



Il backup e la regola 3-2-1

Come non perdere mai i tuoi dati, qualunque cosa succeda

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Indice

Come usare questa dispensa 3

1. Perché un backup, e che cos'è davvero 3

1.1 Le quattro strade verso la perdita dei dati 4

1.2 Copia, sincronizzazione, backup: non sono la stessa cosa 5

2. La regola 3-2-1 6

2.1 Un esempio per la segreteria di una scuola 6

2.2 Il disco lasciato inserito è un errore comune 7

3. Dove tenere le copie: disco, rete, cloud 8

3.1 Disco esterno 8

3.2 Disco di rete 8

3.3 Cloud 8

3.4 La copia incorporata in Windows 11 9

4. Che cosa salvare e ogni quanto 10

4.1 Ogni quanto 11

4.2 Completa, incrementale, versioni 11

5. Provare il ripristino, e il legame con il ransomware 13

5.1 Il backup è la vera difesa contro il ransomware 14

5.2 Backup e disponibilità 14

Esercitazione pratica 16

Le domande che arrivano in aula 17

Glossario 17

Per approfondire 18

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Capire che cos'è un vero backup, applicare la regola 3-2-1 con gli strumenti che hai già e verificare che le copie funzionino davvero, anche dopo un attacco ransomware.

Che cosa saprai fare alla fine

- Distinguere un backup vero da una semplice copia o da una sincronizzazione.
- Applicare la regola 3-2-1 a un computer di segreteria o di casa.
- Scegliere tra disco esterno, rete locale e cloud in base ai dati da proteggere.
- Decidere che cosa salvare e con quale frequenza.
- Provare il ripristino di un file per essere certo che la copia sia utilizzabile.

1. Perché un backup, e che cos'è davvero

Prima o poi un computer si rompe, un file si cancella o qualcuno ti blocca i dati. La domanda non è se succederà, ma se quel giorno avrai una copia.

Immagina la segreteria di un piccolo studio, lo Studio Esempio. Una mattina il computer che custodisce le pratiche dei clienti non si accende più. Dentro ci sono dieci anni di lavoro: contratti, fatture, scansioni. Se non c'è una copia, quel lavoro è perso.

Un **backup** (parola inglese che significa copia di sicurezza) è una copia dei tuoi dati tenuta in un posto diverso dall'originale, pensata per un solo scopo: permetterti di ripartire dopo un guasto, un errore o un attacco.



Le quattro cause più comuni di perdita dei dati

1.1 Le quattro strade verso la perdita dei dati

- **Un guasto**: il disco si rompe, spesso senza segnali;
- **Un errore**: cancelli o sovrascrivi un file per sbaglio;
- **Un furto o un incendio**: il computer sparisce, con tutto quello che contiene;
- **Un ransomware**: un programma dannoso cifra i file e chiede un riscatto.

Nessuna di queste cause avvisa prima. Per questo la copia va fatta **prima** che serva, non dopo.



Guasto, errore, furto o attacco possono far perdere i dati.

1.2 Copia, sincronizzazione, backup: non sono la stessa cosa

Molti pensano di avere un backup perché i file sono anche sul cloud o su una chiavetta. Non sempre è vero. Una **sincronizzazione** tiene due posti identici: se cancelli un file da una parte, sparisce anche dall'altra. Se un ransomware cifra i tuoi file, la cifratura viene sincronizzata a sua volta.



Sincronizzare non basta se si propagano cancellazioni e modifiche.

Cosa fai	Protegge da un guasto?	Protegge da un errore o da un ransomware?
Tieni i file solo sul computer	No	No
Sincronizzi una cartella con il cloud	In parte	Spesso no: l'errore viene copiato anche là
Copi su una chiavetta sempre inserita	In parte	No: il ransomware cifra anche quella
Fai un backup con versioni precedenti e una copia scollegata	Sì	Sì

Avere i file in due posti non basta: conta se la copia può essere raggiunta da chi attacca.

L'IDEA IN UNA RIGA

Un backup serve solo se è separato dall'originale e se, quel giorno, riesci davvero a riaprirlo.

2. La regola 3-2-1

Tre numeri da ricordare: 3 copie, 2 supporti diversi, 1 copia lontana.

La regola 3-2-1 è lo schema che i tecnici usano da anni perché è semplice e regge quasi a tutto. Vediamola un pezzo alla volta.



Tre copie totali: originale e due copie di sicurezza, su due supporti, una fuori sede.

- **3 copie dei dati**: l'originale sul computer più due copie di sicurezza. Se una cosa va storta, ne restano altre due;
- **2 supporti diversi**: per esempio il disco interno del computer e un disco esterno, oppure un disco esterno e il cloud. Supporti diversi si rompono per motivi diversi;
- **1 copia fuori sede**: almeno una copia lontana dall'ufficio, per esempio nel cloud o in un altro edificio. Così un incendio, un allagamento o un furto non portano via tutto.

2.1 Un esempio per la segreteria di una scuola

La segreteria dell'Istituto Esempio lavora sui registri e sulle iscrizioni. Applica la regola così.

Copia	Dove sta	Supporto
Copia 1	I file di lavoro sul computer della segreteria	Disco interno
Copia 2	Un disco esterno, collegato solo durante la copia e poi riposto in un cassetto chiuso a chiave	Disco esterno

Copia	Dove sta	Supporto
Copia 3	Un servizio cloud con cifratura, in un altro luogo	Cloud, fuori sede

Tre copie, due supporti diversi, una fuori sede.



Computer, disco scollegato e copia fuori sede hanno ruoli diversi.

> **QUANDO LA REGOLA HA SALVATO LA GIORNATA**
>
> Un lunedì un virus cifra i file del computer. Il disco esterno era scollegato nel cassetto, quindi è intatto. La segreteria ripulisce il computer, ricarica i dati dalla copia e riparte. La copia nel cloud, in più, ha tenuto al sicuro anche le versioni precedenti dei documenti.

2.2 Il disco lasciato inserito è un errore comune

Un disco esterno sempre collegato al computer è raggiungibile dal ransomware, che lo cifra insieme al resto. La copia davvero al sicuro è quella **scollegata**, o quella che il programma di attacco non riesce a modificare.

> **ATTENZIONE**
>
> Se tutte le tue copie sono collegate al computer, per un ransomware sono una cosa sola. Almeno una copia deve restare fisicamente scollegata o protetta da versioni precedenti.

3. Dove tenere le copie: disco, rete, cloud

Non esiste il supporto perfetto: ognuno ha pregi e difetti, ed è per questo che se ne usano due.



Ogni destinazione ha vantaggi e limiti da considerare.

3.1 Disco esterno

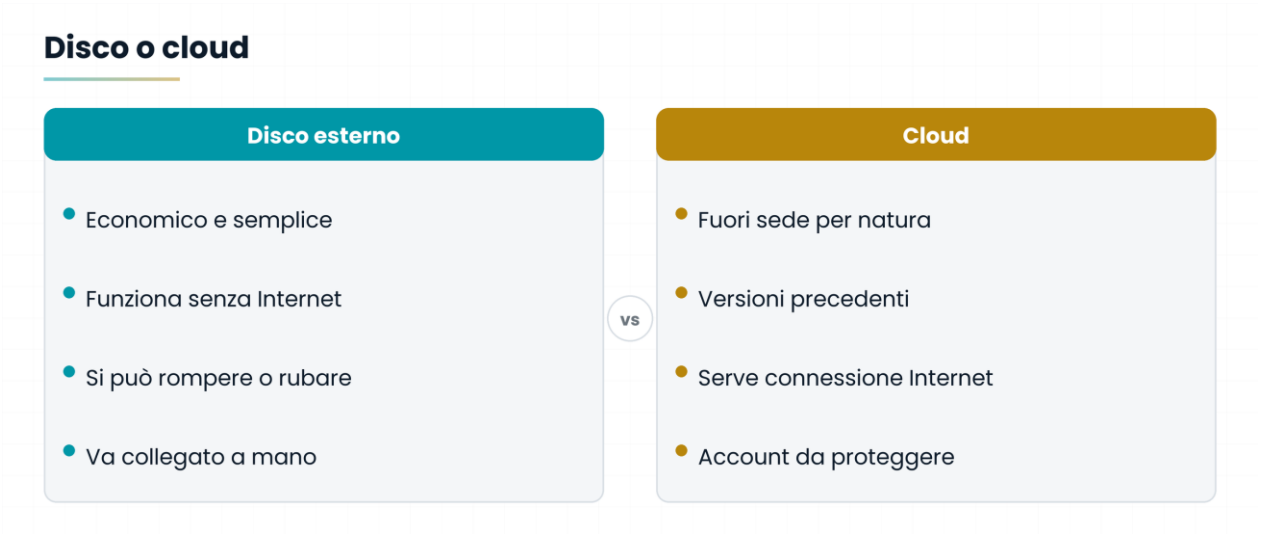
È la scelta più semplice e più economica: lo colleghi alla porta USB (la presa standard dei computer), copi e lo stacchi. Funziona anche senza Internet. Il limite è che è fisico: si può rompere, perdere o rubare, e va ricordato di collegarlo.

3.2 Disco di rete

Un piccolo studio può usare un **NAS**, cioè un apparecchio con uno o più dischi collegato alla rete dell'ufficio, a cui i computer inviano le copie in automatico. È comodo, ma se resta sempre acceso e raggiungibile può essere colpito dal ransomware come i computer. Chiedi al tecnico di configurarlo con copie che non si possano modificare.

3.3 Cloud

Il **cloud** (letteralmente nuvola) significa tenere i file sui computer di un fornitore, raggiungibili via Internet. È la copia fuori sede più comoda: non devi portarla da nessuna parte. Scegli un servizio che conservi le **versioni precedenti** dei file, così puoi tornare a ieri se oggi è stato tutto cifrato.



Disco esterno e cloud a confronto

DATI DI TERZI NEL CLOUD

Se nelle copie ci sono dati personali di clienti, alunni o pazienti, il fornitore del cloud tratta quei dati per tuo conto. Scegli un servizio che dichiari di trattare i dati nell'Unione Europea e fai valutare la scelta al titolare dell'ente, come vedremo nella lezione sulla privacy.



Il cloud deve conservare copie recuperabili e avere accessi protetti.

3.4 La copia incorporata in Windows 11

Windows 11 ha strumenti pronti. Cerca **Backup di Windows** nella casella di ricerca della barra delle applicazioni: ti permette di salvare cartelle e impostazioni sul servizio cloud di

Microsoft (OneDrive). Per salvare su un disco esterno puoi usare la funzione **Cronologia file**, se è disponibile sulla tua versione. I nomi esatti dei menu possono cambiare con gli aggiornamenti: cerca la funzione per nome.

> **IN PAROLE SEMPLICI**
>
> Disco esterno scollegato più cloud con versioni precedenti: due supporti, una copia fuori sede. Per una segreteria è già un ottimo punto di partenza.

4. Che cosa salvare e ogni quanto

Non serve salvare tutto: serve salvare quello che non puoi rifare.

Windows e i programmi si reinstallano. I tuoi documenti, le foto, i database e le mail no. Parti dall'elenco di ciò che, se sparisse domani, ti metterebbe nei guai.



Parti da ciò che non puoi ricreare facilmente.

Da salvare sempre	Da salvare se serve	Di solito si può rifare
Documenti, fogli di calcolo, contratti	Impostazioni dei programmi	Windows
Archivio della posta e rubrica	Elenco dei programmi installati	Programmi scaricabili di nuovo
Fotografie e scansioni	Preferiti del browser	File temporanei

Da salvare sempre	Da salvare se serve	Di solito si può rifare
Database del gestionale o della contabilità	Modelli personalizzati	Cartella dei download già archiviati

Parti dalla prima colonna.

4.1 Ogni quanto

La regola pratica è una domanda: **quanto lavoro posso permettermi di rifare?** Se per te è accettabile rifare il lavoro di un giorno, la copia va fatta ogni giorno. Se perdere una settimana sarebbe un disastro, la copia va fatta più spesso. Per dati che cambiano ogni giorno, come la contabilità, la copia automatica quotidiana è la scelta più sicura.



La frequenza dipende da quanto lavoro puoi permetterti di rifare.

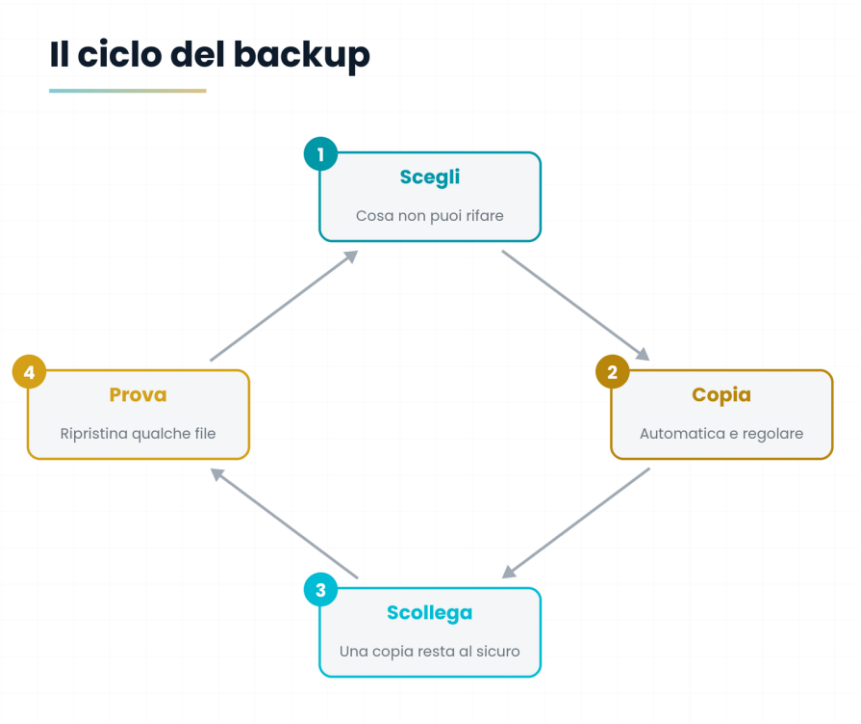
4.2 Completa, incrementale, versioni

- **Copia completa**: ricopia tutto. È la più semplice da usare, ma richiede più spazio e più tempo;
- **Copia incrementale**: salva solo ciò che è cambiato dall'ultima copia. È più leggera;
- **Versioni precedenti**: il programma ricorda più versioni dello stesso file, così puoi recuperare quella di prima di un errore o di un attacco.



Una copia completa salva tutto; un'incrementale salva le modifiche.

> **CASO PRATICO: IL NEGOZIO**
>
> Nel negozio Esempio il registratore di cassa invia ogni sera i dati a un computer. La titolare lascia la copia automatica sul disco esterno e, il venerdì, porta a casa un secondo disco a rotazione. Se il negozio subisce un furto, i dati dell'ultima settimana sono comunque al sicuro.



Il ciclo del backup che funziona

AUTOMATIZZA

Un backup che dipende dalla tua memoria prima o poi salta. Programmalo, e controlla ogni tanto che stia girando.

5. Provare il ripristino, e il legame con il ransomware

Una copia che non hai mai provato a riaprire è solo una speranza.

Capita di scoprire, nel giorno del bisogno, che la copia era vuota, danneggiata o incompleta. Per questo ogni tanto bisogna **provare il ripristino**: scegliere qualche file a caso dalla copia e verificare che si aprano e che siano aggiornati.

1. scegli tre file importanti, di tipo diverso (un documento, un foglio di calcolo, una foto);
2. recuperali dalla copia, mettendoli in una cartella di prova, non sopra gli originali;
3. aprili e controlla che il contenuto sia quello giusto;
4. annota la data della prova e che cosa hai verificato.



Ripristina tre file in una cartella di prova e aprili.

5.1 Il backup è la vera difesa contro il ransomware

Nella lezione sul malware e sul ransomware abbiamo visto che chi ti cifra i file chiede un riscatto. Pagare non dà garanzie: non hai certezza di riavere i dati, e finanzi chi ti ha attaccato. Con una copia recente e scollegata il ricatto perde forza: non hai bisogno dei criminali per riavere i tuoi file.

5.2 Backup e disponibilità

Ricordi le tre proprietà della sicurezza della prima lezione? Il backup difende la **disponibilità**: avere i dati quando servono. Ma attenzione, perché le copie contengono gli stessi dati personali degli originali e vanno protette allo stesso modo.

- **cifra** il disco esterno e le copie (in Windows Pro c'è BitLocker, ne abbiamo parlato nella lezione sui dispositivi);
- tieni il disco in un **luogo chiuso**, non appoggiato sulla scrivania;
- proteggi l'accesso al cloud con una **password lunga e la verifica in due passaggi**;
- quando smaltisci un vecchio disco, **cancellalo in modo sicuro o distruggilo**, non buttarlo.



Anche le copie contengono dati delle persone.

IL LIMITE ONESTO

Un backup non impedisce l'attacco e non evita che i dati rubati vengano diffusi: ti fa solo ripartire. Per questo restano necessari tutte le altre difese del corso: aggiornamenti, prudenza con le mail, password.

Esercitazione pratica

Una breve esercitazione con il tuo computer e un disco esterno o un account cloud che hai già.

1. Elenca su un foglio le cartelle che non vorresti mai perdere: documenti, foto, posta.
2. Controlla dove si trovano oggi: solo sul computer, o anche altrove?
3. Disegna la tua regola 3-2-1: quale è la copia 1, la 2 e la 3, e quale è fuori sede.
4. Fai una copia manuale delle cartelle importanti su un disco esterno e poi scollegalo.
5. Recupera tre file dalla copia in una cartella di prova e aprili.
6. Annota la data e programma un promemoria per ripetere la prova.

CONTROLLO FINALE

Hai almeno una copia scollegata dal computer?

Hai una copia fuori sede?

Sei riuscito a riaprire i file recuperati?

Il disco esterno è in un posto chiuso?

Le domande che arrivano in aula

Basta salvare i file su OneDrive o su Google Drive?

Non da solo. Il cloud sincronizzato copia anche gli errori e, in certi casi, anche i file cifrati da un ransomware. Va bene come copia fuori sede se conserva le versioni precedenti, ma serve almeno un'altra copia su un supporto diverso.

Il cloud è sicuro?

Dipende dal servizio e da come lo usi. Un fornitore serio protegge i suoi sistemi, ma un account con password debole e senza verifica in due passaggi resta il punto debole. Attivala sempre.

Quanto spazio mi serve?

Guarda quanto occupano le cartelle da salvare e scegli un disco di dimensione almeno doppia, così hai spazio per le versioni nel tempo. Un disco esterno di capacità media basta per la maggior parte delle segreterie.

Posso tenere il disco esterno sempre collegato per comodità?

Meglio di no. Se è sempre collegato, un ransomware lo raggiunge e lo cifra. Collegalo per la copia e poi scollegalo.

Ogni quanto devo provare il ripristino?

Più spesso all'inizio, per essere sicuro che tutto funzioni, e poi a intervalli regolari decisi da te. L'importante è farlo davvero e annotarlo.

I dati nel backup sono soggetti alla privacy?

Sì. Le copie contengono gli stessi dati personali degli originali, quindi vanno protette con gli stessi criteri: accesso limitato, cifratura e smaltimento sicuro.

Glossario

Termine	Che cosa significa
Backup	Copia di sicurezza dei dati, tenuta in un posto diverso dall'originale, da usare in caso di perdita o guasto.
Cloud	Archiviazione dei file sui computer di un fornitore, raggiungibili via Internet.
Copia incrementale	Copia che salva solo ciò che è cambiato dall'ultimo backup.

Termine	Che cosa significa
NAS	Piccolo apparecchio con dischi collegato alla rete dell'ufficio, usato per conservare file e copie.
Ransomware	Programma dannoso che cifra i file e chiede un riscatto per restituirli.
Regola 3-2-1	Schema di sicurezza: 3 copie dei dati, su 2 supporti diversi, di cui 1 fuori sede.
Ripristino	Operazione con cui si recuperano i dati dalla copia di sicurezza.
Sincronizzazione	Funzione che mantiene identici due posti: ogni modifica o cancellazione viene ripetuta nell'altro. Non è un backup.
Versioni precedenti	Copie successive dello stesso file, che permettono di tornare a una versione di prima.

Per approfondire

Agenzia per la Cybersicurezza Nazionale (ACN) - indicazioni e buone pratiche sulle copie di sicurezza e sulla difesa dal ransomware

Microsoft, documentazione di Windows 11 - Backup di Windows, Cronologia file e Sicurezza di Windows

Polizia Postale e delle Comunicazioni - consigli per la sicurezza dei dati

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. I nomi dei menu di Windows 11 possono cambiare con gli aggiornamenti: se non trovi una voce, cercala per nome nella casella di ricerca.