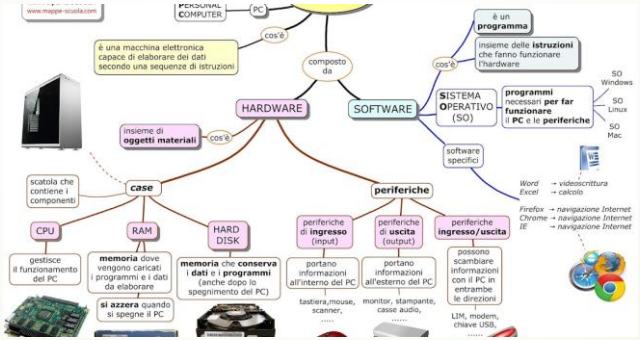
Modulo 1
I FONDAMENTI DELL 'ITC
Introduzione all'Informatica e alle Reti

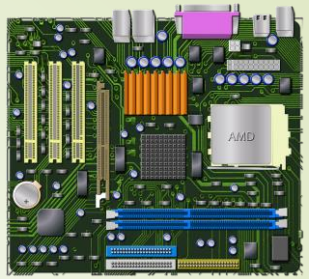


Corso di base su computer, Windows 11, gestione file, reti e sicurezza informatica

Come funziona il computer

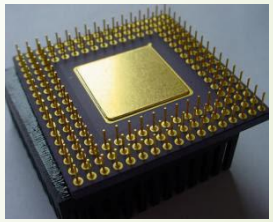
- Hardware: CPU, RAM, Hard Disk, Scheda Madre, Periferiche
- Software: Sistema Operativo, Driver, Applicazioni
- Processo di Avvio: BIOS/UEFI, Bootloader, Kernel del Sistema

Hardware



1.Scheda Madre (Motherboard):
La scheda principale che collega tutti i componenti hardware tra loro, inclusi CPU, RAM, dispositivi di archiviazione e periferiche. Contiene anche il chipset, che gestisce la comunicazione tra la CPU e gli altri componenti.

2.CPU (Unità di Elaborazione Centrale):
La "mente" del computer, responsabile di eseguire le istruzioni. Si occupa di compiti come i calcoli, le operazioni logiche e la gestione dei dati. È il componente chiave che influisce sulle prestazioni, misurato in base alla velocità di clock (GHz) e al numero di core/thread.



3.RAM (Memoria ad Accesso Casuale):
Memoria temporanea utilizzata dalla CPU per archiviare i dati che sono attivamente in uso o in elaborazione. È veloce e volatile, il che significa che i dati vengono persi quando il computer viene spento. La RAM è essenziale per il multitasking e per il funzionamento fluido delle applicazioni.

Hardware

4.Hard Disk (HDD o SSD):

Dispositivi di archiviazione utilizzati per memorizzare il sistema operativo, il software, i file e altro.

- **HDD (Hard Disk Drive)**: Archiviazione magnetica, capacità maggiore, ma velocità di lettura/scrittura più lenta.
- **SSD (Solid State Drive)**: Archiviazione più veloce, più durevole ed efficiente dal punto di vista energetico rispetto agli HDD, ma generalmente più costosa per la stessa capacità.

5.Periferiche:

Dispositivi esterni collegati al computer, come:

- **Dispositivi di input**: Tastiera, mouse, microfono, ecc.
- **Dispositivi di output**: Monitor, stampante, altoparlanti, ecc.
- **Periferiche di archiviazione**: Hard disk esterni, chiavette USB.
- **Periferiche di rete**: Adattatori Wi-Fi, schede Ethernet.

Software

Ecco una panoramica dei principali **software** che hai menzionato:

1.Sistema Operativo (SO):

È il programma principale che gestisce l'hardware del computer e fornisce un'interfaccia per l'interazione con l'utente. Gestisce risorse come CPU, memoria e dispositivi di archiviazione, e consente di eseguire applicazioni. I più comuni sono:

- **Windows** (per PC),
- **macOS** (per computer Apple),
- **Linux** (un sistema operativo open-source con varie distribuzioni come Ubuntu, Fedora, ecc.),
- **Android** (per dispositivi mobili),
- **iOS** (per dispositivi Apple).

2.Driver:

I driver sono programmi che permettono al sistema operativo di comunicare correttamente con l'hardware. Ogni componente hardware, come la scheda grafica, la stampante o la tastiera, ha bisogno di un driver specifico affinché il sistema operativo possa riconoscerlo e utilizzarlo. Ad esempio, i driver per una stampante permettono al computer di inviare correttamente i dati alla stampante, mentre i driver grafici gestiscono la visualizzazione delle immagini sul monitor.

Software

3.Applicazioni:
Le applicazioni sono programmi che l'utente utilizza per svolgere compiti specifici. Possono essere di vario tipo:

- **Software di produttività**: Word processor (come Microsoft Word), fogli di calcolo (come Excel), software di presentazione (come PowerPoint).
- **Browser web**: Come Google Chrome, Mozilla Firefox, Safari, per navigare in internet.
- **Software di grafica**: Photoshop, Illustrator, o programmi di editing video come Adobe Premiere.
- **Giochi**: Programmi creati per l'intrattenimento, che variano da giochi leggeri a quelli più complessi.
- **Software di comunicazione**: Skype, WhatsApp, Zoom, per le videoconferenze o la messaggistica.

Ogni tipo di software ha uno scopo specifico e può essere installato o aggiornato indipendentemente dal sistema operativo.

Processo di Avvio

Il **processo di avvio** di un computer è l'insieme delle operazioni che avvengono quando si accende il computer, fino al caricamento del sistema operativo. Ecco una panoramica delle fasi principali del processo di avvio:

1.BIOS/UEFI (Basic Input Output System / Unified Extensible Firmware Interface):

•BIOS è il firmware tradizionale che si trova sulla scheda madre del computer e gestisce l'inizializzazione dell'hardware al momento dell'accensione del sistema. È il primo software a essere eseguito quando si accende il computer.

•**UEFI** è l'evoluzione moderna del BIOS. A differenza del BIOS, che aveva una limitata interfaccia grafica e funzionalità, UEFI offre una maggiore velocità, supporto per dischi di dimensioni più grandi (oltre 2 TB), interfacce grafiche e più opzioni di sicurezza, come il Secure Boot.

Dopo l'accensione, il BIOS/UEFI esegue una sequenza chiamata **POST (Power-On Self Test)** che verifica che l'hardware (CPU, RAM, scheda madre, ecc.) funzioni correttamente. Se tutto è ok, il BIOS/UEFI cerca il dispositivo di avvio (tipicamente il disco rigido o SSD) per caricare il sistema operativo.

Processo di Avvio

2. Bootloader:

Una volta che il BIOS/UEFI ha trovato il dispositivo di avvio (ad esempio un hard disk o un SSD), il passo successivo è il caricamento del bootloader. Il bootloader è un piccolo programma che carica il sistema operativo in memoria.
A seconda del sistema operativo, il bootloader può essere diverso:
•GRUB (GRand Unified Bootloader): Tipico per Linux. Permette di scegliere tra più sistemi operativi, se sono installati più sistemi (dual boot).
•Windows Boot Manager: Se il sistema operativo è Windows, il bootloader è il "Windows Boot Manager" che carica il kernel di Windows.
•rEFInd: Usato su sistemi con UEFI per gestire il dual boot tra macOS e altri sistemi operativi (Linux, Windows).
Il bootloader carica la parte centrale del sistema operativo, chiamata kernel, che è responsabile di gestire tutte le risorse del sistema (memoria, CPU, dispositivi di I/O, ecc.) e di avviare i vari processi.

3. Caricamento del Sistema Operativo:
Dopo che il bootloader ha caricato il kernel, il sistema operativo comincia a inizializzarsi completamente. A questo punto, il sistema operativo prende il controllo e continua a caricare i driver, il file system e i processi necessari per il corretto funzionamento del computer.
In questa fase, il sistema operativo si avvia e l'utente può iniziare ad interagire con il sistema, aprire applicazioni e utilizzare il computer.
Riepilogo del Processo di Avvio:
1. **Accensione del computer → Il BIOS/UEFI inizia a eseguire il POST.**
2. **Verifica dell'hardware → Se il controllo è positivo, il BIOS/UEFI cerca il dispositivo di avvio.**
3. **Caricamento del Bootloader → Il bootloader viene caricato dal dispositivo di avvio.**
4. **Caricamento del Sistema Operativo → Il bootloader carica il kernel e avvia il sistema** operativo.

Ogni fase è fondamentale per garantire che il computer si avvii correttamente. Se uno di questi passaggi fallisce, il sistema potrebbe non avviarsi o presentare errori.

La parte hardware del computer

- Dispositivi di Input: Tastiera, Mouse, Scanner
- Dispositivi di Output: Monitor, Stampante, Altoparlanti
- Archiviazione: HDD, SSD, Memorie esterne

La parte software del computer

- Tipi di Software: System Software, Application Software, Utility Software
- Sistema Operativo: Windows, Linux, macOS
- Esempi di Software: Microsoft Office, Browser Web, Antivirus

Avviare e spegnere il computer

- • Fasi di avvio del PC: POST, Bootloader, Caricamento OS
- • Spegnimento corretto: Salvataggio dati, Chiusura processi, Shutdown sicuro
- • Modalità di sospensione e ibernazione

Primi passi con Windows 11

- • Interfaccia utente: Menu Start, Barra delle applicazioni, Desktop
- • Gestione delle finestre: Massimizzare, Minimizzare, Affiancare
- • Centro notifiche e Impostazioni rapide

Le icone del sistema operativo

- • Icone di sistema: Cestino, Esplora file, Rete
- • Collegamenti sul Desktop e personalizzazione
- • Creazione e gestione di icone personalizzate

Le finestre di Windows 11

- • Struttura di una finestra: Barra del titolo, Menu, Contenuto
- • Ridimensionamento e spostamento delle finestre
- • Utilizzo della funzione Snap Assist

Gli strumenti di Windows 11

Task Manager: Monitorare processi e prestazioni

Gestione Disco e Pulizia del Sistema

Windows Update e Sicurezza

Installare e disinstallare un'applicazione

- Metodi di installazione: Microsoft Store, File .exe/.msi
- Disinstallazione tramite Pannello di Controllo e Impostazioni
- Gestione delle applicazioni predefinite

File e cartelle

- Tipologie di file: Documento, Immagine, ideo, Audio, Eseguibile

- Struttura delle cartelle e organizzazione

- Attributi e Permessi dei file

Gestire file e cartelle

- Creazione, Eliminazione e Rinominazione
- Copia, Taglia e Incolla: Metodi e scorciatoie
- Uso dell'Esplora File e ricerca avanzata

Lavorare in rete

- Definizione di rete informatica e classificazione (LAN, WAN, WLAN, MAN, PAN)
- Tipologie di connessioni: Ethernet, Wi-Fi, VPN
- Protocolli di rete: TCP/IP, DHCP, DNS

Definizione di rete informatica e classificazione (LAN, WAN, WLAN, MAN, PAN)

- Una **rete informatica** è un sistema di dispositivi e computer interconnessi tra loro che possono scambiarsi dati e risorse, come file, stampanti o connessioni Internet, attraverso un'infrastruttura comune. Le reti informatiche possono variare per dimensione, scopo e modalità di connessione, e si classificano principalmente in base alla loro estensione geografica.

Classificazione delle reti informatiche:

- **LAN (Local Area Network)**:
  - Una rete locale che connette dispositivi (come computer, stampanti e server) in una zona geografica ristretta, ad esempio un edificio o un ufficio.
  - La LAN offre alta velocità di trasmissione dei dati e bassa latenza, ed è solitamente gestita da una singola organizzazione.
  - Tecnologie comuni: Ethernet, Wi-Fi.
- **WAN (Wide Area Network)**:
  - Una rete che copre una vasta area geografica, come una città, un paese o addirittura il mondo intero.
  - La WAN connette più LAN distanti tra loro, utilizzando tecnologie come le linee telefoniche, i satelliti, o connessioni via fibra ottica.
  - Esempi: Internet è una grande WAN che collega miliardi di dispositivi in tutto il mondo.
- **WLAN (Wireless Local Area Network)**:
  - Una rete locale senza fili che permette ai dispositivi di comunicare senza l'uso di cavi, utilizzando tecnologie radio come il Wi-Fi.
  - Si utilizza in ambienti domestici, uffici e luoghi pubblici per offrire una connessione di rete a dispositivi mobili come smartphone, laptop e tablet.
- **MAN (Metropolitan Area Network)**:
  - Una rete che copre una zona geografica di dimensioni maggiori rispetto a una LAN, ma più piccole di una WAN. Solitamente copre un'intera città o una grande area metropolitana.
  - Utilizzata per connettere diverse LAN all'interno di una città, garantendo una velocità di connessione maggiore rispetto alla WAN.
- **PAN (Personal Area Network)**:
  - Una rete di piccole dimensioni, solitamente utilizzata per connettere dispositivi personali come smartphone, tablet, computer e dispositivi indossabili (es. smartwatch).
  - La PAN ha una portata limitata (di solito pochi metri) e può essere realizzata tramite tecnologie come Bluetooth o infrarossi.
- Ogni tipo di rete ha specifiche caratteristiche e vantaggi in base alla sua applicazione e alla sua estensione geografica.

Tipologie di connessioni: Ethernet, Wi-Fi, VPN

- Le **connessioni** in una rete informatica rappresentano il mezzo tramite cui i dispositivi si scambiano dati. Esistono diverse tipologie di connessione, ognuna con caratteristiche uniche che la rendono adatta a determinate situazioni. Le principali tipologie di connessione sono **Ethernet**, **Wi-Fi** e **VPN**. Ecco una panoramica di ciascuna:

Tipologie di connessioni: Ethernet, Wi-Fi, VPN

- **Ethernet**
- **Descrizione**: Ethernet è una delle tecnologie di connessione cablata più comuni per reti locali (LAN). Essa utilizza cavi fisici (tipicamente cavi in rame con connettori RJ45) per collegare i dispositivi in rete.
- **Caratteristiche**:
  - Alta velocità e bassa latenza.
  - Maggiore sicurezza rispetto alle connessioni wireless, poiché è difficile intercettare i dati trasmessi senza accesso fisico alla rete.
  - Affidabilità elevata, con una connessione stabile e senza interferenze.
  - Necessità di infrastruttura cablata, quindi i dispositivi devono essere fisicamente vicini a prese di rete.
- **Uso**: Molto comune nelle reti aziendali o in ambienti domestici dove si desidera una connessione stabile e veloce.

Tipologie di connessioni: Ethernet, Wi-Fi, VPN

- **2. Wi-Fi**
- **Descrizione**: Il Wi-Fi è una tecnologia di connessione senza fili che permette ai dispositivi di connettersi a una rete senza l'uso di cavi, sfruttando onde radio per la trasmissione dei dati.
- **Caratteristiche**:
  - **Comodità**: Gli utenti possono connettersi a Internet e accedere alla rete in qualsiasi punto coperto dal segnale Wi-Fi.
  - **Velocità**: La velocità di connessione dipende dal tipo di standard Wi-Fi (es. Wi-Fi 5, Wi-Fi 6). Generalmente è inferiore rispetto a una connessione cablata Ethernet.
  - **Sicurezza**: Le reti Wi-Fi possono essere vulnerabili a intrusioni se non protette adeguatamente. Tecniche di cifratura come WPA3 sono utilizzate per proteggere i dati.
  - **Interferenze**: Poiché utilizza onde radio, può essere soggetto a interferenze da altri dispositivi o ostacoli fisici.
- **Uso**: Comodamente utilizzato in ambienti domestici, uffici, pubblici, e in dispositivi mobili (smartphone, tablet, laptop).

Tipologie di connessioni: Ethernet, Wi-Fi, VPN

- **3. VPN (Virtual Private Network)**
- **Descrizione**: Una **VPN** è una connessione che crea una "rete privata" sicura sopra una rete pubblica (tipicamente Internet). Utilizzando la crittografia, una VPN garantisce la protezione della privacy e dei dati durante la trasmissione su reti non sicure.
- **Caratteristiche**:
  - **Sicurezza**: Crittografia dei dati per proteggere la privacy degli utenti. Anche se i dati passano attraverso Internet, rimangono protetti.
  - **Accesso remoto**: Le VPN consentono agli utenti di connettersi a una rete aziendale o privata da remoto, come se si trovassero fisicamente in ufficio.
  - **Anonymity**: Nasconde l'indirizzo IP dell'utente, proteggendo l'identità online e impedendo il tracciamento da parte di terzi.
  - **Prestazioni**: A volte può ridurre la velocità di connessione a causa della crittografia, ma ciò dipende dal provider e dal protocollo VPN utilizzato.
- **Uso**: Utilizzato per la navigazione sicura su Internet, per accedere a contenuti geograficamente limitati o per consentire il lavoro remoto in ambito aziendale.

Sicurezza informatica

- Minacce informatiche: Malware, Phishing, Ransomware
- Metodi di protezione: Firewall, Antivirus, Backup
- Autenticazione sicura: Password, 2FA, Biometria

Minacce informatiche

- Le minacce informatiche sono sempre più sofisticate e rappresentano un pericolo concreto per individui e aziende. Tra le più comuni troviamo:
- **Malware**
  Il termine "malware" (software dannoso) include diversi tipi di programmi creati per infiltrarsi o danneggiare un sistema informatico senza il consenso dell'utente. Alcuni esempi:
  - **Virus**: si attaccano a file legittimi e si diffondono quando vengono eseguiti.
  - **Trojan**: si mascherano da software utili, ma una volta installati eseguono attività dannose.
  - **Worm**: si diffondono autonomamente attraverso reti senza bisogno di interazione umana.
  - **Spyware**: raccolgono dati dell'utente senza autorizzazione.

Minacce informatiche

- **Phishing**
  Questa tecnica mira a ingannare le persone per ottenere informazioni sensibili come password, numeri di carte di credito o dati bancari. Spesso si presenta sotto forma di email, messaggi o siti web falsificati che sembrano provenire da fonti affidabili. Varianti includono:
  - **Spear phishing**: attacchi mirati contro individui specifici.
  - **Whaling**: phishing rivolto a dirigenti aziendali di alto livello.
  - **Smishing e Vishing**: attacchi via SMS o telefonate fraudolente.
- **Ransomware**
  È un tipo di malware che blocca l'accesso ai file o al sistema dell'utente, chiedendo un riscatto per ripristinarne l'accesso. Spesso si diffonde tramite email infette o exploit di sicurezza nei sistemi. Alcune varianti criptano i file della vittima (Crypto Ransomware), mentre altre bloccano completamente il sistema (Locker Ransomware).

Come difendersi?

- **Aggiornare software e sistemi operativi** per correggere vulnerabilità.
- **Utilizzare antivirus e firewall** affidabili.
- **Fare attenzione ai link e agli allegati sospetti** nelle email.
- **Eseguire backup regolari** dei dati su dispositivi sicuri e offline.
- **Usare autenticazione a più fattori (MFA)** per proteggere gli account.

Metodi di protezione

Firewall:

- **Funzione:** Un firewall agisce come una barriera tra la tua rete interna (come il tuo computer o la rete domestica) e le reti esterne (come Internet). Monitora e controlla il traffico di rete in entrata e in uscita, bloccando le connessioni non autorizzate o pericolose.
- **Tipi:**
  - Firewall hardware: Dispositivi fisici dedicati alla sicurezza della rete.
  - Firewall software: Programmi installati sul tuo computer o dispositivo per proteggerlo.
- **Importanza:** Essenziale per proteggersi da intrusioni, attacchi informatici e accessi non autorizzati.

Antivirus:

- **Funzione:** Un software antivirus analizza file, programmi e attività del tuo computer alla ricerca di malware (software dannoso), come virus, trojan, spyware e ransomware. Una volta rilevato un malware, l'antivirus lo elimina o lo mette in quarantena.
- **Importanza:** Fondamentale per proteggere il tuo computer da infezioni che possono danneggiare i tuoi file, rubare informazioni personali o compromettere il sistema.
- **Aggiornamenti:** Mantieni sempre aggiornato il tuo antivirus per garantire la massima protezione contro le nuove minacce.

Metodi di protezione

Backup:

- **Funzione:** Il backup consiste nel creare copie di sicurezza dei tuoi dati importanti (file, documenti, foto, ecc.) e archiviarle in un luogo sicuro, separato dal tuo computer o dispositivo principale.
- **Tipi:**
  - Backup locale: Su un disco rigido esterno, chiavetta USB o altro dispositivo di archiviazione.
  - Backup cloud: Su server remoti tramite servizi online.
- **Importanza:** Il backup ti permette di recuperare i tuoi dati in caso di perdita, danneggiamento, furto o attacco informatico (come un ransomware).
- **Frequenza:** Esegui backup regolari dei tuoi dati più importanti.

Come lavorano insieme:

- Il firewall protegge il perimetro della tua rete, bloccando le minacce esterne.
- L'antivirus protegge il tuo computer da malware che potrebbero infiltrarsi attraverso il firewall o tramite altre vie (come email o download).
- Il backup ti protegge dalla perdita di dati, anche in caso di attacchi informatici riusciti.

Autenticazione sicura: Password, 2FA, Biometria

- L'autenticazione sicura è fondamentale per proteggere i dati e prevenire accessi non autorizzati. Ecco le principali tecniche di autenticazione:
- **1. Password** 🔑
- Le password sono il metodo più diffuso, ma spesso il più vulnerabile. Per renderle sicure:
- Usa **password lunghe e complesse** (almeno 12-16 caratteri con lettere, numeri e simboli).
- Evita parole comuni e informazioni personali (nome, data di nascita, ecc.).
- Non riutilizzare la stessa password per più servizi.
- Usa un **password manager** per generare e archiviare password sicure.
- **2. Autenticazione a Due Fattori (2FA/MFA)**
- Aggiunge un ulteriore livello di sicurezza richiedendo un secondo metodo di verifica oltre alla password.
  Tipologie di 2FA:
- **OTP (One-Time Password)**: codici inviati via SMS o email (meno sicuri perché intercettabili).
- **App di autenticazione**: come Google Authenticator, Microsoft Authenticator o Authy, che generano codici temporanei.
- **Chiavi di sicurezza hardware**: dispositivi fisici come YubiKey o Titan Security Key.
- **Notifiche push**: inviate direttamente su un'app di sicurezza per approvazione manuale.
- ,0

Autenticazione sicura: Password, 2FA, Biometria

- **. Biometria** 👆🔍
- Utilizza caratteristiche uniche dell'utente per l'autenticazione:
- **Impronte digitali** (Touch ID, sensori biometrici).
- **Riconoscimento facciale** (Face ID, Windows Hello).
- **Scansione dell'iride o della retina**.
- **Riconoscimento vocale**.
- **Qual è il metodo più sicuro?**
- La combinazione di più fattori (es. **password + 2FA** o **biometria + password**) è la scelta migliore.
- Le **password da sole** sono vulnerabili agli attacchi brute-force e phishing.
- Il **2FA con chiavi fisiche o app di autenticazione** è tra le soluzioni più sicure.
- La **biometria è comoda**, ma può essere meno sicura se i dati biometrici vengono compromessi (non possono essere cambiati come una password).

Informatica verde e sicura

- Risparmio energetico: Standby, Ibernazione, Hardware eco-friendly
- Sicurezza nei dispositivi: Aggiornamenti e gestione dei permessi
- Etica digitale e protezione della privacy

Risparmio energetico:

Modalità Standby:

- **Funzione:**
  - La modalità standby mette il dispositivo in uno stato di basso consumo energetico.
  - Il dispositivo rimane acceso, ma la maggior parte delle funzioni è disattivata.
  - È utile quando si prevede di utilizzare nuovamente il dispositivo in breve tempo, poiché si riattiva rapidamente.
- **Considerazioni:**
  - Anche in standby, il dispositivo consuma energia.
  - Per un risparmio energetico maggiore, è consigliabile spegnere completamente il dispositivo quando non viene utilizzato per periodi prolungati.

Modalità Ibernazione:

- **Funzione:**
  - L'ibernazione salva lo stato attuale del dispositivo sul disco rigido e lo spegne completamente.
  - Al riavvio, il dispositivo riprende esattamente da dove era stato lasciato.
  - È ideale per risparmiare energia quando si prevede di non utilizzare il dispositivo per un lungo periodo.
- **Vantaggi:**
  - Consumo energetico quasi nullo.
  - Ripristino completo dello stato di lavoro.

Risparmio energetico:

Hardware Eco-friendly:

- **Scelta di dispositivi efficienti:**
  - Optare per dispositivi con certificazioni di efficienza energetica (ad esempio, Energy Star).
  - Scegliere componenti hardware a basso consumo (ad esempio, SSD anziché HDD).
- **Ottimizzazione delle impostazioni:**
  - Regolare la luminosità dello schermo.
  - Disattivare le funzioni non necessarie (ad esempio, Wi-Fi, Bluetooth).
  - Utilizzare modalità di risparmio energetico integrate nei sistemi operativi.
- **Smaltimento responsabile:**
  - Smaltire correttamente i dispositivi elettronici obsoleti per ridurre l'impatto ambientale.
  - Riciclo dei componenti.

Consigli aggiuntivi:

- **Prese intelligenti:** Utilizzare prese intelligenti per spegnere completamente i dispositivi quando non in uso.
- **Illuminazione a LED:** Sostituire le lampadine tradizionali con quelle a LED, che consumano meno energia.
- **Gestione dell'alimentazione:** Ottimizzare le impostazioni di gestione dell'alimentazione del sistema operativo per ridurre il consumo energetico.
- Adottando queste pratiche, è possibile ridurre significativamente il consumo energetico e contribuire a un futuro più sostenibile.