ACERCA DEL AUTOR

David Casas M., Administrador de Sistemas Informáticos en Red y Perito Informático. Ha trabajado como director de la empresa *Shopicardiacom, S.L.* desde 1998 desarrollando las típicas funciones de todo técnico informático, diseñando y administrando sistemas y redes, máquinas virtuales con hipervisores de tipo 1 y 2, administración de backups, infraestructura de red, reparación de PCs, ensamblado, ampliaciones, mantenimientos, seguridad informática, backups, procesos, hosting, dominios, servidores privados virtuales, herramientas y plataformas de todo tipo.

Como entusiasta de las computadoras, ha vivido la evolución de la informática desde las primeras máquinas de 8bits, comenzando con un flamante Amstrad CPC464 con monitor color en el que realizó sus primeros pinitos programando en *BASIC*, hasta el uso de la abrumadora tecnología actual en al que la *IA* nos está llevando a la próxima "revolución industrial".

Divulgador de contenidos en plataformas de vídeo online mediante vídeos grabados y emisiones en directo, ha conseguido integrarse en el medio virtual para "*crear puentes sobre la brecha digital y plantar la semillita del árbol de la curiosidad que nos llevará a la mejora de nuestras competencias digitales en el fantástico mundo etéreo del ciberespacio*". Recuerda, "***fácil fácil, sencillo sencillo***".

Autor de "*El Libro de Competencia Digital*" (ISBN-13: 979-8325738852), un fantástico volumen en formato A4 de 457 páginas a todo color que abarca todo el conocimiento fundamental informático desde la invención de los emoticonos al aprendizaje automático, redes neuronales, inteligencia artificial, cadena de bloques y criptomonedas, pasando por historia del hardware, software y comunicaciones. El texto repasa, además, la historia de los personajes históricos desde William de Malmesbury a contemporáneos como Andrew S. Tanenbaum.

En su viaje vital, además, se dedica al voluntario en Protección Civil con titulación de Técnico en Transporte Sanitario.

David Casas Martín

INTRODUCCIÓN

El mundo de las competencias digitales se encuentra en constante cambio debido a la evolución y desarrollo tecnológico. La interconexión de todo tipo de elementos, o dispositivos, en una red global disponible las 24 horas del día nos empujan hacia la necesidad de incorporar habilidades fundamentales para conseguir participar, de forma plena, en la sociedad actual.

El curso **IFCT149: Competencias Digitales para la Ciudadanía – Nivel Avanzado Accesible**, se ha diseñado para que los participantes dispongan de las herramientas necesarias que les ayuden a desenvolverse con confianza y eficacia en estos entornos digitales, fomentando una ciudadanía activa, informada e inclusiva.

El programa formativo de 60 horas se encuadra dentro del catálogo de Especialidades Formativas del Servicio Público Estatal, dependiente del Ministerio de Trabajo y Economía Social, regulado en la Orden TMS/283/2019, de 12 de marzo, y busca, como objetivo estratégico, favorecer la creación de empleo estable y de calidad, contribuir a la competitividad empresarial, garantizar el derecho a la formación laboral y ofrecer garantías de empleabilidad y promoción profesional de los trabajadores.

El viaje a través de las páginas de este libro se centra en el desarrollo de habilidades avanzadas en el uso de tecnologías digitales, con un enfoque especial en la accesibilidad y la inclusión.

Encontrarás contenidos prácticos, esquemas, ilustraciones y algunos cuestionarios de autoevaluación con los que aprenderás a gestionar información digital, programas de colaboración en línea, crear contenido accesible y una aproximación a la seguridad informática y privacidad, entre otros temas clave.

Un curso que garantiza a todas las personas, independientemente de sus capacidades o necesidades específicas, el aprovechamiento al máximo de las herramientas tecnológicas para mejorar su calidad de vida, potenciar la empleabilidad y la participación en la comunidad o mundo digital.

Una vez completado el curso, tendrás capacidad para usar tecnologías digitales de forma avanzada, creativa y responsable, contribuyendo a una sociedad más equitativa, accesible y sostenible.

ESTRUCTURA

Todo el material formativo que se encuentra en este libro abarca el conocimiento necesario para la correcta consecución de los objetivos especificados en el documento oficial publicado dentro del Catálogo de Especialidades Formativas del Servicio Público de Empleo Estatal español y se ha estructurado de tal modo que pueda ser accesible para los participantes independientemente de si la formación se recibe online o mediante clases presenciales dirigidas.

Así, el itinerario se ha dividido en varios módulos que desarrollan las ideas contenidas en dicho documento presentando los diferentes módulos con un contenido teórico y práctico sencillo de entender gracias a los múltiples ejemplos y capturas presentes en el libro.

Además, se invita al lector a que realice sus propias prácticas y búsquedas ampliando la información para mejorar las habilidades propias siguiendo su propio ritmo.

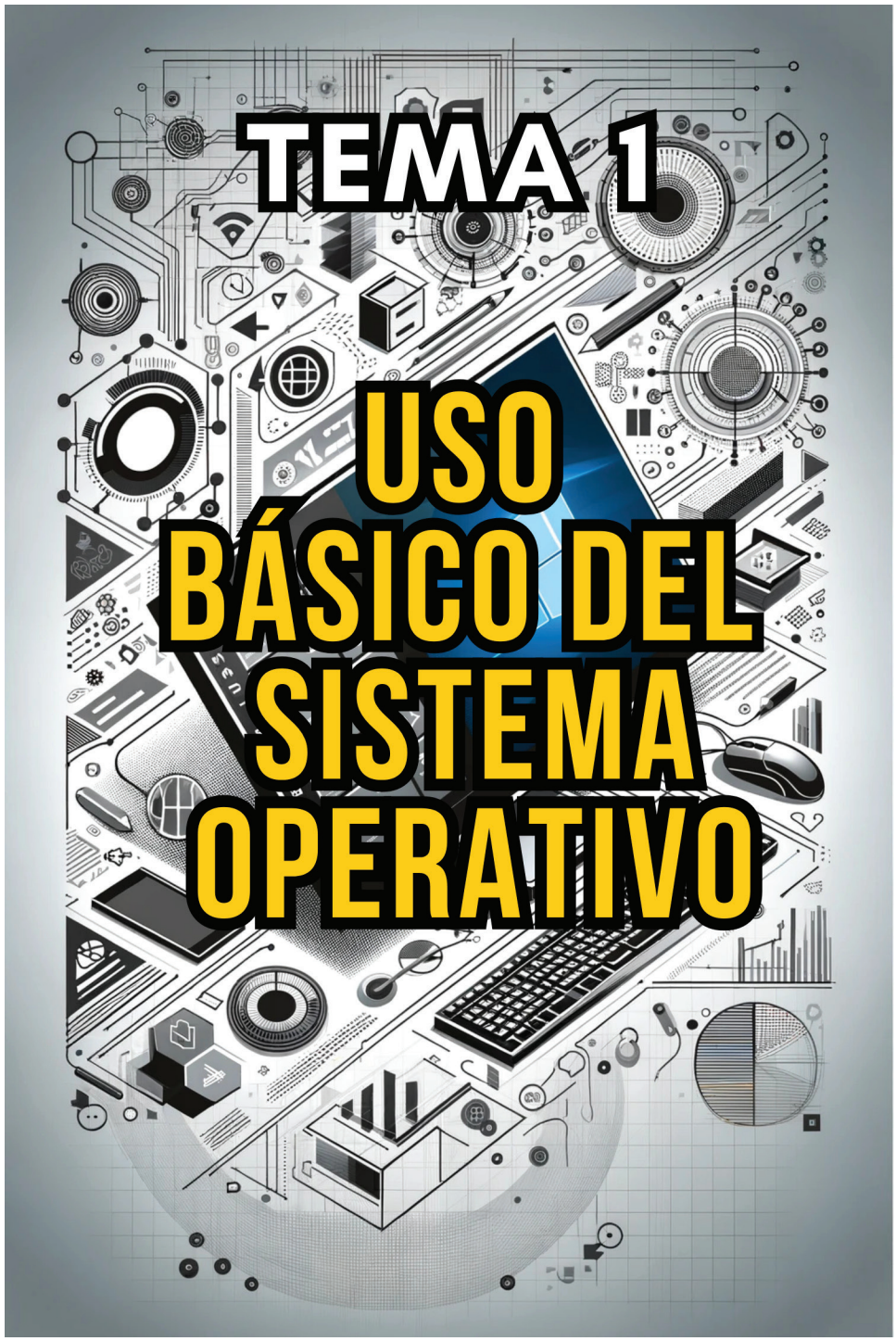
Cada uno de los módulos se desarrollará abarcando los conocimientos necesarios que permitan al lector continuar con su aprendizaje y mejora de las competencias digitales no solo básicas sino, también, avanzadas.

OBJETIVOS

El objetivo principal del curso es capacitar a los participantes para desenvolverse de manera autónoma y eficiente en el ámbito tecnológico, promoviendo tanto la productividad como la responsabilidad digital. Para ello, el programa abarca temas clave como el dominio del sistema operativo y las herramientas de gestión básica, el desarrollo de estrategias avanzadas para la búsqueda y organización de información, y la mejora de la comunicación y la colaboración mediante plataformas digitales. Asimismo, se fomenta la creatividad y la innovación a través de la creación de contenidos accesibles y el aprendizaje inicial de conceptos de programación.

Otro aspecto fundamental del curso es la seguridad en el entorno digital, que se aborda desde la protección de datos personales hasta el uso responsable de las tecnologías. Además, se pone un énfasis especial en la capacidad de resolver problemas técnicos y adaptarse a herramientas emergentes, garantizando una actualización constante y efectiva frente a los desafíos tecnológicos.

Con un equilibrio entre teoría y práctica, este curso busca no solo transmitir conocimientos avanzados, sino también asegurar su aplicación en diferentes contextos profesionales, educativos y sociales, siempre priorizando la accesibilidad y la inclusión.


TEMA 1
USO BÁSICO DEL SISTEMA OPERATIVO

1

USO BÁSICO DEL SISTEMA OPERATIVO

El acercamiento al mundo de la informática va a pasar, necesariamente, por aprender a manejarse con los diferentes sistemas operativos instalados en los ordenadores, teléfonos inteligentes y otros dispositivos.

Este manual te permitirá aprender los conceptos básicos y el funcionamiento de un Sistema Operativo de forma que puedas continuar profundizando con el desarrollo de habilidades y competencias.

1.1 DEFINICIÓN Y TIPOS

Definición

Un sistema operativo (S.O.) es el software fundamental que permite que el hardware de un dispositivo electrónico —como un ordenador, smartphone o tablet, por ejemplo— funcione y sea utilizable por los usuarios. Actúa como un intermediario entre el hardware y las aplicaciones que ejecutamos, gestionando los recursos como la memoria, procesador y dispositivos de entrada y salida.

Por otro lado, proporciona una interfaz que facilita la interacción del usuario con la máquina ya sea mediante la presentación de un entorno gráfico (GUI) manejable con un ratón u otro dispositivo señalador, o mediante una línea de comandos donde se introducen instrucciones (CLI).

GUI: Graphics User Interface. Entorno gráfico amigable que presenta ventanas, menús, iconos y un cursor que utiliza el usuario para manejar el Sistema Operativo.

CLI: Command Line Interface. Terminal de texto con un *prompt* que queda a la espera de recibir instrucciones mediante comandos, atributos y modificadores.

El sistema operativo es el núcleo del funcionamiento de cualquier dispositivo digital, permitiendo la ejecución de programas y la coordinación de todas las actividades internas desde las tareas más básicas a las más complejas.

Además, proporciona los elementos comunes que utilizarán los programas instalados como, por ejemplo, la gestión y administración de archivos, ventanas, iconos, menús y otros componentes necesarios permitiendo un desarrollo más sencillo y rápido de todo tipo de aplicaciones adicionales.

Tipos de Sistemas Operativos

Existen diferentes modelos de clasificación de los sistemas operativos atendiendo a distintos modelos o criterios como, por ejemplo, su diseño, propósito y capacidad de gestión.

A continuación, se presentan las principales clasificaciones:

1.1.1 Por su capacidad de gestión de tareas

- **Monotarea:**

  Son sistemas operativos diseñados para ejecutar una sola tarea a la vez. Es más común en dispositivos o sistemas integrados (embebidos) con funciones específicas. Por ejemplo, algunos sistemas operativos en dispositivos IoT (Internet de las Cosas).

- **Multitarea:**

  Estos sistemas operativos pueden ejecutar múltiples tareas al mismo tiempo, optimizando el uso del procesador. Son los habituales en equipos informáticos que van a ser utilizados por usuarios. Por ejemplo, Microsoft Windows, macOS y Linux.

1.1.2 Por su capacidad de gestión de usuarios

A lo largo de la historia de los sistemas operativos, se ha pasado de soluciones en las que no se requería una gestión de usuarios y permisos ya que los equipos no se conectaban en red o no era habitual que más de una persona utilizara el ordenador. De ese modo se desarrollan, en primer lugar, los sistemas monousuario que evolucionan naturalmente hasta los tipos actuales con gestión múltiple de usuarios como norma general.

- **Monousuario:**

  Permiten el acceso a un solo usuario a la vez. Eran ampliamente utilizados en los primeros equipos informáticos de uso doméstico de la historia. Por ejemplo: MS-DOS, CP/M, DR-DOS.

- **Multiusuario:**

  Soportan la conexión simultánea de varios usuarios que tendrán sus propios entornos, archivos, configuraciones y permisos. Por ejemplo: Unix, Linux, Microsoft Windows, sistemas operativos de servidor, macOS.

1.1.3 Por su propósito

Se desarrolla software para un uso generalista o para dispositivos específicos. En entornos domésticos, empresariales y aquellos donde se requiere la instalación de diferentes paquetes, se requiere la utilización de sistemas operativos que sean capaces de ejecutar una cantidad diversa de programas.

Aquellos dispositivos que van a realizar una serie de tareas concreta o especializada incorporan sistemas operativos creados para esa actividad concreta.

- **Sistemas operativos de propósito general:**

  Se diseñan para la realización de una amplia gama de tareas como la navegación a través de internet, creación de todo tipo de documentos o para jugar. Por ejemplo: Microsoft Windows 10, macOS Ventura, Ubuntu.

- **Sistemas operativos de propósito específico:**

  Diseñados para cumplir funciones concretas como el control de maquinaria o gestión de bases de datos en tiempo real. Suelen instalarse en equipos autónomos o donde se requiere alta disponibilidad y seguridad. Por ejemplo: FreeRTOS para dispositivos embebidos o integrados.

1.1.4 Por su arquitectura

Esta clasificación agrupa los sistemas operativos según el tipo de equipo informático donde se van a instalar.

- **Sistemas operativos de escritorio:**

  Se optimizan para equipos informáticos personales (PC) de sobremesa o portátiles y cuentan con escritorios gráficos operados usando un dispositivo señalador (ratón, touchpad, lápiz óptico). Su curva de aprendizaje es baja ya que se diseñan para ser intuitivos y sencillos. Por ejemplo: Microsoft Windows, macOS, POP!Linux.

- **Para móviles:**

  Se adaptan para su uso con dispositivos como smartphones y tablets con énfasis en su usabilidad táctil y buena eficiencia energética. Por ejemplo, Android o iOS.

- **Sistemas operativos para servidores:**

  Están diseñados para proporcionar diferentes servicios para equipos o usuarios que se conectan. Gestionan redes, aplicaciones empresariales y servicios en nube. Quedan a la escucha para ofrecer los datos que solicita un usuario o programa. Por ejemplo: Microsoft Windows Server, Red Hat Enterprise Linux.

- **Sistemas empotrados (embebidos):**

  Se ejecutan en dispositivos con funciones específicas como electrodomésticos, sistemas de control, cámaras o sistemas de navegación. Por ejemplo: Intel-Samsung Tizen, Wind River Systems VxWorks.

1.1.5 Por su respuesta en tiempo

Los ordenadores se encargan de realizar las tareas que les ordena el usuario. En ocasiones, estas tareas son tiempo-dependientes, es decir, se requiere su ejecución en el mismo instante en el que ocurren o, por el contrario, pueden demorar o ejecutarse en otro momento en función de su prioridad.

- **Sistemas operativos de tiempo real (RTOS):**

  Garantizan la respuesta inmediata ante eventos críticos. Se utilizan en entornos donde un retraso puede causar fallos graves. Por ejemplo: sistemas de control en aviación o dispositivos médicos.

- **No de tiempo real:**

  Ejecutan o procesan las tareas en función de la prioridad de estas sin necesidad de ofrecer respuestas inmediatas. Por ejemplo, los sistemas operativos de uso cotidiano como Microsoft Windows o macOS.

1.2 DIFERENTES VERSIONES Y SISTEMAS OPERATIVOS DISPONIBLES

Los sistemas operativos han ido evolucionando, a lo largo de la historia de la informática, para adaptarse a todo tipo de dispositivos, usos y entornos. Según las características y tipo de hardware para el que se diseñan, es posible clasificarlos en varias categorías.

Además, un sistema operativo concreto cualquiera va recibiendo modificaciones a lo largo del tiempo, incorporando mejoras en rendimiento, seguridad y accesibilidad presentando diferentes versiones de este.

Los diferentes sistemas operativos van a cubrir las necesidades de uso en función del tipo de dispositivo donde se instalan así como los requisitos específicos de cada entorno.

A medida que transcurre el tiempo, cada sistema incorpora modificaciones que agregan nuevas funcionalidades, corrigen errores y mejoran la seguridad, permitiendo a los usuarios contar con nuevas herramientas más eficientes y adaptadas a las demandas tecnológicas actuales.

1.2.1 Sistemas operativos para ordenadores de escritorio y portátiles

Son paquetes de software pensados para ofrecer una experiencia de usuario completa en equipos personales. Incluyen interfaces gráficas avanzadas, herramientas de productividad y compatibilidad con amplio abanico de software.

Los sistemas operativos actuales más comunes tanto en entornos domésticos como empresariales son:

- **Microsoft Windows**

  Es uno de los más utilizados a escala global. Entre sus versiones más conocidas destacan Windows XP, Windows 7, Windows 8, Windows y, recientemente, Windows 11. El desarrollo de este sistema operativo ha ido incorporando mejoras en diseño, compatibilidad con hardware más moderno y nuevas funciones de accesibilidad.

- **MacOS**

  Es un sistema operativo desarrollado por Apple y exclusivo para sus equipos informáticos, aunque se puede instalar y utilizar virtualizado para pruebas. Comenzó con la versión 10.0 (MacOS X) y ha ido evolucionando a versiones como Catalina, Big Sur, Monterrey o Ventura. Cada una de ellas incorpora mejoras en rendimiento y funciones de seguridad.

- **Linux**

  Más que un único sistema operativo, se trata de diferentes distribuciones, o "*distros*" (Ubuntu, Debian, Fedora, Mint, Kali, entre muchas otras).

  Se trata de un sistema operativo muy potente que puede incluir funciones avanzadas que incluyen elementos de arquitectura cliente-servidor. Su característica fundamental es su filosofía de uso libre y la capacidad de personalización, lo que lo convierte en una opción muy extendida tanto en entornos domésticos como profesionales.

1.2.2 Sistemas operativos para móviles

Específicamente diseñados para smartphones y tablets. Se centran en la usabilidad táctil, el uso eficiente de la batería y la integración de aplicaciones enfocadas en la movilidad.

Los más conocidos y habituales son iOS y Android.

- **Android**

  Desarrollado por Google. Es el más utilizado en el mundo. Sus versiones más antiguas llevaban nombres de dulces mientras que las más modernas se denominan con numeración.

- **IOS**

  Lo fabrica Apple para el iPhone y el iPad. Las versiones de iOS se van numerando de forma progresiva (iOS 14, iOS 15, iOS 16, etc) y con cada cambio incorporan mejoras en la experiencia de usuario, rendimiento, seguridad e integración con otros dispositivos de Apple.

1.2.3 Sistemas operativos para servidores

Se enfocan en los servicios corporativos mediante el uso de programas que ofrecen recursos, gestión de redes, bases de datos y archivos. Priorizan la estabilidad, seguridad y escalabilidad.

Estos sistemas son los que permiten la existencia de servicios como las páginas web, el correo electrónico, compartir archivos a través de la red, gestión avanzada de usuarios, sistemas de directorio activo, la nube, etc.

Los más habituales son:

- **Microsoft Windows Server**

  Es la versión de la empresa Microsoft para entornos empresariales, con ediciones como Windows Server 2012, 2016, 2019 y 2022.

- **Linux en servidores**

  Las distribuciones como Red Hat Enterprise (RHEL), Ubuntu Server o CenOS son las que se han posicionado como soluciones robustas, fiables y flexibles para servicios de hosting o aplicaciones corporativas.

1.2.4 Sistemas operativos empotrados o de propósito específico

Son sistemas operativos diseñados para dispositivos con funciones muy concretas como electrodomésticos inteligentes, televisores, automatización industrial o plataformas de Internet de las Cosas (IoT).

Los más conocidos son:

- **Tizen o WebOS**

  Se instalan en televisores inteligentes de Sansung o LG, relojes y otros dispositivos de consumo.

- **FreeRTOS o VxWorks**

  Son frecuentes en sistemas embebidos que requieren respuesta rápida y fiable como, por ejemplo, maquinaria especializada o equipos médicos.

1.3 INICIO, APAGADO, HIBERNACIÓN Y SUSPENSIÓN

El proceso de **inicio** de un sistema operativo, comúnmente llamado "arranque" o "*boot*", consiste en cargar los componentes esenciales del sistema en la memoria principal.

En primer lugar, el hardware lleva a cabo una verificación inicial conocida como *POST* (*Power-On Self-Test*) para comprobar que todos los componentes funcionan correctamente.

Inicio:
Proceso de arranque donde el sistema operativo se carga en la memoria.

Apagado:
Cierre seguro de todos los programas y procesos antes de apagar el hardware.

Hibernación:
Guarda el estado del sistema en el disco duro y apaga el equipo. Ideal para largas pausas de uso.

Suspensión:
Mantiene el estado en la RAM y reduce el consumo energético.

A continuación, se localiza el gestor de arranque (*bootloader*), el cual se encarga de encontrar el sistema operativo y cargarlo en la memoria RAM.

Al final de este proceso se encuentra el "login" o pantalla de inicio de sesión del usuario que solicita las credenciales de acceso tras la cual se accede al escritorio o entorno de trabajo.

El proceso de **apagado** es el procedimiento que ordena el cierre correcto de todos los programas y procesos que se encuentran en ejecución en ese momento, buscando evitar la pérdida de datos o daños en el software.

Cuando el usuario selecciona la opción de apagar, el sistema operativo toma el control del cierre ordenado de aplicaciones, detiene servicios y, finalmente, desconecta la alimentación del equipo. Es un paso fundamental para asegurar que, en el siguiente uso, el dispositivo arranque sin errores ni archivos dañados.

La **hibernación** y la **suspensión** son modos de ahorro de energía que conservan el estado actual de la sesión pero operan de modo diferente.

La hibernación guarda todo el contenido de la memoria (aplicaciones y documentos abiertos) en el disco duro o la unidad de estado sólido (SSD), y luego apaga la computadora por completo. Es un modo ideal para periodos largos de inactividad, ya que no consume energía y se puede retomar el trabajo exactamente en el punto donde se dejó.

Por otro lado, la suspensión mantiene la sesión activa en la memoria RAM (volátil) y reduce significativamente el consumo energético sin apagar el equipo por completo.

Si bien la suspensión permite retomar la actividad de manera casi inmediata, es más adecuada para pausas cortas dado que el PC sigue consumiendo algo de energía para conservar la información en la memoria.

1.4 PROGRAMAS BÁSICOS Y USOS PRINCIPALES

El sistema operativo ofrece un entorno en el que podemos instalar y ejecutar una gran variedad de aplicaciones. Sin embargo, existen algunos programas considerados como "básicos" debido a que cubren necesidades fundamentales de casi cualquier usuario.

A continuación se describen los principales tipos de software que deberían formar parte de la formación en competencias digitales.

1.4.1 Navegador WEB

Definición y funciones

El navegador web —o *browser*— es la puerta de entrada a internet. Permite visualizar páginas web, interactuar con servicios en línea y acceder a cualquier contenido disponible en la red.

Sus funciones principales incluyen:

- Interpretar y mostrar el código HTML, CSS y JavaScript de los sitios web.
- Permitir la navegación por varias pestañas o ventanas.
- Administrar la seguridad y privacidad mediante configuraciones de cookies, contraseñas, bloqueadores de publicidad y filtros de contenido malicioso.

Ejemplos de navegadores

- **Google Chrome**: conocido por su rapidez y amplia compatibilidad con extensiones.
- **Mozilla Firefox**: destaca por su enfoque en la privacidad y el software de código abierto.
- **Microsoft Edge**: evolucionado a partir de Internet Explorer, actualmente basado en Chromium.
- **Safari**: navegador predeterminado en el ecosistema Apple (macOS, iOS).

Consejos de uso

El manejo de un navegador pasa por conocer su menú principal con objeto de asimilar su funcionalidad.

Es importante mantener el navegador lo más actualizado posible para evitar las vulnerabilidades de seguridad que puedan existir.

Es conveniente utilizar marcadores y carpetas para organizar los accesos a la red evitando, si es posible, almacenar usuarios y contraseñas de "login" a los diferentes sitios.

Puede ser interesante configurar la sincronización en la nube para contar con el historial y marcadores en los diferentes dispositivos donde se usa el mismo navegador.

1.4.2 Explorador de archivos

Definición y funciones

El explorador de archivos (o gestor/administrador de archivos) es la herramienta que permite organizar y manejar la información almacenada en el disco duro, memorias externas o unidades de red. Entre sus funciones principales se encuentran:

- Crear, copiar, mover, renombrar y eliminar archivos y carpetas.
- Administrar distintas ubicaciones de almacenamiento (discos duros, unidades USB, almacenamiento en la nube).
- Mostrar información detallada de los archivos (nombre, tamaño, tipo, fecha de modificación).

Ejemplos destacados

- **Windows Explorer (o Explorador de Windows)**: incluye un panel lateral para navegar por las ubicaciones y un panel principal para visualizar el contenido.
- **Finder (macOS)**: muestra un diseño minimalista, con acceso directo a carpetas y servicios de iCloud.
- **Nautilus, Dolphin, Thunar (Linux)**: varias distribuciones Linux tienen su propio explorador, pero comparten funciones básicas similares.

Buenas prácticas

Mantener los archivos digitales bien organizados es esencial para aumentar la productividad y reducir el estrés al buscar documentos. Un primer paso consiste en definir una estructura de carpetas clara y coherente, en la que cada carpeta o subcarpeta responda a un propósito específico. Por ejemplo, puedes crear carpetas principales para proyectos concretos, tipos de archivo (documentos, imágenes o vídeos) o categorías generales (trabajo, estudios o finanzas). Esta organización jerárquica facilita la localización de archivos y previene confusiones.

Además, resulta fundamental nombrar los archivos de manera coherente y sistemática. Incluir fechas en formato "AAAA-MM-DD" y palabras clave descriptivas en los nombres, como en "2025-01-19_Presupuesto_ProyectoX.xlsx", agiliza la búsqueda y ayuda a ubicar rápidamente la información necesaria.

Por último, es aconsejable vaciar de forma regular las carpetas de descargas y los archivos temporales, que suelen acumular material innecesario, duplicados y versiones obsoletas. Invertir unos minutos de manera periódica en esta tarea previene la acumulación excesiva, libera espacio en el dispositivo y contribuye a mantener un entorno de trabajo digital más ordenado y eficiente.

1.4.3 Visores de documentos

Definición y funciones

Los visores de documentos permiten abrir y leer archivos en formatos específicos, generalmente sin ofrecer todas las herramientas de edición de un programa completo. Su función principal es garantizar la correcta visualización de textos, imágenes o elementos incrustados.

Ejemplos y usos

- **Visores de PDF**: Adobe Acrobat Reader, Foxit Reader, SumatraPDF. Permiten la lectura de archivos PDF, anotaciones simples o resaltar texto.
- **Visores de imágenes y documentos ofimáticos**: aplicaciones ligeras que suelen venir preinstaladas en los sistemas operativos o suites ofimáticas, y que abren archivos como .docx, .xlsx o .pptx en modo lectura.

Ventajas

Se trata de software que, normalmente, es de uso libre, rápido y fácil de instalar. Añade funciones que mejoran la operatividad del propio sistema.

El consumo de recursos del sistema es menor ya que no se instalan funciones adicionales de edición del documento comparada con las herramientas completas.

Son adecuados para los usuarios que solo requieren la apertura o impresión de estos archivos.

1.4.4 Procesadores de texto

Los procesadores de texto son programas diseñados o enfocados en la creación, edición y formato de documentos de texto. Permiten escribir, revisar ortografía, añadir imágenes, tablas e ilustraciones además de controlar los formatos de los párrafos, márgenes, páginas o tipos de letra. Son esenciales para redactar cartas, informes, proyectos o cualquier otro tipo de documento escrito.

Ejemplos destacados

- **Microsoft Word**: parte de la suite Microsoft 365 (antes Office), líder en el ámbito empresarial y académico.
- **Google Docs**: aplicación web gratuita que facilita el trabajo colaborativo en línea, con guardado automático en la nube.
- **LibreOffice Writer**: herramienta de software libre con funcionalidades avanzadas y gran compatibilidad de formatos.

Funciones clave de un procesador de textos

Las aplicaciones de edición de textos suelen ofrecer una amplia gama de opciones que mejoran la presentación y la colaboración en documentos digitales. Entre estas se incluyen diversos estilos y formatos para resaltar el contenido (como negrita, cursiva y subrayado), la posibilidad de usar viñetas para organizar ideas de manera clara y concisa, así como funciones para la inserción de tablas, imágenes y enlaces que facilitan la integración de información visual y referencias externas.

Además, cuentan con herramientas de revisión ortográfica y gramatical, esenciales para garantizar la corrección del texto y optimizar el flujo de trabajo. En entornos colaborativos, la utilidad de control de cambios y la inserción de

comentarios permite a varios usuarios revisar, modificar o discutir diferentes aspectos del documento sin perder el historial de ediciones.

Por último, estas aplicaciones ofrecen múltiples opciones de exportación, brindando compatibilidad con formatos tan variados como .docx, .pdf y .odt, lo que contribuye a una mayor versatilidad y facilita la difusión de los documentos en distintas plataformas.

- Estilos y formatos (negrita, cursiva, subrayado, viñetas, etc.).
- Inserción de tablas, imágenes y enlaces.
- Revisión ortográfica y gramatical.
- Control de cambios y comentarios para trabajos colaborativos.
- Opciones de exportación a diversos formatos (.docx, .pdf, .odt, etc.).

1.4.5 Bases de datos

Definición y funciones

El software de bases de datos, o motores, permite recopilar, organizar y gestionar información de forma estructurada, facilitando la búsqueda y el análisis de datos.

Aunque es un tema que pueda parecer que escapa de los temas que se tratan en toda actividad de mejora de competencias digitales, es importante conocer, al menos, los fundamentos.

Manejar una herramienta básica de bases de datos puede ser muy útil en diferentes ámbitos (administración, gestión de proyectos, inventarios, etc).

Ejemplos destacados

- **Microsoft Access**: orientado a soluciones pequeñas o medianas y con una interfaz gráfica intuitiva.
- **MySQL Workbench**: para quienes necesitan gestionar grandes volúmenes de información y realizar consultas SQL avanzadas.
- **SQLite**: suele utilizarse en aplicaciones móviles y de escritorio por su ligereza y simplicidad.

Las bases de datos constituyen herramientas esenciales para la gestión y organización de información, ya que permiten la creación de tablas con campos y tipos de datos definidos, como texto, número o fecha, entre otros.

Gracias a esta estructura, es posible clasificar y manejar la información de manera eficiente, al tiempo que las consultas permiten filtrar y analizar los datos de forma rápida y precisa según las necesidades de cada usuario.

Además, la posibilidad de generar formularios e informes ofrece una vía práctica para la entrada y presentación de la información, facilitando la revisión de resultados y la recopilación de nuevos datos.

Por último, la integración con otros programas potencia la utilidad de las bases de datos al permitir la importación y exportación de información desde distintas fuentes, optimizando así el flujo de trabajo y la conectividad entre aplicaciones.

Características principales

- Creación de tablas con campos y tipos de datos definidos (texto, número, fecha, etc.).
- Realización de consultas para filtrar y analizar la información.
- Capacidad de generar formularios e informes para la presentación y entrada de datos.
- Integración con otros programas para la importación o exportación de datos.

1.4.6 Hojas de cálculo

Definición y funciones

Las hojas de cálculo son aplicaciones diseñadas para manipular y analizar datos numéricos. Funcionan a partir de celdas organizadas en filas y columnas donde se pueden ingresar fórmulas, realizar operaciones matemáticas y estadísticas, así como presentar los resultados en forma de tablas o gráficos.

Ejemplos destacados

- **Microsoft Excel**: estándar de la industria, con numerosas funciones, tablas dinámicas y macros para automatizar tareas complejas.

- **Google Sheets**: versión en la nube que permite la colaboración en tiempo real y la integración con otros servicios de Google.
- **LibreOffice Calc**: alternativa de software libre, compatible con muchos formatos y con gran variedad de funciones.

Herramientas importantes de una hoja de cálculo

- Funciones matemáticas y lógicas (SUMA, SI, CONTAR, PROMEDIO, etc.).
- Creación de gráficos (barras, líneas, sectores) para la representación visual de datos.
- Uso de tablas dinámicas para el análisis rápido de grandes volúmenes de información.
- Formato condicional para resaltar valores o tendencias significativas.

1.4.7 Editores gráficos

Definición y funciones

Los editores gráficos permiten crear, retocar o manipular imágenes, ilustraciones y fotografías.

Dependiendo de su nivel de complejidad, pueden servir para tareas sencillas de edición o para trabajos profesionales de diseño y retoque avanzado.

Ejemplos destacados

- **Paint** (Windows) o **Preview** (macOS): herramientas básicas, enfocadas en retoques simples y anotaciones.
- **GIMP**: Software libre y multiplataforma con funciones avanzadas de edición de imágenes.
- **Adobe Photoshop**: uno de los más reconocidos a nivel profesional, cuenta con herramientas punteras de retoque y composición fotográfica.

Aplicaciones principales

- Redimensionar y recortar imágenes.
- Ajustar brillo, contraste y otros parámetros de color.
- Añadir o eliminar elementos mediante capas y filtros.
- Diseñar gráficos para redes sociales, presentaciones o publicidad.

1.5 RESUMEN

El conocimiento y dominio de estos programas básicos facilita la productividad y la eficiencia en el entorno digital. Tanto si se utilizan para fines personales como profesionales, es fundamental aprender a instalar, configurar y emplear estas aplicaciones de manera segura y organizada. Además, entender sus principales funciones y buenas prácticas permite aprovechar todo su potencial, agilizando el trabajo diario y mejorando la calidad de los resultados.

- **Navegador web**:
  Chrome, Firefox, Safari, Edge.
- **Explorador de archivos**:
  Windows Explorer, Finder (macOS), Nautilus (Linux).
- **Visores de documentos**:
  Adobe Reader, Foxit Reader.
- **Procesadores de texto**:
  Microsoft Word, Google Docs, LibreOffice Writer.
- **Bases de datos**:
  Microsoft Access, MySQL Workbench.
- **Hojas de cálculo**:
  Microsoft Excel, Google Sheets, LibreOffice Calc.
- **Editores gráficos**:
  Paint, GIMP, Photoshop.

1.6 EJERCICIO PRÁCTICO: ORGANIZACIÓN, EDICIÓN Y VISUALIZACIÓN DE ARCHIVOS

Objetivo general

Dominar acciones básicas del sistema operativo: crear carpetas, renombrarlas, gestionar archivos, usar un procesador de texto, guardar documentos en diferentes formatos y abrirlos con visores. Así afianzarás lo aprendido sobre exploradores de archivos, procesadores de texto, visores de documentos y otras utilidades básicas.

PRÁCTICA 1. Identifica tu sistema operativo

1. **Observa qué** sistema operativo **(S.O.) usas**:
   - En Windows, pulsa en el menú Inicio y escribe "Información del Sistema" o "Acerca de" para ver la versión (por ejemplo, Windows 10 o Windows 11).
   - En macOS, haz clic en el icono de la manzana (arriba a la izquierda) y selecciona "Acerca de este Mac".
   - En Linux, puede variar según la distribución, pero normalmente verás la información en "Configuración del Sistema" o ejecutando el comando lsb_release -a en la terminal.
2. **Anota** la versión o nombre exacto: (ej. "Windows 10 Home versión 22H2" / "macOS Ventura 13.x" / "Ubuntu 22.04 LTS"). Este paso te ayuda a familiarizarte con cómo identificar y describir tu entorno.

PRÁCTICA 2. Crea una carpeta y organiza archivos

1. **Abre el explorador de archivos** (Windows), Finder (macOS) o tu gestor de archivos en Linux (Nautilus, Dolphin, etc.).
2. **Crea una carpeta** nueva en tu escritorio (o en otra ubicación que prefieras). Ponle un nombre descriptivo y organizado.
3. Por ejemplo: 2025-01-19_Ejercicios_Practicos.
4. **Dentro de esa carpeta**, crea dos subcarpetas:
   - Documentos.
   - Imágenes.

5. **Guarda estos nombres con un criterio ordenado** (tal como se explica en el texto sobre buenas prácticas), usando fecha y palabras clave si deseas.

   Por ejemplo: 2025-01-19_Documentos en vez de solo Documentos.

PRÁCTICA 3. Crea y guarda un documento de texto

1. **Abre un procesador de texto**:

   Microsoft Word, LibreOffice Writer o Google Docs (si prefieres hacerlo en la nube).

2. **Escribe un texto breve** donde incluyas:
   - El tipo y versión de sistema operativo que estás usando (de la Parte 1 del ejercicio).
   - Una breve definición, con tus propias palabras, de "¿Qué es un sistema operativo?"
   - Algún listado de las carpetas que acabas de crear en el paso anterior.

3. **Ponle formato** (utiliza negrita, cursiva o viñetas) para practicar:
   - Resalta en **negrita** la definición de sistema operativo.
   - Crea una lista con viñetas describiendo las carpetas (ejemplo: Documentos, Imágenes…).

4. **Guarda** el archivo en la carpeta Documentos que creaste en el paso anterior.
   - Asigna un nombre claro, por ejemplo: 2025-01-19_SistemaOperativo.docx.

PRÁCTICA 4. Exporta a PDF y ábrelo con un visor

1. **Exporta** o **guarda** tu documento como PDF (la mayoría de los procesadores de texto ofrecen esta función en "Guardar como…" o "Exportar a PDF").

2. Guarda este PDF también en la carpeta Documentos, con un nombre similar: 2025-01-19_SistemaOperativo.pdf.

3. **Abre** el archivo PDF con el visor que tengas disponible: Adobe Acrobat Reader, Foxit Reader, Vista Previa (macOS), etc. Comprueba que se vea correctamente lo que escribiste.

PRÁCTICA 5. Organiza una imagen y edítala (muy básico)

1. **Descarga** o localiza una imagen que tengas (fotografía o icono).
2. **Muévela** (o cópiala) a la carpeta Imágenes que creaste.
3. **Abre** esa imagen con un editor básico: Paint (Windows), Preview (macOS) o un editor más avanzado como GIMP (multiplataforma).
4. **Realiza un ajuste sencillo**: por ejemplo, recortar un poco la imagen o añadir una anotación (texto).
5. **Guarda** los cambios usando "Guardar como…" y añade un nombre que refleje la edición (por ejemplo: FotoRecortada.jpg) para mantener orden.

PRÁCTICA 6. (Opcional) Crea una hoja de cálculo sencilla

1. **Abre** un programa de hoja de cálculo: Microsoft Excel, LibreOffice Calc o Google Sheets.

   Introduce en la primera columna, fila 1 hasta 5, algunos valores numéricos.
2. **Usa** una función simple, como =SUMA(A1:A5) (o =SUM(A1:A5) si tu aplicación está en inglés), para comprobar la suma de esos valores.
3. **Guarda** el archivo con un nombre claro (ej. 2025-01-19_EjemploCalculo.xlsx) en tu carpeta Documentos.

PRÁCTICA 7. Revisa y limpia tu carpeta de descargas (buenas prácticas)

1. Abre la carpeta de descargas (o "Downloads").
2. Elimina los archivos que ya no necesites.
3. Mueve los archivos importantes a tus carpetas organizadas (por ejemplo, a Documentos o Imágenes).
4. Vacía la Papelera o la papelera de reciclaje para finalizar la limpieza.

1.6.1 Resultado final y conclusiones

Tras completar estos pasos:

- **Habrás identificado tu** sistema operativo y comprendido la importancia de saber su versión.
- **Crearás una estructura de carpetas** (estructura jerárquica) y nombrarás archivos de forma organizada.
- **Manejarás un procesador de textos** para crear un documento, darle formato y exportarlo a PDF.
- **Aprenderás a abrir tu documento** con un visor de PDF y a manipular una imagen con un editor básico.
- De forma opcional, **experimentarás con hojas de cálculo**, trabajando con valores numéricos y funciones simples.
- **Aplicarás buenas prácticas** de limpieza y organización al gestionar archivos descargados.

Este ejercicio reúne, de manera integrada, varios de los conceptos expuestos en el texto: el uso del explorador de archivos, la importancia de un procesador de texto, la visualización en PDF, la edición básica de imágenes y las buenas prácticas de organización digital.

1.7 AUTOEVALUACIÓN (10 PREGUNTAS)

El propósito de este examen es comprobar que los conceptos estudiados se han asimilado correctamente y, al mismo tiempo, ofrecer una oportunidad para repasar y reforzar los aprendizajes adquiridos de manera relajada; te invitamos a realizarlo con serenidad, sin verlo como una presión, sino como un recurso constructivo que confirma tu dominio del tema y te impulsa a continuar mejorando.

Toma el tiempo que necesites y consulta las partes que no recuerdes o no hayas comprendido bien.

1. **¿Cuál es la función principal de un sistema operativo?**
   a) Permitir solo la navegación web.
   b) Controlar exclusivamente la conexión a internet de un dispositivo.
   c) Actuar como intermediario entre el hardware y las aplicaciones, gestionando recursos y facilitando la interacción usuario-equipo.
   d) Funcionar únicamente como una interfaz gráfica para el usuario.

2. **¿Qué caracteriza a un sistema operativo multitarea?**
   a) Solo permite ejecutar una tarea a la vez.
   b) Puede ejecutar múltiples tareas de manera simultánea.
   c) No necesita memoria RAM para funcionar.
   d) Funciona únicamente en dispositivos móviles.

3. **¿Cuál de los siguientes ejemplos corresponde a un sistema operativo monousuario?**
   a) macOS
   b) Linux
   c) Windows 10
   d) MS-DOS

4. **¿Cuál de estas opciones describe mejor un sistema operativo de tiempo real (RTOS)?**
   a) Garantiza la respuesta inmediata ante eventos críticos.
   b) Está diseñado solo para la navegación por internet.
   c) No requiere actualizarse nunca.
   d) No se utiliza en entornos industriales ni médicos.

5. **Según el texto, uno de los navegadores más utilizados, conocido por su rapidez y amplia compatibilidad de extensiones, es:**
   a) Microsoft Edge.
   b) Google Chrome.
   c) Safari.
   d) Mozilla Firefox.

6. ¿Cuál de los siguientes programas sirve principalmente para organizar y manejar los archivos en un equipo?

a) Explorador de archivos (Windows), Finder (macOS) o Nautilus (Linux).
b) GIMP o Photoshop.
c) Google Chrome o Mozilla Firefox.
d) Microsoft Excel o Google Sheets.

7. ¿Cuál de los siguientes ejemplos se menciona como un sistema operativo para servidores?

a) iOS.
b) Android.
c) Red Hat Enterprise Linux (RHEL).
d) Tizen.

8. ¿Qué acción realiza el sistema operativo cuando el usuario selecciona "apagar" el equipo?

a) Aumenta la velocidad del procesador para optimizar el rendimiento.
b) Cierra correctamente los programas y procesos en ejecución y luego desconecta la alimentación.
c) Pone el equipo en suspensión indefinida consumiendo energía de la batería.
d) Reinicia la memoria RAM sin cerrar ninguno de los programas.

9. ¿Qué programa se caracteriza por permitir la creación, edición y formato de documentos de texto con funciones como revisión ortográfica y control de cambios?

a) Adobe Acrobat Reader.
b) Microsoft Word (u otros procesadores de texto).
c) Paint (Windows) o Preview (macOS).
d) Microsoft Excel (u otras hojas de cálculo).

10. El modo de hibernación de un sistema operativo consiste en:

a) Mantener la sesión activa en la memoria RAM sin apagar el equipo.
b) Cerrar todos los programas y reiniciar el sistema operativo.
c) Guardar el estado de la memoria en el disco duro o SSD y apagar completamente el equipo.
d) Borrar permanentemente los datos de la memoria para liberar espacio.

Respuestas correctas

1-C, 2-B, 3-D, 4-A, 5-B, 6-A, 7-C, 8-B, 9-B, 10-C.

¡**Enhorabuena**! Si has conseguido una buena puntuación, te invito a que continúes aprendiendo. Y, si consideras que no es suficiente, puedes repasar aquellos puntos que necesites revisar.

1.8 GESTIÓN DE ARCHIVOS Y CARPETAS

La gestión de archivos y carpetas es una de las competencias digitales esenciales para cualquier persona que utilice un sistema informático. Consiste en organizar, clasificar y manipular la información que se almacena en el disco duro, unidades externas y/o en la nube.

Un buen manejo de archivos y carpetas incrementa la productividad, facilita la localización de datos y reduce el riesgo de pérdida de información.

1.8.1 Estructura y organización de la información

La correcta gestión y organización de la información es un pilar fundamental para garantizar la eficiencia en entornos laborales, académicos y personales.

En la actualidad, el volumen de documentos y archivos digitales que manejamos puede llegar a ser abrumador si no contamos con criterios claros para su clasificación y almacenamiento. Por ello, establecer una estructura coherente y aplicar convenciones adecuadas se convierte en la piedra angular de cualquier sistema de archivos bien organizado.

En los siguientes apartados aprenderemos, en primer lugar, la importancia de mantener una jerarquía clara que nos facilitará la búsqueda y acceso rápido a la información.

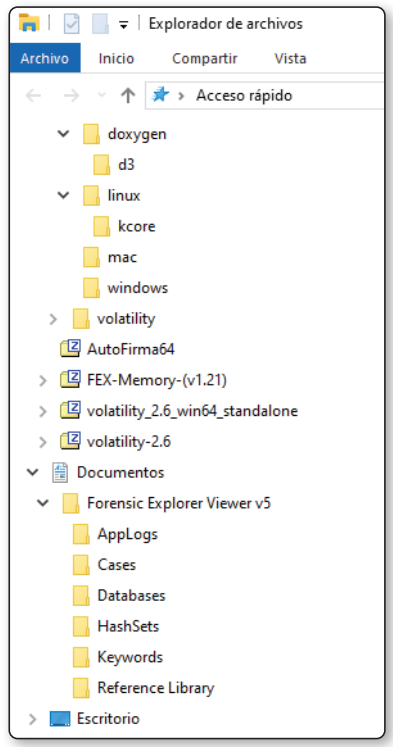


Figura 1.1. Árbol de directorios jerárquico

Posteriormente, se explican las mejores prácticas de nomenclatura para asegurar que cualquier persona, sin importar su experiencia o rol, pueda comprender el contenido de los archivos antes de abrirlos.

Por último, se presenta una breve revisión de los tipos de sistemas de archivos más comunes, resaltando sus características, limitaciones y ventajas, con el fin de orientar la selección más adecuada según las necesidades y el entorno de uso.

1.8.1.1 LA JERARQUÍA O ÁRBOL

La "jerarquía" de los archivos se refiere a la estructura en forma de árbol que permite organizar las carpetas, subcarpetas y archivos de un modo coherente que nos permita encontrar los datos de modo fácil y sencillo.

Mantener una estructura de carpetas lógica y coherente facilita la búsqueda y el acceso a los archivos. Por ejemplo, puedes crear una carpeta raíz para cada

proyecto, asignatura o departamento y, dentro de ella, subcarpetas para documentos, imágenes, bases de datos, etc.

De esta manera, se evita la acumulación de archivos sueltos en el Escritorio o en la carpeta de Descargas, se reduce la duplicación de información y permite mejorar la colaboración con otros usuarios, ya que cualquiera puede orientarse mejor si la estructura es ordenada.

1.8.1.2 CONVENCIONES DE NOMENCLATURA

En el momento de creación de un archivo o carpeta, conviene utilizar nombres de archivo descriptivos, de forma que se entienda su contenido o sirva como referencia sin tener que abrirlo.

Cada tipo de sistema operativo puede permitir el uso de diferentes combinaciones de caracteres pero, en general, se deben evitar los considerados como especiales (, /, :, *, ?, “, <, >, |) ya que puede provocar errores de compatibilidad.

Añadir, hacia el final del nombre del archivo o carpeta, la fecha y versión ofrece la posibilidad de controlar la evolución del documento (ej.: “Informe_ Ventas_2024_v2.docx”).

1.8.1.3 TIPOS DE SISTEMAS DE ARCHIVO (FS)

Los “*File Systems*” o Sistemas de Ficheros son la forma cómo el sistema operativo gestiona y organiza los archivos en el dispositivo de almacenamiento (disco duro, unidad de estado sólido, etc).

Cada sistema operativo utiliza el suyo propio aunque existe la posibilidad de leer y escribir documentos entre los diferentes sistemas gracias al soporte adicional que se puede instalar.

Cada sistema de ficheros ofrece características diferentes relacionadas con la seguridad, tamaño máximo de los archivos y compatibilidad.

Conocer las limitaciones y ventajas del sistema de archivos ayuda a decidir el formato más apropiado para las unidades USB, discos duros externos o instalaciones duales con dos o más sistemas operativos instalados en un mismo disco duro en diferentes particiones.

Los más comunes actualmente son: **NTFS (Windows)**, **APFS (macOS)**, **ext4 (Linux)**, **FAT32** y **exFAT.**

1.9 OPERACIONES BÁSICAS CON ARCHIVOS Y CARPETAS

La gestión de archivos y carpetas abarca desde su creación, ya sea mediante menús contextuales o comandos en la terminal, hasta su eliminación directa o a través de la papelera/reciclaje, pasando por el cambio de nombre y la organización coherente de su contenido. Además, incluye la posibilidad de copiar y mover documentos, generando duplicados o reubicándolos según sea necesario, y se apoya en potentes motores de búsqueda e indexación que facilitan la localización de información en sistemas Windows (Opciones de Índice), macOS (Spotlight) o Linux (herramientas como Catfish o Recoll).

Los siguientes puntos te muestran las operaciones más habituales con archivos y carpetas. Es recomendable practicar para interiorizar su funcionamiento:

1. **Creación de archivos y carpetas**
   - En la mayoría de los sistemas, basta con hacer clic derecho → "Nuevo" → "Carpeta" o "Archivo" (dependiendo de la aplicación que esté creando el documento).
   - También es posible crearlos desde la línea de comandos (ej.: mkdir en Linux/Mac o md en Windows para crear carpetas).
2. **Renombrar**
   - Se puede renombrar un archivo o carpeta haciendo clic derecho → "Cambiar nombre" o pulsando la tecla F2 en Windows.
   - Resulta útil para mantener una nomenclatura coherente y clara en todos los documentos.
3. **Copiar y mover**
   - **Copiar**: se duplica el archivo/carpeta, creando un segundo ejemplar. La versión original permanece en su ubicación.
   - **Mover**: el archivo/carpeta se transfiere a otra ubicación, eliminándose de la original.
   - Es posible realizar estas acciones mediante menús contextuales (clic derecho → "Copiar" / "Cortar" y luego "Pegar"), atajos de teclado (Ctrl + C, Ctrl + X, Ctrl + V en Windows, o Cmd + C, Cmd + X, Cmd + V en macOS) o líneas de comando (cp, mv en Linux/Mac; copy, move en Windows).

4. **Eliminar**
   - Los archivos o carpetas se pueden borrar enviándolos a la "Papelera" (macOS/Linux) o "Papelera de reciclaje" (Windows).
   - El vaciado de la papelera/reciclaje los elimina de forma definitiva.
   - Con línea de comandos (ej. rm en Unix/Linux, del en Windows), se eliminan directamente sin pasar por la papelera, por lo que hay que ser precavido.
5. **Búsqueda e indexación**
   - Los sistemas operativos modernos incluyen motores de búsqueda para localizar documentos por nombre, extensión o incluso contenido.
   - En Windows se puede configurar la indexación desde las Opciones de Índice en el Panel de Control, mientras que en macOS se utiliza Spotlight para búsquedas rápidas. En Linux, herramientas como Catfish, Recoll o el propio buscador de archivos del entorno de escritorio facilitan la localización.

1.10 COPIAS DE SEGURIDAD Y VERSIONADO

La protección de datos comienza con la creación de copias de seguridad locales, ya sea guardando duplicados en discos duros externos o unidades USB, lo que reduce significativamente el riesgo de pérdida ante fallos del disco duro o ataques de malware. Además, el versionado de documentos contribuye a un mejor control de los cambios: puede realizarse de forma manual (añadiendo sufijos como "v1", "final" o "revisado") o mediante herramientas de control de versiones como Git o Subversion, fundamentales en entornos colaborativos para registrar y revertir modificaciones. Por último, las copias de seguridad en la nube a través de servicios como OneDrive, Google Drive, Dropbox o iCloud permiten sincronizar y acceder fácilmente a los archivos desde diversos dispositivos, así como restaurar versiones anteriores en caso de borrado o modificación accidental.

La estrategia 3-2-1 de backup recomienda mantener al menos tres copias de los datos, almacenadas en dos tipos de medios diferentes, y con una de esas copias ubicada fuera del lugar principal (offsite). Este enfoque reduce el riesgo de pérdida de información en caso de fallas, desastres o ataques, asegurando que siempre exista un respaldo disponible:

- **Tres copias de seguridad**: contar con al menos tres copias de los datos garantiza que, ante una falla o corrupción de un respaldo, aún haya otras alternativas seguras para restaurar la información.

  Por ejemplo: tienes un archivo importante en el disco duro de tu ordenador (copia 1), haces un respaldo automático en un disco duro externo (copia 2) y, adicionalmente, subes el archivo a un servicio de almacenamiento en la nube (copia 3).

- **Dos tipos de medios diferentes**: emplear distintos soportes (por ejemplo, disco duro y almacenamiento en la nube) protege contra problemas específicos de un medio en particular, como fallas físicas o incompatibilidades tecnológicas.

  Por ejemplo: una de tus copias está en un disco duro externo (medio 1) y la otra en la nube (medio 2). Así, si hay un problema mecánico con el disco externo, aún dispones de la copia en internet, y viceversa.

- **Una copia fuera del lugar principal (offsite)**: almacenar al menos un respaldo en una ubicación externa (o en la nube) protege los datos en caso de desastres locales, incendios o robos, asegurando la disponibilidad de la información.

  Por ejemplo: guardas un disco duro de respaldo en la casa de un familiar u otro local alternativo. De esta manera, si sucede un desastre en tu ubicación principal (incendio, inundación, robo), tus datos siguen protegidos en otro lugar.

1.10.1 Puntos clave

1. **Copias de seguridad locales**
   - Guardar duplicados de la información en discos duros externos o unidades USB.
   - Realizar backups periódicos minimiza la pérdida de datos ante fallos en el disco duro o ataques de malware.
2. **Versionado de documentos**
   - Puede realizarse manualmente añadiendo sufijos a los nombres de los archivos (v1, v2, final, revisado, etc.).
   - Herramientas de control de versiones (Git, Subversion) son muy útiles en entornos de desarrollo o producción colaborativa, asegurando que cada modificación quede registrada y sea reversible.

3. **Copias de seguridad en la nube**
   - Servicios como OneDrive, Google Drive, Dropbox o iCloud ofrecen la sincronización automática de carpetas y archivos.
   - Permiten acceder a la información desde distintos dispositivos y restablecer versiones anteriores en caso de borrado o modificación accidental.
   - Existen opciones que permiten crear nubes personales de forma sencilla como, por ejemplo, OpenMediaVault o CasaOS.

1.11 PROGRAMAS DE COMPRESIÓN Y DESCOMPRESIÓN

Los archivos comprimidos se han convertido en una solución muy práctica a la hora de gestionar y transferir información. Su objetivo principal es reducir el espacio que ocupan los documentos en el disco o en la transmisión por internet, permitiendo un uso más eficiente de los recursos de almacenamiento y de ancho de banda. Además, la compresión de archivos resulta especialmente útil para agrupar múltiples documentos en un único paquete, lo que facilita enormemente su envío a través de correo electrónico u otras plataformas, y simplifica su organización y almacenamiento.

Otra ventaja destacada es la posibilidad de proteger los archivos con contraseña, añadiendo una capa extra de seguridad al momento de compartir información sensible. Asimismo, existen métodos para dividir archivos muy grandes en varias partes más pequeñas, lo que resulta conveniente cuando se manejan límites de tamaño en servicios de correo o de almacenamiento en la nube. De esta forma, las herramientas de compresión se convierten en aliadas indispensables tanto para usuarios domésticos como profesionales.

1.11.1 Formatos más populares

Hay gran cantidad de formatos de compresión o empaquetado de archivos. A continuación te muestro los más habituales en cada sistema operativo:

- **ZIP**: es el formato más común y goza de una amplia compatibilidad en prácticamente todos los sistemas operativos. Su facilidad de uso y soporte nativo en muchas plataformas lo convierten en la opción predilecta para la mayoría de los usuarios.

- **RAR**: destaca por ofrecer un alto nivel de compresión, lo que puede reducir considerablemente el tamaño de los archivos. Sin embargo, para crear y descomprimir archivos RAR se necesita un software específico (como WinRAR o UnRAR), que a menudo no está incluido de forma predeterminada en algunos sistemas.
- **7z**: aporta una excelente tasa de compresión y es de código abierto. Este formato se maneja principalmente con el programa 7-Zip, disponible de manera gratuita para diversas plataformas.
- **Tar/GZ (Unix/Linux)**: constituye el formato habitual en sistemas de tipo Unix. Generalmente, se utiliza primero la herramienta tar para agrupar los archivos, y posteriormente se aplica la compresión gzip (gz). Este proceso en dos pasos es muy versátil en entornos Linux y similares.

1.11.2 Herramientas de compresión/descompresión

Los sistemas operativos actuales cuentan con soporte nativo para el empaquetado, compresión y descompresión de archivos en varios formatos diferentes.

Como práctica, te invito a que pruebes las típicas en función del sistema operativo que tengas instalado en tu máquina:

- **Windows**: el propio Explorador de archivos incluye la función de comprimir y descomprimir archivos en formato ZIP sin necesidad de instalar aplicaciones adicionales. Esta característica nativa agiliza la gestión de ficheros comprimidos para la mayoría de los usuarios de PC.
- **macOS**: al igual que en Windows, el Finder de macOS permite crear y extraer archivos ZIP de forma predeterminada. Gracias a esta función nativa, los usuarios de Apple pueden comprimir y descomprimir rápidamente sin complicaciones ni programas externos.
- **Linux**: en este entorno se recurre principalmente a herramientas de línea de comandos como *tar*, *gzip* o *unzip*, aunque muchas distribuciones ofrecen interfaces gráficas que facilitan la compresión y descompresión. Esto hace que Linux sea un sistema muy flexible, pues se adapta tanto a usuarios avanzados como a quienes prefieren un manejo más visual.
- **Aplicaciones dedicadas**: existen numerosos programas que ofrecen opciones avanzadas de compresión, entre ellos WinZip, WinRAR, 7-Zip y PeaZip. Estas herramientas permiten cifrar archivos para mayor seguridad, añadir registros de recuperación para reparar datos dañados y, además, dividir archivos grandes en partes más pequeñas, cubriendo así una amplia gama de necesidades tanto personales como profesionales.

1.12 INTEGRACIÓN CON LA NUBE Y ACCESO REMOTO

El uso de servicios de **almacenamiento en la nube** se ha convertido en una práctica cada vez más habitual gracias a soluciones como Google Drive, OneDrive, iCloud o Dropbox.

Estos sistemas permiten guardar y sincronizar documentos en internet, ofreciendo la gran ventaja de acceder a la información desde cualquier dispositivo conectado.

Además, proporcionan funcionalidades valiosas como la copia de seguridad automática y la colaboración en tiempo real facilitando el trabajo en equipo.

Sin embargo, al depender de un servicio externo que proporciona un tercero, pueden surgir inquietudes acerca de la privacidad de los documentos y, sobre todo, la necesidad de conexión perpetua o constante a la red.

Para gestionar de manera eficaz este tipo de servicios, existen las llamadas **carpetas sincronizadas**, que cada proveedor habilita a través de aplicaciones específicas.

Estas aplicaciones suelen crear una carpeta local que se vincula directamente con la nube, de modo que cualquier modificación se refleja de forma inmediata en todos los dispositivos asociados.

A nivel organizativo, es recomendable establecer una estructura clara que separe los documentos de trabajo —aquellos que requieren colaboración— de los archivos personales, aplicando los permisos adecuados para mantener el orden y la seguridad.

Por otro lado, cuando se necesita acceder a documentos ubicados en un equipo remoto, ya sea para soporte técnico, colaboración o simplemente manejo de ficheros a distancia, resulta útil recurrir a **herramientas de acceso remoto**.

El escritorio remoto (Remote Desktop en Windows, VNC, TeamViewer, AnyDesk) permite conectarse a la interfaz de otra máquina y trabajar como si se estuviera frente a ella.

Asimismo, el uso de protocolos de red como FTP, SFTP, SMB o WebDAV facilita el intercambio de archivos de manera segura entre varios usuarios o equipos, complementando así las posibilidades de colaboración y acceso fuera de la nube.

> Te invito a que investigues acerca de estos servicios y practiques con su uso. Ello te permitirá mejorar tu conocimiento y asimilar estos conceptos.

1.12.1 Puntos clave

1. **Almacenamiento en la nube**
   - Soluciones como Google Drive, OneDrive, iCloud o Dropbox permiten guardar y sincronizar archivos en internet.
   - Ventajas: acceso a los documentos en cualquier lugar, copia de seguridad automática, colaboración en tiempo real con otras personas.
   - Inconvenientes: requiere conexión a internet; depender de un servicio externo puede plantear dudas respecto a la privacidad.
2. **Carpetas sincronizadas**
   - Cada proveedor ofrece aplicaciones que crean una carpeta local sincronizada con la nube. Los cambios efectuados se reflejan en todos los dispositivos asociados a la misma cuenta.
   - A nivel organizativo, conviene diferenciar los documentos de trabajo (colaborativos) de los personales, estableciendo permisos y estructuras claras.
3. **Acceso remoto a archivos**
   - Es posible conectarse a otra máquina a través de escritorio remoto (Remote Desktop en Windows, VNC, TeamViewer, AnyDesk) para acceder a su sistema de archivos.
   - Herramientas de red (FTP, SFTP, SMB, WebDAV) permiten compartir archivos entre varios usuarios o equipos.

1.13 BUENAS PRÁCTICAS PARA LA GESTIÓN DE ARCHIVOS Y CARPETAS

Como ya hemos visto en puntos anteriores, es importante seguir una serie de normas básicas que nos permitan mantener una estructura lógica, sencilla y limpia que nos facilite la tarea de almacenar los archivos y carpetas de forma que sea fácil encontrar los documentos guardados en el disco duro.

A continuación, te muestro algunas buenas prácticas que te servirán para cumplir con este propósito.

1.13.1 Puntos clave

1. **Organización y orden**
   - Establecer una jerarquía clara de carpetas desde el inicio evita la confusión a largo plazo.
   - Ubicar de forma consistente los archivos según su naturaleza (documentos de texto, hojas de cálculo, imágenes, etc.) o por proyectos.
2. **Gestión de espacio en disco**
   - Limpiar periódicamente las carpetas de Descargas, Documentos, Temporales y la papelera/reciclaje, ya que suelen llenarse con archivos temporales o desactualizados.
   - Monitorizar el uso de espacio con herramientas nativas (por ejemplo, "Liberar espacio" en Windows) o de terceros (GrandPerspective en macOS, Baobab en Linux).
3. **Manejo de archivos grandes**
   - Comprimir para ahorrar espacio y facilitar el envío o la descarga.
   - Dividir en varias partes para sobrepasar límites de tamaño en adjuntos de correo electrónico o servicios de la nube.
4. **Etiquetado y metadatos**
   - Algunos sistemas operativos (macOS y ciertas distribuciones de Linux) permiten añadir etiquetas o comentarios a los archivos para facilitar su clasificación.
   - Se pueden emplear aplicaciones específicas de gestión documental que permitan indexar el contenido de los archivos y organizar los metadatos.
5. **Prevención y recuperación de errores**
   - Realizar copias de seguridad ante cambios importantes.
   - Evitar realizar acciones masivas (borrar, mover) sin verificar primero los archivos involucrados.
   - Utilizar la función de "Deshacer" (Ctrl + Z / Cmd + Z) cuando se cometa un error involuntario en la gestión de archivos.

1.14 RESUMEN

La gestión de archivos y carpetas es un aspecto fundamental del uso eficiente de cualquier sistema operativo.

Con una estructura bien definida, nombres de archivos coherentes, copias de seguridad frecuentes y buenas prácticas de compresión, se logra un entorno informático ordenado, seguro y mucho más productivo.

Además, la integración de la nube y la posibilidad de acceder remotamente a los datos ampliarán las capacidades de colaboración y movilidad, factores clave en la era digital.

El enfoque metódico y consciente al manejar los archivos ahorra tiempo, minimiza riesgos y sienta las bases de un trabajo de calidad.

1.15 EJERCICIO PRÁCTICO: ORGANIZACIÓN, COPIAS DE SEGURIDAD Y COMPRESIÓN/DESCOMPRESIÓN

A continuación, te invito a que realices algunas prácticas que te ayudarán a entender mejor la segunda parte del primer tema. Toma el tiempo que necesites.

Este ejercicio te permitirá **experimentar** con los conceptos del texto y adaptar cada técnica a tu propio entorno de trabajo. Si te sientes cómodo, puedes incluso **incluir más pasos**, añadir otras herramientas de respaldo o compresión, y probar con diferentes sistemas de archivos en varias plataformas. De este modo, reforzarás tu dominio de la gestión de archivos y carpetas en cualquier situación.

PRÁCTICA 1. Crea un entorno de trabajo

1. **Crea una carpeta principal** llamada, por ejemplo, Proyecto_Ejercicio.
2. Dentro de esa carpeta, genera tres **subcarpetas** con nombres descriptivos, por ejemplo:
   - Documentos.
   - Imágenes.
   - Presentaciones.

(Si lo deseas, puedes añadir más subcarpetas según tus propias necesidades o inventar categorías diferentes).

PRÁCTICA 2. Añade contenido real o ficticio

1. Coloca **al menos un archivo** de texto (Word, LibreOffice o .txt) en la carpeta Documentos.
2. Incluye **varias imágenes** (pueden ser fotos personales o imágenes de muestra) en la carpeta Imágenes.
3. Crea una **presentación** (PowerPoint, Keynote, PDF con diapositivas, etc.) en la carpeta Presentaciones.
4. Asegúrate de que algunos archivos contengan información ficticia pero realista (un pequeño informe, unas diapositivas de presentación, etc.).

PRÁCTICA 3. Aplica convenciones de nomenclatura

1. **Renombra** cada archivo para que su nombre sea descriptivo. Por ejemplo, en vez de "presentación1.pptx", puedes utilizar "Presentacion_Producto_v1.pptx".
2. **Evita** caracteres especiales (/, , :, *, ?, ", <, >, |) o espacios excesivos.
3. Añade, si quieres, la **fecha** o la **versión** al nombre de cada archivo (ej. Informe_Ventas_2025_v2.docx).

PRÁCTICA 4. Organiza copias de seguridad

1. Crea una **copia** de la carpeta Proyecto_Ejercicio en otra ubicación (por ejemplo, en un disco duro externo o una carpeta distinta del disco principal).
2. Practica la **estrategia 3-2-1** si te es posible:
   - **3 copias** en total: el original, otra en un dispositivo externo y, opcionalmente, súbelo a un servicio en la nube (Google Drive, OneDrive, Dropbox, etc.).
   - **2 medios diferentes**: disco local + disco externo, por ejemplo.
   - **1 copia fuera de tu ubicación principal**: si puedes, utiliza la nube o lleva el disco externo a otra ubicación.
3. **Simula** que has modificado uno de los archivos de texto o presentación, añádele "v2" al final del nombre y vuelve a hacer una **copia** en la misma estructura. Verifica que cuentas con ambas versiones (v1 y v2).

PRÁCTICA 5. Prueba la compresión

1. **Selecciona** los archivos de la carpeta principal Proyecto_Ejercicio (o una de las subcarpetas) y comprímelos en un **archivo ZIP** (o formato RAR, 7z, según prefieras).
2. Observa el **tamaño** resultante del archivo comprimido y compáralo con el tamaño original de los archivos.
3. (Opcional) Si tu software de compresión lo permite, **protege** el archivo ZIP con contraseña o **divide** un archivo grande en varias partes para ver cómo funciona.

PRÁCTICA 6. Subida y sincronización en la nube

1. Si tienes cuenta en un servicio de **almacenamiento en la nube** (Google Drive, OneDrive, Dropbox…), **sube** la carpeta comprimida o la carpeta original Proyecto_Ejercicio.
2. **Comprueba** que los archivos sincronizan correctamente:
   - Haz un cambio en uno de los documentos (por ejemplo, añade más texto a tu informe).
   - Observa si el cambio aparece reflejado en la versión disponible en la nube y en otros dispositivos sincronizados.

PRÁCTICA 7. Acceso remoto (opcional)

1. Descarga o utiliza una **herramienta de acceso remoto** (TeamViewer, AnyDesk o la propia función de escritorio remoto del sistema operativo).
2. Desde otro dispositivo o ubicación, **conéctate** remotamente a tu equipo principal.
3. **Accede** a la carpeta Proyecto_Ejercicio y comprueba que puedes ver y manipular los mismos archivos.
4. Explica brevemente en un documento o a modo de reflexión cómo este método puede ser útil en un entorno colaborativo o de soporte.

1.16 AUTOEVALUACIÓN (10 PREGUNTAS)

El siguiente examen es una propuesta con 10 preguntas de tipo test con una única respuesta válida. Puedes tomarte el tiempo que necesites o, incluso, volver a repasar el contenido del texto. Este examen está pensado para que tú mismo puedas comprobar si has aprendido los conceptos de la segunda parte del tema 1. Tómate el tiempo que necesites y responde con tranquilidad. Recuerda que se trata de un examen de autoevaluación.

1. ¿Qué ventaja principal ofrece mantener una jerarquía de carpetas clara?

a) Aumenta el consumo de espacio en disco.
b) Impide el uso de servicios en la nube.
c) Facilita la búsqueda y el acceso a los archivos.
d) Evita que otros usuarios puedan colaborar.

2. ¿Qué son los caracteres especiales que se recomienda evitar en el nombre de un archivo o carpeta?

a) Aquellos que mejoran la compatibilidad entre sistemas operativos.
b) Símbolos que pueden causar errores de compatibilidad y fallos en el sistema.
c) Letras minúsculas y números.
d) Solo los acentos y eñes.

3. ¿Cuál de los siguientes sistemas de archivos (File Systems) es propio de macOS?

a) NTFS.
b) APFS.
c) ext4.
d) FAT32.

4. En la estrategia 3-2-1 de copias de seguridad, ¿qué significa la "1"?

a) Conservar al menos una carpeta vacía para guardar archivos nuevos.
b) Guardar al menos una copia en la misma partición del disco duro.
c) Almacenar un respaldo en una ubicación o medio externo (offsite).
d) Hacer una sola copia de seguridad en la nube.

5. ¿Para qué sirve la acción de *mover* un archivo o carpeta?

a) Crea un duplicado y conserva el original en su ubicación.
b) Cifra el archivo o carpeta para mayor seguridad.
c) Transfiere el archivo o carpeta a otra ubicación y lo elimina de la ubicación original.
d) Cambia el nombre del archivo o carpeta de manera automática.

6. ¿Cuál es la principal ventaja de usar formatos de compresión como ZIP o 7z?

a) Incrementar el tamaño de los archivos para mayor seguridad.
b) Garantizar que solo se puedan abrir en un sistema operativo concreto.
c) Reducir el tamaño de los archivos para ahorrar espacio y facilitar su envío.
d) Hacer que los archivos sean incompatibles con herramientas de búsqueda.

7. ¿Qué característica destaca en las herramientas de control de versiones (por ejemplo, Git)?

a) Solo permiten guardar una versión final de cada archivo.
b) Se utilizan exclusivamente en sistemas Windows.
c) Ofrecen un historial de modificaciones y posibilidad de revertir cambios.
d) Impiden la colaboración simultánea de varios usuarios.

8. ¿Cuál de las siguientes afirmaciones describe mejor las carpetas sincronizadas con la nube?

a) Son carpetas locales cuyo contenido se mantiene idéntico en la nube, reflejando cambios en tiempo real.
b) Carpetas que se utilizan únicamente para copias de seguridad manuales.
c) Son invisibles para el usuario y solo se activan si hay conexión Wi-Fi.
d) Solo permiten guardar archivos de texto y hojas de cálculo.

9. Al utilizar herramientas como TeamViewer, AnyDesk o Remote Desktop, ¿qué operación se está realizando principalmente?

a) Compresión en la nube.
b) Acceso remoto a otro equipo y su sistema de archivos.
c) Eliminación masiva de archivos duplicados.
d) Creación de particiones para distintos sistemas operativos.

10. ¿Cuál de las siguientes prácticas NO favorece una buena gestión de archivos y carpetas?

a) Etiquetar y añadir metadatos a los archivos para facilitar su clasificación.
b) Dividir archivos grandes en partes más pequeñas cuando sea necesario.
c) Almacenar todos los archivos directamente en el Escritorio sin jerarquía.
d) Limpiar periódicamente las carpetas de Descargas y la papelera/reciclaje.

Respuestas correctas

1-C, 2-B, 3-B, 4-C, 5-C, 6-C, 7-C, 8-A, 9-B, 10-C

¡**Enhorabuena**! Si has acertado la mayoría de las respuestas, significa que has comprendido los aspectos esenciales de la gestión de archivos y carpetas. En caso contrario, repasa las secciones pertinentes del texto para reforzar tus conocimientos.

1.17 GESTIÓN DE LOS USUARIOS

La seguridad en un sistema informático comienza con la correcta gestión de los usuarios y las contraseñas.

Estos elementos permiten controlar quién accede al equipo, a qué recursos puede acceder y qué acciones puede realizar.

Una administración adecuada de las cuentas de usuario y una política de contraseñas robusta son esenciales para mantener la integridad, la confidencialidad y la disponibilidad de la información.

1.17.1 Los usuarios

La correcta administración de cuentas de usuario es un aspecto esencial para garantizar tanto la seguridad como la eficiencia de cualquier sistema operativo.

En este contexto, **distinguir entre los diferentes tipos de cuentas disponibles** resulta clave para asignar los privilegios adecuados a cada persona o situación: desde el control total de un administrador hasta el acceso limitado de un usuario estándar o un invitado.

Mantener un control adecuado de quién puede realizar modificaciones profundas en el sistema y quién solo puede usar aplicaciones o archivos de forma limitada ayuda a prevenir problemas de seguridad y de estabilidad.

Por otro lado, es imprescindible conocer las herramientas de cada plataforma para la creación y configuración de cuentas.

Ya sea mediante paneles de control gráficos o utilizando la línea de comandos, cada sistema —Windows, macOS y Linux— ofrece distintas opciones para que el administrador del equipo gestione los permisos y la información personal.

Escoger la modalidad de cuenta más adecuada —local o vinculada a la nube u online— también contribuye a una experiencia de usuario más completa y a un control eficiente de datos y configuraciones.

Adoptar buenas prácticas resulta determinante para mantener un entorno seguro y organizado.

Entre ellas se encuentra el uso diario de cuentas estándar, la definición de contraseñas sólidas para las cuentas con privilegios elevados y la restricción o cancelación de las cuentas invitadas cuando no se utilicen.

De este modo, se reduce el riesgo de accesos no autorizados y se garantiza un correcto funcionamiento del sistema a lo largo del tiempo.

1.17.2 Puntos clave

1. **Tipos de cuentas de usuario**
   - **Cuenta de administrador**: tiene control total sobre el sistema. Puede instalar y desinstalar software, crear y eliminar cuentas, y modificar la configuración de seguridad. Debido a su alto nivel de privilegios, conviene usarla solo cuando sea estrictamente necesario (por ejemplo, para configurar o actualizar el sistema).
   - **Cuenta estándar o de usuario limitado**: permite al usuario trabajar con aplicaciones y documentos sin realizar cambios críticos en el sistema. Es la opción recomendada para el uso diario, ya que limita la posibilidad de dañar la configuración del equipo o instalar software malicioso de forma inadvertida.
   - **Cuentas invitadas (Guest)**: ofrecen un acceso temporal y restringido al sistema. Son útiles si alguien necesita usar el equipo de forma puntual, sin acceder a la información personal ni a la configuración.
2. **Creación y administración de cuentas**
   - **En Windows**: se gestiona desde el "Panel de Control" o la "Configuración" (en versiones más recientes), apartado "Cuentas". Es

posible crear cuentas locales o asociarlas a una cuenta de Microsoft para sincronizar datos y configuraciones en la nube.

- **En macOS**: se administra en "Preferencias del Sistema" → "Usuarios y grupos". Se pueden crear distintos perfiles (Administrador, Estándar, Compartido, Invitado).
- **En Linux**: existen herramientas gráficas (como la configuración de "Usuarios") o la línea de comandos para crear y administrar cuentas (comandos *adduser, deluser, usermod*, etc.).

3. **Buenas prácticas de uso de cuentas**
   - Utilizar una cuenta estándar para las tareas cotidianas y la cuenta de administrador únicamente para labores de instalación y mantenimiento.
   - Definir contraseñas complejas para las cuentas con privilegios elevados.
   - Deshabilitar o proteger las cuentas invitadas cuando no se usen, evitando accesos no controlados.

¿Cuáles son las 10 contraseñas más comunes (e inseguras) en el mundo hispanoparlante?

No se recomienda el uso de ninguna de estas contraseñas, pues resultan extremadamente vulnerables ante ataques de fuerza bruta o intentos de acceso no autorizado.

Posición	Contraseña
1	123456
2	contraseña
3	hola123
4	123456789
5	tequiero
6	admin
7	miamor
8	qwerty
9	12345
10	abc123

1.18 CONTRASEÑAS SEGURAS

La protección de la información comienza, en gran medida, por establecer contraseñas lo suficientemente sólidas como para evitar que los atacantes obtengan acceso no autorizado a datos y dispositivos.

Las contraseñas débiles representan una de las vías más frecuentes para la intrusión en sistemas, puesto que pueden ser adivinadas o descifradas empleando técnicas de fuerza bruta o ingeniería social.

En un mundo cada vez más digitalizado, la fortaleza de las credenciales se convierte en un factor decisivo para resguardar la privacidad y salvaguardar datos personales o profesionales.

Para crear contraseñas robustas, se recomiendan varios criterios imprescindibles.

La longitud mínima sugerida es de doce caracteres, combinando letras mayúsculas, letras minúsculas, números y símbolos especiales.

Este conjunto variado dificulta considerablemente los ataques automatizados. Del mismo modo, se desaconseja rotundamente reutilizar la misma contraseña en distintos servicios, ya que la filtración de uno de ellos podría exponer de golpe todas las cuentas relacionadas.

También resulta vital evitar secuencias obvias (como “1234”, “qwerty”) o incluir información personal fácilmente identificable (fechas de nacimiento, nombres de familiares o mascotas).

Ante la complejidad de memorizar varias contraseñas seguras, existen herramientas de almacenamiento (gestores de contraseñas) que permiten proteger estas credenciales de manera eficaz.

Programas como KeePass, LastPass, 1Password o Bitwarden guardan los datos en un archivo cifrado, de forma que solo sea necesario recordar la clave maestra para acceder al resto.

Además, algunas soluciones en la nube, como iCloud Keychain o el gestor integrado en Google/Chrome, facilitan la sincronización de contraseñas entre distintos dispositivos.

Eso sí, la protección de la cuenta principal cobra una importancia aún mayor, porque su compromiso podría brindar acceso a toda la información guardada.

En cuanto a la frecuencia con la que se deben modificar las contraseñas, durante muchos años se aconsejó hacerlo cada cierto periodo (tres o seis meses).

No obstante, en la actualidad se cuestiona esta práctica, puesto que llevarla a cabo en plazos muy cortos puede conducir a la creación de contraseñas poco fiables (con secuencias repetitivas o variaciones mínimas).

Por esta razón, se propone cambiar la contraseña únicamente cuando existan pruebas o indicios de una posible filtración, de un uso indebido o de cualquier amenaza que ponga en riesgo su seguridad.

De este modo, es más probable que se mantenga un equilibrio saludable entre la robustez de las credenciales y la facilidad de su gestión.

1.18.1 Puntos clave

1. **Importancia de la fortaleza de la contraseña**

   Las contraseñas débiles constituyen una de las brechas de seguridad más habituales. Un atacante que logre adivinar o descifrar una contraseña puede obtener acceso no autorizado a datos privados, instalar software malicioso o incluso tomar el control completo del equipo

2. **Criterios para crear contraseñas seguras**

   - **Longitud mínima**: idealmente 12 caracteres o más.
   - **Mezcla de caracteres**: combinar letras (mayúsculas y minúsculas), números y símbolos especiales.
   - **No reutilizar contraseñas**: una misma contraseña usada en múltiples cuentas multiplica el riesgo, pues si se filtra en un sitio, compromete la seguridad en todos los demás.
   - **Evitar patrones obvios**: no incluir nombres propios, fechas de cumpleaños ni secuencias fáciles (1234, “qwerty”, etc.).

3. **Herramientas de almacenamiento de contraseñas**

   - **Gestores de contraseñas** (KeePass, LastPass, 1Password, Bitwarden, etc.) permiten guardar todas las contraseñas en un archivo cifrado y solo hay que recordar una clave maestra.
   - **En la nube** (por ejemplo, iCloud Keychain o el gestor integrado de Google/Chrome) facilita la sincronización de contraseñas entre

dispositivos, pero requiere una correcta protección de la cuenta principal.

4. **Políticas de cambio de contraseñas**
   - Durante años se recomendó cambiar las contraseñas periódicamente (cada 3 o 6 meses).
   - En la actualidad, la tendencia indica que cambiar contraseñas con demasiada frecuencia puede llevar a malas prácticas (contraseñas repetitivas o con pequeñas variaciones).
   - Se recomienda cambiar la contraseña siempre que existan indicios de que ha sido comprometida.

1.19 ESTRATEGIAS DE SEGURIDAD BÁSICA

La seguridad básica de un sistema informático comienza con la realización regular de actualizaciones, tanto del sistema operativo como de las aplicaciones instaladas.

Los fabricantes suelen publicar parches y revisiones de manera periódica, con el fin de corregir brechas de seguridad detectadas y de mejorar el rendimiento. Mantener el software al día, ya sea activando las actualizaciones automáticas o realizándolas manualmente, constituye una de las medidas más eficaces para prevenir que los fallos de seguridad sean explotados por ciberdelincuentes.

En segundo lugar, contar con herramientas de protección como antivirus y antispyware resulta imprescindible para evitar infecciones.

El antivirus se encarga de detectar y eliminar amenazas clásicas, tales como virus, troyanos o gusanos, además de otros tipos de malware más sofisticados. Mientras tanto, el antispyware se especializa en identificar programas espía diseñados para recopilar datos personales sin el consentimiento del usuario. Entre ambos, ofrecen una salvaguarda imprescindible para preservar la integridad del equipo y la privacidad de la información.

Además, el uso de un cortafuegos (firewall) es fundamental para controlar el tráfico de red que ingresa o sale del dispositivo, bloqueando aquellos intentos de conexión que no cumplan con las reglas establecidas. La mayoría de los sistemas operativos —Windows, macOS y muchas distribuciones de Linux— incluyen un cortafuegos básico preinstalado, que conviene mantener activo para reducir la exposición a ataques externos.

Como hemos estudiado en puntos anteriores, la gestión de cuentas de usuario y permisos es un pilar esencial. Dado que las cuentas de administrador suelen tener acceso pleno al sistema, su uso debe limitarse para tareas específicas de configuración o mantenimiento.

En entornos empresariales, el establecimiento de políticas y directivas de grupo estrictas ayuda a añadir capas de protección, restringiendo la instalación de software no deseado y el acceso a información confidencial.

Por último, la navegación segura a través de internet engloba varias prácticas recomendables. Mantener los navegadores web siempre actualizados, utilizar extensiones confiables y habilitar filtros antiphishing es clave para evitar páginas fraudulentas o maliciosas.

Conviene comprobar el candado de seguridad (HTTPS) antes de introducir datos privados en un sitio web lo que ayuda a garantizar la confidencialidad de la comunicación, blindando las credenciales y la información financiera frente a posibles interceptaciones de los datos.

1.19.1 Puntos clave

1. **Actualizaciones del sistema y del software**
   - Las empresas desarrolladoras publican parches y actualizaciones periódicas para corregir vulnerabilidades y mejorar la estabilidad.
   - Activar las actualizaciones automáticas o realizarlas manualmente con frecuencia reduce el riesgo de explotación de fallos de seguridad.
2. **Antivirus y antispyware**
   - **Antivirus**: detección y eliminación de malware (virus, troyanos, gusanos, etc.). Herramientas como Windows Defender, Avast, Kaspersky, Norton o McAfee son ejemplos comunes.
   - **Antispyware**: especializados en detectar y eliminar programas espía que recolectan información sin consentimiento.
3. **Cortafuegos (firewall)**
   - Controla las conexiones de red, permitiendo o bloqueando el tráfico entrante y saliente según reglas definidas.
   - Por defecto, muchos sistemas operativos (Windows, Linux y macOS) incluyen un firewall básico que conviene mantener activado.

4. **Control de cuentas y permisos**
   - Limitar el uso de cuentas de administrador para minimizar el impacto de un software malintencionado.
   - Revisar las "Políticas de seguridad" y las "Directivas de grupo" en entornos empresariales para establecer restricciones adicionales.
5. **Navegación segura**
   - Utilizar navegadores actualizados y extensiones confiables para bloquear anuncios o sitios maliciosos.
   - Activar filtros antiphishing que identifiquen intentos de suplantación de identidad.
   - Verificar el candado de seguridad (HTTPS) en sitios que requieran datos sensibles, como credenciales o datos bancarios.

1.20 MÉTODOS ADICIONALES DE PROTECCIÓN

En el ámbito de la ciberseguridad, reforzar los mecanismos de protección se ha convertido en una necesidad ante el crecimiento de amenazas digitales.

Más allá de las medidas más básicas, existen métodos adicionales que aportan una seguridad extra y evitan que los atacantes se hagan con el control de equipos y cuentas de usuario. **Entre ellos se incluyen la autenticación en dos factores, el control parental y las restricciones de usuario, el cifrado de disco y dispositivos, así como la aplicación de políticas de respaldo**.

La autenticación en dos factores (2FA) añade una capa adicional a la tradicional contraseña, requiriendo un código de verificación que se recibe por SMS, correo electrónico o se genera mediante aplicaciones especializadas (Google Authenticator, Authy, Microsoft Authenticator, etc.). Esta doble barrera reduce considerablemente las posibilidades de que una persona no autorizada entre en una cuenta con solo conocer la contraseña, protegiendo así información sensible y accesos privados.

Por otro lado, el control parental y las restricciones de usuario cumplen una función esencial cuando se trata de limitar y supervisar el uso de dispositivos. Esta opción, presente en la mayoría de los sistemas operativos, permite restringir el tiempo de uso, bloquear contenidos o aplicaciones inadecuadas y llevar un registro de la actividad. Gracias a ello, los adultos pueden garantizar un entorno seguro para menores de edad o para usuarios con necesidades específicas.

En materia de protección de datos, el cifrado de disco y dispositivos destaca por su capacidad para salvaguardar la información almacenada incluso si el equipo es robado o extraviado. Con herramientas como BitLocker (Windows) o FileVault (macOS), el contenido del disco duro se encuentra totalmente cifrado y solo es accesible con la clave de descifrado correspondiente. El mismo enfoque se puede extender a unidades externas (memorias USB, discos duros portátiles), proporcionando mayor tranquilidad a la hora de transportar o compartir archivos confidenciales.

Para finalizar, las políticas de respaldo (backup) constituyen una salvaguarda imprescindible contra posibles fallos de hardware o ataques de ransomware. Mantener copias de seguridad periódicas, tanto en soportes locales (discos duros externos) como en la nube (OneDrive, Google Drive, Dropbox, etc.), ofrece una forma efectiva de asegurar la disponibilidad de la información en caso de incidentes.

De este modo, la combinación de todos estos métodos adicionales de protección aporta una defensa robusta que disminuye el riesgo de sufrir pérdidas o accesos indebidos.

1.20.1 Puntos clave

1. **Autenticación en dos factores (2FA)**
   - Añade una capa adicional a la contraseña, solicitando un código de verificación enviado al teléfono o generado por una aplicación específica (Google Authenticator, Authy, Microsoft Authenticator, etc.).
   - Reduce drásticamente la posibilidad de que un atacante acceda a la cuenta con solo conocer la contraseña.
2. **Control parental y restricciones de usuario**
   - Los sistemas operativos permiten establecer restricciones de tiempo o contenidos para cuentas de menores de edad o usuarios con necesidades específicas.
   - Posibilita filtrar sitios web inapropiados, bloquear ciertas aplicaciones y monitorear la actividad.
3. **Cifrado de disco y dispositivos**
   - Herramientas como **BitLocker** (Windows) o **FileVault** (macOS) cifran todo el contenido del disco, de modo que si el equipo es robado

o se extravía, la información permanecerá inaccesible sin la clave de descifrado.

- Existen soluciones para unidades externas (USB, discos portátiles), proporcionando seguridad adicional a archivos transportados o compartidos.

4. **Políticas de respaldo (backup)**
   - Realizar copias de seguridad periódicas de los datos importantes protege frente a fallos del hardware y ataques de ransomware.
   - Pueden combinarse copias locales (discos duros externos) con copias en la nube (OneDrive, Google Drive, Dropbox, etc.) para mayor seguridad.

1.21 RESUMEN

Gestión de usuarios: creación de cuentas con permisos específicos (administrador vs. estándar).

Contraseñas seguras: uso de caracteres variados y longitud mínima de 12.

Seguridad básica: actualizaciones automáticas del SO. Antivirus y cortafuegos. Control parental y restricciones.

La formación de los usuarios constituye un eslabón fundamental en la cadena de seguridad. Enseñarles a reconocer correos potencialmente maliciosos, a evitar enlaces desconocidos y a instalar únicamente software confiable contribuye notablemente a prevenir incidentes.

Es interesante llevar a cabo una revisión periódica de la actividad del sistema (mediante logs y registros) resulta clave para detectar movimientos sospechosos en entornos de red o servidores. Junto con estas medidas, contar con políticas de contraseñas claras y fácilmente recordables facilita el uso de claves robustas que dificulten el acceso no autorizado.

La adopción de un plan de contingencia es otro pilar esencial. Este debería contemplar acciones como la restauración de copias de seguridad, el cambio urgente de contraseñas comprometidas y la notificación inmediata a las áreas correspondientes.

Para concluir con esta parte del tema 1, te recuerdo la importancia de gestionar adecuadamente las cuentas de usuario, de emplear contraseñas complejas y de mantener actualizadas las medidas de seguridad básicas (sistema operativo, antivirus y cortafuegos).

Una inversión constante en la formación y la prevención no solo fortalece la infraestructura informática, sino que marca la diferencia entre un entorno seguro y uno expuesto a amenazas.

1.22 EJERCICIO PRÁCTICO: USUARIOS, CONTRASEÑAS Y SEGURIDAD

Como con cada parte estudiada hasta ahora, es el momento de realizar algunas prácticas con objeto de afianzar y mejorar el conocimiento adquirido. De nuevo, te recomiendo que realices estas actividades tranquilamente y tomándote el tiempo que necesites o, incluso, cambiando o agregando lo que consideres interesante.

Sigue los pasos indicados y, si es posible, intenta hacer las acciones propuestas usando un sistema operativo real o una máquina virtual. Si quieres, intenta documentar cada proceso con capturas de pantalla o notas detalladas.

PRÁCTICA 1. Creación y gestión de usuarios

1. **Creación de dos cuentas**
   - Crea una cuenta de tipo **Administrador** para labores de configuración.
   - Crea una cuenta **Estándar** para el uso cotidiano.

   Objetivo: diferenciar los privilegios de usuario y entender la importancia de limitar el uso de la cuenta Administrador.

2. **Restricción de la cuenta invitada**
   - Si tu sistema lo permite, habilita la cuenta **Invitado** (Guest) y comprueba las restricciones por defecto.
   - Deshabilítala o protégela con un método seguro cuando no la uses.

   Objetivo: ver en la práctica cómo se configuran los permisos de una cuenta con acceso limitado.

3. **Revisión de políticas de seguridad**
   - Investiga en tu sistema dónde se ubican las opciones de "Políticas de seguridad" o "Directivas de grupo" (por ejemplo, en Windows busca *gpedit.msc* o la sección "Políticas de seguridad local").
   - Explora brevemente las configuraciones relacionadas con la creación y administración de usuarios.

   Objetivo: familiarizarse con las opciones avanzadas de configuración, especialmente en entornos empresariales.

PRÁCTICA 2. Contraseñas seguras

1. **Creación de una contraseña robusta**
   - Define una contraseña de, al menos, **12 caracteres** para la cuenta Administrador, mezclando letras mayúsculas, minúsculas, números y símbolos.
   - Explora la diferencia entre usar una contraseña "fácil" y otra "compleja" (por ejemplo, intenta cambiar la contraseña a algo muy sencillo y comprueba cómo el sistema lo evalúa).

   Objetivo: poner en práctica los criterios recomendados para el diseño de contraseñas seguras.

2. **Uso de un gestor de contraseñas**
   - Instala o abre un gestor de contraseñas (KeePass, LastPass, Bitwarden u otro de tu preferencia).
   - Añade un registro para tus cuentas recién creadas y comprueba cómo el gestor protege la información.

   Objetivo: entender las ventajas de un repositorio cifrado para almacenar credenciales y simplificar su uso.

3. **Políticas de cambio de contraseñas**
   - Realiza un cambio de contraseña simulado en tu cuenta estándar, motivado por una "filtración hipotética".
   - Documenta cuánto tiempo inviertes en generar una nueva contraseña segura y en actualizar la información en el gestor de contraseñas (o en diferentes servicios si los usas).

   Objetivo: valorar la conveniencia de cambiar solo cuando haya indicios de compromiso y no de forma periódica sin justificación.

PRÁCTICA 3. Medidas de seguridad básica

1. **Comprobación de actualizaciones**
   - Verifica que tu sistema operativo y las aplicaciones principales estén **al día** (busca actualizaciones y aplícalas si están disponibles).
   - Si procede, activa la opción de **actualizaciones automáticas** o programa una búsqueda periódica.

   Objetivo: ver en acción una de las prácticas más efectivas para prevenir ataques basados en vulnerabilidades conocidas.

2. **Instalación o configuración de antivirus y antispyware**
   - En caso de no tener un antivirus, instala uno (por ejemplo, Windows Defender, Avast, Kaspersky, etc.) o asegúrate de que el de tu sistema esté activo.
   - Revisa la configuración de análisis en tiempo real y el registro de últimas detecciones (si las hubiera).

   Objetivo: familiarizarse con la protección contra malware y con las opciones habituales que ofrecen estos programas.

3. **Configuración del cortafuegos (firewall)**
   - Accede al panel de configuración del cortafuegos de tu sistema operativo.
   - Verifica que esté **activado** y revisa brevemente las reglas o perfiles (p. ej. red pública, privada o de dominio).

   Objetivo: entender cómo se controlan las conexiones entrantes y salientes para reforzar la seguridad de la red.

4. **Navegación segura**
   - Usa un navegador actualizado con extensiones antiphishing o bloqueadores de contenido publicitario malicioso.
   - Accede a un sitio web seguro (con candado HTTPS) e identifica en qué parte de la barra de direcciones se indica la conexión cifrada.

   Objetivo: reconocer en la práctica cómo funcionan los filtros de seguridad y la verificación de páginas web confiables.

PRÁCTICA 4. Métodos adicionales de protección

1. **Activación de la autenticación en dos factores (2FA)**
   - Escoge un servicio en línea que utilices (correo, banco, redes sociales) y **habilita la 2FA**.
   - Descarga o utiliza una aplicación de autenticación (Google Authenticator, Authy, etc.) para generar los códigos.

   Objetivo: experimentar de primera mano cómo esta capa extra de seguridad dificulta el acceso de terceros no autorizados.

2. **Prueba de cifrado de dispositivos**
   - Si tu sistema lo permite (Windows: BitLocker; macOS: FileVault), habilita el cifrado en una unidad USB o una carpeta virtual.
   - Verifica que, tras extraer y volver a conectar la unidad, se te solicite la clave para acceder al contenido.

   Objetivo: comprobar el valor de cifrar datos sensibles y entender que, sin la clave correcta, la información permanece inaccesible.

3. **Copia de seguridad (backup)**
   - Crea una **copia de seguridad local** de tus documentos o archivos importantes (por ejemplo, en un disco duro externo).
   - Sube algún fichero relevante a un servicio de la **nube** (OneDrive, Google Drive, Dropbox, etc.).

   Objetivo: verificar lo sencillo que resulta generar backups y cómo la combinación de varias ubicaciones (local y nube) aumenta la seguridad de la información.

Con este ejercicio, habrás aplicado de forma práctica los conocimientos sobre **gestión de usuarios, contraseñas seguras, seguridad básica del sistema y métodos adicionales de protección**.

Adquirirás una visión más sólida e integral de la ciberseguridad básica y estarás mejor preparado para implementar medidas preventivas en entornos profesionales o personales.

1.23 AUTOEVALUACIÓN (10 PREGUNTAS)

Para consolidar el conocimiento, te propongo la realización de un pequeño cuestionario que te ayudará a comprobar si has aprendido los conceptos básicos de esta parte del tema 1.

Del mismo modo que con las pruebas anteriores, relájate y tómate el tiempo que necesites. El objetivo final de este cuestionario es que puedas determinar el nivel adquirido.

1. **¿Qué tipo de cuenta se recomienda para el uso diario, con el fin de limitar modificaciones críticas en el sistema?**
   a) Cuenta de administrador.
   b) Cuenta invitada.
   c) Cuenta estándar.
   d) Cuenta remota.

2. **¿Cuál es la longitud mínima sugerida para contraseñas seguras según el texto?**
   a) 8 caracteres.
   b) 10 caracteres.
   c) 12 caracteres.
   d) 16 caracteres.

3. **¿Para qué sirven los gestores de contraseñas (KeePass, LastPass, 1Password, Bitwarden, etc.)?**
   a) Analizar el disco duro en busca de virus.
   b) Almacenar contraseñas en un archivo cifrado.
   c) Bloquear páginas web maliciosas.
   d) Acelerar el rendimiento del sistema operativo.

4. **¿Qué práctica se recomienda en relación con la cuenta de administrador?**
   a) Emplearla para todas las tareas diarias.
   b) Compartirla con otros usuarios.
   c) Usarla solo cuando sea estrictamente necesario.
   d) Eliminarla de forma permanente.

5. ¿Cuál de las siguientes NO es una recomendación para crear contraseñas seguras?

a) Combinar letras, números y símbolos.
b) Reutilizar una contraseña en varios servicios.
c) Superar los 12 caracteres de longitud.
d) Evitar secuencias evidentes como “1234”.

6. ¿Qué medida se considera fundamental para evitar infecciones de malware en un equipo?

a) Desactivar las actualizaciones automáticas.
b) Contar con un antivirus/antispyware actualizado.
c) Usar el firewall sin reglas definidas.
d) Emplear exclusivamente una cuenta de administrador.

7. ¿Cuál es la práctica sobre contraseñas que se ha cuestionado en la actualidad por generar claves poco fiables?

a) Cambiarlas solo cuando haya señales de filtración.
b) Usar símbolos y mayúsculas en la contraseña.
c) Cambiarlas con demasiada frecuencia.
d) Emparejarlas con un segundo factor de autenticación.

8. ¿Qué función desempeña el firewall (cortafuegos) en un sistema?

a) Bloquea todos los programas que intenten ejecutarse.
b) Controla y filtra el tráfico de red entrante y saliente.
c) Cifra el contenido de todo el disco duro.
d) Instala parches de seguridad de forma automática.

9. ¿Qué técnica añade una capa adicional a la contraseña para validar la identidad del usuario?

a) Uso de una cuenta invitada.
b) Configuración de directivas de grupo.
c) Autenticación en dos factores (2FA).
d) Detección de software espía.

10. ¿Cuál es una de las medidas más eficaces para proteger la información almacenada en caso de robo o extravío del equipo?

a) Desactivar la cuenta invitada.
b) Configurar una contraseña corta y fácil de recordar.
c) Utilizar cifrado de disco como BitLocker o FileVault.
d) Navegar siempre con filtros antiphishing activos.

Respuestas correctas

1-C, 2-C, 3-B, 4-C, 5-B, 6-B, 7-C, 8-B, 9-C, 10-C.

¡Enhorabuena! Si has acertado la mayoría de las preguntas, significa que has asimilado correctamente los principios básicos sobre **usuarios, contraseñas y seguridad informática**.

Mantener estos conocimientos al día y ponerlos en práctica contribuirá de forma decisiva a proteger tus dispositivos, tus datos y tu entorno digital. ¡Sigue así!.

1.24 BACKUP O COPIA DE RESPALDO

La copia de seguridad es el último escudo de protección contra la pérdida de información. No solo cubre situaciones de fallo en los discos duros, sino también ataques de ransomware, eliminación accidental de archivos y otras incidencias que pueden comprometer la integridad o la accesibilidad de los datos.

En esencia, consiste en la realización de un volcado o copia de aquellos datos que podamos considerar como esenciales: documentación, proyectos, imágenes, firmas digitales, etc.

En caso de ocurrencia de un desastre, podremos restaurar la información preservada de un modo más o menos sencillo.

Los puntos importantes del backup son:

- **Protección frente a desastres**: si ocurre un fallo del sistema o se sufre un ataque malicioso, el usuario puede restaurar los archivos afectados.
- **Recuperación de versiones**: un buen sistema de backup permite acceder a versiones anteriores de un archivo o proyecto, útil cuando se generan errores en la última versión o se necesitan referencias de modificaciones pasadas.

- **Tranquilidad laboral y personal**: en entornos empresariales, la ausencia de copias de seguridad puede derivar en pérdidas económicas y de reputación. A nivel personal, garantiza que archivos valiosos (fotos, documentos, vídeos) no se pierdan irremediablemente.

1.25 TIPOS DE COPIA DE SEGURIDAD

Hasta hace algunos años, el coste por gigabyte almacenado era alto, por lo que se diseñaron algunas estrategias que permitían optimizar el espacio requerido para la realización de los volcados de seguridad: **copia completa, copia incremental y copia diferencial.**

1. **Copia completa (Full Backup)**

   Se guarda absolutamente todo el contenido que se desea proteger. La ventaja principal es su simplicidad a la hora de restaurar, pues solo se necesita esta única copia para recuperar la totalidad de la información. Sin embargo, demanda mayor tiempo de proceso y espacio de almacenamiento.

2. **Copia incremental**

   Solo se respaldan los archivos que han cambiado desde la última copia (ya sea completa o incremental). Esto ahorra tiempo y espacio, aunque la restauración puede ser más compleja, pues se necesitan la copia completa inicial y todas las copias incrementales posteriores.

3. **Copia diferencial**

   Similar a la incremental, pero se basa siempre en la última copia completa. De esta manera, se generan backups algo más grandes que los incrementales (al acumularse los cambios desde la copia completa), pero se reduce la complejidad en la restauración, ya que solo requiere la copia completa más la última copia diferencial.

En la actualidad se pueden encontrar dispositivos de almacenamiento masivo a precios bastante bajos por lo que se puede recomendar realizar las copias de seguridad completas directamente o mediante compresión de los datos y mantener distintos ciclos del volcado.

1.26 MÉTODOS DE ALMACENAMIENTO

Podemos clasificar los sistemas de almacenamiento por su ubicación en el espacio. Así, tenemos la posibilidad de realizar los backups en discos duros o memorias de estado sólido conectadas en el momento o usar servicios en línea —la nube—.

1. **Almacenamiento local**
   - **Discos duros externos o memorias USB**: sencillos de utilizar y rentables en coste. Pueden guardarse en un lugar seguro para protegerlos de incidentes físicos (incendios, robos, inundaciones, etc.).
   - **Sistemas de Red (NAS)**: un *Network Attached Storage* permite centralizar los backups y acceder a ellos desde cualquier ordenador conectado a la misma red. Suele utilizarse en oficinas y pequeños negocios.
2. **Almacenamiento en la nube**
   - **Servicios en línea**: Google Drive, OneDrive, Dropbox o iCloud permiten la sincronización automática de carpetas. Esto facilita la continuidad del trabajo y reduce el riesgo de pérdida, ya que la información reside en servidores remotos.
   - **Plataformas de backup dedicadas**: Backblaze, Carbonite o Acronis, enfocadas específicamente en copias de seguridad, con opciones de cifrado avanzado y la posibilidad de recuperar archivos específicos o todo el sistema.
3. **Almacenamiento mixto**

   Combina copias locales y en la nube para optimizar la seguridad y la accesibilidad. Por ejemplo, se puede realizar un backup completo en un disco duro externo y, de forma complementaria, sincronizar los archivos más críticos en un servicio de nube.

1.27 HERRAMIENTAS DE COPIA DE SEGURIDAD

Existe una gran cantidad de programas que facilitan la tarea. Desde el copiado manual hasta la programación del volcado en horarios concretos, empaquetando o comprimiendo los archivos, agregando medidas de seguridad adicionales como la inclusión de una contraseña al paquete, etc.

En el mundo digital actual, la protección de datos es fundamental, y los sistemas operativos más utilizados ofrecen herramientas integradas o de terceros para facilitar la creación de copias de seguridad.

Estas herramientas permiten a los usuarios programar y automatizar el respaldo de sus archivos, garantizando la seguridad y disponibilidad de la información en caso de pérdida o fallos del sistema.

Windows cuenta con dos opciones principales para realizar copias de seguridad. Por un lado, el *Historial de archivos* (File History) se enfoca en guardar copias incrementales de archivos ubicados en bibliotecas, el escritorio y carpetas seleccionadas, lo que permite recuperar versiones anteriores de los documentos. Por otro lado, la herramienta *Copia de seguridad y restauración* (Backup and Restore) ofrece la posibilidad de programar copias completas o diferenciales, almacenándolas en un disco externo o en una ruta de red.

En el caso de **macOS**, la solución más destacada es *Time Machine*. Esta herramienta realiza copias de seguridad incrementales de manera automática, guardando versiones horarias, diarias y semanales de los archivos en un disco externo. Su interfaz visual facilita la restauración de datos, lo que la convierte en una opción muy intuitiva y eficaz para los usuarios de Apple.

Por su parte, **Linux** ofrece una amplia variedad de aplicaciones para gestionar copias de seguridad. Entre las más populares se encuentran *Déjà Dup* (integrada en Ubuntu), *Timeshift* y *Back InTime*, que permiten programar respaldos regulares. Además, los usuarios de Linux pueden aprovechar herramientas de sincronización con la nube, como *Rclone* o *Syncthing*, para mantener sus datos seguros y accesibles desde cualquier lugar.

En resumen, cada sistema operativo proporciona opciones robustas para la creación de copias de seguridad, ya sea mediante utilidades integradas o aplicaciones de terceros. Es recomendable automatizar este proceso y verificar periódicamente la integridad de las copias para garantizar la protección de los datos en todo momento.

1.27.1 Puntos clave

Windows

- *Historial de archivos* (File History): guarda copias incrementales de archivos ubicados en bibliotecas, escritorio y carpetas seleccionadas.
- *Copia de seguridad y restauración* (Backup and Restore): permite programar copias completas o diferenciales en un disco externo o ruta de red.

macOS

- *Time Machine*: solución de backup incremental que guarda copias horarias, diarias y semanales en un disco externo. Facilidad de restauración gracias a su interfaz visual.

Linux

- Existen múltiples aplicaciones: *Déjà Dup* (Ubuntu), *Timeshift*, *Back InTime*, y herramientas de sincronización con la nube (Rclone, Syncthing, etc.).

1.28 BUENAS PRÁCTICAS EN LA PLANIFICACIÓN DE BACKUPS

La creación de copias de seguridad es un proceso esencial para proteger la información crítica, pero no basta solo con realizar respaldos. Es fundamental seguir estrategias y buenas prácticas que garanticen la integridad, seguridad y disponibilidad de los datos. A continuación, se presentan tres principios clave para una gestión eficaz de las copias de seguridad.

Regla 3-2-1

Esta regla es un estándar ampliamente aceptado en la gestión de respaldos. Consiste en mantener al menos **tres copias** de los datos: la original y dos respaldos adicionales. Estas copias deben almacenarse en **dos soportes o formatos diferentes**, como un disco duro externo y un servicio de almacenamiento en la nube.

Además, es crucial que **una de las copias** se conserve en una ubicación distinta a la principal, ya sea en la nube o en otra sede física. Este enfoque minimiza el riesgo de pérdida total de datos en caso de desastres como incendios, robos o fallos técnicos.

Pruebas de restauración

Realizar copias de seguridad no es suficiente si no se verifica que los datos pueden recuperarse correctamente. Por ello, es recomendable llevar a cabo **pruebas de restauración** de manera periódica.

Estas pruebas permiten asegurarse de que los archivos o sistemas respaldados se han copiado de forma íntegra y de que el proceso de recuperación funciona según lo esperado.

Sin esta verificación, existe el riesgo de descubrir errores en el momento menos oportuno, cuando los datos sean realmente necesarios.

Cifrado y protección de copias

Cuando las copias de seguridad contienen información sensible, es imprescindible protegerlas contra accesos no autorizados. Para ello, se recomienda **cifrar los respaldos** utilizando contraseñas robustas.

El cifrado garantiza que, en caso de pérdida o robo de la unidad de almacenamiento, los datos permanezcan seguros y solo puedan ser accedidos por personas autorizadas. Esta medida es especialmente importante cuando se utilizan dispositivos portátiles o servicios en la nube.

En conclusión, la implementación de estas prácticas no solo asegura la disponibilidad de los datos, sino que también protege la información contra riesgos físicos, técnicos y de seguridad.

Automatizar los respaldos, seguir la regla 3-2-1, realizar pruebas de restauración y cifrar las copias son pasos esenciales para una estrategia de backup efectiva y confiable.

1.28.1 Puntos clave

1. **Regla 3-2-1**:
   - Mantener al menos 3 copias de los datos.
   - Guardarlas en 2 soportes o formatos diferentes (por ejemplo, un disco duro externo y la nube).

- Conservar 1 copia fuera de la ubicación principal (almacenamiento en la nube o en otra sede).

2. **Pruebas de restauración**:
   Periódicamente, conviene probar la recuperación de los archivos o sistemas respaldados para asegurarse de que todo se ha copiado correctamente y de que el procedimiento de restauración funciona.

3. **Cifrado y protección de copias**:
   Si los backups contienen información sensible, se recomienda cifrarlos con una contraseña robusta, evitando el acceso no autorizado en caso de pérdida o robo de la unidad de almacenamiento.

1.29 BITLOCKER Y LA PROTECCIÓN DE LOS DATOS

Bitlocker es una herramienta de Windows para el cifrado del disco duro que se ha incluido en las ediciones o versiones profesionales y empresariales del sistema operativo Windows.

Su finalidad es la de proteger la información almacenada en el equipo de accesos no autorizados lo que es especialmente relevante en caso de pérdida o robo del dispositivo.

1.29.1 Definición de cifrado de disco

El **cifrado** consiste la transformación de los datos en un formato ilegible si no se dispone de la contraseña o clave adecuada. Al cifrar todo el disco o una partición, se impide que un tercero pueda extraer la información al acceder físicamente a la unidad de forma ilícita.

- **Cifrado completo del disco (FDE)**: protege todo el sistema, incluidas las áreas de arranque y los archivos del sistema operativo.
- **Cifrado de volumen/partición**: solo la sección seleccionada (partición) queda protegida.

1.29.2 Cómo funciona Bitlocker

Requisitos previos

Para utilizar BitLocker, es necesario contar con una edición compatible de Windows, como **Windows 10 Pro**, **Windows 11 Pro** o las versiones **"Enterprise"** o **"Education"**.

Además, se recomienda disponer de un módulo **TPM (Trusted Platform Module)** en el equipo, ya que este facilita la gestión de claves y la verificación de la integridad del sistema.

Sin embargo, también es posible habilitar BitLocker sin TPM, aunque en este caso será necesario utilizar una contraseña o una clave almacenada en un USB para desbloquear la unidad cifrada.

Proceso de activación

El proceso de activación de BitLocker es sencillo y se realiza a través de la configuración del sistema.

- **Acceso a la configuración**: el usuario puede acceder a BitLocker desde el **Panel de Control** o el **Administrador de BitLocker**, donde selecciona la unidad que desea cifrar.
- **Método de desbloqueo**: durante la configuración, el usuario elige el método de desbloqueo, que puede ser mediante **TPM** (con o sin un PIN adicional), una **contraseña** o una **clave de recuperación**.
- **Inicio de la encriptación**: una vez configurado, BitLocker comienza a cifrar los datos existentes en segundo plano, lo que permite seguir utilizando el equipo durante el proceso. El tiempo requerido para completar el cifrado depende de la capacidad del disco y la velocidad del hardware.

Claves de recuperación

Cuando se cifra una unidad, BitLocker genera automáticamente una **clave de recuperación (Recovery Key)**.

Esta clave es fundamental para acceder a los datos en caso de que el método de desbloqueo habitual falle (por ejemplo, si se olvida la contraseña o si hay un problema con el TPM).

- **Almacenamiento seguro**: es crucial guardar esta clave en un lugar seguro, preferiblemente fuera del equipo. Algunas opciones recomendadas incluyen almacenarla en una **cuenta de Microsoft**, en un **gestor de contraseñas** o incluso imprimirla en papel.
- **Importancia de la clave**: si no se puede acceder al disco por algún motivo, la única forma de desbloquearlo será introduciendo la clave de recuperación. Por ello, perder esta clave puede resultar en la pérdida permanente de los datos.

1.29.3 Ventajas del uso de Bitlocker

BitLocker ofrece una serie de ventajas clave que la convierten en una solución eficaz para proteger la información confidencial. Estas ventajas no solo garantizan la seguridad de los datos, sino que también facilitan su uso y gestión, tanto para usuarios individuales como para organizaciones.

Protección de datos confidenciales

Una de las principales ventajas de BitLocker es su capacidad para proteger los datos almacenados en una unidad, incluso en situaciones de riesgo físico.

Gracias al cifrado, nadie podrá leer o copiar la información, aunque el disco duro sea extraído del equipo o el portátil sea robado.

Esto es especialmente importante en entornos donde la confidencialidad de los datos es crítica, como en empresas o instituciones que manejan información sensible.

Integración con el sistema operativo

Al ser una solución nativa de Windows, BitLocker se integra perfectamente con el sistema operativo. Esto simplifica su configuración y gestión, ya que no es necesario instalar software adicional ni preocuparse por problemas de compatibilidad.

Además, su integración permite una actualización constante y un soporte técnico directo por parte de Microsoft, lo que asegura un funcionamiento óptimo y seguro.

Transparencia para el usuario

Una vez activado, BitLocker opera de manera silenciosa en segundo plano, sin requerir acciones adicionales por parte del usuario. Esto significa que el cifrado

no interfiere con el uso diario del equipo, manteniendo la productividad mientras protege los datos.

El usuario solo necesita interactuar con BitLocker en situaciones específicas, como al desbloquear una unidad o recuperar datos mediante la clave de recuperación.

Posibilidad de cifrar dispositivos extraíbles

BitLocker no se limita a proteger los discos internos del equipo. Con la función **BitLocker To Go**, también es posible cifrar dispositivos extraíbles, como memorias USB o discos externos.

Esta característica es especialmente útil para quienes transportan información confidencial en dispositivos portátiles, ya que garantiza que los datos estén protegidos incluso si el dispositivo se pierde o es robado.

Resumiendo, BitLocker combina seguridad avanzada, facilidad de uso y una integración perfecta con Windows, lo que la convierte en una herramienta esencial para la protección de datos. Su capacidad para cifrar tanto unidades internas como dispositivos extraíbles, junto con su funcionamiento transparente, la hace ideal para usuarios y organizaciones que buscan mantener su información segura sin complicaciones.

1.29.4 Consideraciones importantes y limitaciones

Como resumen final, voy a mostrarte algunos puntos clave que se deben tener en cuenta a la hora de usar Bitlocker por defecto en un equipo informático:

- **Pérdida de la clave de recuperación**: si se olvida la contraseña o no se conserva la clave, la información será irrecuperable.
- **Rendimiento**: el cifrado puede, en ciertos casos, impactar en el rendimiento, aunque en la mayoría de los equipos modernos es apenas perceptible gracias a la aceleración por hardware.
- **Compatibilidad con otras plataformas**: un disco cifrado con BitLocker no se leerá fácilmente en macOS o Linux sin herramientas específicas de terceros.
- **Bloqueos en actualizaciones**: en ocasiones, las actualizaciones del sistema podrían requerir que se introduzca la clave de recuperación si detectan cambios sustanciales en el hardware o en la configuración del arranque.

1.30 SINERGIA ENTRE BACKUPS Y CIFRADO

La protección de datos no se limita a una sola estrategia, sino que requiere combinar herramientas y prácticas complementarias.

Aunque el cifrado, como el que ofrece BitLocker, es fundamental para evitar accesos no autorizados, no reemplaza la necesidad de realizar copias de seguridad.

Ambas medidas deben trabajar en conjunto para garantizar la seguridad, integridad y disponibilidad de la información.

A continuación, te muestro los puntos clave de esta unión o sinergia:

Copias cifradas

Una de las mejores prácticas es asegurarse de que las copias de seguridad también estén protegidas mediante cifrado.

Esto puede lograrse almacenando la información en soportes encriptados o utilizando herramientas como **BitLocker To Go** (para dispositivos extraíbles), **VeraCrypt** u otras soluciones de cifrado multiplataforma.

De esta manera, incluso si los soportes de backup caen en manos equivocadas, los datos permanecerán inaccesibles sin la clave correspondiente.

Verificación de restauración

Realizar copias de seguridad cifradas no es suficiente si no se verifica que estas pueden restaurarse correctamente.

Es crucial probar periódicamente que las copias cifradas pueden abrirse y recuperarse utilizando las claves adecuadas. Este paso asegura que, en caso de necesidad, los datos estarán disponibles y que no se producirán errores durante el proceso de restauración.

Protección ante ransomware

El cifrado de datos, como el que proporciona BitLocker, protege contra accesos no autorizados, pero no previene ataques de ransomware que cifren o secuestren archivos en uso.

Para defenderse contra este tipo de amenazas, es esencial contar con copias de seguridad externas almacenadas **offline** o en la nube con control de versiones.

Estas copias permiten recuperar los datos sin necesidad de pagar rescates y garantizan que la información no se pierda definitivamente.

En conclusión, la combinación de cifrado y copias de seguridad es fundamental para una estrategia de protección de datos robusta. Mientras el cifrado protege contra accesos no autorizados, las copias de seguridad aseguran la disponibilidad y recuperación de la información en caso de fallos, ataques o desastres. Implementar ambas medidas de manera coordinada es la mejor forma de garantizar la seguridad y resiliencia de los datos.

1.31 RESUMEN

La protección de los datos es un aspecto crítico en el uso de sistemas informáticos, tanto a nivel personal como profesional.

En esta parte, hemos abordado dos pilares fundamentales para garantizar la integridad y disponibilidad de la información: las copias de seguridad (backups) y el cifrado de unidades con herramientas como BitLocker. Ambos elementos trabajan en conjunto para proteger los datos ante fallos de hardware, ataques informáticos o accesos no autorizados.

Las copias de seguridad son el último recurso para recuperar información en caso de desastres, como fallos de disco, ransomware o eliminación accidental de archivos.

Existen diferentes tipos de backups (completos, incrementales y diferenciales), cada uno con sus ventajas y desventajas en términos de tiempo, espacio y complejidad de restauración.

Además, los métodos de almacenamiento pueden variar desde dispositivos locales (discos duros externos o NAS) hasta servicios en la nube, e incluso combinaciones de ambos para maximizar la seguridad y accesibilidad.

Herramientas integradas en sistemas operativos, como el Historial de archivos en Windows, Time Machine en macOS o aplicaciones como Déjà Dup en Linux, facilitan la automatización y gestión de estos procesos.

Por otro lado, el cifrado de datos, especialmente con herramientas como BitLocker, protege la información contra accesos no autorizados, incluso en casos de robo o extracción física del disco. BitLocker, integrado en versiones profesionales de Windows, ofrece cifrado completo del disco o de particiones, y permite proteger

dispositivos extraíbles con BitLocker To Go. Sin embargo, el cifrado no sustituye la necesidad de realizar copias de seguridad, ya que no protege contra ransomware ni fallos del sistema.

Para una estrategia de protección de datos efectiva, es crucial seguir buenas prácticas como la regla 3-2-1 (tres copias, dos soportes, una fuera del sitio), realizar pruebas periódicas de restauración y cifrar las copias de seguridad para evitar accesos no autorizados.

La combinación de backups y cifrado garantiza no solo la seguridad de los datos, sino también su disponibilidad y recuperación en situaciones críticas.

En conclusión, la implementación de estas medidas, junto con la automatización y verificación periódica, asegura una protección robusta y confiable de la información, minimizando riesgos y garantizando la continuidad en entornos personales y profesionales.

1.32 EJERCICIO PRÁCTICO: BACKUP Y SEGURIDAD AVANZADA

A través de este ejercicio práctico, como estudiante aprenderás a configurar una estrategia básica de copias de seguridad y cifrado de datos utilizando las herramientas integradas en Windows, aplicando buenas prácticas para garantizar la seguridad y disponibilidad de la información.

Te recomiendo, una vez más, que te tomes tu tiempo y repases aquellos puntos que necesites. El objetivo de esta práctica es ayudarte a interiorizar los conceptos teóricos y puedas aplicarlos al uso cotidiano de la informática en tu entorno.

Práctica 1: identificar datos críticos

- Selecciona una carpeta en tu equipo que contenga archivos importantes (documentos, fotos, proyectos, etc.).
- Haz una lista de los archivos que considerarías críticos y justifica por qué deben ser respaldados.

Objetivo: reconocer la información esencial que debe protegerse.

Práctica 2: configurar una copia de seguridad con historial de archivos (Windows)

- Conecta un disco duro externo o USB a tu equipo.
- Accede a "Configuración" > "Actualización y seguridad" > "Copia de seguridad".
- Activa "Historial de archivos" y selecciona la unidad externa como destino.
- Configura la frecuencia de las copias (por ejemplo, cada hora) y selecciona la carpeta crítica identificada en el Paso 1.

Objetivo: aprender a crear copias de seguridad incrementales.

Práctica 3: realizar una copia de seguridad completa manual

- Usa la herramienta "Copia de seguridad y restauración" (Windows 7) en Windows 10/11.
- Selecciona "Crear una copia de seguridad ahora" y elige la unidad externa como destino.
- Incluye la carpeta crítica y realiza la copia completa. Compara el tiempo y espacio utilizado con el Historial de archivos.

Objetivo: entender el proceso de creación de una copia completa.

Práctica 4: cifrar una unidad con BitLocker

- Accede a "Este equipo", haz clic derecho en la unidad externa y selecciona "Activar BitLocker".
- Elige un método de desbloqueo (contraseña o clave en USB).
- Guarda la clave de recuperación en un lugar seguro (por ejemplo, en una cuenta de Microsoft o impresa).
- Inicia el cifrado y observa cómo funciona en segundo plano.

Objetivo: aprender a proteger datos mediante cifrado.

Práctica 5: simular una restauración de datos

- Elimina o modifica algunos archivos de la carpeta crítica.
- Usa el Historial de archivos para restaurar una versión anterior de los archivos eliminados o modificados.
- Comprueba que los datos se han recuperado correctamente.

Objetivo: verificar la integridad y accesibilidad de las copias de seguridad.

Práctica 6: proteger una copia de seguridad con cifrado

- Usa BitLocker To Go para cifrar la unidad externa donde se almacenan las copias de seguridad.
- Verifica que la unidad cifrada no puede ser accedida sin la contraseña o clave de recuperación.
- Prueba a restaurar datos desde la unidad cifrada para asegurarte de que el proceso funciona correctamente.

Objetivo: aplicar cifrado a una copia de seguridad para mayor seguridad.

Práctica 7: implementar la regla 3-2-1

- Crea una segunda copia de seguridad de la carpeta crítica en otro soporte (por ejemplo, en la nube usando Google Drive o OneDrive).
- Asegúrate de que una de las copias esté fuera del sitio (por ejemplo, en la nube o en otro dispositivo físico en una ubicación diferente).
- Documenta tu estrategia de backup, indicando dónde se almacena cada copia y cómo se protege (cifrado, contraseñas, etc.).

Objetivo: aplicar una estrategia de backup robusta y segura.

1.33 AUTOEVALUACIÓN (10 PREGUNTAS)

Toma el tiempo que necesites y consulta las partes que no recuerdes o no hayas comprendido bien. Recuerda que el objetivo de cada test de autoevaluación es darte la posibilidad de que tú mismo seas capaz de identificar si has logrado entender y aprender los conceptos propuestos en cada capítulo.

Solo una opción es válida.

1. **¿Cuál es el objetivo principal de una copia de seguridad (backup)?**
   a) Aumentar la velocidad del sistema.
   b) Proteger los datos ante pérdidas o fallos.
   c) Eliminar archivos innecesarios.
   d) Mejorar el rendimiento del hardware

2. **¿Qué herramienta de Windows permite realizar copias de seguridad incrementales?**
   a) BitLocker.
   b) Historial de archivos.
   c) Time Machine.
   d) VeraCrypt.

3. **¿Qué ventaja principal tiene una copia de seguridad completa (Full Backup)?**
   a) Ocupa menos espacio que otros tipos de backup.
   b) Es más rápida de realizar que una incremental.
   c) Solo requiere una copia para restaurar todos los datos.
   d) No necesita verificaciones posteriores.

4. **¿Qué es BitLocker?**
   a) Una herramienta para comprimir archivos.
   b) Un software de copias de seguridad en la nube.
   c) Una herramienta de cifrado de discos en Windows.
   d) Un programa para eliminar malware.

5. **¿Qué establece la regla 3-2-1 en la gestión de copias de seguridad?**
   a) Realizar 3 copias, usar 2 métodos de cifrado y almacenar 1 en la nube.
   b) Mantener 3 copias, en 2 soportes diferentes, con 1 copia fuera del sitio.
   c) Hacer 3 backups diarios, 2 semanales y 1 mensual.
   d) Usar 3 herramientas diferentes, 2 locales y 1 en la nube.

6. ¿Qué método de desbloqueo NO es compatible con BitLocker si no hay un módulo TPM?
a) Contraseña.
b) Clave en un USB.
c) PIN adicional.
d) Huella dactilar.

7. ¿Qué herramienta de macOS realiza copias de seguridad incrementales automáticas?
a) Time Machine.
b) Historial de archivos.
c) Déjà Dup.
d) Backup and Restore.

8. ¿Por qué es importante realizar pruebas de restauración periódicas?
a) Para aumentar la velocidad del sistema.
b) Para asegurarse de que las copias de seguridad son funcionales.
c) Para eliminar archivos duplicados.
d) Para reducir el espacio de almacenamiento utilizado.

9. ¿Qué tipo de copia de seguridad solo guarda los cambios realizados desde la última copia completa?
a) Completa (Full Backup).
b) Incremental.
c) Diferencial.
d) Espejo (Mirror).

10. ¿Qué herramienta de Linux es popular para realizar copias de seguridad?
a) Time Machine.
b) Historial de archivos.
c) Déjà Dup.
d) BitLocker.

Respuestas correctas

1-B, 2-B, 3-C, 4-C, 5-B, 6-D, 7-A, 8-B, 9-C, 10-C

¡Enhorabuena! Si has acertado la mayoría de las respuestas, significa que has comprendido los aspectos esenciales de la gestión de archivos y carpetas. En caso contrario, repasa las secciones pertinentes del texto para reforzar tus conocimientos.


TEMA 2
NAVEGACIÓN INTELIGENTE Y GESTIÓN EFICIENTE DE INFORMACIÓN