MIM
Ministero dell'Istruzione
e del Merito

SICURNAUTI
LA TUA GUIDA NELLA GALASSIA DIGITALE

LA CONSERVAZIONE DEI DATI E IL *BACKUP*

www.unica.istruzione.gov.it

INDICE DEI CONTENUTI

1 LA SICUREZZA DEI DATI NELL'ERA DIGITALE: CONTESTO E IMPORTANZA

Nell'attuale ecosistema digitale, i **dati** rappresentano uno dei **beni più preziosi** per cittadini, professionisti ed Enti istituzionali.
Dati personali, documenti di lavoro, fotografie, credenziali di accesso e in generale tutto ciò che produciamo e utilizziamo in formato digitale costituisce un **patrimonio informativo di valore**. Sempre più spesso le attività quotidiane, sia personali che lavorative, sono supportate da **strumenti digitali**, esponendo i dati a un rischio elevato di **perdita o compromissione** improvvisi. Inoltre, nella maggior parte dei casi, il loro **recupero risulta complesso**, costoso o persino impossibile.

Nonostante la crescente dipendenza dalle informazioni digitali, permane una limitata consapevolezza dei rischi connessi alla loro conservazione. Diventa, quindi, essenziale adottare un approccio strutturato alla **protezione dei dati**, fondato sul concetto di riservatezza, integrità e disponibilità.

2 RISCHI E MINACCE NELLA CONSERVAZIONE QUOTIDIANA DEI DATI

La perdita o la compromissione dei dati raramente è il risultato di un unico evento isolato, più frequentemente deriva da una **combinazione di fattori**. Conoscere i rischi che possono portare al danneggiamento o alla violazione delle informazioni digitali rappresenta il primo passo per sviluppare comportamenti responsabili e costruire un sistema di protezione efficace e sostenibile nel tempo.

Tra i **principali rischi** possiamo individuare:

Virus e *malware*

Attraverso l'apertura di *link* contenuti nelle e-mail, il *download* di allegati o a seguito dell'accesso a siti non sicuri, **virus**, ***ransomware*** e altri ***malware*** possono penetrare nei sistemi **compromettendo *file* e archivi**. In alcuni casi, i dati vengono danneggiati o resi inutilizzabili, in altri, l'accesso può essere completamente bloccato fino al pagamento di un riscatto.
(*Rif. Brochure #7 – La sicurezza dei dispositivi mobili e Brochure #3 - Attenzione ai click*).

→ Oltre ai danni economici, tali incidenti possono causare **interruzioni delle attività** e **perdita di informazioni sensibili**.

Configurazioni errate dei sistemi di *backup* (*misconfiguration*)

Una configurazione non corretta dei sistemi di *backup* può esporre dati sensibili *online* o renderli accessibili a utenti non autorizzati. Questo rischio è spesso dovuto ad una mancata gestione delle impostazioni predefinite, dei permessi o dei controlli di sicurezza.

→ Una configurazione inadeguata **può vanificare le strategie di *backup***, rendendo i dati accessibili o non protetti.

Mancato aggiornamento dei dispositivi

Sistemi, dispositivi e applicazioni non aggiornati o privi delle necessarie misure di sicurezza possono essere facilmente sfruttati da attaccanti per ottenere l'accesso ai dati o ai sistemi di *backup in-cloud*.

→ Mancati aggiornamenti possono esporre i dati a furto, perdita o alterazione.

Guasti *hardware* e malfunzionamenti tecnici

Molti utenti tendono a dare per scontata l'affidabilità dei dispositivi digitali. È quindi importante ricordare che ***hard disk***, **SSD**, ***server*** e **schede di memoria** sono **strumenti soggetti a usura e deterioramento** nel tempo. Anche in assenza di segnali evidenti, un componente può smettere improvvisamente di funzionare a causa di un guasto meccanico o un difetto di fabbricazione, rendendo inaccessibili tutti i dati archiviati.

→ In mancanza di **copie di sicurezza aggiornate**, il recupero dei dati può risultare complesso e oneroso.

Errori umani

Una delle cause più frequenti di perdita di dati è rappresentata da **azioni o comportamenti non intenzionali**. Una cancellazione accidentale di un dato o un documento, la sovrascrittura involontaria di un *file* importante o la formattazione errata di un dispositivo possono verificarsi con **estrema facilità**, soprattutto durante operazioni di *routine*.

→ Senza un sistema di *backup* adeguato, anche una **piccola distrazione** può tradursi nella **perdita definitiva** di informazioni rilevanti.

Eventi esterni e fattori ambientali

Anche i **fattori esterni** possono compromettere la corretta conservazione dei dati. Eventuali danni e perdite dei supporti di archiviazione dovuti a **circostanze imprevedibili**, come alluvioni o altri eventi che colpiscono i locali in cui sono custoditi, possono **minare l'integrità e la disponibilità** delle informazioni.

→ Senza adeguate **misure di protezione** e **copie** dei dati in ambienti sicuri, la perdita può essere totale e definitiva.

3 COME DIFENDERSI? STRATEGIE PER MANTENERE AL SICURO IL PATRIMONIO DIGITALE

La protezione dei dati non si limita all'utilizzo di sistemi o strumenti di sicurezza tecnologicamente avanzati, ma richiede un approccio metodico e continuativo da parte dell'utente. Una strategia efficace combina misure tecniche e l'adozione di comportamenti responsabili.

Ecco alcuni dei modi più efficaci per proteggere il patrimonio digitale ed evitare la perdita dei dati:

Backup* e *cloud storage

Senza il *backup*, anche un singolo imprevisto può tradursi nella perdita definitiva di contenuti costruiti nel tempo. Per questo motivo rappresenta la **misura di protezione più efficace**: creare copie di sicurezza significa garantire la possibilità di ripristinare documenti, archivi e informazioni in caso di guasto, errore umano o attacco informatico.

Ove possibile, e qualora i sistemi lo consentano, è buona pratica programmare ***backup* automatici con cadenza regolare**, nonché conservare copie di sicurezza in locale oppure tramite *cloud storage*.

> Il ***backup* locale** prevede il salvataggio su dispositivi fisici, come *hard disk* esterni o SSD. Questa soluzione garantisce rapidità di accesso, ma espone il dispositivo al rischio di danneggiamento, furto o perdita che possono compromettere i dati conservati.

> Il ***cloud storage***, invece, consente di archiviare i dati su *server* remoti, protetti da sistemi di sicurezza avanzati e monitorati continuamente. Con questa soluzione, anche in caso di rottura o smarrimento del computer, le informazioni restano disponibili e recuperabili. Inoltre, molti servizi *cloud* permettono di ripristinare versioni precedenti in caso di modifiche errate o corruzione dei dati.

Cifratura dei dati

Quando parliamo di cifratura o crittografia ci riferiamo allo strumento che consente di **rendere illeggibili i *file*** a chi non possiede la chiave o la *password* di accesso. La **cifratura** è particolarmente importante per documenti contenenti informazioni personali, finanziarie o sensibili. Applicarla sia ai dispositivi locali, sia ai dati archiviati nel *cloud*, **rafforza** significativamente il **livello di sicurezza** complessivo e **tutela la riservatezza**.

Conservazione su più supporti

Salvare i dati su **più supporti** (ad esempio, *hard disk* esterni, dispositivi rimovibili e servizi *cloud*) aumenta la **resilienza** del **sistema di archiviazione** poiché garantisce **continuità operativa** e consente un **ripristino rapido** senza bloccare le attività quotidiane o lavorative.

Esiste un metodo estremamente efficace per proteggere le informazioni digitali: la "**regola del *backup* 3-2-1**", raccomandata dalle principali *best practice* di settore promosse dal *National Institute of Standards and Technology* (NIST) e dall'*European Union Agency for Cybersecurity* (ENISA). Questa strategia permette di **ridurre** drasticamente il **rischio di perdita totale dei dati** e garantisce che documenti, archivi e *file* importanti siano sempre recuperabili, anche in caso di eventi imprevisti.

La regola si basa su **tre principi fondamentali**:

- **3 copie dei dati**: non basta conservare solo l'originale, è necessario avere almeno due copie aggiuntive. Questo assicura che, se una copia venisse smarrita o danneggiata, si avrebbero comunque a disposizione le altre due;

- **2 supporti diversi**: le copie devono essere conservate su due tipi differenti di supporto, come un *hard disk* esterno e un servizio *cloud*. In questo modo, un guasto o un malfunzionamento di un dispositivo non compromette le copie originali conservate sull'altro;

- **1 copia *offsite* (fuori sede)**: almeno una copia deve essere conservata in un luogo separato dall'originale, ad esempio in un *cloud* o su un *server* remoto. In questo modo, anche eventi imprevisti come furti o incendi non mettono a rischio tutte le copie contemporaneamente.

Seguire la regola 3-2-1 significa trasformare il *backup* da semplice abitudine a vera e propria **strategia di protezione**: ogni duplicazione ha uno scopo, ogni supporto riduce il rischio e la copia *offsite* garantisce sicurezza anche nei casi più critici. Inoltre, è necessario mantenere le **copie costantemente aggiornate**, prevedendo *backup* regolari e verifiche periodiche del corretto salvataggio dei dati. Una copia non sincronizzata o mai testata può rivelarsi inutile nel momento del ripristino, costringendo a ripartire da versioni incomplete o obsolete.

Esiste una **variante più evoluta della regola 3-2-1**, nota come **regola 3-2-1-1-0**, sviluppata per rispondere alle minacce informatiche moderne, in particolare agli attacchi *ransomware*.

Questa versione introduce **due ulteriori elementi di sicurezza**:

- **1 copia aggiuntiva *offline***, conservata su un supporto non connesso alla rete e protetto da modifiche o cancellazioni;

- **verifica** periodica dei ***backup*** tramite test di ripristino, volta ad assicurare che le copie siano integre e che i dati possano essere effettivamente recuperati senza errori.

L'evoluzione della regola 3-2-1 sottolinea un principio fondamentale: non è sufficiente disporre di **copie di sicurezza**, ma è necessario che queste siano **diversificate**, **isolate** dalle minacce e regolarmente **testate**, affinché il *backup* rappresenti una reale misura di resilienza e non solo una percezione di sicurezza.

4 CASI REALI DI PERDITA DI DATI

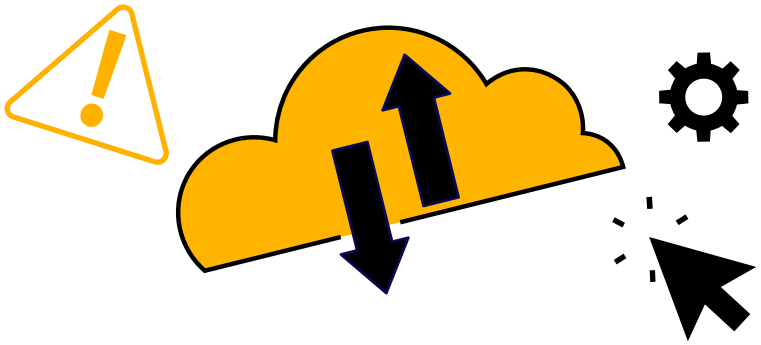
Incendio in un *data center*: persi circa otto anni di documentazione digitale

A ottobre 2025 un **grave incendio** ha colpito un *data center* che ospitava una **piattaforma di archiviazione *cloud***, utilizzata da un Ente pubblico, causando la **distruzione completa dei sistemi informatici** presenti nella struttura. L'evento ha provocato la perdita permanente di oltre 858 *terabyte* di dati, equivalenti a circa otto anni di attività e documentazione digitale. Secondo quanto emerso, il **sistema non disponeva di copie di *backup*** indipendenti o di soluzioni di replica in siti alternativi. Questo ha reso **impossibile** il **recupero delle informazioni** andate distrutte. Le conseguenze sono state immediate e rilevanti: interruzione dei servizi digitali, blocco delle comunicazioni via e-mail, indisponibilità di portali istituzionali e rallentamenti nelle attività amministrative. L'incidente ha evidenziato come, anche in presenza di infrastrutture *cloud*, **l'assenza di una strategia di *backup*** possa trasformare un evento straordinario in una **perdita definitiva di dati**.

Attacco informatico ad un'università italiana

Nel febbraio 2026 un'importante università italiana è stata vittima di un **attacco *ransomware*** che ha crittografato dati e documenti, rendendo impossibile l'accesso alle informazioni e ai servizi per studenti, docenti e personale amministrativo. L'attacco ha impattato registri accademici, portali per la prenotazione degli esami, sistemi di gestione interna e posta elettronica istituzionale, **interrompendo attività quotidiane e causando disagi immediati**. Studenti impossibilitati a prenotare esami, personale amministrativo bloccato nelle procedure burocratiche, docenti senza accesso a registri e materiali didattici: un'intera Istituzione resa temporaneamente inattiva a causa della vulnerabilità dei sistemi. Fonti giornalistiche riportano che i tecnici dell'università, insieme alle autorità competenti, abbiano lavorato per ripristinare i sistemi a partire dai *backup* disponibili. Non è ancora chiaro però se tutte le copie siano integre o se alcuni dati risultino danneggiati o parzialmente irrecuperabili.

Questo caso è significativo perché evidenzia quanto sia **fondamentale avere strategie di *backup* affidabili e testate**: **senza copie** di sicurezza complete e aggiornate, **un attacco *ransomware* può fermare l'operatività** di intere organizzazioni e complicare drasticamente il recupero dei dati.



Intervento realizzato dal Ministero dell'Istruzione e del Merito e finanziato a valere sul Fondo per la gestione della cybersicurezza nell'ambito della misura 71 e 73 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 dell'Agenzia per la Cybersicurezza Nazionale

www.unica.istruzione.gov.it