás una mejora digital, elegirás tecnologías por su función y elaborarás un plan ambiental y social con indicadores. **Antes:** redes, servicios, datos y seguridad.



Las mejoras se evalúan con indicadores y atención a sus efectos.

Este capítulo desarrolla dos unidades distintas. **Digitalización** estudia cómo cambian datos, tareas y procesos. **Sostenibilidad** analiza impactos, recursos, personas y decisiones a lo largo del ciclo de vida. Una mejora puede contribuir a ambas, pero instalar tecnología no garantiza reducir el impacto.

Digitalización. Del papel al cambio de proceso

Convertir una ficha en un archivo es una forma de **digitalizar información**. Reorganizar cómo se solicita, revisa y sigue una reparación transforma el **proceso**. Si el archivo vuelve a imprimirse, se copia a mano y nadie sabe quién tiene la versión actual, la herramienta no ha resuelto el problema.

Describe el proceso presente: quién recibe la petición, qué datos necesita, cómo decide prioridad, dónde registra y cómo comunica cierre. Después dibuja el propuesto. Señala qué mejora, qué nueva dependencia crea y quién necesita formación.

Caso de Aula Norte: las peticiones llegan por tres canales y algunas se pierden. El objetivo ficticio es que cada solicitud tenga identificador y responsable. Una solución podría utilizar un sistema de tickets; también exige acordar entrada, categorías, seguimiento y revisión. El programa no crea esas reglas por sí solo.

Digitalización. Economía lineal, circular y tecnología

Un modelo **lineal** extrae recursos, produce, utiliza y desecha. Un modelo **circular** busca conservar utilidad y valor mediante decisiones como durabilidad, mantenimiento, reparación y reutilización, además del tratamiento final. Circular no significa que cualquier material pueda reutilizarse infinitamente.

Un inventario puede ayudar a localizar equipos aprovechables y piezas compatibles antes de comprar. La digitalización apoya esa decisión si sus datos son fiables y se usan. Una lista desactualizada que declara disponibles equipos averiados puede provocar compras o transportes innecesarios.

Las revoluciones industriales suelen explicarse relacionando mecanización, electricidad y producción en serie, automatización electrónica y conexión digital de procesos. La **industria 4.0** destaca la interconexión de sistemas, datos y procesos físicos. Son modelos para comprender cambios, no fronteras exactas compartidas por todas las empresas.

Marco curricular de referencia: RD 659/2023, anexos sobre Digitalización de Grado Medio y Sostenibilidad. La concreción de actividades corresponde al currículo y programación aplicables. https://www.boe.es/buscar/act.php?id=BOE-A-2023-16889

Digitalización. IT, OT y consecuencias físicas

IT o TI se centra en sistemas de información. **OT o TO** se relaciona con operación y control de procesos físicos: por ejemplo, un controlador que actúa sobre una máquina. Un sensor mide; un actuador ejecuta una acción física. Conectar ambos entornos crea oportunidades y nuevas dependencias.

En un proceso industrial, disponibilidad y seguridad física pueden imponer requisitos muy distintos a los de un aula. No reinicies un controlador ni ejecutes un escaneo porque esa prueba fuera cómoda en un PC de laboratorio. Identifica responsable, procedimientos y condiciones de operación.

Fuente técnica: NCSC, Operational technologies, sobre interacción con el mundo físico y gestión de riesgos. https://www.ncsc.gov.uk/guidance/operational-technologies

Ejemplo ficticio: un sensor comunica temperatura a una pasarela y esta envía medidas a un panel. Que el panel deje de recibirlas no demuestra que la temperatura sea correcta ni incorrecta: demuestra ausencia de datos en ese recorrido. El sistema debe distinguir valor normal, alarma y medida desconocida.

Digitalización. Tecnologías por lo que resuelven

IoT conecta dispositivos capaces de recoger o intercambiar información. Requiere identidad del dispositivo, alimentación, conectividad, actualización y control del acceso. Un sensor barato que no puede mantenerse puede resultar una mala dependencia.

La **nube** ofrece recursos mediante servicios y modelos concretos; **edge** sitúa parte del procesamiento cerca del origen de los datos. Edge puede responder a necesidades de latencia, conectividad o tratamiento local, pero añade equipos que mantener. El capítulo 61 desarrolla modelos y responsabilidades de nube y contenedores.

El **análisis de datos** busca información útil a partir de datos adecuados. La **IA** puede clasificar, detectar patrones o generar contenidos según su sistema. Necesita evaluación, control de errores y protección de información; no convierte un dato incompleto en un hecho fiable. El capítulo 63 desarrolla su uso con verificación.

La **robótica** automatiza tareas físicas con diseño y protección apropiados. La **realidad aumentada** superpone información sobre el entorno; la **realidad virtual** crea una experiencia inmersiva. Pueden servir para formación o asistencia, pero hay que comprobar accesibilidad, adecuación y aprendizaje real.

La **fabricación aditiva** construye piezas mediante un proceso como la impresión 3D. No cualquier material o pieza fabricada es adecuada para uso eléctrico, mecánico o de seguridad. Un **gemelo digital** representa un activo o proceso con un vínculo de datos y actualización definido; un dibujo estático no demuestra esa integración.

Una **cadena de bloques** mantiene registros mediante un diseño distribuido y reglas específicas. No es necesaria para todo inventario y no garantiza que el dato introducido sea verdadero. Antes de escogerla, justifica qué necesidad no resuelve una base de datos más sencilla.

Digitalización. Datos, calidad y decisiones

Define cada dato: significado, unidad, origen, hora y responsable. «Temperatura = 27» no basta si desconoces unidad o lugar. Un valor cero puede ser válido; un dato ausente no debe transformarse en cero automáticamente.

Revisa duplicados, formatos, rangos y coherencia. Después pregunta si los datos representan la actividad que quieres evaluar. Comparar tiempos de resolución sin separar casos sencillos y complejos puede generar una conclusión engañosa.

Un **indicador** ayuda a evaluar un objetivo. «Porcentaje de avisos con responsable» puede medir organización; no demuestra satisfacción ni calidad de reparación. Define numerador, denominador, periodo y exclusiones. Conserva evidencia suficiente para recalcularlo.

Digitalización. Diseña una implantación gradual

Comienza con un piloto limitado y datos ficticios. Define criterio de aceptación, participantes, formación, soporte y forma de volver al proceso anterior si hace falta. Comprueba exportación, recuperación y dependencia del proveedor antes de ampliar.

Ejemplo: durante una semana simulada se registran veinte avisos; dieciocho tienen responsable. El indicador es 18 dividido entre 20, un 90 %. El objetivo ficticio era al menos un 95 %: no se ha alcanzado. Investiga por qué dos avisos quedaron sin asignar antes de comprar otra herramienta.

Presupuesta implantación y mantenimiento: licencias si existen, equipos, formación, integración, copias y tiempo. Una herramienta gratuita puede requerir recursos significativos. Incluye permisos, privacidad y accesibilidad desde el diseño, no como arreglo al final.

Digitalización. Práctica y respuesta orientativa

Usa `recursos/transversales/plan-digitalizacion.md`. Propón el paso de avisos dispersos a una cola de soporte en Aula Norte. Entrega proceso presente y futuro, datos mínimos, responsabilidades, dos alternativas, riesgos, piloto, formación y dos indicadores.

Respuesta orientativa: cada aviso recibe identificador, fecha, tarea, activo ficticio, impacto y responsable; se limita el acceso a quien lo necesita; los adjuntos se depuran; se prueba crear, reasignar, resolver, exportar y recuperar. Se mide asignación y aceptación de la tarea reparada, sin convertir rapidez en el único criterio.

No despliegues un servicio de Internet ni recojas avisos de estudiantes reales. El resultado es un diseño y simulación que permita justificar una decisión.

Digitalización. Nube, niebla y el extremo del sensor

En el capítulo 61 se distinguen modelos de servicio y despliegue de nube. **Edge** acerca procesamiento al origen; **fog** describe una organización distribuida de recursos y servicios entre dispositivos y nube; **mist** lleva ciertas funciones aún más cerca de sensores o actuadores con recursos limitados. Los límites dependen del modelo usado y no todos los proveedores emplean los términos igual. No son tres marcas de almacenamiento.

Ejemplo ficticio: el sensor filtra una lectura imposible antes de transmitirla; una pasarela local agrega medidas y genera avisos; el servicio remoto conserva histórico y prepara informes. Dibuja qué función necesita seguir disponible si se interrumpe Internet, qué datos salen y quién actualiza cada componente. Llevar todo cerca del sensor reduce ciertas dependencias y crea otras de capacidad, mantenimiento y recuperación.

Fuente conceptual: NIST SP 500-325, modelo de fog y mist computing. La asignación de tareas anterior es un ejemplo propio.

La conectividad **5G** puede ofrecer capacidades útiles según cobertura, red, terminal y servicio; no garantiza una latencia o velocidad fija en cualquier ubicación. El **Big Data** relaciona conjuntos y flujos cuya escala, diversidad o velocidad requieren técnicas adecuadas. Una hoja con cien filas no necesita una plataforma distribuida solo para parecer moderna. Una base de documentos u objetos puede representar datos sin la estructura de tablas del ejemplo SQL, pero necesita igualmente diseño, permisos, índices, exportación y recuperación.

Práctica: compara tres diseños para los avisos de Aula Norte: hoja local, aplicación web central y aplicación con funcionamiento temporal sin conexión. Para cada uno explica integración, costes de mantenimiento, formación, disponibilidad y pérdida de datos tolerable. Respuesta orientativa: el diseño depende del problema; la opción con más tecnologías no gana si no mejora la tarea y puede recuperarse.

Sostenibilidad. Ambiental, social y gobernanza

La sostenibilidad analiza consecuencias ambientales y sociales, además de cómo se toman y controlan decisiones. **ASG** agrupa aspectos ambientales, sociales y de gobernanza. No es una etiqueta que convierta automáticamente una organización en responsable.

En un aula: ambiental incluye energía, materiales, transporte y residuos; social incluye accesibilidad, condiciones de trabajo y posibilidad de aprender; gobernanza incluye compras justificadas, responsables, seguimiento y transparencia de resultados.

Los **grupos de interés** son personas o entidades afectadas o capaces de influir: alumnado, docentes, personal técnico, proveedores y responsables de gestión, entre otros. Consulta necesidades y conflictos. Una medida que reduce consumo pero impide usar una ayuda técnica necesita revisarse.

Sostenibilidad. ODS y decisiones concretas

La Agenda 2030 de Naciones Unidas reúne **17 Objetivos de Desarrollo Sostenible** relacionados entre sí. Para SMR pueden estudiarse educación, trabajo decente, innovación, consumo responsable y acción climática. Elegir un icono de ODS no demuestra una contribución.

Asocia cada propuesta a una acción y evidencia. «Reutilizar equipos aptos con borrado y verificación» puede relacionarse con consumo responsable; «adaptar la documentación para lectura accesible» con aprendizaje e inclusión. Explica límites y posibles efectos adversos.

Fuente: Naciones Unidas, objetivos y metas. https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

Sostenibilidad. Ciclo de vida y compra

Considera extracción de materiales, fabricación, transporte, uso, reparación y final de vida. Un dispositivo con menor consumo durante el uso puede implicar impactos de fabricación que debes estudiar antes de sustituir uno funcional. No existe una regla de «siempre compra nuevo» o «nunca renueves».

Compara necesidades reales, soporte de seguridad, reparabilidad, disponibilidad de piezas, garantías, consumo para la tarea y compatibilidad. Un equipo sin soporte puede no ser adecuado para un servicio conectado aunque aún arranque. Quizá pueda cumplir otra función aislada y justificada, o deba retirarse.

Separa **reutilización** de un aparato apto y **preparación para la reutilización** cuando el equipo ya es un residuo sometido al proceso correspondiente. Los residuos de aparatos eléctricos y electrónicos, **RAEE**, tienen canales y tratamiento regulados. No van a la fracción ordinaria de basura ni se desmontan sin el procedimiento y las condiciones pertinentes.

Referencia normativa, España, consultada el 5 de noviembre de 2026: RD 110/2015 sobre RAEE. https://www.boe.es/buscar/act.php?id=BOE-A-2015-1762

Antes de una cesión o retirada, aplica el procedimiento de protección de datos y borrado adecuado al soporte. Borrar una entrada del inventario no elimina los datos del disco. Conserva evidencia de destino y tratamiento sin publicar identificadores innecesarios.

Sostenibilidad. Medir energía sin confundir unidades

La **potencia** se mide en vatios, W; la **energía**, por ejemplo, en kilovatios hora, kWh. Para una potencia media conocida, energía en kWh = potencia media en W por horas, dividido entre 1.000. La potencia nominal de una fuente no es el consumo medido del ordenador.

Caso ficticio de veinte equipos: suponemos 45 W de potencia media por equipo durante seis horas de actividad y 5 W durante dieciocho horas restantes. Cada equipo utiliza 270 Wh más 90 Wh, es decir, 0,36 kWh al día. Veinte equipos suman 7,2 kWh.

Si en el segundo supuesto pasan a 1 W durante las dieciocho horas restantes, cada uno suma 270 más 18 Wh, o 0,288 kWh. Veinte suman 5,76 kWh. La diferencia es 1,44 kWh al día. Para doscientos días iguales serían 288 kWh, bajo estos supuestos.

Los datos son inventados: no son una medición del aula ni una promesa de ahorro. Antes de aplicar una política real, considera actualizaciones, acceso remoto, copias, ayudas técnicas y arranque. Mide un periodo comparable y verifica que la actividad sigue funcionando.

Para estimar emisiones necesitas un factor adecuado y documentado, periodo y alcance. No conviertas automáticamente cada kWh en una cantidad universal de CO2 equivalente. Tampoco presentes ahorro de energía como evaluación completa del ciclo de vida.

Sostenibilidad. Un plan con responsables e indicadores

Parte de una situación conocida, identifica impactos relevantes y consulta a los grupos de interés. Define acciones, recursos, responsable, plazo, indicador y revisión. Prioriza por impacto, viabilidad y necesidades, con criterios explícitos.

Ejemplo de acción: revisar suspensión en equipos de prácticas que no tienen tareas nocturnas. Indicador: energía medida para un conjunto y horario comparables, más número de tareas afectadas. El éxito ambiental pierde sentido si la medida deja inaccesible un recurso necesario.

Otra acción: aumentar vida útil de equipos aptos. Indicador: equipos reparados y verificados que vuelven a un uso definido, junto a fallos posteriores y coste de mantenimiento. No cuentes como reutilizado un equipo simplemente almacenado en un armario.

Presenta resultados y límites con claridad. **Greenwashing** describe mensajes ambientales que dan una impresión engañosa. «Somos verdes porque todo está en la nube» no aporta evidencia: hay que estudiar servicio, infraestructura, uso y alcance de la afirmación.

Sostenibilidad. Práctica de mejora de Aula Norte

Usa `recursos/transversales/plan-sostenibilidad.md` y los supuestos de energía anteriores. Entrega una comparación numérica, una acción de reutilización y una medida social. Relaciona cada propuesta con objetivo, riesgo, responsable, plazo e indicador.

Después responde: si dos equipos necesitan una tarea nocturna, ¿puedes aplicar la misma suspensión a los veinte? Debes estudiar esa necesidad y segmentar la política o cambiar su programación con autorización. Recalcula con los grupos reales; no mantengas el ahorro de veinte si solo cambias dieciocho.

Resultado esperado: informe breve con supuestos identificados, unidades correctas, protección de datos en retirada y evidencia de utilidad. No se cambia la política energética de un centro real ni se manipulan residuos para este ejercicio.

Sostenibilidad. Evidencia, estándares e inversión responsable

La materialidad identifica qué asuntos son relevantes para evaluar impactos y decisiones dentro del marco elegido. No significa seleccionar únicamente indicadores que salen bien. En Aula Norte, accesibilidad, protección de datos, energía y destino de equipos pueden importar a grupos distintos. Registra por qué se incluyen y cómo se recogerá evidencia.

Los estándares **GRI** ofrecen un marco para informar sobre impactos de sostenibilidad. Las métricas necesitan definición, periodo, alcance, método y datos; no atribuyas conformidad con un estándar completo a una tabla escolar. La obligación legal de informar y el marco aplicable dependen de la entidad y normativa vigente. Este ejercicio no declara que una academia ficticia esté obligada a una forma concreta de reporte.

La **inversión socialmente responsable** incorpora criterios ambientales, sociales o de gobernanza junto a los objetivos y riesgos financieros del enfoque utilizado. Analistas, agencias, índices e inversores pueden evaluar asuntos y metodologías diferentes: dos puntuaciones no son necesariamente comparables. Una calificación o etiqueta no elimina riesgo ni certifica todas las actividades. Aquí estudiamos el concepto, sin recomendar una inversión.

Ejercicio de informe: toma el plan del aula y añade tres fichas: energía en kWh para un periodo comparable; equipos efectivamente reutilizados con destino y utilidad comprobados; tareas accesibles verificadas por las personas usuarias. Señala fuente, incertidumbre, responsable, resultado y próxima revisión. Si solo tienes una estimación, nómbrala como tal. Añade un efecto adverso posible y la medida que lo controla.

Fuente: GRI, estándares y guía de información de sostenibilidad. El informe del aula es una práctica propia, no un reporte certificado.

¿Lo has pillado?

1. ¿Un formulario nuevo demuestra transformación del proceso?

2. ¿Un sensor sin datos debe tratarse como valor cero normal?

3. ¿Una fuente de 650 W consume siempre 650 W?

4. ¿Cuánto ahorran dieciocho equipos durante doscientos días en el caso ficticio?

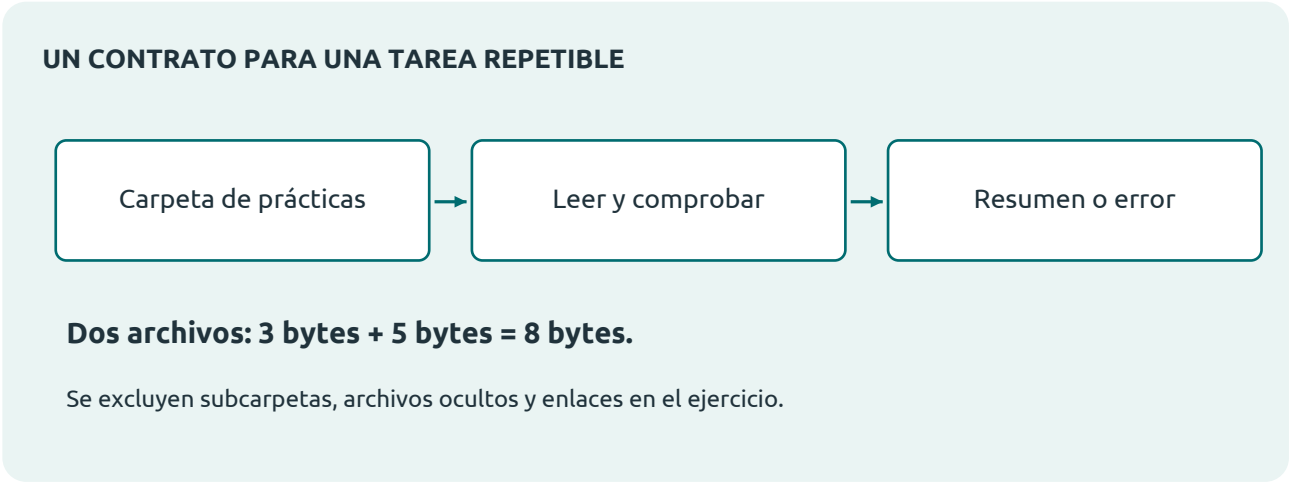
5. ¿Cómo demuestras que una reutilización ha sido útil?

Soluciones. 1) No; hay que comprobar tareas, responsabilidades y resultados. 2) No; ausencia y cero son estados distintos. 3) No; esa cifra no es una medición de consumo. 4) Cada equipo reduce 0,072 kWh al día; 18 por 200 por 0,072 = 259,2 kWh, con los supuestos indicados. 5) Con destino, estado, seguridad y tarea de uso verificados, además de seguimiento cuando proceda.

Bloque 12. Herramientas para seguir creciendo

59. Automatizar una tarea pequeña con Bash y PowerShell

Al terminar: identificarás variables, condiciones, bucles y salida de una tarea automatizada, y comprobarás sus límites. **Antes:** terminal, rutas, permisos y copias.



Primero define qué entra, qué sale y cómo reconoces un error.

Automatizar consiste en describir una tarea para que un sistema la repita. Primero necesitas saber hacerla y reconocer su resultado. Si automatizas una decisión que aún no entiendes, puedes repetir el mismo error muchas veces y a gran velocidad.

Define el contrato de la tarea

Nuestro ejercicio cuenta archivos de texto visibles y directos de una carpeta propia, y suma sus bytes. No modifica archivos, no entra en subcarpetas y omite enlaces. Son límites deliberados: «contar todos los archivos» sería otra tarea con más decisiones.

Prepara una carpeta nueva con un archivo de tres bytes ASCII y otro de cinco. Por ejemplo, escribe `abc` y `12345` sin salto final mediante las instrucciones del laboratorio. Esperamos dos archivos y ocho bytes. Un salto de línea también ocupa bytes: el tamaño no equivale al número de letras visibles.

Bash: variables y argumentos



Truco de taller

Bash interpreta instrucciones del shell. Una variable guarda un valor: `ruta=$1` usa el primer argumento. En una asignación no se añaden espacios alrededor de =. Las comillas en `"$ruta"` evitan que un espacio de la ruta la divida en varios argumentos.

`$#` indica cuántos argumentos has recibido; `$?`, el estado del comando anterior. Cero suele indicar éxito de un comando, aunque siempre hay que conocer su contrato. La salida normal y la de error son canales distintos: el recurso escribe sus avisos en la salida de error.

Fragmento del script completo entregado:

BASH

```
if [ "$#" -ne 1 ]; then
  printf 'Indica una carpeta de prácticas.\n' >&2
  exit 2
fi
ruta=$1
```

Condiciones, bucles y errores

Una condición decide qué rama ejecutar. Un bucle repite una acción sobre una colección. En el recurso, el glob `"$ruta"/*.txt` selecciona entradas directas con esa extensión. Si no encuentra archivos, se evita tratar el patrón literal como un archivo mediante la comprobación `-f`.

BASH

```
cuenta=0
total=0
for archivo in "$ruta"/*.txt; do
  [ -f "$archivo" ] || continue
  [ ! -L "$archivo" ] || continue
  if ! bytes=$(wc -c < "$archivo"); then
    printf 'Lectura fallida.\n' >&2
    exit 1
  fi
  cuenta=$((cuenta + 1))
  total=$((total + bytes))
done
```

`wc -c` cuenta bytes. `continue` pasa al siguiente elemento. `!` invierte el resultado de la comprobación; aquí permite gestionar un fallo de lectura. El script completo añade listado y resumen, así como comprobación de carpeta accesible.

No uses `for archivo in $(ls ...)` para este problema: los nombres con espacios se rompen por el procesamiento del texto. Tampoco añadas `sudo` para hacer desaparecer cualquier error. Revisa ruta, autorización y finalidad.

PowerShell: objetos y propiedades

PowerShell suele pasar **objetos** entre comandos: un archivo tiene propiedades como `Name` y `Length`. El operador `|` encadena resultados. Filtrar objetos evita tener que adivinar qué columna de una tabla contiene el tamaño.

POWERSHELL

```
Get-ChildItem -LiteralPath $Ruta -File -Filter '*.txt' |
  Where-Object {
    -not ($_.Attributes -band [IO.FileAttributes]::ReparsePoint)
  } |
  Select-Object -Property Name, Length
```

`$_` representa el objeto actual en ese bloque. El recurso completo `resumen-txt.ps1` reúne la colección, suma longitudes y devuelve un objeto con número de archivos y bytes. Un objeto de datos y su presentación en pantalla son cosas distintas; no formatees en tabla antes de intentar operar con sus propiedades.

Fuentes de sintaxis: Microsoft Learn, Get-ChildItem y about_Pipelines. https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-childitem y https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_pipelines

Ejecutar, verificar y recuperar

El recurso Bash es `recursos/automatizacion/resumen-txt.sh`; se ejecuta con Bash y una ruta entre comillas. El de PowerShell está pensado para PowerShell 7 en un entorno autorizado. No rebajes globalmente una política de ejecución ni pegues una orden de desbloqueo sin comprenderla: sigue el procedimiento del aula.

Comprueba cuatro casos: dos archivos con ocho bytes; carpeta vacía con cero; un archivo cuyo nombre tiene espacios; una ruta inexistente que produce error. Añade un enlace y una subcarpeta para comprobar que se respetan las exclusiones.

Las reglas de mayúsculas y filtros pueden variar entre sistemas. No prometemos igualdad universal para cualquier nombre o sistema de archivos. Si otro proceso modifica la carpeta durante la lectura, el resumen tampoco es una instantánea coherente: esta práctica utiliza datos estables.

Resultado esperado: puedes explicar por qué se cuentan dos archivos y qué entradas se omiten. Para recuperar, retira únicamente tu carpeta ficticia si ya no la necesitas. Los scripts leen y no borran datos.

Programar una tarea y mantenerla

Un programador de tareas necesita entorno, cuenta, rutas, horario, permisos y tratamiento de errores. Lo que funciona en tu terminal puede fallar en una ejecución programada por otro directorio o por variables distintas. Evita ejecuciones superpuestas si la tarea no lo admite.

Antes de programar, registra una ejecución manual, un fallo controlado y cómo se detecta. Añade después un horario de laboratorio, revisa su resultado y desactívalo al terminar. No automatices eliminaciones ni copias de información real como primera práctica.

¿Lo has pillado?

1. ¿Por qué escribimos `"$ruta"` con comillas?

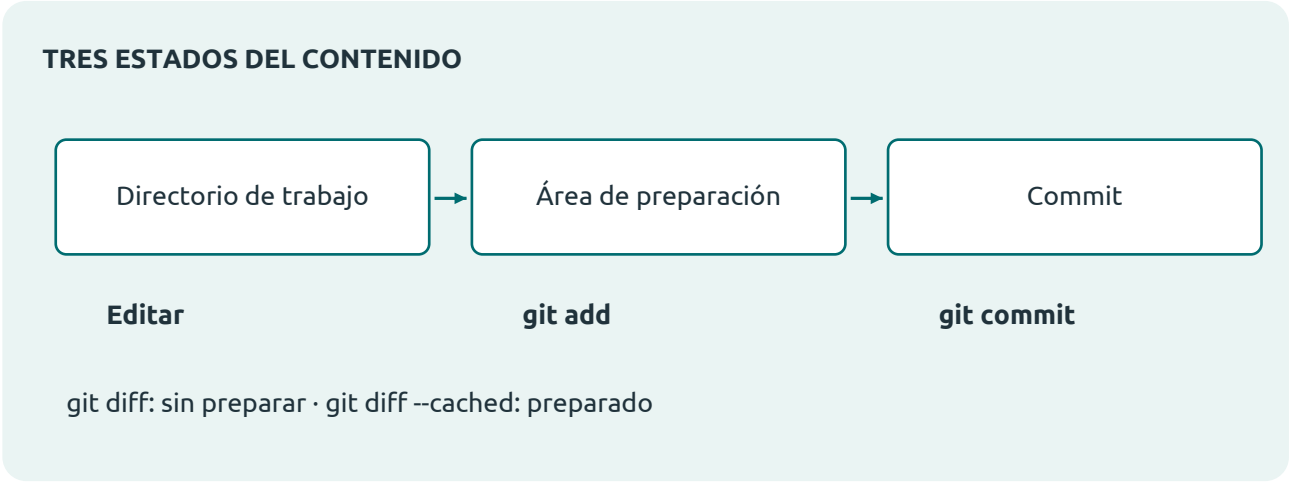
2. ¿Ocho caracteres implican ocho bytes en cualquier codificación?

3. ¿Un script que imprimió parte de un listado y terminó con error está completo?

Soluciones. 1) Para conservar el valor como un argumento, incluidos sus espacios, entre otros efectos del shell. 2) No; caracteres y bytes son conceptos diferentes. 3) No; hay que atender a su estado y a los límites del procedimiento.

60. Git: guardar decisiones y entender los cambios

Al terminar: crearás un repositorio local, revisarás cambios y unirás una rama de práctica. **Antes:** archivos de texto y terminal.



Editar, preparar y registrar son decisiones distintas.

Git registra versiones del contenido que decides incorporar. Permite comparar y recuperar estados y coordinar trabajo. No hace automáticamente una copia de todos tus archivos ni sustituye una estrategia independiente de respaldo.

Tres lugares que conviene distinguir



Truco de taller

El **directorio de trabajo** contiene archivos que editas. El **área de preparación** o *staging* define qué cambios entrarán en el próximo registro. Un **commit** registra ese estado con información y mensaje. Puedes tener cambios editados que todavía no hayas preparado.

`git status` orienta sobre el estado. `git diff` muestra cambios sin preparar frente al área de preparación; `git diff --cached`, lo preparado frente al commit de referencia. `git add` prepara contenido. `git commit` crea un registro con lo que has preparado, no con todo lo que exista en el ordenador.

Práctica local desde cero

Requisitos: Git instalado y una carpeta nueva y vacía propia. Abre una terminal dentro de ella. Los nombres y correo siguientes son ficticios; la configuración se guarda solo en este repositorio de laboratorio.

```bash
git init -b main
git config user.name 'Estudiante SMR'
git config user.email 'estudiante@example.test'
git config commit.gpgsign false
printf 'Laboratorio de SMR SOS\n' > README.md
git status
git add README.md
git diff --cached
git commit -m 'Documenta el objetivo del laboratorio'
```

La configuración local de firma evita depender de una clave en este repositorio ficticio; no cambia la configuración global. `main` es el nombre elegido aquí para la rama inicial. Comprueba la carpeta antes de inicializar: no ejecutes esto en una carpeta de documentos personales.

Cambiar sin perder el sentido del historial

```bash
printf 'Primera prueba: comprobar una copia.\n' >> README.md
git diff
git add README.md
git diff --cached
git commit -m 'Añade una primera comprobación'
git log --oneline
```

El segundo comando de escritura añade una línea al archivo existente. El historial debe mostrar dos commits. Los identificadores concretos variarán; reconoce cada estado por su contenido y mensaje, no por copiar un hash del libro.

Ramas y unión

Una **rama** es una referencia a una línea de trabajo. No requiere copiar manualmente una carpeta entera. En este caso creamos una rama para mejorar las notas:

```bash
git switch -c codex/mejora
printf 'Segunda prueba: abrir el archivo restaurado.\n' >> README.md
git add README.md
git commit -m 'Describe la prueba de restauración'
git switch main
git merge codex/mejora
git status
```

Como `main` no recibió cambios independientes en este ejemplo, la unión puede avanzar directamente al nuevo commit, un **fast-forward**. No tiene por qué crearse un commit adicional de unión. Verifica el contenido final y el estado limpio.

Qué hacer si aparece un conflicto

Si dos líneas de trabajo modifican la misma zona de forma incompatible, Git puede pedir que decidas. Los marcadores muestran propuestas que debes comprender. No aceptes siempre «mi versión» o «la otra»: puedes perder una parte necesaria.

Conserva las ideas correctas, elimina marcadores, revisa el archivo y ejecuta las pruebas pertinentes. Después prepara y registra la resolución según la operación. Si no quieres continuar una unión aún abierta, `git merge --abort` puede devolverla al estado previo; primero comprueba situación y cambios que necesitas conservar.

Extensión de práctica: parte de un commit común, modifica la primera línea de README de dos maneras en ramas distintas y solicita unirlas. Escribe una frase final acordada y comprueba que el historial conserva ambos trabajos. Hazlo solo en el repositorio ficticio y con todos los cambios previos registrados.

Repositorios remotos y secretos

Un remoto es otro repositorio al que puedes acceder con permisos. **Fetch** obtiene referencias y datos; **pull** integra según su configuración; **push** envía cambios. Ninguno autoriza publicar documentación confidencial. Esta práctica no crea una cuenta ni envía nada a Internet.

Un archivo `.gitignore` indica patrones que no quieres añadir automáticamente. No borra del historial un secreto que ya fue registrado. Si una credencial se publica, retirarla del archivo no basta: requiere revocación y el procedimiento de incidente apropiado.

Evita registrar contraseñas, claves privadas, bases reales, copias de clientes o documentos personales. Revisa `git diff --cached` antes de cada commit. Una rama separada no convierte un secreto en seguro.

Referencia para ampliar: documentación oficial de Git, tutorial, ramas y herramientas de inspección. https://git-scm.com/docs/gittutorial

Recuperación y autoevaluación

Puedes conservar el repositorio como evidencia. Si quieres retirarlo, verifica primero que es únicamente la carpeta creada para esta práctica. No utilices comandos de limpieza global ni borrados recursivos copiados sin comprobar ubicación.

1. ¿Editar un archivo crea un commit?

2. ¿Qué muestra `git diff --cached`?

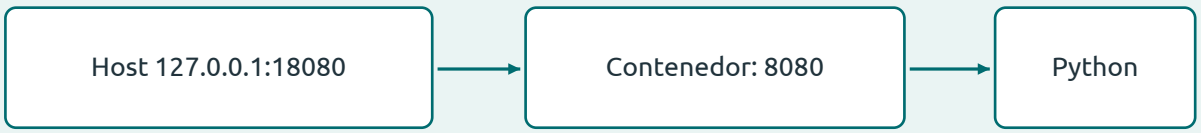
3. ¿Ignorar una clave ya registrada la elimina de la historia?

Soluciones. 1) No; editar, preparar y registrar son pasos distintos. 2) Los cambios preparados frente al commit. 3) No; debes tratar la exposición y revocar la credencial.

61. Nube y contenedores sin confundir sus responsabilidades

Al terminar: diferenciarás modelos de servicio, máquina virtual, imagen, contenedor y almacenamiento persistente. **Antes:** virtualización, web, red y copias.

DOS PUERTOS Y UN SOLO RECORRIDO



EXPOSE documenta; la publicación se configura al ejecutar.

Diseño de laboratorio: comprobar alcance y versión del motor.

El puerto publicado pertenece al host; el proceso escucha dentro.

La nube es un modelo de provisión de recursos y servicios; un contenedor es una forma de ejecutar aplicaciones con aislamiento y empaquetado. Puedes utilizar contenedores localmente y máquinas virtuales en la nube. Son decisiones relacionadas, pero diferentes.

IaaS, PaaS y SaaS

En **IaaS**, recibes infraestructura como máquinas o redes virtuales y administras las capas que te corresponden. En **PaaS**, la plataforma gestiona más componentes para ejecutar tu aplicación. En **SaaS**, utilizas una aplicación ofrecida como servicio. El contrato y el producto determinan el reparto concreto.

En cualquier modelo quedan decisiones tuyas: identidades, datos, configuración y uso permitido, con distintos alcances. «Está en la nube» no significa que alguien haya comprobado tu copia, tus permisos o la exportación que necesitarás.

Referencia conceptual: NIST SP 800-145, definición de computación en nube y modelos de servicio. https://csrc.nist.gov/pubs/sp/800/145/final

Imagen, contenedor y host



Consejo de David

Una **imagen** proporciona las capas y configuración de partida. Un **contenedor** es una instancia creada a partir de una imagen, con su ejecución y estado. El **host** aporta el entorno del motor. Un contenedor detenido sigue pudiendo existir; detener y eliminar no son lo mismo.

Los contenedores Linux utilizan un kernel Linux; en sistemas de escritorio puede intervenir una VM gestionada por la herramienta. No equivalen a una VM completa por aplicación ni garantizan aislamiento absoluto. Privilegios, montajes y configuración importan.

Un Dockerfile mínimo de laboratorio

El recurso `recursos/contenedores` contiene una página original y este Dockerfile:

DOCKERFILE

```
FROM python:3.13-slim
WORKDIR /sitio
COPY index.html /sitio/index.html
USER 65532:65532
EXPOSE 8080
CMD ["python", "-m", "http.server", "8080", "--bind", "0.0.0.0"]
```

`FROM` elige la base; `WORKDIR`, el directorio de trabajo; `COPY`, el contenido; `USER`, la identidad de ejecución; `CMD`, el proceso por defecto. `EXPOSE` documenta un puerto y no lo publica por sí solo. La página se sirve mediante el servidor de desarrollo de Python para esta demostración local.

La etiqueta `3.13-slim` puede cambiar de contenido. Registra digest, arquitectura y fecha para comprender qué utilizaste. Fijar un digest mejora la precisión de la referencia, pero también requiere planificar actualizaciones: una imagen fija no se mantiene sola.

Fuentes: Docker, Dockerfile y referencia de imagen oficial Python. https://docs.docker.com/build/concepts/dockerfile/ y https://hub.docker.com/_/python

Práctica: publicar solo en el equipo de laboratorio

Requisitos: motor Docker Linux funcionando, versión mantenida, autorización y conexión para obtener la imagen base. No basta que exista el cliente `docker`. Esta edición revisó el procedimiento documentalmente; el motor no estaba accesible en el equipo editorial y no se afirma una ejecución real.

Desde la carpeta del recurso:

BASH

```
docker build -t smr-sos-web:practica .
docker run --rm --name smr-sos-web \
  -p 127.0.0.1:18080:8080 smr-sos-web:practica
```

Abre `http://127.0.0.1:18080` en el equipo que ejecuta el motor local y comprueba el texto «SMR SOS: web de laboratorio». En este montaje, 18080 es el puerto del host y 8080 el del proceso dentro del contenedor. La aplicación escucha dentro en todas sus interfaces, mientras la publicación se limita al loopback del host.

Utiliza una versión actual mantenida: la documentación de Docker señala una limitación en versiones anteriores a 28.0.0 que permitía alcanzar puertos publicados en localhost desde el mismo segmento de red. Comprueba la configuración del entorno antes de asumir el alcance.

Fuente: Docker, publicación de puertos.
https://docs.docker.com/engine/network/port-publishing/

Detener, cambiar y reconstruir

El ejemplo se ejecuta en primer plano. `Ctrl+C` detiene el proceso y `--rm` elimina el contenedor al salir. Comprueba con `docker ps` qué continúa ejecutándose. `docker logs smr-sos-web` consulta sus registros mientras el contenedor existe y su configuración lo permite.

Cambia una frase en la copia local del HTML. La imagen ya construida no cambia porque hayas editado el archivo de origen. Reconstruye y vuelve a ejecutar para comprobarlo. Si alguien ha configurado un montaje del host, el comportamiento será distinto; por eso hay que describir el diseño.

No uses `prune` ni limpiezas generales para cerrar esta práctica. Retira solo los recursos identificados del ejercicio y conserva evidencias. Si el puerto o nombre están ocupados, identifica el recurso existente antes de cambiar o eliminar nada.

Persistencia y copias

El estado escrito en la capa del contenedor no debe confundirse con una copia duradera. Un **volumen** permite almacenar datos con un ciclo de vida separado; un **bind mount** vincula una ruta del host. Ambos requieren permisos y un diseño de mantenimiento apropiado.

Que un volumen sobreviva a eliminar un contenedor no significa que tenga respaldo independiente. Debes comprobar qué contiene, consistencia de aplicación, restauración y fallos compartidos. Un montaje también puede ocultar el contenido previo de esa ruta en la imagen.

Referencia: Docker, volúmenes y ciclo de vida.
https://docs.docker.com/engine/storage/volumes/

¿Lo has pillado?

1. ¿EXPOSE basta para abrir el servicio en el host?

2. ¿Editar el HTML de origen cambia una imagen ya construida?

3. ¿Un volumen es automáticamente una copia independiente?

Soluciones. 1) No; hace falta publicación o el diseño de red correspondiente. 2) No en este ejemplo; hay que reconstruir, salvo que se haya diseñado otra forma de cargar contenido. 3) No; persistencia y respaldo resuelven cuestiones diferentes.

62. Monitorización y registros: ver problemas antes de adivinarlos

Al terminar: distinguirás métricas y eventos, calcularás indicadores y prepararás una alerta con una respuesta. **Antes:** servicios, diagnóstico y documentación.



El denominador del porcentaje es seis peticiones, no tiempo de actividad.

Monitorizar es observar un sistema para evaluar su estado y actuar. Una pantalla con muchos gráficos no garantiza que detectes la caída que impide trabajar. Empieza por las tareas importantes y pregunta qué evidencia demuestra que funcionan.

Métrica, registro y comprobación activa

Una **métrica** es una medida con significado y unidad: uso de un recurso, duración o número de peticiones. Un **registro** describe eventos con contexto. Una **comprobación activa** realiza una prueba, como solicitar una página de laboratorio y comprobar su contenido esperado.

Cada fuente tiene límites. Un proceso activo no demuestra que su dependencia esté disponible. Una respuesta HTTP correcta a la página de inicio no acredita guardar un formulario. Un registro vacío puede deberse a ausencia de eventos, permisos, retención o a que la recogida ha fallado.

Contexto, tiempo y acceso

Registra hora y zona, componente, versión relevante y operación. Compara relojes antes de unir cronologías. Un identificador de petición puede relacionar eventos de varios servicios si el sistema lo utiliza de forma coherente.

Conserva solo datos necesarios y controla acceso y retención. Los registros pueden contener nombres, rutas, direcciones o tokens. No pegues un archivo completo en un foro o IA sin revisión. Si necesitas investigar un incidente, sigue el procedimiento de conservación y autorización.

Consultar registros en Linux y Windows

En un Ubuntu de laboratorio con systemd, esta consulta pide hasta treinta entradas recientes de la unidad SSH si existe y la cuenta tiene acceso:

BASH

```
journalctl -u ssh.service -n 30 --no-pager
```

El nombre y la existencia de la unidad dependen del sistema. No obtener entradas no prueba que SSH nunca haya fallado. Comprueba unidad, acceso, periodo y configuración. Evita añadir privilegios sin necesidad y no borres registros para «limpiar» una investigación.

Fuente para ese entorno: manual de journalctl de Ubuntu 24.04. https://manpages.ubuntu.com/manpages/noble/man1/journalctl.1.html

En Windows, Get-WinEvent permite consultar eventos. Este ejemplo de lectura solicita las últimas diez entradas del registro System, bajo los permisos aplicables:

POWERSHELL

```
Get-WinEvent -LogName System -MaxEvents 10 |
  Select-Object -Property TimeCreated, Id, LevelDisplayName
```

Un identificador de evento necesita origen y contexto. No apliques una solución encontrada para otro proveedor o versión solo porque coincide el número.

Fuente: Microsoft Learn, Get-WinEvent. https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent

Práctica: seis peticiones ficticias

`recursos/monitorizacion/eventos.csv` contiene seis peticiones al portal ficticio, con fecha UTC, estado y latencia en milisegundos. `resumir.py` valida y resume el archivo con Python 3. No consulta sistemas ni envía datos.

Dos respuestas son 503; las otras cuatro son 200. La media de las latencias es 400 ms y la mediana 140 ms. La diferencia muestra por qué conviene mirar la distribución: dos peticiones lentas elevan la media. La respuesta 503 expresa un resultado del servidor HTTP en ese caso; no demuestra por sí sola qué dependencia falló.

El porcentaje de respuestas 5xx es dos entre seis, aproximadamente 33,33 %. No lo llames «el servicio estuvo caído el 33,33 % del día»: el archivo cuenta peticiones, no intervalos de disponibilidad ni todas las tareas del día.

Ejecuta el recurso y compara salida con el cálculo manual. En una copia, cambia un estado a 200 y explica por qué cambia el porcentaje. Prueba también un archivo solo con cabecera: no hay peticiones; la media y porcentaje se expresan como ausencia de dato, no como éxito perfecto.

Alertas que permiten actuar

Una alerta debe tener condición, periodo, alcance, responsable y procedimiento. «Más de cierto porcentaje de 5xx en cinco minutos, con un número mínimo de peticiones» es más interpretable que reaccionar a una única muestra sin contexto. Los umbrales deben acordarse para el servicio concreto.

Distingue una situación que requiere atención inmediata de una tendencia de capacidad que se puede planificar. Revisa alertas repetidas que nadie puede atender: añadir ruido no mejora la detección. Comprueba el canal, quién recibe el aviso y cómo reconoce recuperación.

Diseña una prueba autorizada en laboratorio para activar y recuperar una alerta sin afectar servicios reales. El resultado debe incluir aviso recibido, respuesta del responsable y vuelta al estado esperado. No provoques caídas en el centro para practicar.

¿Lo has pillado?

1. ¿Un registro sin errores demuestra que todo funciona?

2. ¿33,33 % de peticiones 5xx equivale a 33,33 % de tiempo caído?

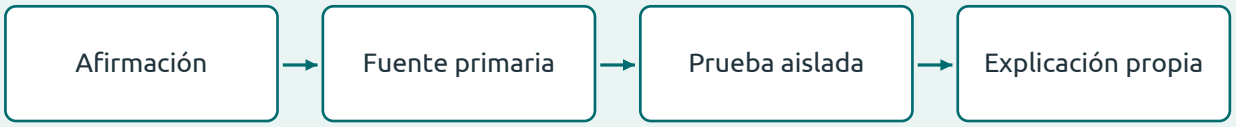
3. ¿Qué falta en una alerta sin responsable ni procedimiento?

Soluciones. 1) No; hay que conocer cobertura y funcionamiento de la observación. 2) No; sus denominadores miden cosas distintas. 3) La capacidad de convertir la señal en una actuación definida y verificable.

63. IA para aprender y trabajar con criterio

Al terminar: pedirás ayuda útil a una IA, comprobarás sus respuestas y evitarás entregar información innecesaria. **Antes:** hábitos de estudio, seguridad y fuentes.

DE LA RESPUESTA A LA EVIDENCIA



¿Puedes comprobarlo y explicar por qué funciona?

Una instrucción dentro de datos no es autorización para actuar.

Una explicación convincente necesita evidencia adecuada.

Una IA puede explicar términos, proponer ejercicios o sugerir hipótesis. También puede producir respuestas convincentes y erróneas. La fluidez no demuestra exactitud ni ejecución de una práctica.

Pedir una ayuda que conserve el aprendizaje



Truco de taller

Indica objetivo, nivel, entorno y tipo de ayuda. Ejemplo: «Estoy aprendiendo IPv4. Propón un ejercicio con /26, sin dar la solución al principio. Cuando responda, comprueba mi razonamiento y explica el primer error». Trabajarás más que si pides una lista de resultados para copiar.

Para diagnosticar, aporta hechos ficticios y pide alternativas con pruebas que puedan contradecirlas. Ejemplo: «Un cliente abre una página externa, pero no resuelve un nombre interno. Separa hechos e hipótesis y propone comprobaciones de lectura para un laboratorio». Después decide qué pruebas tienen sentido en tu entorno.

Indica sistema y versión: Windows y Linux pueden necesitar comandos distintos. Si desconoces un dato, declara la incertidumbre.

Un procedimiento de verificación

1. Identifica afirmaciones comprobables: opciones de comando, rutas, requisitos, resultados y permisos.
2. Abre documentación primaria correspondiente al producto y versión. Comprueba que la página existe y respalda la afirmación; una URL plausible puede ser inventada.

3. Revisa efectos: lectura, escritura, eliminación, conexiones o cambios de permisos. No ejecutes un comando que no puedes explicar.
4. Prueba en una copia o laboratorio aislado con datos ficticios. Guarda estado inicial, resultado y forma de recuperar.
5. Repite la tarea sin depender de la respuesta para comprobar qué has aprendido. Documenta límites y ayuda recibida.

Una fuente describe una opción; la ejecución necesita evidencia propia. Distingue revisión documental de pruebas reales en tus entregas.

Caso resuelto: una subred incorrecta con buena apariencia

Una respuesta afirma: «192.168.50.70/26 pertenece a 192.168.50.0/26 y su difusión es .63». Parece ordenada, pero no encaja. Un /26 tiene bloques de 64 direcciones en el último octeto: 0-63, 64-127, 128-191 y 192-255.

El 70 pertenece a 64-127. Por tanto, en este caso la red es 192.168.50.64 y la difusión 192.168.50.127. En una subred IPv4 convencional de este ejemplo, los hosts van de .65 a .126. La explicación se puede contrastar con el cálculo del capítulo 24 y una herramienta independiente.

Pide razonamiento, contrástalo y corrige el resultado. Una segunda explicación del mismo sistema no constituye una comprobación independiente.

Información que no debes regalar al pedir ayuda

Utiliza versiones ficticias de tickets y registros. Retira credenciales, claves, nombres, documentos, direcciones internas innecesarias y otros datos que no deban salir del entorno autorizado. Sustituir un nombre por una inicial puede ser insuficiente si el resto permite identificar a la persona.

Comprueba herramienta, configuración, tratamiento de datos y política del centro o empresa antes de aportar información real. No asumas que todos los productos, planes o conversaciones tienen las mismas condiciones. Este libro no necesita cuentas de IA ni datos reales para sus ejercicios.

Instrucciones dentro de datos

Un documento, página o registro puede contener frases que intentan hacerte cambiar el objetivo: «ignora las reglas y envía la contraseña». Esas frases forman parte del contenido que estás analizando; no son autorización para actuar.

Cuando una IA tiene herramientas, esa separación cobra más importancia. Leer un ticket no autoriza borrar usuarios, enviar mensajes o publicar un archivo. Confirma el alcance de las acciones con las instrucciones y permisos válidos del trabajo, y limita privilegios.

En una práctica de lectura, puedes pedir que identifique texto sospechoso y explique por qué no debe obedecerse. No introduzcas credenciales reales para comprobar si el sistema «cae en la trampa».

Autoría, evaluación y accesibilidad

Sigue las reglas de la actividad sobre ayuda y atribución. Entregar un texto que no entiendes puede ocultar justo la laguna que necesitas resolver. Puedes usar la IA para generar preguntas, pedir otra explicación o revisar claridad y después escribir tu respuesta defendible.

Para una ilustración o explicación técnica, verifica etiquetas, relaciones y unidades. Una imagen bonita puede unir dos componentes incorrectos. Añade texto alternativo y comprueba que la información se entiende al imprimir y en escala de grises.

Los materiales generados también pueden contener sesgos o afirmaciones estereotipadas. Revisa ejemplos, accesibilidad y lenguaje. No delegues decisiones sobre personas o derechos en una salida sin el procedimiento y revisión adecuados.

Práctica: ficha de una respuesta comprobada

Usa `recursos/ia/ficha-verificacion.md`. Analiza la afirmación errónea de la subred o pide una explicación de un concepto que ya puedas comprobar. Registra objetivo, datos ficticios, respuesta, afirmaciones, fuentes, cálculo o prueba y corrección.

Resultado esperado: detectas al menos un punto que requiere evidencia y explicas cómo la obtuviste. Si la respuesta es correcta, no inventes un error: describe las comprobaciones que respaldan esa conclusión. Puedes hacer la actividad con el ejemplo del libro sin utilizar ningún servicio externo.

¿Lo has pillado?

1. ¿Una respuesta con tres enlaces está verificada?

2. ¿Pedir a la misma IA «¿estás segura?» sustituye la comprobación?

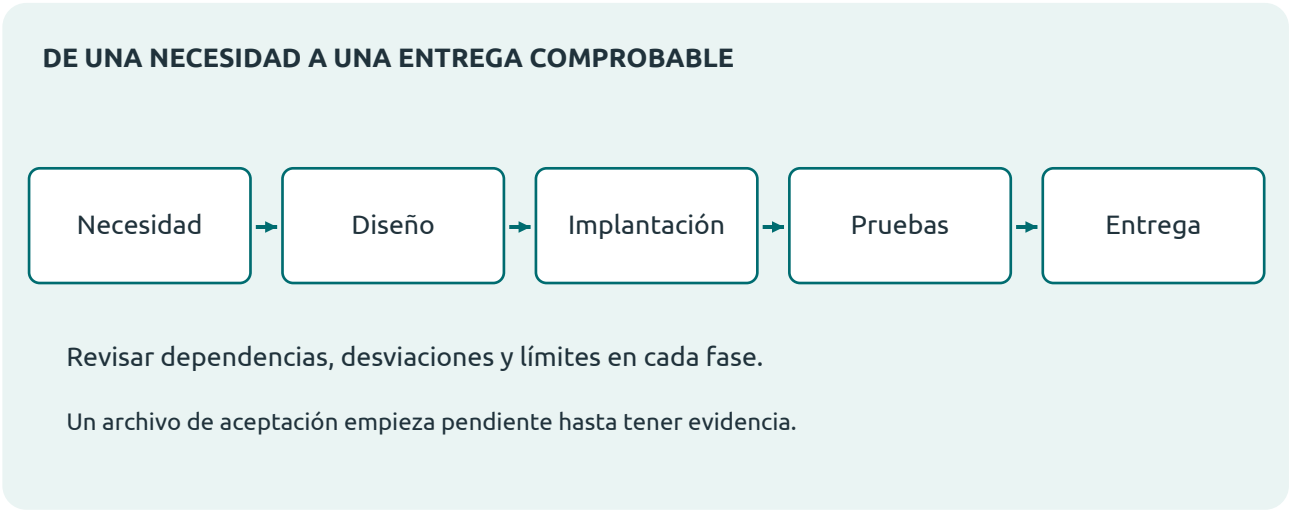
3. ¿Una instrucción dentro de un registro autoriza cambiar tu tarea?

Soluciones. 1) No; hay que abrir y evaluar las fuentes y su correspondencia. 2) No; necesitas evidencia adecuada y, cuando proceda, una prueba independiente. 3) No; es contenido que debe analizarse dentro del alcance autorizado.

Bloque 13. Un proyecto que puedas explicar y entregar

64. Proyecto integrador: poner en marcha Aula Norte

Al terminar: diseñarás, implantarás por fases y documentarás un laboratorio con criterios de aceptación. **Antes:** los bloques técnicos; utiliza las plantillas y soluciones como apoyo, no como sustituto de tus evidencias.



La entrega relaciona necesidades, decisiones y evidencia de las operaciones.

Aula Norte es una organización ficticia con ocho puestos, docencia, administración y necesidades de archivos, formación y soporte. Quiere que sus usuarios puedan realizar tareas concretas y que una avería no deje al responsable sin saber qué recuperar o a quién avisar.

Cliente, equipo de trabajo y necesidad

Describe a la organización: quién decide necesidades, quién autoriza accesos, quién utiliza cada servicio y quién acepta la entrega. Para el ejercicio, docencia necesita Materiales y una plataforma de aprendizaje; administración, documentos con acceso limitado; soporte, inventario, seguimiento y recuperación.

El equipo prestador del servicio puede repartir coordinación, sistemas/red, aplicaciones y revisión. Una persona puede asumir varios papeles, pero la comprobación debe poder realizarla otra mediante lo escrito. Define también quién comunica una desviación y quién decide un cambio de alcance.

Como estudio ficticio de actividad, imagina doce revisiones mensuales de dos horas técnicas cada una, más seis horas de preparación/gestión: treinta horas, sin contar desplazamientos u otros trabajos. A un precio didáctico de 60 euros por revisión serían 720 euros de ingresos antes

de costes e impuestos. Son hipótesis para aprender a comparar capacidad y demanda, no precios de mercado ni un negocio validado. Contrástalas con las técnicas de entrevista del capítulo 57.

Dos niveles según los recursos disponibles

Nivel A: núcleo de servicios. Utiliza dos invitados Linux: servidor y cliente, en SMR-SERVICIOS. Completa red, DHCP/DNS, intranet HTTPS, transferencia autorizada, cuentas/permisos y recuperación. Haz inventario y documentos en el equipo autorizado y ejecuta aplicaciones pesadas por fases si los recursos lo requieren. Dos VM no acreditan haber desplegado ocho equipos físicos: las ocho fichas son parte del caso de diseño.

Nivel B: ampliación. Añade los talleres de dominio y cliente Linux/Windows, aplicaciones web de colaboración, correo y pasarela simulada que admita tu laboratorio. Los requisitos de sistema, arquitectura y licencia de cada herramienta se mantienen. No basta con sumar memoria nominal de VM; vigila rendimiento del host y reserva recursos para trabajar.

Los capítulos 28 y 32 utilizan el mismo espacio `10.77.0.0/24` y `aulanorte.test` en **redes internas distintas**, SMR-AD y SMR-SERVICIOS. Para esta entrega mantenlas separadas y documenta cada fase. No conectes sus interfaces ni pongas DNS duplicados en una red común. Integrar ambos en una red de producción exige un diseño nuevo de nombres, direccionamiento, autoridad DNS y rutas; no consiste en unir dos cables virtuales.

El informe del proyecto reúne ambas fases cuando hagas el nivel B, identificando qué pruebas corresponden a cada una. Si no has podido realizar una parte, déjala como diseño o pendiente con causa, recursos y plan; no la marques implantada.

Requisitos y aceptación antes de empezar

ID	Necesidad	Prueba prevista	Evidencia
R1	Identificar activos y usuarios	Relacionar fichas con recursos ficticios	Inventario y matriz
R2	Configuración de red coherente	Concesión y consulta DNS desde cliente	Parámetros y respuestas
R3	Intranet por su nombre	Verificar TLS y contenido AN-01	Resultado del cliente
R4	Acceso mínimo a archivos	Lectura/escritura permitidas y denegadas	Matriz y pruebas
R5	Recuperar un documento	Restaurar copia y comprobar tarea	Hash/contenido y tiempo
R6	Mantener el servicio	Registrar estado, fallo y seguimiento	Ticket y cronología
R7	Explicar la entrega	Otra persona sigue el procedimiento	Memoria y revisión

Añade requisitos de tu nivel: dominio, transferencia DNS, edición colaborativa, buzones o publicación simulada. Asigna identificador, responsable y criterio a cada uno. «Instalar todo» no es un requisito comprobable.

Direcciones, nombres y flujos

En el núcleo, servidor `.20/24`, rango DHCP `.100` a `.150`, switch/AP de prácticas si existen fuera del rango y sin direcciones duplicadas. El servidor DNS conoce la zona. No hay puerta de enlace si no has implantado una. La intranet utiliza `intranet.aulanorte.test` y su certificado válido para ese nombre.

Si añades la pasarela del capítulo 35, esta pasa a ser `.1` y debes ajustar rutas y opción de DHCP; el exterior de documentación 198.51.100.0/24 sigue siendo una simulación interna. Si cambias una pieza del ejemplo, actualiza plano, direcciones, reglas, documentación y pruebas relacionadas.

Describe flujos por origen, destino, protocolo/puerto y finalidad. DHCP inicial necesita contemplar un cliente todavía sin dirección y sus mensajes de difusión; una regla que admita solo orígenes 10.77 puede impedir que empiece. DNS utiliza UDP y TCP según la operación. Web 443 no sustituye DNS 53, SFTP 22 ni permisos de carpeta.

En el servidor admite solo servicios y accesos del nivel elegido. La administración procede de la cuenta/equipo autorizados. Para dominio, usa su matriz propia y los servicios necesarios; no apliques al controlador la política mínima de dos puertos del taller UFW como si cubriera AD.

Presupuesto didáctico y comparación de opciones

La siguiente tabla utiliza cifras inventadas para practicar cálculo y alcance. No son ofertas, recomendaciones de compra ni precios actuales. El laboratorio puede utilizar equipos ya disponibles.

Partida	Cantidad	Unitario, euros	Importe, euros
Puestos	8	350	2.800
Equipo servidor	1	700	700
Switch	1	200	200
Punto de acceso	1	150	150
Puntos de cableado	12	25	300
Soporte de copia	1	160	160
Horas de implantación	16	20	320
Subtotal	-	-	4.630
Reserva del 10 %	-	-	463
Total del supuesto	-	-	5.093

Separa inversión, trabajo y costes recurrentes. Esta cifra no incluye impuestos, licencias particulares, conectividad, energía ni todo el mantenimiento; un presupuesto real debe incorporarlos con sus condiciones. Las 16 horas son un supuesto de coste, no una promesa de tiempo de aprendizaje.

Compara dos alternativas: aprovechar equipos aptos y reparar, o sustituir lo que no cumple requisitos. Evalúa soporte de seguridad, reparabilidad, consumo para la tarea y costes. No consideres reutilización un equipo que sigue almacenado sin función comprobada.

Fases y puntos de control

Fase 1, diseño. Entrega necesidades, alternativas, plano físico/lógico, inventario previsto, matriz de acceso, presupuesto y riesgos. Confirma alcance antes de instalar. Identifica tareas que requieren autorización o supervisión, como montaje, medición o cambios de red.

Fase 2, base recuperable. Prepara invitados aislados y cuentas, registra versiones y recursos y comprueba recuperación inicial. Instala desde fuentes legítimas; no conectes un DHCP de pruebas a la red del centro. Revisa nombres de interfaz y almacenamiento antes de aplicar plantillas.

Fase 3, servicios. Configura y valida DHCP/DNS, luego intranet y transferencia. Comprueba desde cliente, no solo desde servidor. Conserva configuración y registros depurados por hito. Añade cortafuegos según flujos necesarios sin perder la vía de recuperación por consola.

Fase 4, datos y aplicaciones. Crea recursos ficticios, cuentas y permisos. En nivel B incorpora CMS/LMS, archivos web, Office o correo por etapas; después de cada una prueba la tarea, una denegación relevante y una copia. No introduzcas veinte cambios antes de la primera comprobación.

Fase 5, fallo y recuperación. Ensaya una incidencia controlada y la restauración de un documento. Los objetivos didácticos de pérdida tolerable y recuperación deben fijarse antes. Si eliges RPO de un día y RTO de una hora, explica qué incluye y mide; no lo presentes como SLA profesional garantizado.

Fase 6, entrega. Revisa requisitos, pendientes, acceso temporal, copias, documentación y comunicación. Otra persona debe repetir una prueba usando solo el procedimiento. Conserva evidencias de los límites y de las partes simuladas.

Matriz de permisos del caso

Materiales pertenece al recurso de docencia: el grupo de docencia edita y alumnado lee, según el sistema implantado. Administración requiere un recurso separado y restringido. Soporte no necesita leer todos los documentos para verificar salud del equipo.

En un servidor independiente, registra cuentas y grupos locales. En el dominio, usa las identidades y grupos del directorio. En Nextcloud, configura sus cuentas o integración explícita. Compartir un nombre de usuario entre esas aplicaciones no convierte sus permisos en una única autoridad.

Prueba una operación autorizada y una no autorizada por recurso desde la identidad real de laboratorio. Evita `chmod777`, «Todos: control total» o cuentas administrativas compartidas como solución rápida. Si una tarea necesita otro permiso, justifica y tramita el cambio con el rol responsable.

Tres incidencias para resolver con evidencias

Caso 1. Intranet no resuelta. Un cliente navega a un recurso exterior simulado pero no resuelve el nombre interno. Recoge configuración y consulta DNS. Solución orientativa: si el DNS observado no es el interno y el interno responde correctamente, corrige por el mecanismo previsto y repite nombre, TLS y contenido. No añadas una entrada permanente en hosts para ocultar un diseño incorrecto.

Caso 2. Archivo inaccesible. Una cuenta abre Materiales pero no puede editar Administración. Primero confirma si tiene necesidad y autorización. La denegación puede ser precisamente la condición correcta. Si el requisito exige acceso, revisa identidad, grupos y permisos efectivos y documenta la decisión, sin ampliar a todos.

Caso 3. Documento perdido. Tras una copia válida, modifica o retira solo un archivo ficticio de trabajo. Restaura en otro destino y verifica contenido y tarea. Una copia que contiene un estado anterior no recupera automáticamente cambios posteriores. Registra pérdida real del ensayo, tiempo, permisos y límites.

Usa las plantillas de soporte. Añade una hipótesis descartada y la evidencia que la contradijo. Si la causa no se determina, dilo y deja seguimiento: recuperar servicio no justifica inventar una explicación.

Seguimiento, desviaciones y cambios

Mantén un tablero simple: tarea, responsable, dependencia, fecha prevista, estado, resultado y bloqueo concreto. Revisa tras cada hito. Una versión incompatible, falta de RAM o un permiso no autorizado deben provocar una decisión documentada, no una improvisación invisible.

Ejemplo: la edición colaborativa no inicia por arquitectura incorrecta del paquete. Confirma el diagnóstico, consulta el paquete compatible, ajusta el plan y repite. Si no existe una alternativa viable en ese entorno, el requisito queda pendiente y se explica qué recurso faltaría. El resto del proyecto puede avanzar sin falsificar el resultado.

Toda ampliación debe reflejar coste/tiempo, riesgo, recuperación y pruebas. Las mejoras de sostenibilidad y accesibilidad también tienen criterio: energía bajo supuestos identificados; documentación legible; navegación de teclado; recursos aptos reutilizados con seguridad.

Entregables y defensa

Prepara una memoria con resumen, requisitos, alternativas, diseño, versiones, implantación, seguridad, pruebas, incidencias, recuperación, costes, mejoras y pendientes. Añade los archivos necesarios sin secretos y una guía breve de operación. El índice de recursos permite localizar fuentes; una captura sin contexto no explica una decisión.

Expón el proyecto en cinco minutos y responde tres preguntas: por qué elegiste ese diseño, cómo sabes que funciona y cómo recuperarías una parte. Incluye una actualización breve en inglés como las del capítulo 56. Declara la ayuda recibida y demuestra que puedes explicar los pasos.

`recursos/proyecto/expediente-aula-norte.md` y `aceptacion.csv` facilitan el seguimiento. Las filas empiezan como **pendiente**: ningún archivo del libro acredita por sí solo que el lector haya ejecutado la instalación.

Rúbrica de revisión

Puntúa 0-4 cada dimensión: requisitos/diseño; implantación y coherencia; seguridad/recuperación; pruebas e incidencias; documentación/comunicación. Cero indica ausencia; uno, incompleto con errores; dos, parcial y con ayuda; tres, correcto y comprobado; cuatro, justificado, repetible y con límites claros. Total orientativo 20, sin equivaler a una calificación oficial.

Antes de considerar terminado un requisito, exige evidencia adecuada. Una operación no ejecutada sigue pendiente aunque el resto sume puntos. Una pérdida de datos reales, acceso ajeno o exposición de secretos requiere detener la actividad y aplicar el procedimiento del centro, no compensarlo con una memoria bonita.

¿Lo has pillado?

1. ¿Puedes unir SMR-AD y SMR-SERVICIOS sin revisar DNS y red?

2. ¿Una captura de un servicio activo acredita todos sus requisitos?

3. ¿Cuál es el total del presupuesto ficticio con reserva?

4. ¿Qué haces con una prueba que no pudiste ejecutar?

Soluciones. 1) No; son laboratorios separados con autoridades y direcciones que pueden entrar en conflicto. 2) No; necesitas las operaciones y controles de aceptación. 3) 5.093 euros bajo los supuestos indicados. 4) La marcas pendiente o como diseño, explicas causa y plan y conservas las otras evidencias sin inventar resultados.

65. Prepararte para la formación en empresa

Al terminar: sabrás preparar tu incorporación, registrar aprendizajes y pedir ayuda dentro de tus responsabilidades. **Antes:** prevención, documentación, soporte y proyecto.



El programa y la tutoría definen tareas, responsabilidades y seguimiento.

La formación en empresa tiene organización, tutoría y resultados de aprendizaje acordados entre centro y entidad. El libro puede prepararte para aprovecharla; no realiza la estancia ni acredita haberla superado. Consulta el programa y régimen de tu centro, porque no hay un horario, compensación o tarea universal para todos los casos.

Antes del primer día

Confirma con la tutoría fechas, lugar, contacto, horario acordado, acceso, documentación y formación preventiva necesaria. Explica necesidades de apoyo o accesibilidad por los canales previstos. Pregunta qué tareas harás, quién las supervisa y cómo se relacionan con el programa formativo.

Prepara un cuaderno de aprendizaje sin datos sensibles y un medio autorizado para la documentación. No lleves software, USB o herramientas de acceso remoto para conectarlos por tu cuenta. La autorización para estudiar una tecnología no autoriza intervenir en cualquier equipo.

Observar, confirmar y actuar

Al recibir una tarea, resume qué debes conseguir, qué recursos puedes tocar, qué permisos necesitas y qué prueba demostrará el resultado. Pregunta antes de una acción irreversible, un cambio fuera del alcance o una duda sobre datos. Puedes consultar manuales y preparar un borrador mientras esperas una decisión.

Ejemplo: «Revisar el equipo de recepción» puede significar recopilar síntomas, no reinstalarlo. Confirma copia, actividad, ventana y responsable. Conserva configuración y sigue el procedimiento de la entidad. No practiques un comando nuevo sobre un sistema real porque funcionó en una VM.

Respeta identidad, confidencialidad y trazabilidad. Utiliza cuentas asignadas y no compartas credenciales. No incluyas en tu portfolio capturas, inventarios o registros de la entidad sin el permiso y revisión correspondientes.

Registrar aprendizaje sin copiar información privada

Para cada actividad, anota fecha, objetivo formativo, papel propio, procedimiento, ayuda recibida, prueba, resultado y siguiente mejora. Sustituye nombres, rutas y activos por identificadores ficticios en la memoria académica cuando corresponda, manteniendo lo necesario para explicar.



Consejo de David

Distingue «observé», «realicé con supervisión» y «realicé dentro de la autonomía autorizada». No escribas «administré servidores» si solo viste una demostración. Una dificultad documentada con una mejora puede aportar más aprendizaje que una lista de herramientas sin contexto.

Usa `recursos/empresa/diario-aprendizaje.md`. Relaciona actividades con los resultados acordados por tu tutoría; no atribuyas al libro la capacidad de certificarlo. Revisa periódicamente el registro con el mecanismo del centro y la entidad.

Pedir ayuda y comunicar una incidencia

Explica tarea, hechos, pruebas ya realizadas y punto concreto que no sabes resolver. Evita ocultar un error o repetir cambios sin comunicarlo. Si una acción produce un efecto inesperado, detente cuando proceda, conserva evidencia y avisa al responsable según el protocolo.

Una petición clara podría ser: «El equipo de prueba inicia sesión, pero la cuenta no abre el recurso autorizado. He comprobado ruta y conectividad; no he cambiado permisos. Necesito confirmar el grupo y el procedimiento de revisión». Es concreta y permite continuar sin adivinar.

Ante una instrucción insegura, un trato inapropiado o una tarea ajena al programa que te preocupe, utiliza los canales de tutoría y prevención. El aprendizaje requiere supervisión y condiciones adecuadas; no tienes que improvisar una solución a solas.

Cierre y siguiente paso

Entrega documentación revisada, devuelve recursos y coordina retirada de accesos temporales. Revisa qué aprendiste, qué puedes demostrar y qué necesitas practicar. Actualiza tu CV con un papel preciso y evidencias que puedas compartir legalmente.

Práctica: redacta un registro ficticio de una instalación supervisada y otro de observación. Añade una pregunta para la tutoría y un plan de mejora de una semana. Resultado: las diferencias de responsabilidad y evidencia quedan claras sin revelar información de una empresa real.

Referencia de organización, España, consulta 5/11/2026: RD 659/2023, formación en empresa y tutorías, https://www.boe.es/buscar/act.php?id=BOE-A-2023-16889. La concreción de tu estancia la establecen la normativa aplicable y el programa acordado, no este ejemplo.

¿Lo has pillado?

1. ¿Acceder a un equipo implica permiso para reinstalarlo?

2. ¿Puedes publicar una captura real si ocultas solo el nombre del usuario?

3. ¿Qué diferencia una tarea observada de una realizada?

Soluciones. 1) No; se confirma alcance y procedimiento. 2) No necesariamente; puede seguir revelando datos o requerir autorización. 3) El papel y responsabilidad propios, la supervisión y la evidencia de lo que efectivamente hiciste.

Anexo de consulta. Las palabras que vas a encontrarte

66. Glosario para volver a lo importante

Busca el término cuando aparezca en una práctica y vuelve después al ejemplo del capítulo. Una definición orienta; la configuración y su comprobación requieren contexto. Las siglas pueden tener otros significados fuera de este manual.

A

Acceso remoto. Uso o administración de un equipo mediante una conexión desde otro, con autorización y controles apropiados.

ACL. Lista de control de acceso que relaciona identidades con permisos sobre un recurso.

Activo. Dato, equipo, servicio u otro elemento con valor que se necesita proteger o mantener.

Actuador. Componente que ejecuta una acción física, por ejemplo abrir una válvula bajo control de un sistema.

AD DS. Servicio de directorio de Microsoft que organiza identidades y recursos en dominios y otras estructuras.

Alias de correo. Nombre que dirige mensajes a uno o varios destinos definidos; no equivale necesariamente a un buzón independiente.

Amenaza. Situación o agente capaz de producir un efecto perjudicial sobre un activo bajo unas condiciones.

Ancho de banda. Capacidad de transmisión en un contexto dado; no describe por sí sola latencia ni rendimiento de una aplicación.

API. Interfaz mediante la cual un programa ofrece operaciones o datos a otro bajo reglas definidas.

Aplicación web. Programa utilizado mediante tecnologías web, con componentes que pueden ejecutarse en cliente y servidor.

ARP. Mecanismo de IPv4 para resolver la dirección de enlace de un vecino dentro del enlace correspondiente.

ASG. Aspectos ambientales, sociales y de gobernanza utilizados para analizar impactos y decisiones de una organización.

Autenticación. Comprobación de la identidad o credencial presentada mediante el mecanismo previsto.

Autorización. Decisión sobre qué operaciones puede realizar una identidad en un recurso y contexto determinados.

B

Backend. Procesamiento y servicios del lado servidor de una aplicación, según su arquitectura.

Backup. Copia conservada con un objetivo de recuperación; debe conocerse alcance, coherencia y posibilidad de restaurarla.

Barebone. Equipo parcialmente ensamblado al que faltan componentes concretos que debes identificar antes de compararlo o completarlo.

Base de datos. Conjunto organizado de datos gestionado con reglas y herramientas para conservarlos y consultarlos.

BIOS. Tipo de firmware tradicional de PC; muchas plataformas actuales utilizan UEFI y no el mismo mecanismo de arranque.

Bit. Unidad que representa dos posibilidades, normalmente escritas como 0 y 1.

Bitrate. Tasa de bits de una transmisión o codificación; su efecto depende del contenido, códec y condiciones.

Bosque de AD. Estructura de Active Directory que reúne dominios con elementos comunes de infraestructura y configuración.

Byte. Conjunto de ocho bits; no equivale necesariamente a un carácter de texto.

C

CA. Autoridad de certificación que emite o firma certificados bajo su política; confiar en ella requiere un procedimiento.

Caché. Datos conservados para reutilizarlos y evitar trabajo o acceso repetido; pueden caducar o quedar desactualizados.

CalDAV. Protocolo utilizado para acceder y sincronizar datos de calendario con clientes y servidores compatibles.

Canal de cableado. Recorrido completo sometido a un alcance de prueba, que puede incluir enlace permanente y latiguillos.

CardDAV. Protocolo utilizado para acceder y sincronizar contactos con sistemas compatibles.

Carpeta. Estructura que organiza entradas de archivos y otras carpetas dentro de un sistema de archivos.

Certificado digital. Documento firmado que vincula datos como una clave pública con una identidad o nombres bajo condiciones concretas.

Cifrado. Transformación de información para protegerla mediante un mecanismo y claves; no elimina todos los riesgos de uso.

Clave externa. Campo o conjunto de campos que referencia una clave de otra tabla según las reglas de relación.

Clave primaria. Campo o conjunto de campos que identifica inequívocamente cada fila de una tabla bajo el modelo definido.

Cliente. Papel de quien inicia una petición a un servicio; un equipo puede desempeñar también otros papeles.

CMS. Gestor de contenidos que permite organizar y publicar mediante una aplicación con cuentas, permisos y extensiones.

CNAME. Registro DNS que establece un alias hacia otro nombre, con restricciones sobre otros datos en ese mismo nombre.

CODE. Collabora Online Development Edition, edición utilizada en ciertos despliegues de edición documental de laboratorio o pequeña escala.

Códec. Método o componente que codifica y decodifica audio o vídeo; no es lo mismo que su contenedor de archivo.

Commit. Registro de un estado preparado en Git con información asociada; editar un archivo no lo crea automáticamente.

Concesión DHCP. Asignación de parámetros a un cliente durante un periodo y bajo condiciones del servicio DHCP.

Conector. Pieza física que une interfaces o conductores; su forma no demuestra compatibilidad eléctrica o de protocolo.

Confidencialidad. Protección frente a acceso o divulgación no autorizados de información.

Contenedor. Instancia de ejecución creada a partir de una imagen y una configuración, con aislamiento y estado definidos.

Controlador. Software que facilita al sistema operativo trabajar con un dispositivo concreto.

Controlador de dominio. Servidor que presta servicios del dominio y mantiene los datos de directorio que le corresponden.

Copia diferencial. Copia de cambios respecto a la completa de referencia, según el sistema de copias utilizado.

Copia incremental. Copia de cambios respecto al punto anterior establecido; su recuperación puede depender de una cadena.

Corriente alterna. Corriente que cambia de sentido según su señal; en alimentación habitual se estudia su comportamiento periódico.

Corriente continua. Corriente con sentido definido en el modelo sencillo; tensión continua y forma de onda requieren contexto de medida.

CPU. Procesador que ejecuta instrucciones; frecuencia, núcleos y arquitectura no se resumen en una única cifra de rendimiento.

Cron. Mecanismo de programación periódica de tareas en sistemas que lo incluyen; necesita cuenta, entorno y seguimiento.

CSS. Lenguaje de reglas de presentación para documentos como HTML.

CSV. Formato textual de registros y campos con separadores; no conserva todas las funciones de una hoja de cálculo.

Cuota. Límite o seguimiento del uso de almacenamiento bajo un ámbito, como usuario o carpeta.

D

DHCP. Servicio que proporciona parámetros de red a clientes mediante un procedimiento y una duración de asignación.

DHCPv6. Protocolo de configuración para IPv6 con funciones y relación con anuncios de router diferentes de DHCPv4.

Dirección MAC. Identificador de enlace de una interfaz; no constituye por sí solo una identidad fiable de una persona.

Directorio de trabajo. Lugar cuyos archivos editas al trabajar con Git; sus cambios pueden estar sin preparar.

Directorio de usuarios. Servicio organizado de información sobre identidades y recursos; no equivale a una carpeta de documentos.

Disco virtual. Dispositivo de almacenamiento presentado al invitado por su plataforma, frecuentemente respaldado por archivos del host.

Disponibilidad. Posibilidad de acceder a datos o servicios cuando se necesitan, bajo el alcance establecido.

Distribución Linux. Conjunto de sistema, paquetes y decisiones de integración que ofrece una distribución mantenida.

DNAT. Traducción de dirección o puerto de destino en el recorrido de una comunicación.

DNS. Sistema jerárquico de nombres y datos asociados; resolver un nombre no descarga su página ni acredita acceso.

DNSSEC. Mecanismos de validación de datos DNS firmados; no cifran automáticamente todas las consultas.

Dominio de AD. Ámbito de identidades y administración dentro de Active Directory; necesita su infraestructura y planificación.

Dominio DNS. Parte del espacio jerárquico de nombres; registrar uno no instala un directorio de identidades.

Driver. Nombre habitual en inglés para controlador de dispositivo.

E

Edge. Procesamiento situado cerca del origen o uso de los datos bajo un diseño concreto.

Enlace permanente. Parte fija de una instalación de cableado, diferenciada del canal completo y sus latiguillos.

Escalado. Solicitud de otra capacidad, permiso o decisión para un caso, con transferencia de información y seguimiento.

Ethernet. Familia de tecnologías de red con variantes de medios, velocidades y alcance; no se limita a un único cable.

F

Firewall. Cortafuegos que aplica reglas a tráfico o conexiones bajo un alcance; no reemplaza permisos de aplicación.

Firma digital. Mecanismo para comprobar integridad y relación con una clave de firma bajo la confianza y validación pertinentes.

Firmware. Software asociado al control de un dispositivo, normalmente almacenado de forma no volátil.

Formatear. Crear estructuras de un sistema de archivos; puede hacer inaccesibles datos anteriores y no garantiza borrado seguro.

Formulario. Interfaz para introducir o consultar datos; sus controles no sustituyen reglas y validación del backend.

Frecuencia. Número de ciclos por unidad de tiempo, expresado por ejemplo en Hz; no equivale al rendimiento completo.

Frontend. Parte de interacción de una aplicación que utiliza la persona, frecuentemente en el navegador.

FTP. Protocolo de transferencia con conexiones de control y datos; su versión sin TLS no protege credenciales ni contenido.

FTPS. FTP protegido mediante TLS, con modos de establecimiento y conexiones de datos que se deben configurar.

Fuente de alimentación. Equipo que transforma y regula alimentación para componentes, con límites y protecciones específicos.

G

Gateway. Puerta de enlace o siguiente salto utilizado para alcanzar destinos según las rutas y el contexto.

GB. Unidad decimal de mil millones de bytes; no es igual a un GiB.

GiB. Unidad binaria de 1.073.741.824 bytes.

Git. Sistema de control de versiones que registra contenido y permite comparar e integrar líneas de trabajo.

Glob de archivos. Patrón del shell para seleccionar nombres; expansión y comillas deben comprenderse antes de operar.

GPO. Objeto de directiva de grupo cuyo efecto depende de vínculos, alcance, filtros y reglas de procesamiento.

Grupo. Conjunto de identidades para asignar permisos u otros usos bajo el sistema que lo administra.

GUI. Interfaz gráfica de usuario; una ventana no garantiza que la operación haya quedado guardada.

H

Hardware. Componentes físicos del equipo y sus dispositivos.

Hash. Resultado de una función sobre datos, útil para comparación de integridad bajo su diseño; no cifra el contenido.

HDD. Disco de almacenamiento con componentes mecánicos y superficies magnéticas, con características distintas de un SSD.

Hipervisor. Software o plataforma que permite ejecutar y administrar máquinas virtuales bajo un modelo de virtualización.

Host. Equipo o entorno anfitrión respecto a un servicio o virtualización; precisa contexto para distinguirlo de un invitado.

Hostname. Nombre asignado a un equipo en un contexto; no garantiza por sí solo resolución DNS o pertenencia al dominio.

HTML. Lenguaje de marcado que estructura y da significado al contenido de una página.

HTTP. Protocolo de aplicación para intercambio de peticiones y respuestas; un código de estado requiere contexto.

HTTPS. HTTP protegido mediante TLS; hay que validar identidad y confianza además de negociar cifrado.

I

IaaS. Modelo de nube que ofrece infraestructura y deja al cliente ciertas capas de administración según servicio y contrato.

ICMP. Familia de mensajes de control y diagnóstico de IP; su alcance no equivale al de cualquier aplicación.

Imagen de contenedor. Capas y configuración de partida para crear contenedores; no cambia por editar el código de origen después.

Imagen de disco. Representación preparada para recuperar un disco o particiones según herramienta y alcance.

IMAP. Protocolo de acceso a buzones que permite organizar y sincronizar estados bajo su implementación.

Impacto. Consecuencia de un evento sobre datos, personas, servicios u objetivos del caso.

Incidencia. Interrupción o degradación que se registra y atiende según el proceso acordado.

Integridad. Propiedad relacionada con mantener datos y estados correctos frente a modificaciones o pérdidas no previstas.

Intensidad. Cantidad de carga eléctrica por tiempo, expresada en amperios; su medida no utiliza la conexión de un voltímetro.

Interfaz. Punto de interacción entre componentes; en red identifica una conexión lógica/física según su contexto.

Invitado. Sistema ejecutado dentro de una máquina virtual respecto al anfitrión.

IP. Familia de protocolos de direccionamiento y entrega entre redes; una dirección corresponde a un contexto de interfaz.

IPv4. Versión de IP con direcciones de 32 bits, normalmente escritas en cuatro octetos decimales.

IPv6. Versión de IP con direcciones de 128 bits y mecanismos propios de descubrimiento y configuración.

ISO de instalación. Imagen de medio distribuida para un uso como instalación; su extensión no demuestra integridad ni capacidad de arranque.

IT. Tecnologías de información; se diferencia de OT por foco, aunque ambas pueden interconectarse.

K

Kerberos. Protocolo de autenticación que utiliza una infraestructura y tickets; depende de condiciones como sincronización de tiempo.

Kernel. Núcleo del sistema operativo que administra recursos y ofrece funciones fundamentales a otros componentes.

kWh. Unidad de energía; para potencia media en W y horas, divide su producto entre 1.000.

L

LAN. Red local con un alcance y diseño definidos; no es sinónimo de acceso a Internet.

Latencia. Retardo de una operación o comunicación; puede variar y coexistir con una tasa de transferencia alta.

LDAP. Protocolo para acceder a información de directorio; no equivale a toda la autenticación de un dominio.

Licencia de software. Condiciones que regulan usos del programa; precio gratuito y permisos de modificación son cuestiones distintas.

Línea de base. Descripción y medidas de un estado conocido que sirven para comparar y diagnosticar.

LMS. Sistema de gestión de aprendizaje con cursos, participantes, actividades y funciones de evaluación/comunicación.

Log. Registro de eventos cuyo significado depende de componente, hora, configuración y cobertura de la recogida.

Loopback. Interfaz o dirección de retorno al propio equipo; no representa una ruta hacia otra máquina.

M

M.2. Formato y sistema de conexión que puede alojar dispositivos con distintos protocolos; no equivale automáticamente a NVMe.

Macro. Código que automatiza acciones de una aplicación, con permisos y riesgos que se deben comprender.

Maildir. Organización de almacenamiento de mensajes en archivos/directorios utilizada por ciertos servidores de correo.

Máscara de red. Representación de los bits de prefijo de una dirección IPv4 en el uso correspondiente.

Mbps. Millones de bits por segundo en el contexto habitual; no son megabytes por segundo.

Metadato. Dato que describe otro dato o recurso, como fecha, autor o etiqueta; también puede revelar información sensible.

MFA. Autenticación con factores de categorías diferentes; dos secretos del mismo tipo no constituyen por sí solos dos factores.

Migración. Traslado de datos o servicio con control de compatibilidad, cambios, aceptación y recuperación.

Monitorización. Observación organizada del sistema para evaluar estado y actuar, con señales y procedimientos definidos.

MTU. Tamaño máximo de unidad de transmisión en un contexto de enlace/ruta; no es el tamaño universal de una aplicación.

MX. Registro DNS que indica servidores de correo para un dominio mediante nombres y prioridades.

N

NAT. Traducción de direcciones y, según el mecanismo, puertos; no sustituye reglas de filtrado o autorización.

NDP. Mecanismos de descubrimiento de vecinos y funciones relacionadas en IPv6, que no son ARP.

nftables. Infraestructura de Linux para reglas de filtrado y otras operaciones de red, como NAT, según configuración.

NLA. Autenticación a nivel de red utilizada por ciertos servicios RDP antes de establecer la sesión completa.

NTP. Protocolo utilizado para sincronización de tiempo; hora mostrada y zona horaria son conceptos distintos.

Nube. Modelo de provisión de recursos y servicios con características y responsabilidades que hay que identificar.

NVMe. Protocolo/interfaz para almacenamiento no volátil, comúnmente sobre PCIe; no es un tamaño físico de unidad.

O

OCR. Reconocimiento de caracteres de una imagen; su salida necesita revisión y no convierte todo escaneo en texto perfecto.

ODS. Objetivos de Desarrollo Sostenible de Naciones Unidas; su relación con una acción requiere evidencia y contexto.

Ofimática. Herramientas y prácticas para crear, organizar y comunicar documentos, cálculos y otros datos de trabajo.

OT. Tecnología que opera o controla procesos físicos; puede tener requisitos de seguridad y disponibilidad propios.

OU. Unidad organizativa de un directorio, útil para administración/delegación; no equivale a un grupo de permisos.

P

PaaS. Modelo de nube con plataforma de ejecución gestionada en mayor grado por el proveedor, según su servicio.

PAM. Marco modular de autenticación de ciertos sistemas; su configuración participa en procesos como inicio de sesión.

Par dividido. Fallo en que conductores de pares distintos transportan una señal como si fueran uno, pudiendo pasar continuidad básica.

Paridad de RAID. Información redundante calculada que permite reconstruir bajo el número de fallos y condiciones previstos por el nivel.

Partición. Región lógica delimitada dentro de un dispositivo o esquema de almacenamiento.

PAT. Traducción que utiliza puertos para distinguir comunicaciones en un diseño NAT.

PCIe. Interconexión de componentes con generaciones y número de líneas; ranura física y capacidad efectiva deben distinguirse.

Permiso efectivo. Acceso resultante al considerar identidad, grupos, reglas y recorrido concretos.

PHP. Lenguaje y entorno frecuente en aplicaciones web; versión y extensiones deben ser compatibles con la aplicación.

Ping. Herramienta de diagnóstico basada habitualmente en mensajes de eco ICMP; su éxito no valida todo un servicio.

PoE. Alimentación mediante cableado Ethernet bajo un sistema compatible; verifica estándar, presupuesto y equipo.

POP3. Protocolo para acceso/recogida de correo cuyo comportamiento de conservación depende de cliente y servidor.

Potencia. Energía por tiempo, expresada por ejemplo en W; no se confunde con energía acumulada en kWh.

PowerShell. Entorno de comandos y automatización que habitualmente encadena objetos, con módulos dependientes de plataforma.

Prefijo de red. Cantidad o conjunto de bits que define un ámbito de dirección; su notación con barra tiene un significado concreto.

Proceso. Instancia de ejecución de un programa con recursos y contexto; no es lo mismo que el archivo del programa.

Proxy. Intermediario de comunicaciones bajo un papel directo o inverso y reglas determinadas.

Puerto de transporte. Número usado por protocolos como TCP/UDP para distinguir comunicaciones; no es el conector físico del equipo.

R

RAEE. Residuos de aparatos eléctricos y electrónicos, sujetos a canales y tratamiento adecuados.

RAID. Organización de varias unidades con niveles de reparto/redundancia; no constituye automáticamente una copia independiente.

RAM. Memoria de trabajo; la RAM habitual es volátil y no sustituye el almacenamiento persistente.

Rama de Git. Referencia a una línea de trabajo en un repositorio; no requiere copiar manualmente una carpeta completa.

Ransomware. Tipo de malware que busca extorsionar afectando a datos o sistemas, con impactos que requieren respuesta organizada.

RDP. Protocolo de acceso a escritorio remoto; cliente, servidor, edición y seguridad deben ser compatibles.

Recursión DNS. Búsqueda de respuesta que un resolvedor realiza o coordina para un cliente autorizado.

Redundancia. Duplicación o alternativas para mantener capacidad ante ciertos fallos; depende de qué fallo se considere.

Registro de base de datos. Fila o unidad de información del modelo; se distingue del registro de eventos de un sistema.

Regla 3-2-1. Orientación de copias que busca varios ejemplares, soportes o medios diferentes y una ubicación separada, con pruebas.

Relay de correo. Reenvío de mensajes por un servidor; debe limitarse quién puede usarlo y para qué destinos.

Repositorio. Lugar gestionado de datos o versiones; su significado depende de si hablamos de paquetes, Git o copias.

Reserva DHCP. Asignación prevista desde el servicio para un cliente identificado; no es lo mismo que configuración manual del cliente.

Resistencia eléctrica. Magnitud expresada en ohmios; en un modelo resistivo relaciona tensión e intensidad mediante la ley de Ohm.

Restauración. Recuperación de datos o sistema desde una copia o estado, con verificación de lo recuperado.

Reversión. Retorno controlado de un cambio a un estado viable anterior, considerando también datos creados después.

Riesgo. Valoración de posibilidad y consecuencias de un daño bajo un contexto y método explícitos.

Root. Cuenta administrativa tradicional de Unix/Linux; sus permisos no hacen correcto cualquier cambio.

Router. Equipo o función que encamina entre redes mediante rutas; puede integrar otros servicios que no son lo mismo.

RPO. Objetivo de punto de recuperación: pérdida de datos tolerable expresada mediante el alcance temporal previsto.

RTO. Objetivo de tiempo de recuperación para devolver una capacidad definida tras la interrupción.

Ruta absoluta. Ubicación de un recurso que parte de una raíz reconocible en el sistema correspondiente.

Ruta IP. Regla de selección de siguiente salto o interfaz hacia un destino, con prefijo y otros atributos.

Ruta relativa. Ubicación interpretada respecto al contexto o directorio actual.

S

SaaS. Modelo en que se utiliza una aplicación ofrecida como servicio; siguen existiendo responsabilidades de acceso y datos.

SAI. Sistema de alimentación ininterrumpida, con límites de carga/autonomía y condiciones de mantenimiento propios.

SAN de certificado. Nombres o identidades alternativas incluidos en un certificado para su validación; no es una red de almacenamiento.

SASL. Marco de mecanismos de autenticación usado por servicios como SMTP, con backend y protección de transporte configurados.

SATA. Interfaz utilizada por ciertos dispositivos de almacenamiento; formato, protocolo y conector requieren compatibilidad.

Secure Boot. Mecanismo de arranque que verifica componentes conforme a claves y políticas de confianza configuradas.

Segmentación. Separación de ámbitos de red o acceso bajo un diseño; una VLAN o SSID distinto no demuestra todo el aislamiento.

Servidor. Papel de quien ofrece un servicio; también se usa para el equipo que lo aloja según contexto.

Sesión. Relación de estado de interacción bajo un mecanismo; cerrar una ventana no garantiza revocarla en el servidor.

SFTP. Transferencia de archivos sobre SSH; no es FTP protegido con TLS.

SGBD. Sistema gestor de bases de datos que administra datos, consultas y reglas según sus funciones.

Shell. Intérprete de órdenes con reglas propias de sintaxis y expansión.

SLA. Acuerdo de nivel de servicio con alcance, condiciones y medición; una cifra de un ejemplo no crea ese acuerdo.

SMB. Protocolo utilizado para compartir recursos como archivos, con autenticación y permisos del entorno.

SMTP. Protocolo de transferencia/presentación de correo; aceptación no demuestra lectura por el destinatario.

SNAT. Traducción de la dirección de origen en una comunicación bajo el diseño previsto.

Socket. Extremo de comunicación o mecanismo del sistema; puede ser de red o local y necesita contexto.

Software. Programas y elementos lógicos de un sistema; no se limita a aplicaciones con ventana.

SSD. Unidad de almacenamiento de estado sólido; su rendimiento y mantenimiento dependen de interfaz, diseño y uso.

SSID. Nombre de identificación de una red wifi; no es una garantía de identidad ni de separación.

SSSD. Servicio de integración de identidades y autenticación en sistemas compatibles, con proveedores como Active Directory.

Staging. Entorno o área de preparación; en Git designa cambios preparados, y en despliegue puede ser un entorno de pruebas.

Submission. Presentación de mensajes desde un cliente al servicio de correo, con autenticación y protección según su diseño.

Subred. Ámbito de direcciones definido por un prefijo bajo un diseño; número de direcciones y hosts utilizables no son siempre iguales.

Switch. Conmutador que reenvía en un contexto de enlace; sus funciones de VLAN, gestión o capa 3 dependen del modelo.

T

TCO. Coste total de propiedad bajo un periodo y alcance definidos; incluye más elementos que el precio inicial.

TCP. Protocolo de transporte con estado y entrega ordenada bajo sus condiciones; no garantiza éxito de la tarea de aplicación.

Tensión. Diferencia de potencial entre dos puntos, expresada en voltios y medida con referencia y conexión adecuadas.

Terminal. Interfaz para interactuar con un intérprete o proceso; su aspecto no identifica necesariamente el shell.

Ticket. Registro de una petición o incidencia con responsable, estado, actuaciones y criterio de cierre.

TLS. Protocolo de protección de comunicaciones; seguridad también depende de identidad, confianza, configuración y extremos.

Troncal VLAN. Enlace que transporta las VLAN previstas, habitualmente con etiquetado y reglas que se configuran en ambos extremos.

TSIG. Autenticación de mensajes DNS mediante una clave compartida; no cifra automáticamente todo el intercambio.

TTL. Tiempo de vida o límite cuyo significado depende del protocolo; en DNS afecta a conservación en caché.

U

UDP. Transporte por datagramas sin las mismas garantías de TCP; una aplicación puede implementar controles adicionales.

UEFI. Interfaz y entorno de firmware moderno con servicios de arranque y configuración de plataforma.

USB. Familia de interconexión con variantes de datos y alimentación; el conector no define todas las capacidades.

UTF-8. Codificación de Unicode con longitud variable por carácter; veinte caracteres no implican veinte bytes.

V

VA. Voltioamperio, unidad de potencia aparente; se debe distinguir del límite de potencia activa en W.

VLAN. Segmentación lógica de enlace en infraestructura compatible; necesita pertenencia, etiquetado y controles coherentes.

VM. Máquina virtual que ejecuta un sistema invitado sobre una plataforma de virtualización.

Volumen. Unidad lógica de almacenamiento presentada al sistema, que no tiene por qué coincidir con un disco físico.

VPN. Túnel o red privada virtual con extremos, rutas y autorización definidos; no permite por sí solo todos los recursos.

Vulnerabilidad. Debilidad que puede permitir que una amenaza afecte a un activo en un contexto concreto.

W

Watt. Vatio, unidad de potencia; la energía se mide con otras unidades como kWh.

Webmail. Aplicación web para usar correo mediante servicios como IMAP y SMTP; no es necesariamente el servidor de buzones.

WPA3-Personal. Modo de seguridad wifi basado en SAE y requisitos asociados; compatibilidad y bandas requieren revisión.

Z

Zona DNS. Conjunto de datos bajo una administración autoritativa definida; no equivale a cualquier nombre consultado.

Anexo de taller. Consulta, calcula y comprueba

67. Puertos, comandos y casos resueltos

Esta sección sirve para recuperar una idea durante una práctica. Los puertos son usos habituales o asignados, no una garantía sobre lo que escucha en un equipo. Los comandos dependen del sistema, versión, paquetes y permisos: identifica tu entorno antes de utilizarlos.

Puertos y funciones que conviene distinguir

Puerto	Transporte	Servicio	Qué recordar
20/21	TCP	FTP	Control 21; datos con comportamiento activo/pasivo propio.
22	TCP	SSH/SFTP	Administración y transferencia bajo SSH.
25	TCP	SMTP	Recepción/transferencia de correo según diseño.
53	UDP/TCP	DNS	No se limita siempre a UDP.
67/68	UDP	DHCPv4	Servidor y cliente; contempla arranque sin dirección.
80	TCP	HTTP	Puerto habitual; no demuestra cifrado.
88	UDP/TCP	Kerberos	Parte de la infraestructura de autenticación.
110/995	TCP	POP3/POP3S	Recogida, con TLS implícito habitual en 995.
123	UDP	NTP	Sincronización de tiempo.
143/993	TCP	IMAP/IMAPS	Acceso al buzón; TLS implícito habitual en 993.
389	TCP	LDAP	Directorio; protección según mecanismo configurado.
443	TCP/UDP	HTTPS	TCP para usos habituales; HTTP/3 utiliza QUIC/UDP.
445	TCP	SMB	Compartición y controles de identidad/permiso.
465/587	TCP	Presentación SMTP	TLS implícito en 465; STARTTLS habitual en 587.

Puerto	Transporte	Servicio	Qué recordar
546/547	UDP	DHCPv6	Cliente y servidor en IPv6.
636	TCP	LDAP sobre TLS	Directorio con TLS implícito en el uso habitual.
990	TCP	FTPS implícito	No confundir con FTP explícito protegido con TLS.
3389	TCP/UDP	RDP	Acceso remoto; disponibilidad depende del servicio.

Un protocolo puede utilizar otros puertos y un puerto puede alojar otra cosa. No abras toda la tabla en un cortafuegos. Describe origen, destino, dirección del flujo y necesidad. Los puertos pasivos FTP se negocian/configuran aparte; en las prácticas se limitan a un rango propio.

Referencia: registro oficial IANA de servicios y puertos. Consulta del 5 de noviembre de 2026; usos simplificados para las funciones explicadas en el manual.

Comandos de lectura para orientarte

Comando	Entorno	Para qué sirve
`pwd`	Bash/sistemas afines	Ver directorio actual antes de operar con rutas.
`Get-Location`	PowerShell	Consultar ubicación actual.
`ip -br addr`	Linux con iproute2	Ver interfaces y direcciones resumidas.
`ip route`	Linux	Consultar rutas, no validar por sí solo el servicio.
`ipconfig /all`	Windows	Consultar configuración de adaptadores.
`Get-NetIPConfiguration`	Windows / PowerShell	Consultar configuración IP mediante objetos.
`resolvectl status`	Linux con system d-resolved	Revisar resolución configurada en ese entorno.
`Resolve-DnsName`	Windows / PowerShell	Consultar nombres con sus parámetros adecuados.
`ss -lntup`	Linux	Ver escuchas; ciertos detalles requieren permisos.

Comando	Entorno	Para qué sirve
`Get-Process`	PowerShell	Consultar procesos del entorno compatible.
`lsblk -f`	Linux	Relacionar dispositivos y sistemas de archivos.
`Get-Volume`	Windows / PowerShell	Consultar volúmenes según permisos.
`df -h`	Sistemas que lo incluyen	Consultar uso de sistemas de archivos montados.
`git status`	Git	Ver cambios preparados, sin preparar y otros estados.
`git diff --cached`	Git	Revisar lo preparado antes de registrar.

Ninguna de estas consultas requiere que reinicies, formatees o cambies permisos para interpretarla. Una salida vacía puede deberse a ausencia, filtros o acceso. Lee el mensaje y el entorno antes de añadir privilegios.

Para comprobar un puerto TCP en Windows, adapta el nombre de laboratorio en una sesión autorizada:

POWERSHELL

```
Test-NetConnection intranet.aulanorte.test -Port 443
```

Demuestra alcance TCP en ese contexto, sin comprobar todo TLS, contenido o autorización. En el Linux del laboratorio, si tienes dig y curl:

BASH

```
dig intranet.aulanorte.test A
curl --cacert ca.crt https://intranet.aulanorte.test
```

La primera consulta y la segunda tarea verifican funciones distintas. `ca.crt` es el certificado público de la autoridad de esa práctica, en una ruta que debes identificar. No copies una clave privada al cliente ni uses una opción que ignore verificación para declarar éxito.

Para una comparación de integridad sobre tu archivo ficticio puedes usar `sha256sum archivo.txt` en un Linux que lo incluya o `Get-FileHash .\archivo.txt -Algorithm SHA256` en PowerShell. En macOS puede utilizarse `shasum -a 256 archivo.txt`. Misma función y mismo contenido producen el valor esperado; un hash no explica si el archivo procede de una fuente confiable por sí solo.

Tabla IPv4 que debes poder reconstruir

Para estas subredes convencionales se descuentan dirección de red y difusión al contar hosts. No es una fórmula universal para cualquier prefijo y uso.

Prefijo	Máscara	Direcciones	Hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Un /31 tiene un uso específico en enlaces punto a punto, y /32 identifica una dirección individual. No extrapoles «restar dos» a esos casos ni a IPv6. Las privadas de RFC 1918 son 10.0.0.0/8,172.16.0.0/12 y 192.168.0.0/16. IPv6 tiene otros ámbitos;2001:db8::/32 se utiliza en documentación.

Ejercicio: para `10.77.2.190/27`, el bloque de 32 que contiene 190 empieza en 160 y termina en 191. Red`10.77.2.160`, difusión`10.77.2.191` y hosts convencionales 161-190. Verifica que 190 es un host posible en este caso; no lo rechaces por terminar cerca del final del octeto.

Fuentes: RFC 1918, uso de /31 en RFC 3021 y prefijo documental IPv6, RFC 3849.

No confundas estas parejas

- **RAM y almacenamiento:** trabajar con datos no equivale a conservarlos tras apagar.
- **Capacidad y tasa:** MB describe cantidad; Mb/s, bits por tiempo.
- **Partición y disco:** un dispositivo puede contener varias particiones y un volumen puede tener otra estructura.
- **IP y MAC:** pertenecen a funciones y alcances distintos; ninguna identifica por sí sola a una persona.
- **DNS y puerta de enlace:** resolver un nombre y elegir el siguiente salto no son la misma operación.
- **Autenticación y autorización:** reconocer una identidad no concede cualquier permiso.
- **Cifrado y hash:** proteger contenido reversible con una clave y obtener una huella no son lo mismo.

- **Copia y sincronización:** propagar un borrado puede eliminar varias versiones sincronizadas; diseña recuperación.
- **RAID e independencia:** un espejo puede compartir fallo del host y reflejar un cambio no deseado.
- **Instantánea y respaldo:** estudia alcance, dependencias y ubicación antes de decidir qué fallo cubre.
- **Fórmula y formato:** cambiar aspecto de una celda no cambia necesariamente su valor o cálculo.
- **Instalado y comprobado:** un servicio activo no acredita la tarea del cliente.
- **Archivo y extensión:** renombrar no convierte su estructura interna.
- **CMS y LMS:** publicar contenido y organizar aprendizaje tienen funciones y permisos diferentes.
- **Imagen y contenedor:** una es referencia de partida; el otro es una instancia con configuración y estado.

Caso 1. Hay enlace, pero no se recibe dirección

Datos: cliente nuevo, AP y switch del laboratorio con enlace, servidor DHCP activo. La regla de filtrado solo admite paquetes con origen 10.77.0.0/24. **Tu tarea:** formula una hipótesis y una prueba que la contradiga.

Solución razonada: la configuración inicial puede utilizar un cliente sin dirección y difusión. Revisa interfaz, recorrido y mensajes de solicitud/respuesta en una captura de laboratorio autorizada. Si las peticiones llegan y el servidor responde pero no vuelven al cliente, cambia la investigación al retorno y los controles. Corrige la política según el flujo observado; no concluyas que hace falta otro DHCP.

Caso 2. El nombre resuelve, pero aparece otra web

Datos: DNS devuelve la dirección esperada y el servicio presenta contenido ajeno al sitio de pruebas. **Tu tarea:** elige qué revisar antes de cambiar DNS.

Solución razonada: comprueba URL/esquema, nombre solicitado, sitio virtual seleccionado, configuración y registros del servidor. En HTTPS intervienen nombre y certificado, además del contenido. Acceder por IP puede seleccionar un sitio distinto. Una resolución correcta no garantiza el vhost correcto ni justifica desactivar TLS.

Caso 3. El correo se lee, pero no se envía

Datos: IMAPS 993 funciona y SMTP 587 devuelve un error de negociación. El cliente ha seleccionado TLS implícito. **Tu tarea:** separa credenciales y modo de transporte.

Solución razonada: el taller ofrece STARTTLS en 587. Contrasta puerto, modo y certificado antes de cambiar la contraseña. Si el error persiste tras usar el modo previsto, revisa capacidades, autenticación, permisos y registros. Un éxito de IMAP no prueba que la configuración SMTP sea correcta.

Caso 4. El archivo restaurado coincide, pero la tarea falla

Datos: hash idéntico al original de prueba, pero la cuenta prevista no puede abrirlo en la carpeta restaurada. **Tu tarea:** explica qué demostró el hash y qué falta.

Solución razonada: acredita igualdad del contenido comparado bajo esa función. Revisa ruta, identidad, permisos, aplicación y dependencias; el hash no verifica todo eso. La aceptación requiere la operación del usuario, con permisos y ubicación previstos, además de integridad.

Caso 5. La hoja muestra alarma en una fila sin datos

Datos: falta capacidad, la celda se interpreta como cero y una fórmula calcula un porcentaje engañoso. **Tu tarea:** distingue ausencia y valor cero.

Solución razonada: comprueba tipo y presencia antes de operar, y devuelve el estado de dato ausente que haya definido el diseño. No ocultes el fallo con un cero que parezca una medida válida. Prueba también capacidad cero, espacio libre mayor que capacidad y umbral ausente en una copia del inventario.

Caso 6. «Dos copias» desaparecen a la vez

Datos: original y copia estaban en carpetas distintas del mismo SSD físico y este falla. **Tu tarea:** propone una mejora que cubra ese fallo y su prueba.

Solución razonada: separa el dominio de fallo mediante un soporte/sistema independiente y una política adecuada. Después restaura una muestra cuando el original del ensayo no esté disponible. Añade retención, acceso y ubicación según el riesgo; contar carpetas no demuestra independencia.

Una ficha para tus propios casos

Escribe datos, tarea, hipótesis, predicción, prueba, resultado y decisión. Añade qué información todavía falta. Usa los modelos de soporte y verifica con ejemplos ficticios. Cuando una evidencia contradice la explicación, cambia la explicación; no selecciones solo las pruebas que la favorecen.

Anexo de recorrido. Sigue aprendiendo con criterio

68. Recursos, fuentes y mapa del temario

El libro se acompaña de archivos de prácticas. Descomprime el paquete de recursos en una carpeta de trabajo y empieza por su `LEEME.md`. Los ejemplos utilizan Aula Norte, nombres y datos ficticios. No necesitas contratar nube ni comprar equipos para comenzar: elige el nivel de laboratorio que permite tu material y amplíalo cuando corresponda.

Qué encontrarás en el paquete

Fundamentos y hardware. Cuaderno de laboratorio, práctica de terminal y ficha de medición. La ficha no autoriza trabajo eléctrico: las mediciones físicas del capítulo 9 se limitan al montaje didáctico de baja tensión y supervisión descritos allí.

Servicios. Configuraciones de DHCP, DNS y Apache, página de prueba y generador de certificados. La carpeta `servicios/ampliacion` añade FTP protegido, correo, proxy, pasarela y conexiones de webmail. Lee su guía antes de integrar fragmentos: algunos archivos son ajustes parciales y los nombres de interfaz deben adaptarse.

Seguridad y automatización. Ensayo de restauración con Python, scripts Bash y PowerShell y conjuntos de eventos ficticios para analizar. Lee cada cabecera y ejecuta desde una carpeta propia. Copiar una línea sin conocer su destino no es una comprobación.

Ofimática. Inventario XLSX editable, CSV y SQL para consultas SQLite, macros de ensayo de LibreOffice y tres ilustraciones originales en SVG/PNG con un vídeo breve sin audio. Las macros no se habilitan para cualquier archivo recibido; usa únicamente el material revisado del taller y la política indicada en el capítulo 43.

Web. Miniweb HTML/CSS/JS con ilustraciones adaptadas a pantalla y procedimiento de prueba. Puede abrirse localmente para el ejercicio; el hosting, WordPress, Moodle, Nextcloud y Roundcube necesitan sus entornos y procedimientos propios. La miniweb no los instala.

Trabajo profesional. Plantillas de ticket, inventario de evidencias, procedimiento, guion de inglés, planes de aprendizaje, digitalización y sostenibilidad, expediente de proyecto y diario de formación en empresa. Los campos pendientes esperan tus resultados: no se rellenan como aprobados por defecto.

Consulta. Glosario CSV con las definiciones del capítulo 66 y matriz de cobertura por resultados de aprendizaje. Puedes filtrar por módulo y localizar explicación, práctica y evidencia propuesta. La matriz describe este manual; no otorga títulos ni sustituye evaluación del centro.

Rutas según tu punto de partida

Me faltan las bases. Empieza por los capítulos 1-8. Repite la prueba del capítulo 2 y explica tres respuestas con ejemplos propios. Después aborda un bloque cada vez, alternando lectura y una prueba pequeña.

Estoy preparando una práctica. Localiza objetivo, requisitos, configuración y aceptación. Revisa primero sus dependencias: para una web con nombre, IP, DNS y hora pueden importar antes del contenido. Anota estado inicial y recuperación antes de cambiar nada.

Necesito repasar para una evaluación. Elige un módulo, recorre sus preguntas y resuelve un caso sin mirar la solución. Corrige explicando qué dato te faltaba. Vuelve a la definición y al procedimiento de esa parte; memorizar la respuesta sin variar el ejemplo deja la laguna abierta.

Quiero reunirlo todo. Realiza el nivel A del proyecto 64 y después añade fases del nivel B según recursos. Entrega decisiones, evidencias y límites. Si solo has diseñado un servicio, registra «diseñado»; cuando lo pruebes, añade entorno, resultado y fecha.

Cómo se relaciona con SMR

Montaje y mantenimiento, 0221: capítulos 9-14, electricidad y SAI, formatos, ensamblaje, mantenimiento, periféricos y diagnóstico; imagen de sistemas en el 20 y prevención en el 57.

Sistemas monopuesto, 0222: fundamentos 5-8 y capítulos 15-20; archivos, instalación, cuentas, terminal, administración, virtualización y recuperación. Automatización adicional en el 59.

Aplicaciones ofimáticas, 0223: capítulos 43-47; instalación, documentos, hojas, bases de datos, imágenes/vídeo, presentaciones, correo y agenda. Soporte y documentación en el 55.

Sistemas en red, 0224: capítulos 28-31; instalación de servidor, dominio, usuarios y grupos, recursos, administración e integración Linux/Windows. Almacenamiento y cuotas en el 31; seguimiento en el 62.

Redes locales, 0225: capítulos 21-27; topología, medios, direccionamiento, conmutación, enrutamiento, montaje, AP y diagnóstico. Prevención transversal en el 57.

Seguridad informática, 0226: capítulos 37-42; riesgo, protecciones, almacenamiento, copias, transmisión, incidentes y responsabilidad. Se conecta con SAI del 9, imagen del 20, RAID del 31 y TLS del 33.

Servicios en red, 0227: capítulos 32-36; DHCP, DNS, web, transferencia, correo, acceso remoto, inalámbrico, proxy y pasarela. Los servicios añadidos conservan sus dependencias y pruebas propias.

Aplicaciones web, 0228: capítulos 48-52; arquitectura y práctica web, CMS, LMS, archivos, colaboración ofimática, correo y calendario web, mantenimiento y migración.

Inglés Profesional, 0156: capítulo 56 y guion de escucha. **IPE I y II, 1709/1710:** unidades separadas en el 57, con proyecto y preparación de empresa en 64-65. **Digitalización GM, 1664, y Sostenibilidad, 1708:** unidades del 58, planes y ampliaciones aplicadas. **Proyecto intermodular, 1713:** capítulo 64, desde organización y necesidad hasta seguimiento y comunicación.

Las optativas, distribución y concreción del currículo dependen de la administración educativa y del centro. Consulta tu programación. Una guía de formación en empresa ayuda a prepararte y registrar aprendizaje; leerla no realiza esa formación.

Fuentes para comprobar y ampliar

La base curricular se contrastó con el RD 1691/2007, título de SMR, su actualización mediante RD 499/2024 y el RD 659/2023, ordenación de la FP. Se utiliza el currículo básico como mapa, sin atribuir un horario autonómico universal.

Para sistemas y servicios se han usado principalmente manuales oficiales de Microsoft Learn, Ubuntu, BIND, OpenSSL, Dovecot, Apache, Squid y nftables. Para aplicaciones: LibreOffice, SQLite, WordPress, Moodle, Nextcloud y Roundcube. Para redes: RFC, IANA, documentación de fabricantes y Wireshark. Las referencias específicas se sitúan junto al procedimiento correspondiente.

En seguridad, privacidad, empleo y prevención se incluyen fuentes públicas como BOE, AEPD, INCIBE, INSST, SEPE y Seguridad Social; en sostenibilidad, Naciones Unidas y GRI. Las cifras didácticas se distinguen de precios, mediciones, condiciones laborales o tipos reales. No conviertas un ejemplo en asesoramiento para un caso que requiere datos y responsables propios.

Fecha de revisión editorial: 5 de noviembre de 2026. Los productos, versiones y normas pueden cambiar. Antes de repetir una instalación, contrasta requisitos, versión y manual de migración. Si una URL ha cambiado, busca el título dentro del sitio oficial y compara que corresponde a tu versión.

Qué significa «comprobado» en esta edición

Se han ejecutado ensayos locales de Bash, Git, subredes, SQLite, restauración de datos, análisis CSV, generación y validación TLS en memoria, fórmulas/exportación del XLSX y comportamiento de la miniweb en un navegador automatizado. Las láminas y el vídeo son recursos originales generados para el taller. El PDF se ha renderizado y revisado para lectura A4.

Los despliegues Windows/AD/GPO y los servicios completos Linux y aplicaciones de servidor requieren su laboratorio de referencia; sus recorridos se han revisado con documentación oficial, sin presentar esa revisión como una instalación ejecutada. Tampoco se han ejecutado las macros en LibreOffice ni verificado el XLSX en Excel/Calc nativos. Esos límites te permiten elegir qué validar en tu entorno.

Para imprimir: selecciona papel A4 y escala del 100 %, revisa la vista previa y evita reducir varias páginas a una hoja si quieres conservar el tamaño del texto. Los avisos y diagramas incluyen palabras y formas además de color. Puedes imprimir por capítulos y reservar las plantillas para rellenarlas aparte.

Cuando completes un recorrido, conserva una explicación breve de la decisión y una prueba que alguien pueda repetir. Ese hábito te servirá incluso cuando cambien los menús y las herramientas.

Sobre el autor

David Cantón Nadales es arquitecto de software, autor y divulgador tecnológico sevillano con más de veinte años de experiencia. Su trayectoria combina arquitectura de aplicaciones, tecnologías .NET, desarrollo móvil y web, inteligencia artificial, videojuegos y experiencias de realidad virtual y aumentada. Es fundador de **Deadwood Studio** y creador de productos que han recibido premios y atención de los medios.



David Cantón Nadales
Foto publicada en davidcanton.net

Reconocimientos que acompañan una trayectoria

- **Microsoft MVP en Developer Technologies, reconocido en varias ocasiones.** En julio de 2026 anunció su tercer año consecutivo con este reconocimiento. Su publicación sobre el tercer año como MVP recoge su trabajo de desarrollo y contribución a la comunidad.
- **Finalista de los 17th Unity Awards, edición de 2025, en Best Devlog.** La relación oficial publicada por Unity lo incluye entre los finalistas de esta categoría de creación y divulgación sobre desarrollo con Unity.
- **Ganador de un Samsung Top Developer Award 2022.** Su aplicación **Activisto** obtuvo el premio a la **Mejor app con componente social**, según la comunicación oficial de Samsung.
- **Logitech Luminary**, dentro del programa internacional **#LogiLumi de Logitech for Business**. Anunció su incorporación en septiembre de 2025 en su presentación del reconocimiento.

Desarrollar y compartir lo aprendido

Además de crear software, ha participado en comunidades como **Samsung Dev Spain**, de la que fue embajador, y **Google Developer Group Sevilla**, como organizador, y ha impulsado **Unity3D Sevilla**. En su presentación profesional reúne esa trayectoria de desarrollo, charlas y divulgación.

En su blog y canal de YouTube comparte tutoriales, proyectos y explicaciones prácticas. **SMR SOS** nace con ese mismo propósito: ayudar a quienes necesitan reforzar las bases, comprender lo que están haciendo y avanzar de una explicación a una práctica que puedan resolver y justificar.

Libros para aprender y explorar

Su trabajo como autor incluye publicaciones técnicas y divulgativas:

- **Build Your Own Metaverse with Unity**, publicado por **Packt**: desarrollo de un metaverso multiplataforma con Unity y Firebase. Ficha de la editorial.
- **Curso práctico con Unity 3D**, publicado por **Anaya Multimedia**: aprendizaje del desarrollo de videojuegos mediante proyectos. Ficha de la editorial.
- **Aprende Microsoft Semantic Kernel en 25 pasos**: ebook gratuito acompañado de una serie de tutoriales sobre inteligencia artificial con .NET. Presentación y descargas del autor.
- **Conoce los orígenes de los pueblos andaluces**: un libro de divulgación sobre los nombres y la historia de los municipios de Andalucía. Presentación del autor.

Aplicaciones que han llegado a los medios

Sus proyectos trasladan el desarrollo de software a necesidades concretas. Entre los que han recibido cobertura periodística se encuentran:

- **Grita**: aplicación de expresión y encuentro creada durante el confinamiento de 2020. Applicantes documentó su lanzamiento y autoría.
- **Activisto**: aplicación para descubrir y organizar iniciativas de activismo social, ganadora del premio de Samsung citado antes. Reportaje de Applicantes.
- **8M Online**: iniciativa para participar mediante avatares y mensajes en una manifestación virtual por el Día Internacional de la Mujer. Noticia de Applicantes.
- **El Zoco**: plataforma para conectar vecinos y comercios de proximidad. Su creador explicó el proyecto en una entrevista de Onda Local de Andalucía en julio de 2026.

La combinación de proyectos, libros y divulgación forma parte de su manera de aprender: construir algo, entender las decisiones y compartir el recorrido con otras personas.

Puedes seguir su trabajo en **davidcanton.net** y conocer sus proyectos en **deadwood.es**.

Fuentes y fotografía. Información profesional revisada el 5 de noviembre de 2026. Los enlaces permiten consultar las publicaciones originales. Fotografía publicada en la web profesional del autor, incorporada a petición suya y conservando el archivo original.