

Cifrare i documenti con LibreOffice

Documenti di testo e PDF – Windows, macOS, Linux – gratuito

Prima di iniziare

LibreOffice va scaricato esclusivamente dal sito ufficiale it.libreoffice.org e mantenuto aggiornato. Per la cifratura dei PDF è necessaria la **versione 25.8 o successiva**, che consente di esportare in formato PDF 2.0 con cifratura AES-256. La versione installata si verifica dal menu **Aiuto** → **Informazioni su LibreOffice** (su Mac: **LibreOffice** → **Informazioni su LibreOffice**).

La procedura A1 produce un PDF protetto, apribile con qualsiasi lettore di PDF: è la soluzione consigliata per i documenti da consultare. La procedura A2 protegge il documento di testo modificabile, utile quando più colleghi devono lavorare sullo stesso file.

Procedura A1 – Esportare un PDF protetto da password (consigliata)

1. Aprire il documento in LibreOffice Writer.
2. Dal menu scegliere **File** → **Esporta come** → **Esporta come PDF...**
3. Nella scheda **Generale**, nel menu a tendina della versione, selezionare **PDF 2.0**, che garantisce la cifratura AES-256. Non selezionare le versioni PDF/A, che non ammettono la protezione con password.
4. Aprire la scheda **Sicurezza** e premere il pulsante **Imposta password...**
5. Nella sezione relativa alla **password di apertura** inserire la password e ripeterla nel campo di conferma. La sezione relativa alla password dei permessi può essere lasciata vuota: da sola non protegge il contenuto.
6. Premere **OK**, poi **Esporta**, scegliere la cartella e il nome del file e premere **Salva**.

Procedura A2 – Salvare il documento di testo con password

1. Dal menu scegliere **File** → **Salva con nome...** e mantenere il formato **Documento di testo ODF (.odt)**.
2. Nella parte inferiore della finestra spuntare la casella **Salva con password** e premere **Salva**.
3. Inserire la password nel campo relativo alla **password di apertura del file** e ripeterla per conferma. Non è necessario impostare la password di modifica, che da sola non protegge il contenuto.
4. Premere **OK**. Il documento potrà essere aperto solo inserendo la password; la protezione resta attiva a ogni salvataggio successivo.

Da ricordare. PDF 2.0 con password di apertura, oppure “Salva con password”. Non utilizzare la sola password dei permessi o di modifica. Verificare sempre, riaprendo il file, che la password venga richiesta.

Cifrare i documenti con Microsoft Office

Documenti Word, fogli Excel e PDF – Windows e Mac

Prima di iniziare

La cifratura richiede l'applicazione **Word installata sul computer** (Microsoft 365 o Office 2016 e versioni successive). Word per il web, cioè la versione che si usa nel browser, non consente di impostare la password di apertura, mentre permette di aprire i documenti già protetti. Il documento va salvato nel formato **.docx**: il vecchio formato .doc utilizza una protezione non più adeguata.

Procedura B1 – Proteggere il documento Word con password (consigliata)

1. Aprire il documento in Word.
2. Dal menu scegliere **File** → **Informazioni** → **Proteggi documento** → **Crittografa con password**.
3. Inserire la password e premere **OK**; ripeterla nella finestra successiva e premere di nuovo **OK**.
4. Salvare il documento (**File** → **Salva** oppure Ctrl+S): la protezione diventa effettiva con il salvataggio.

Su Mac la stessa funzione si trova nella scheda **Revisione** → **Proteggi documento**, impostando la password nel campo relativo all'apertura del documento. Per i fogli Excel il percorso è analogo: **File** → **Informazioni** → **Proteggi cartella di lavoro** → **Crittografa con password**.

Procedura B2 – Salvare un PDF protetto da password

1. Dal menu scegliere **File** → **Salva con nome** e, come tipo di file, selezionare **PDF**.
2. Premere il pulsante **Opzioni...**, spuntare la casella **Crittografa il documento con una password** e premere **OK**.
3. Premere **Salva**: Word chiederà di inserire la password e di ripeterla. Per i PDF Word ammette password di non più di 32 caratteri, limite sufficiente per una password composta secondo i criteri del § 9; se la password scelta lo supera, occorre utilizzare la procedura B1.

Funzioni da non utilizzare

Non cifrano il documento, che resta leggibile a chiunque lo apra: **Limita modifica** e **Segna come finale** (scheda Revisione); la sola **password di modifica** impostabile da Salva con nome → Strumenti → Opzioni generali; la **protezione del foglio** di Excel. Se il documento si trova in una cartella sincronizzata con **OneDrive**, occorre verificare che la versione non cifrata non resti disponibile nella cronologia delle versioni.

Da ricordare. File → Informazioni → Proteggi documento → Crittografa con password, oppure PDF con l'opzione "Crittografa il documento con una password". Verificare sempre, riaprendo il file, che la password venga richiesta.

Cifrare file e cartelle con 7-Zip

Archivi cifrati di file di qualsiasi formato – Windows – gratuito

Quando utilizzarlo

7-Zip è utile per proteggere **file di qualsiasi formato** (scansioni, immagini, fogli di calcolo) o **più file insieme**, raccolti in un unico archivio cifrato da inviare per posta elettronica o da condividere, e per proteggere i documenti della scuola conservati su un computer personale il cui disco non sia cifrato. Il programma va scaricato **esclusivamente dal sito ufficiale 7-zip.org**, diffidando dei siti con nomi simili.

Chi riceve l'archivio deve avere 7-Zip installato: Esplora file di Windows non è in grado di aprire gli archivi cifrati. I colleghi che utilizzano un Mac possono aprirli con il programma gratuito Keka.

Procedura – Creare un archivio cifrato

1. Selezionare il file, i file o la cartella da proteggere, fare clic con il tasto destro e scegliere **7-Zip** → **Aggiungi all'archivio...** In Windows 11 la voce compare dopo aver scelto **Mostra altre opzioni**.
2. Nel campo **Archivio** indicare un nome neutro, che non contenga il nome dell'alunno.
3. Come **formato dell'archivio** selezionare **7z**.
4. Nella sezione **Crittografia** inserire la password, ripeterla e verificare che il **metodo di crittografia** sia **AES-256**.
5. Spuntare la casella **Crittografa i nomi dei file**, così che senza password non sia visibile nemmeno l'elenco dei documenti contenuti.
6. Premere **OK**: nella stessa cartella verrà creato il file con estensione **.7z**. Eliminare quindi gli originali non cifrati, se non devono essere conservati sul dispositivo.

Aprire un archivio cifrato

Fare clic con il tasto destro sull'archivio, scegliere **7-Zip** → **Estrai file...** e inserire la password. Terminata la consultazione, **eliminare i file estratti**, in particolare sui computer condivisi.

Da evitare

Il formato **zip** con metodo **ZipCrypto**, che offre una protezione debole; la funzione di Windows **Invia a** → **Cartella compressa**, che non consente di impostare alcuna password; gli archivi creati senza spuntare **Crittografa i nomi dei file**.

Da ricordare. Formato 7z, metodo AES-256, casella "Crittografa i nomi dei file" spuntata. Verificare che la password venga richiesta già per visualizzare il contenuto dell'archivio.

Cifrare una chiavetta USB con BitLocker To Go

Chiavette USB e dischi esterni – Windows 10 e 11 Pro, Education, Enterprise

Prima di iniziare

BitLocker To Go è una funzione integrata in Windows che cifra per intero una chiavetta USB o un disco esterno: da quel momento ogni file copiato sulla chiavetta è automaticamente protetto. La cifratura può essere **attivata** soltanto sulle edizioni Pro, Education ed Enterprise di Windows, normalmente in uso sui computer della scuola; la chiavetta cifrata può invece essere **aperta e utilizzata** su qualsiasi computer Windows, anche nell'edizione Home, inserendo la password. I Mac non sono in grado di leggerla senza programmi aggiuntivi: in questo caso si veda la [scheda G](#).

Prima di procedere è opportuno salvare altrove una copia dei file già presenti sulla chiavetta. La procedura può richiedere da pochi minuti a oltre un'ora, a seconda della capacità del dispositivo, e durante l'operazione la chiavetta **non deve essere rimossa**.

Procedura – Attivare BitLocker sulla chiavetta

1. Inserire la chiavetta, aprire **Esplora file** e selezionare **Questo PC**.
2. Fare clic con il tasto destro sulla chiavetta e scegliere **Attiva BitLocker** (in Windows 11, dopo aver scelto **Mostra altre opzioni**). In alternativa: **Pannello di controllo** → **Sistema e sicurezza** → **Crittografia unità BitLocker**, sezione **Unità dati rimovibili – BitLocker To Go**.
3. Spuntare **Usa una password per sbloccare l'unità**, inserire la password e ripeterla; premere **Avanti**.
4. Scegliere come salvare la **chiave di ripristino**, un codice di 48 cifre che consente di aprire la chiavetta se la password viene dimenticata: **Salva in un file** (da conservare in un luogo sicuro, mai sulla chiavetta stessa) oppure **Stampa la chiave di ripristino**. Sui dispositivi della scuola, seguire le indicazioni dell'amministratore di sistema.
5. Alla domanda sulla porzione da crittografare scegliere **Crittografa l'intera unità** se la chiavetta è già stata utilizzata (i file cancellati potrebbero altrimenti restare leggibili), oppure **Crittografa solo lo spazio utilizzato** se è nuova.
6. Scegliere la **Modalità compatibile**, adatta alle unità da utilizzare su computer diversi, e premere **Avvia crittografia**. Attendere il messaggio di completamento.

Utilizzare la chiavetta cifrata

Inserendo la chiavetta in un computer Windows compare la richiesta di password: dopo averla inserita, la chiavetta si utilizza normalmente. Non spuntare l'opzione di sblocco automatico sui computer condivisi. Al termine, rimuovere la chiavetta con la funzione **Rimozione sicura dell'hardware**: una volta estratta, torna a essere protetta.

Da ricordare. Password di tre parole e due cifre scelte a caso ([§ 9 della nota](#)), diversa da quella del consiglio di classe; chiave di ripristino conservata separatamente dalla chiavetta; "Crittografa l'intera unità" per le chiavette già utilizzate.

Cifrare il disco del computer con BitLocker

Computer e notebook con Windows 10 e 11

Prima di iniziare

La cifratura del disco protegge tutti i dati del computer in caso di furto o smarrimento. Sui **computer della scuola** l'attivazione e la custodia delle chiavi di ripristino competono all'**amministratore di sistema**: questa scheda è rivolta principalmente ai docenti che intendano proteggere il proprio computer personale. Prima di procedere è opportuno eseguire una copia di sicurezza dei dati e collegare il notebook all'alimentazione.

Windows offre due funzioni, a seconda dell'edizione: **BitLocker**, nelle edizioni Pro ed Education, e **Crittografia dispositivo**, disponibile anche nell'edizione Home sui computer che soddisfano i requisiti hardware. L'edizione installata si verifica in **Impostazioni** → **Sistema** → **Informazioni su**, alla voce **Edizione**.

Verificare se la cifratura è già attiva

Sui computer più recenti, installati o ripristinati con Windows 11 versione 24H2 o successiva, la cifratura può essere già attiva. Aprire **Impostazioni** → **Privacy e sicurezza** → **Crittografia dispositivo**: se l'interruttore è attivo, il disco è già cifrato. In questo caso occorre soltanto assicurarsi di disporre della chiave di ripristino, che nei computer personali è di norma salvata nell'account Microsoft (consultabile all'indirizzo account.microsoft.com/devices/recoverykey). Se la voce Crittografia dispositivo non compare, il computer non supporta questa funzione e occorre utilizzare BitLocker, se disponibile, o cifrare i singoli documenti (schede [A](#), [B](#), [C](#) e [G](#)).

Procedura E1 – Windows Home: Crittografia dispositivo

1. Accedere a Windows con un **account Microsoft**, necessario per il salvataggio automatico della chiave di ripristino.
2. Aprire **Impostazioni** → **Privacy e sicurezza** → **Crittografia dispositivo** e attivare l'interruttore.
3. Verificare, all'indirizzo indicato sopra, che la chiave di ripristino sia stata salvata, annotandone eventualmente una copia da conservare in luogo sicuro, separato dal computer.

Procedura E2 – Windows Pro ed Education: BitLocker

1. Aprire **Pannello di controllo** → **Sistema e sicurezza** → **Crittografia unità BitLocker** (oppure cercare "Gestisci BitLocker" dal menu Start).
2. In corrispondenza dell'unità del sistema operativo (di norma C:) scegliere **Attiva BitLocker**.
3. Scegliere come salvare la **chiave di ripristino**: nell'account Microsoft, in un file su un'unità esterna o stampata. Non salvarla sul disco che si sta cifrando.
4. Scegliere **Crittografia l'intera unità** per un computer già in uso e la **Nuova modalità di crittografia**, adatta ai dischi interni.
5. Lasciare spuntata l'opzione **Esegui controllo di sistema BitLocker**, premere **Continua** e riavviare il computer quando richiesto. La cifratura prosegue in background: il computer può essere utilizzato normalmente.

Da ricordare. La cifratura del disco protegge i dati quando il computer è spento o bloccato: l'accesso a Windows deve essere protetto da una password robusta, diversa da quelle utilizzate per altri servizi, e il blocco automatico dello schermo deve essere attivo. Senza la chiave di ripristino, in caso di guasto, i dati non sono recuperabili.

Cifrare il disco e le chiavette USB su Mac

FileVault e cifratura dal Finder – macOS

Procedura F1 – Cifrare il disco con FileVault

FileVault è la funzione di macOS che cifra l'intero disco del Mac. Sui computer della scuola va attivata a cura dell'amministratore di sistema; sui Mac personali può essere attivata dal docente. È opportuno eseguire prima una copia di sicurezza con Time Machine.

1. Aprire il menu **Apple** → **Impostazioni di Sistema** → **Privacy e sicurezza**.
2. Scorrere fino alla sezione **FileVault** e premere **Attiva...**; inserire la password dell'utente quando richiesta.
3. Scegliere come consentire lo sblocco del disco in caso di password dimenticata: tramite l'**account iCloud** oppure mediante una **chiave di recupero**. In quest'ultimo caso, trascrivere la chiave e conservarla in un luogo sicuro, separato dal computer.
4. Premere **Continua**. La cifratura procede in background mentre il Mac viene utilizzato normalmente; lo stato di avanzamento è visibile nella stessa sezione.

Procedura F2 – Cifrare una chiavetta USB dal Finder

Una chiavetta cifrata con questa procedura è leggibile **soltanto sui Mac**. Per le chiavette da utilizzare anche su Windows si veda la [scheda G](#).

1. Inserire la chiavetta e individuarla nella barra laterale del **Finder**.
2. Fare clic con il tasto destro (o Ctrl+clic) sulla chiavetta e scegliere **Codifica “nome della chiavetta”...**
3. Inserire la password, ripeterla e aggiungere un suggerimento che non la renda intuibile; premere **Codifica disco**.
4. Se la voce Codifica non compare, la chiavetta ha un formato non compatibile: occorre inizializzarla con **Utility Disco**, scegliendo il formato **APFS (codificato)**, dopo aver salvato altrove i file che contiene, che verranno cancellati.

Da ricordare. FileVault protegge i dati quando il Mac è spento o bloccato: l'account utente deve essere protetto da una password robusta, diversa da quelle utilizzate per altri servizi, e il blocco dello schermo deve essere attivo. Conservare la chiave di recupero separatamente dal computer.

Creare un contenitore cifrato con VeraCrypt

Chiavette USB e computer personali – Windows, macOS, Linux – gratuito e open source

Quando utilizzarlo

VeraCrypt è un programma gratuito e open source che crea un **contenitore cifrato**: un file che, una volta aperto con la password, si comporta come un'unità disco aggiuntiva nella quale copiare e modificare i documenti, che vengono cifrati e decifrati automaticamente. È utile per le chiavette USB da utilizzare su sistemi diversi (Windows e Mac) e per i docenti che non possono o non vogliono cifrare il disco del proprio computer personale ma devono conservarvi documenti della scuola.

Il programma va scaricato **esclusivamente dal sito ufficiale veracrypt.io**. L'installazione richiede i diritti di amministratore, e VeraCrypt deve essere installato su ogni computer sul quale si intende aprire il contenitore; su Mac richiede anche il componente gratuito macFUSE. Per queste ragioni è indicato soprattutto per i dispositivi personali.

Procedura G1 – Creare il contenitore

1. Avviare VeraCrypt e premere **Crea un volume**.
2. Scegliere **Crea un file contenitore cifrato** e poi **Volume VeraCrypt standard**; premere **Avanti**.
3. Premere **Seleziona file...**, scegliere la posizione (ad esempio la chiavetta USB o la cartella Documenti) e indicare un nome neutro per il contenitore; premere **Salva** e poi **Avanti**.
4. Lasciare le impostazioni predefinite di cifratura (**AES**, hash **SHA-512**) e premere **Avanti**.
5. Indicare la **dimensione** del contenitore, adeguata ai documenti da conservare (ad esempio 2 GB), e premere **Avanti**.
6. Inserire la **password**, scelta secondo i criteri del [§ 9 della nota](#) (tre parole e due cifre scelte a caso), e ripeterla; premere **Avanti**.
7. Come file system scegliere **exFAT**, se il contenitore deve essere aperto anche su Mac, oppure **NTFS** per l'uso sul solo Windows. Muovere il mouse in modo casuale all'interno della finestra finché la barra non è completa, quindi premere **Formatta** e, al termine, **Esci**.

Procedura G2 – Aprire e chiudere il contenitore

1. Avviare VeraCrypt, selezionare una lettera di unità libera nell'elenco e premere **Seleziona file...** per scegliere il contenitore.
2. Premere **Monta** e inserire la password: il contenitore compare in Esplora file (o nel Finder) come una normale unità disco, nella quale copiare, aprire e modificare i documenti.
3. Al termine del lavoro tornare in VeraCrypt, selezionare l'unità e premere **Smonta**: i documenti tornano a essere inaccessibili senza password.

Da ricordare. VeraCrypt non consente il recupero di una password dimenticata: senza di essa i documenti sono perduti. Conservare una copia di sicurezza dei documenti negli spazi istituzionali e smontare sempre il contenitore al termine del lavoro.