

1.4 GESTIÓN DE ARCHIVOS: ORGANIZACIÓN, ALMACENAMIENTO Y COMPRESIÓN

La gestión de archivos es una de las competencias digitales más importantes en el uso cotidiano del ordenador. Cada vez que creamos un documento, descargamos una imagen, instalamos un programa, guardamos una foto del móvil o enviamos un archivo adjunto por correo, estamos trabajando con archivos y carpetas. Si no existe un criterio claro de organización, la información se dispersa, se duplican documentos, se pierden versiones importantes y se desperdicia tiempo buscando datos que “sabemos que están en alguna parte”.

Por el contrario, cuando el usuario domina los conceptos básicos de archivo, carpeta, sistema de archivos, almacenamiento local y en la nube, compresión y copias de seguridad, puede trabajar de forma ordenada, eficiente y segura. En este apartado se explican todos estos elementos de manera progresiva, con un enfoque práctico orientado a que el lector pueda aplicar los contenidos en su propio entorno digital.

1.4.1 Concepto de archivo y tipos de archivos digitales

Un archivo es una unidad de información almacenada en un dispositivo digital, identificada por un nombre y una extensión. Cada archivo contiene datos en un determinado formato y está asociado a una o varias aplicaciones capaces de abrirlo o modificarlo.

a) Partes del nombre de un archivo

En la mayoría de sistemas operativos, el nombre de un archivo se compone de tres elementos:

- Nombre descriptivo: identifica el contenido del archivo.
- Punto separador: indica que a continuación aparece la extensión.
- Extensión: define el tipo de archivo y su formato interno.

Ejemplos:

- informe_auditoria_enero.docx.
- foto_viaje_roma.jpg.
- presentacion_proyecto_final.pptx.

La extensión permite al sistema operativo asociar el archivo a un programa por defecto. Así, al hacer doble clic sobre un .docx, se abre el procesador de textos; sobre un .jpg, el visor de imágenes; y sobre un .mp4, el reproductor de vídeo.

b) Grandes familias de archivos

Aunque existen cientos de formatos, es útil agruparlos en categorías:

- Archivos de texto y documentos: .txt, .docx, .odt, .pdf.
- Archivos de hoja de cálculo y datos: .xlsx, .ods, .csv.
- Archivos de presentación: .pptx, .odp.
- Archivos de imagen: .jpg, .png, .gif, .tiff.
- Archivos de audio y vídeo: .mp3, .wav, .mp4, .avi, .mkv.
- Archivos comprimidos: .zip, .rar, .7z, .tar.gz.
- Archivos ejecutables o instaladores: .exe, .msi, .pkg, .apk (en móviles).

Conocer la extensión ayuda a decidir cómo abrir el archivo, qué programa utilizar y qué precauciones tomar (por ejemplo, con archivos ejecutables o adjuntos sospechosos).

1.4.2 Carpetas, subcarpetas y estructura jerárquica del sistema de archivos

Una carpeta es un contenedor virtual que agrupa archivos y otras carpetas (subcarpetas). Su función principal es facilitar la organización de la información.



a) Estructura en forma de árbol

El sistema de archivos se organiza como un árbol:

- Una unidad o raíz principal (por ejemplo, C: en Windows).
- Carpetas principales (Documentos, Imágenes, Descargas, Música).
- Subcarpetas dentro de cada una de ellas.
- Archivos almacenados en distintas ramas.

Ejemplo de estructura:

- Documentos.
 - Proyectos.
 - Proyecto_A.
 - ◆ Informe_A.docx.
 - ◆ Datos_A.xlsx.
 - Proyecto_B.
 - Facturas.
 - 2024.
 - 2025.

Esta estructura jerárquica permite localizar los archivos siguiendo una ruta ordenada, como por ejemplo:

C:\Usuarios\Ana\Documentos\Proyectos\Proyecto_A\Informe_A.docx.

b) **Ventajas de una buena jerarquía de carpetas**

- Facilita la localización rápida de documentos.
- Evita duplicados innecesarios.
- Permite separar proyectos, años o clientes.
- Favorece las copias de seguridad ordenadas.

Una estructura caótica, con todos los archivos en el Escritorio o en Descargas, termina dificultando el trabajo diario y aumenta el riesgo de pérdida de información.

1.4.3 Administradores de archivos en distintos sistemas operativos

Para gestionar archivos y carpetas, los sistemas operativos incluyen programas específicos:

- En Windows: explorador de archivos.
- En macOS: Finder.
- En Linux: gestores como Nautilus (GNOME), Dolphin (KDE), Thunar (XFCE), entre otros.

Estos administradores permiten:

- Ver el contenido de unidades y carpetas.
- Crear nuevas carpetas.
- Copiar, mover, renombrar o eliminar archivos.
- Ordenar por nombre, fecha, tamaño o tipo.
- Buscar archivos por nombre o tipo.
- Acceder a unidades externas y a ubicaciones de red.

Comprender el funcionamiento básico del administrador de archivos es indispensable para cualquier usuario, ya que es la “puerta de entrada” al sistema de información del equipo.

1.4.4 Estrategias de organización eficiente de archivos y carpetas

La organización no consiste solo en “tener carpetas”, sino en aplicar un criterio estable en el tiempo. Cada usuario o empresa puede desarrollar su propio sistema, pero es importante que sea coherente, comprensible y sencillo.

a) Principios generales de organización

- Agrupar documentos por temática, proyecto o área (trabajo, estudios, personal).
- Crear subcarpetas para años, clientes o asignaturas.
- Evitar usar el Escritorio como almacén principal.
- Mantener vacía o limpia la carpeta Descargas, moviendo los archivos a su destino definitivo.
- Revisar periódicamente para eliminar archivos obsoletos o duplicados.

b) Nomenclatura clara de archivos

Un buen nombre de archivo debe ser:

- Descriptivo: “acta_reunion_2025-03-10.docx”.
- Coherente con otros archivos del mismo proyecto.
- Libre de caracteres problemáticos como / * ? < > |.
- Ordenable por fecha si se usa el formato AAAA-MM-DD.

Ejemplos:

- informe_auditoria_clienteX_2025-02-15.pdf.
- cv_nombre_apellidos_2025.docx.
- proyecto_web_memoria_v2.docx.

Nombres genéricos como “documento1.docx” o “nuevo.pdf” dificultan la localización y obligan a abrirlos para saber su contenido.

1.4.5 Operaciones básicas con archivos y carpetas

El usuario debe manejar con soltura las operaciones más habituales, ya que forman parte del día a día en cualquier entorno informático.

a) Crear archivos y carpetas

- Crear una nueva carpeta para agrupar documentos de un proyecto.
- Guardar un nuevo archivo desde un programa eligiendo su ubicación correcta.

b) Copiar, mover y renombrar

- Copiar: genera una copia del archivo en otra ubicación sin eliminar el original.
- Mover: traslada el archivo de una carpeta a otra, eliminándolo de la ubicación anterior.
- Renombrar: permite cambiar el nombre del archivo para hacerlo más descriptivo.

Estas operaciones pueden realizarse mediante:

- Botones y menús contextuales (clic derecho).
- Atajos de teclado (Ctrl + C, Ctrl + X, Ctrl + V).
- Arrastrar y soltar con el ratón.

c) Eliminar y restaurar

- Al eliminar un archivo, normalmente pasa a la Papelera de reciclaje (Windows) o a la Papelera (macOS).
- Desde allí puede restaurarse si la eliminación fue accidental.
- Si se vacía la papelera, la recuperación se complica y puede requerir herramientas especiales.

Por ello, conviene revisar siempre qué se va a eliminar antes de vaciar la papelera.

1.4.6 Búsqueda de archivos

Cuando la organización falla o simplemente no recordamos dónde guardamos algo, la función de búsqueda resulta imprescindible.

Los administradores de archivos y los sistemas operativos permiten buscar según:

- Nombre del archivo o parte del nombre.
- Tipo de archivo (documento, imagen, vídeo).
- Fecha de modificación.
- Tamaño aproximado.
- En algunos casos, contenido interno (por ejemplo, palabras dentro de un documento).

Buenas prácticas:

- Recordar palabras clave del nombre o del contenido.
- Limitar la búsqueda a una carpeta o unidad concreta para no escanear todo el sistema.
- Usar filtros de fecha cuando se sabe aproximadamente cuándo se creó o modificó el archivo.

1.4.7 Almacenamiento local, externo y en la nube

Los archivos no solo se guardan en el disco interno del ordenador. Hoy en día, existen múltiples opciones de almacenamiento que conviene conocer.

a) Almacenamiento local

Incluye:

- Disco duro (HDD) interno.
- Unidad de estado sólido (SSD).
- Memoria interna de tablets o smartphones.

Ventajas:

- Acceso rápido sin conexión a Internet.
- Mayor control directo del usuario.

Limitaciones:

- Riesgo de pérdida por avería física, robo o fallo del sistema.
- Capacidad limitada.

b) Almacenamiento externo

Se trata de dispositivos conectados desde el exterior:

- Memorias USB.
- Discos duros externos.
- Tarjetas SD.

Son útiles para:

- Transportar información entre equipos.
- Realizar copias de seguridad.
- Ampliar temporalmente la capacidad de almacenamiento.

c) Almacenamiento en la nube

Consiste en guardar archivos en servidores remotos accesibles por Internet:

- Google Drive.
- OneDrive.
- Dropbox.
- iCloud.

Ventajas:

- Acceso desde distintos dispositivos.
- Sin riesgo de pérdida física por avería del equipo.
- Posibilidad de compartir documentos fácilmente.

Aspectos a tener en cuenta:

- Depender de la conexión a Internet.
- Respetar la confidencialidad y la seguridad de los datos.
- Comprobar la capacidad gratuita disponible y, si es necesario, valorar planes de pago.

1.4.8 Copias de seguridad y protección frente a pérdida de datos

Las copias de seguridad (backups) son esenciales para evitar la pérdida definitiva de información por fallos del sistema, virus, errores humanos o robos.



a) Tipos de copias de seguridad

- Copia completa: incluye todos los archivos seleccionados.
- Copia incremental: solo guarda los cambios desde la última copia.
- Copia diferencial: guarda los cambios desde la última copia completa.

b) Estrategias recomendadas

Una estrategia muy extendida es la regla 3-2-1:

- Tener al menos tres copias de los datos.
- Guardarlas en dos tipos de soportes distintos (por ejemplo, disco interno y disco externo).
- Mantener al menos una copia fuera del lugar habitual (por ejemplo, en la nube).

Buenas prácticas:

- Programar copias automáticas periódicas.
- Verificar de vez en cuando que las copias pueden restaurarse correctamente.
- Proteger las copias con contraseña si contienen información sensible.

1.4.9 Compresión de archivos y envíos eficientes

La compresión permite reducir el tamaño de uno o varios archivos agrupándolos en un único contenedor.

a) Función de la compresión

- Disminuir el espacio ocupado en disco.
- Facilitar el envío de múltiples archivos en un solo paquete.
- Proteger el contenido mediante contraseña, en algunos formatos.

b) Formatos y programas habituales

Formatos de compresión:

- .zip (muy extendido y compatible).
- .rar.
- .7z.
- .tar.gz (muy común en entornos Linux).

Programas:

- Herramientas integradas del sistema (Windows y macOS descomprimen .zip).
- 7-Zip.
- WinRAR.
- WinZip.

c) **Uso típico en entornos académicos y profesionales**

Ejemplos:

- Enviar por correo una carpeta completa de documentos comprimida como proyecto_final.zip.
- Archivar trabajos antiguos en paquetes comprimidos para liberar espacio.
- Descargar material formativo agrupado en un solo archivo.

1.4.10 Seguridad en la gestión de archivos

Por último, la gestión de archivos debe incluir medidas de seguridad básicas.

Buenas prácticas:

- No abrir archivos adjuntos de correos sospechosos.
- Evitar ejecutar programas descargados de páginas no oficiales.
- Analizar con antivirus los archivos procedentes de memorias USB desconocidas.
- Usar permisos de acceso adecuados en entornos compartidos (por ejemplo, en redes de empresa).
- Cifrar archivos o carpetas cuando contengan información especialmente sensible.

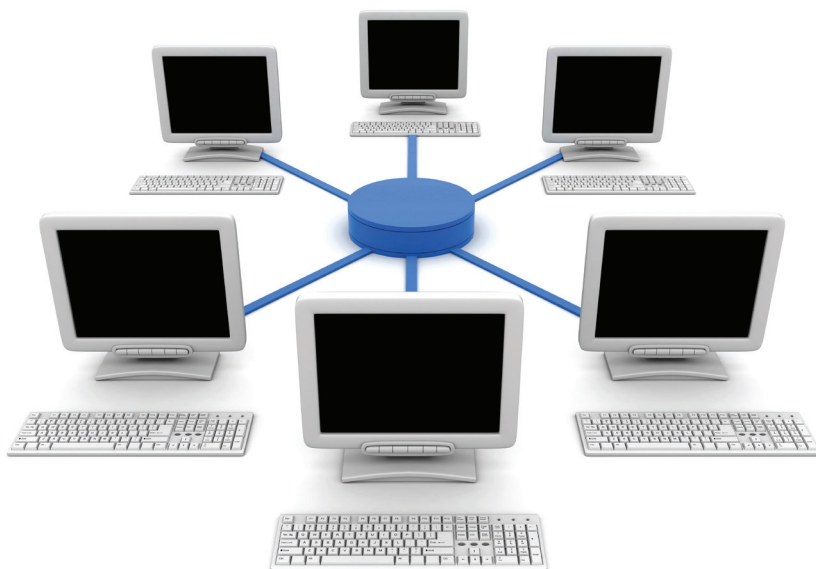
La gestión de archivos es una habilidad transversal que acompaña al usuario en todas sus actividades digitales. Saber qué es un archivo, cómo se organiza en carpetas, cómo se buscan documentos, qué opciones de almacenamiento existen, cómo se hacen copias de seguridad y cómo se comprimen datos permite trabajar de forma más profesional, ahorrar tiempo y reducir considerablemente el riesgo

de pérdida de información. Este apartado completa la base técnica del módulo, preparando al lector para un uso avanzado y seguro del ordenador en cualquier contexto académico o laboral.

1.5 REDES

Las redes informáticas constituyen uno de los pilares fundamentales del mundo digital contemporáneo. Gracias a ellas podemos navegar por Internet, intercambiar archivos, enviar correos electrónicos, participar en videoconferencias, acceder a plataformas educativas, utilizar servicios en la nube y colaborar en proyectos. Aunque desde la perspectiva del usuario parezca un proceso simple —por ejemplo, conectarse al Wi-Fi de casa—, detrás existe una estructura compleja que permite que la información viaje ordenadamente entre dispositivos, servidores y aplicaciones.

Dominar los conceptos básicos sobre redes es esencial para cualquier persona que utilice tecnología de forma habitual, pues permite comprender cómo se conecta un dispositivo, qué elementos necesita una red, qué diferencias existen entre conexiones cableadas e inalámbricas y qué medidas de seguridad deben implementarse para evitar riesgos. Este apartado explica de manera progresiva y didáctica los fundamentos de las redes, incorporando ejemplos cotidianos que facilitan su comprensión.



1.5.1 Concepto de red informática y funciones principales

Una red informática es un conjunto de dispositivos conectados entre sí para compartir información, recursos y servicios. Estos dispositivos pueden ser ordenadores, teléfonos móviles, impresoras, tabletas, servidores, cámaras, televisores inteligentes y un largo etcétera.

Las redes permiten:

- Comunicar dispositivos entre sí sin necesidad de soportes físicos como USB o discos externos.
- Compartir documentos, carpetas y recursos de forma centralizada.
- Acceder a Internet desde múltiples equipos.
- Utilizar aplicaciones colaborativas en línea.
- Conectar impresoras o unidades de almacenamiento accesibles por varios usuarios.
- Facilitar la administración de sistemas y servicios digitales.

Una red puede ser tan pequeña como dos dispositivos conectados mediante un cable o tan grande como Internet, considerada la mayor red del mundo, formada por millones de redes interconectadas.

1.5.2 Elementos básicos de una red

Para que una red funcione correctamente, necesita la combinación de tres tipos de componentes: dispositivos finales, dispositivos de interconexión y medios de transmisión.

a) Dispositivos finales

Son los equipos que el usuario emplea para conectarse a la red o consumir servicios digitales. Entre ellos se encuentran:

- Ordenadores de sobremesa.
- Portátiles.
- Tablets.
- Smartphones.
- Impresoras conectadas en red.
- Televisores inteligentes.
- Cámaras IP y dispositivos IoT (domótica).

Estos dispositivos generan, reciben o transforman la información digital que circula por la red.

b) Dispositivos de red

Son equipos especializados que gestionan el flujo de datos entre los dispositivos finales:

- **Router:** conecta una red local con Internet, distribuye direcciones IP, gestiona el tráfico y ofrece funciones de seguridad.
- **Switch:** permite conectar varios dispositivos mediante cable dentro de la misma red local.
- **Punto de acceso (Access Point):** ofrece conectividad inalámbrica a dispositivos Wi-Fi.
- **Servidores:** alojan aplicaciones, archivos, bases de datos o servicios compartidos.

Sin estos elementos sería imposible distribuir la conexión entre varios equipos o compartir recursos.

c) Medios de transmisión

La información viaja a través de diferentes medios:

- **Cable Ethernet:** conexión cableada de alta velocidad y estabilidad.
- **Fibra óptica:** permite velocidades muy elevadas en grandes distancias.
- **Wi-Fi:** conexión inalámbrica flexible y cómoda.
- **Redes móviles (4G, 5G):** conectividad a Internet desde dispositivos móviles.

Cada medio tiene ventajas específicas en términos de seguridad, velocidad y alcance.

1.5.3 Direcciones, protocolos y funcionamiento interno

Para que dos dispositivos puedan comunicarse necesitan identificarse y seguir un conjunto común de reglas.

a) Dirección IP

Es un número único que identifica a cada dispositivo dentro de una red. Existen dos formatos:

- **IPv4:** formada por valores entre 0 y 255 (ej.: 192.168.1.35).
- **IPv6:** más extensa, diseñada para sustituir a IPv4 (ej.: 2001:db8:85a3::8a2e).

b) Protocolo TCP/IP

Es el conjunto de normas que permite que los datos viajen de un punto a otro. Sus funciones incluyen:

- Dividir la información en paquetes.
- Indicar desde dónde se envían y hacia dónde se dirigen.
- Comprobar errores durante la transmisión.
- Ordenar y reensamblar los datos al llegar a destino.

Todo Internet funciona con TCP/IP.

c) DNS (Domain Name System)

Permite traducir nombres fáciles de recordar en direcciones IP. Por ejemplo:

- El usuario escribe: *www.ramaeditorial.com*.
- El sistema lo convierte en una dirección IP para localizar el servidor correspondiente.

Sin el DNS, tendríamos que memorizar números complejos en lugar de nombres.

1.5.4 Tipos de redes según su alcance

Las redes se clasifican en función del tamaño que abarcan y de su finalidad.

a) PAN (Personal Area Network)

Es una red de área personal. Incluye dispositivos conectados alrededor de una persona, como:

- Móvil y manos libres Bluetooth.
- Ordenador y reloj inteligente.

b) LAN (Local Area Network)

Red de área local que abarca un espacio reducido como:

- Una vivienda.
- Una oficina.
- Un aula.
- Un laboratorio.

Es el tipo más común.

c) **WLAN (Wireless LAN)**

Es una LAN que utiliza tecnología inalámbrica (Wi-Fi) en lugar de cables.

d) **MAN (Metropolitan Area Network)**

Cubre un área urbana o campus universitario. Puede conectar múltiples edificios.

e) **WAN (Wide Area Network)**

Red de larga distancia que conecta ciudades o países. Internet es la WAN más grande del mundo.

1.5.5 Tipos de conexión: cableada e inalámbrica

La forma en que un dispositivo se conecta determina su velocidad, estabilidad y seguridad.

a) **Conexión cableada**

Características:

- Muy estable.
- Velocidad elevada y constante.
- Mayor seguridad frente a accesos no autorizados.

Ideal para:

- Oficinas.
- Ordenadores de sobremesa.
- Servidores.
- Equipos de gaming o diseño.

b) **Conexión Wi-Fi**

Ventajas:

- Movilidad.
- Comodidad.
- Sin cables.

Limitaciones:

- Pérdida de velocidad con la distancia.
- Interferencias con paredes o electrodomésticos.
- Seguridad dependiente de la configuración del router.

1.5.6 Acceso a redes

a) Acceso cableado

Incluye:

- Conectar el cable Ethernet al dispositivo.
- Recibir automáticamente una dirección IP del router (DHCP).
- Acceder a Internet o recursos internos.

b) Acceso a redes Wi-Fi

Pasos básicos:

1. Seleccionar una red Wi-Fi disponible.
2. Introducir la contraseña correcta.
3. Esperar a que se establezca la conexión.

Recomendable:

- Evitar redes públicas o abiertas sin cifrado.
- Cambiar la contraseña Wi-Fi del router periódicamente.

c) Redes domésticas vs. redes corporativas

Las redes corporativas suelen incluir:

- Políticas de seguridad estrictas.
- Control de accesos por usuario.
- Firewalls avanzados.
- Servidores internos de archivos.

Las redes domésticas son más sencillas, pero igualmente necesitan protección adecuada.

1.5.7 Seguridad en redes

La seguridad es fundamental para evitar intrusiones, fraude, espionaje de datos o propagación de malware.

a) Riesgos en redes Wi-Fi

Una red mal configurada puede permitir:

- Robo de datos personales.
- Interceptación de contraseñas.
- Acceso a dispositivos conectados.
- Uso fraudulento de la conexión.

b) Ataques frecuentes

- **Man in the middle:** interceptan información entre dispositivos.
- **Sniffing:** capturan tráfico no cifrado.
- **Accesos no autorizados** a routers o PCs.
- **Propagación de malware** dentro de una red.

c) Buenas prácticas de protección

- Cambiar la contraseña por defecto del router.
- Utilizar WPA2 o WPA3 como cifrado Wi-Fi.
- Desactivar el WPS del router.
- Actualizar el firmware del router.
- Crear una red de invitados para dispositivos ajenos.
- No compartir archivos sin permisos adecuados.

1.5.8 Recursos compartidos en red

Una de las grandes ventajas de una red es poder compartir recursos.

a) Carpetas compartidas

Permiten:

- Compartir archivos entre equipos.
- Acceder a documentos desde otros dispositivos de la red.
- Centralizar información en un servidor interno.

b) Impresoras de red

Una sola impresora puede ser utilizada por múltiples usuarios. Beneficios:

- Ahorro económico.
- Mayor control de documentos.
- Acceso desde varios equipos.

1.5.9 Herramientas para diagnosticar problemas de red

Los sistemas operativos incluyen utilidades que permiten comprobar el estado de la red.

a) Comandos básicos

- ping: verifica si un dispositivo responde.
- ipconfig o ifconfig: muestra la configuración de red.
- tracert o traceroute: muestra el camino que sigue un paquete hasta su destino.

b) Solucionadores automáticos

Windows, macOS y Linux incluyen asistentes que detectan:

- Problemas de adaptación de red.
- Conflictos de dirección IP.
- Fallos en la conexión con DNS.

1.6 SEGURIDAD Y BIENESTAR

La seguridad y el bienestar digital son dimensiones esenciales del uso responsable de los equipos informáticos y dispositivos tecnológicos. A diario interactuamos con ordenadores, teléfonos móviles, plataformas en la nube, redes sociales, servicios bancarios en línea y herramientas de comunicación. Esta exposición constante implica riesgos, tanto para la información que manejamos (archivos, datos personales, contraseñas, fotografías, documentos profesionales), como para nuestra salud física y mental. Por ello, comprender cómo proteger los dispositivos, adoptar buenas prácticas digitales y mantener hábitos saludables frente a la tecnología es fundamental para cualquier usuario.

Este apartado analiza, desde un enfoque integral y didáctico, los conceptos de **seguridad de la información, protección del equipo, malware, bienestar físico y mental y cómputo verde**. Su objetivo es proporcionar al lector conocimientos prácticos aplicables en cualquier contexto digital: hogar, educación, empresa y entornos de colaboración en línea.

1.6.1 Protección de la información

La información es uno de los activos más valiosos en la era digital. Su pérdida o robo puede provocar daños personales, económicos, reputacionales y legales. Por ello, protegerla es una prioridad absoluta.



a) **Tipos de información que deben protegerse**

1. **Datos personales**

DNI, dirección, números de teléfono, datos bancarios, credenciales.

2. **Información profesional o académica**

Informes, trabajos, investigaciones, proyectos, bases de datos.

3. **Contenido digital privado**

Fotografías, vídeos, documentos personales o familiares.

4. **Datos de terceros**

Información de clientes, alumnos, pacientes o compañeros.

5. **Credenciales de acceso**

Contraseñas, claves, preguntas de recuperación, códigos de verificación.

Toda esta información constituye un objetivo atractivo para atacantes y debe gestionarse con responsabilidad.

b) **Buenas prácticas de seguridad de la información**

1. **Uso responsable de contraseñas**

Una contraseña segura debe ser:

- Larga (mínimo **12 caracteres**).
- Compleja (mezcla de mayúsculas, minúsculas, números y símbolos).

- Única por servicio (no repetir la misma contraseña en todas partes).
- Cambiada de forma periódica.

Ejemplos de contraseñas débiles que deben evitarse:

- “123456”.
- “contraseña”.
- “qwerty2025”.
- Nombres de mascotas o fechas de nacimiento.

Es muy recomendable utilizar un **gestor de contraseñas**, como KeePass, Bitwarden o el administrador integrado del navegador.

2. Doble factor de autenticación (2FA)

Consiste en añadir una segunda capa de seguridad.

Ejemplos:

- Código enviado por SMS.
- Código generado por una app (Google Authenticator, Authy).
- Llaves físicas como YubiKey.

El 2FA reduce enormemente el riesgo de robo de cuentas incluso si la contraseña se ve comprometida.

3. Copias de seguridad (backup)

La pérdida de información no solo puede producirse por un ataque informático, sino también por fallos del sistema, borrados accidentales o daños físicos en el dispositivo.

Tipos de copias de seguridad:

- **Completa**: copia todo el sistema.
- **Incremental**: copia solo lo que cambió desde el último backup.
- **Diferencial**: copia cambios desde la última copia completa.

Buenas prácticas:

- Realizar copias automáticas.
- Guardarlas en un lugar distinto (nube + disco externo).
- Verificar periódicamente que funcionan.

4. Actualizaciones del sistema

Las actualizaciones del sistema operativo y del software corrigen vulnerabilidades. Ignorarlas deja el equipo expuesto.

Debe actualizarse:

- Windows, macOS o Linux.
- Navegadores web.
- Antivirus y firewalls.
- Aplicaciones críticas (correo, ofimática, mensajería).