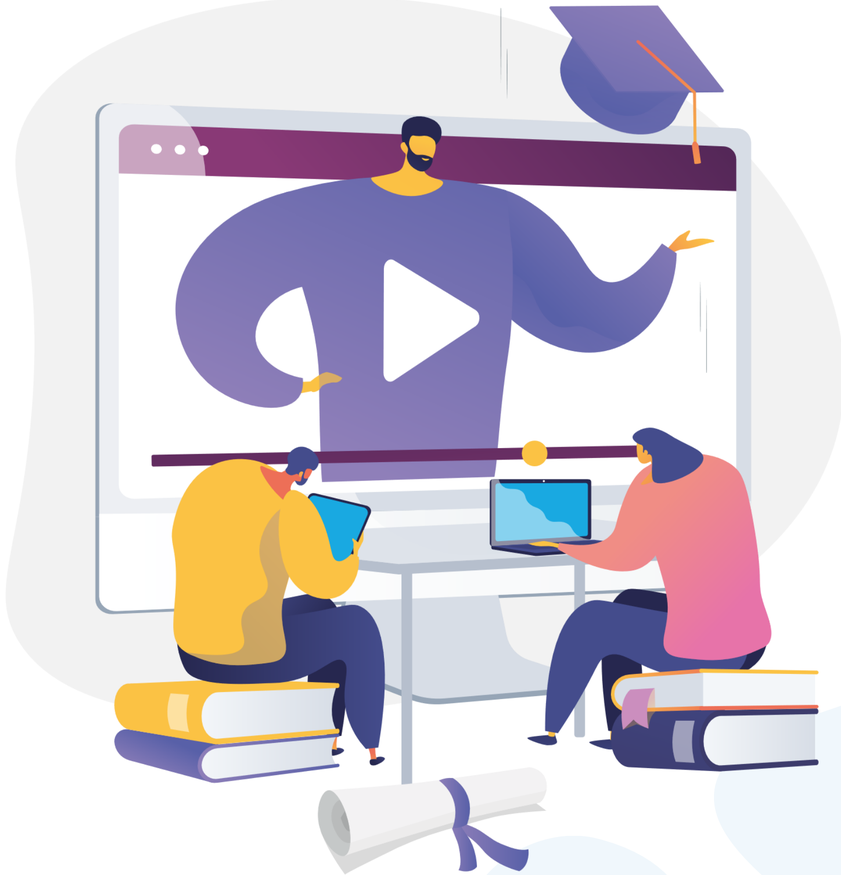
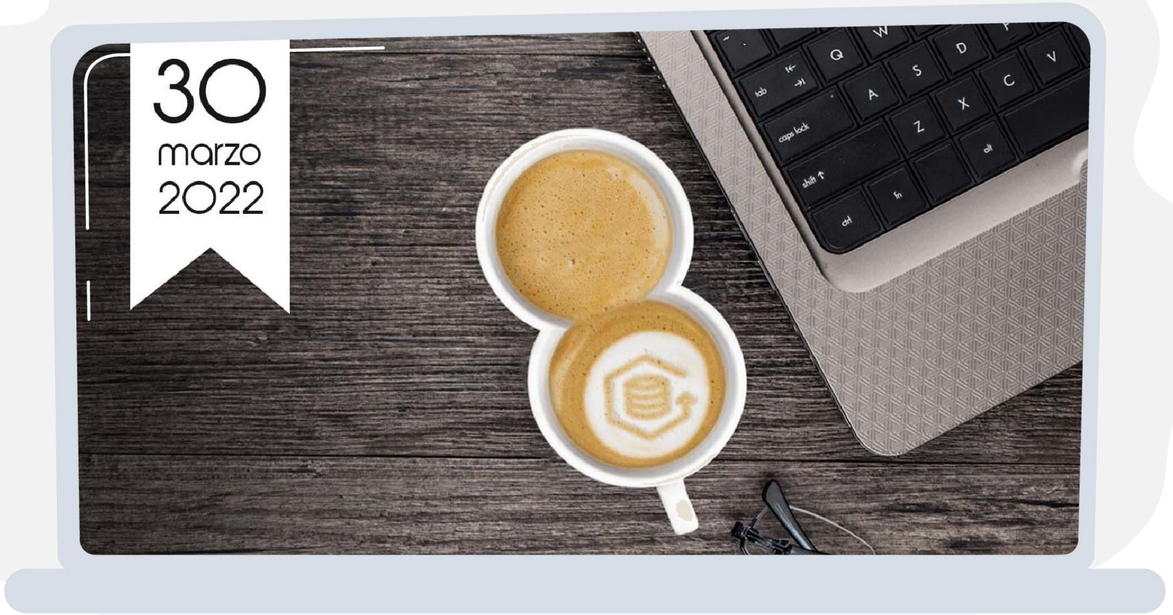
DIGITAL Academy

by register.it



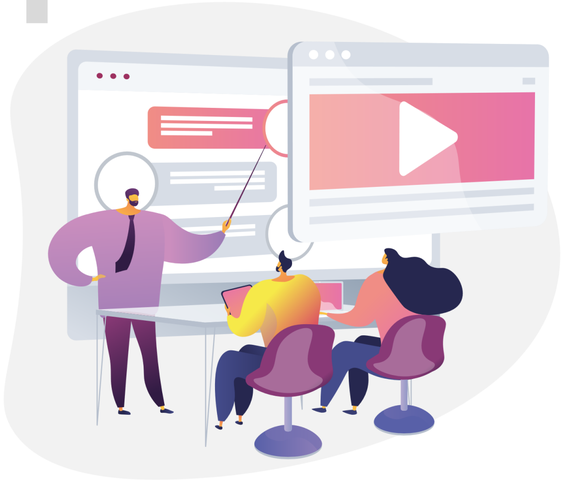
Backup, il valore della **disponibilità dei dati**



Register.it e la Digital Academy

La mission di **Register.it** è quella di accompagnare persone e aziende nella **creazione della propria presenza online** con un **percorso di miglioramento continuo.**

1 Webinar



2 Certificazioni

3 Network

Web Agency Network

La “**Web Agency Network**" è una **rete di rivenditori accreditati** garantita da Register.it.

Lo scopo è quello di **mettere in contatto i clienti finali di Register.it** che cercano rivenditori garantiti su tutto il territorio nazionale **con i Business Partner accreditati e certificati**.

Entrano a far parte della "**Web Agency Network**" i clienti Business Partner che **hanno ottenuto almeno una certificazione della Digital Academy** di Register.it.

Programma Business Partner

Il **programma Business Partner di Register.it** si rivolge ad agenzie e professionisti del web e del digitale in tutta Italia come consulenti IT, web agency, web developer e web designer.

I clienti che hanno aderito al programma hanno numerosi vantaggi come **sconti riservati** su tutta la vasta gamma di prodotti di Register.it, **consulenza personalizzata** e dedicata, **servizio di assistenza tecnica prioritaria** e molto altro.

.I nostri speakers

Alessio Rossi - Security & Compliance manager
Sviluppo, implementazione e mantenimento di politiche e programmi di gestione della compliance e della sicurezza aziendale in Register.it.

Daniele Melosi - Service Management Manager
Amministrazione, gestione e supporto all'infrastruttura IT e ai servizi di rete di Register.it. Verifica del corretto funzionamento dei sistemi hardware e software aziendali.

Argomenti di questo webinar

- Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici.
- Il backup come approccio professionale alla gestione operativa e come presidio di continuità.
- Tipologie di soluzioni di backup e modalità di gestione.
- Soluzioni professionali di backup - Acronis Cyber Backup
- Procedure e gestione dei backup in Register.it

Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici

Dati da rapporto 2021 del CLUSIT sulla sicurezza ICT in Italia

- Nel **2020** gli attacchi con impatto “Critical” rappresentavano il 13% del totale, quelli di livello “High” il 36%, quelli di livello “Medio” il 32% e quelli di livello “Basso” il 19%. Complessivamente, gli **attacchi gravi** con effetti molto importanti (High) o devastanti (Critical) nel 2020 erano il **49%** del campione.

- Nel **primo semestre 2021** gli attacchi gravi con effetti molto importanti (High) sono il 49%, quelli devastanti (Critical) rappresentano il 25%, quelli di impatto significativo (Medium) il 22%, e quelli con impatto basso solo il 4%. In questo caso gli attacchi con impatto **Critical** e **High** sono il **74%**

Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici

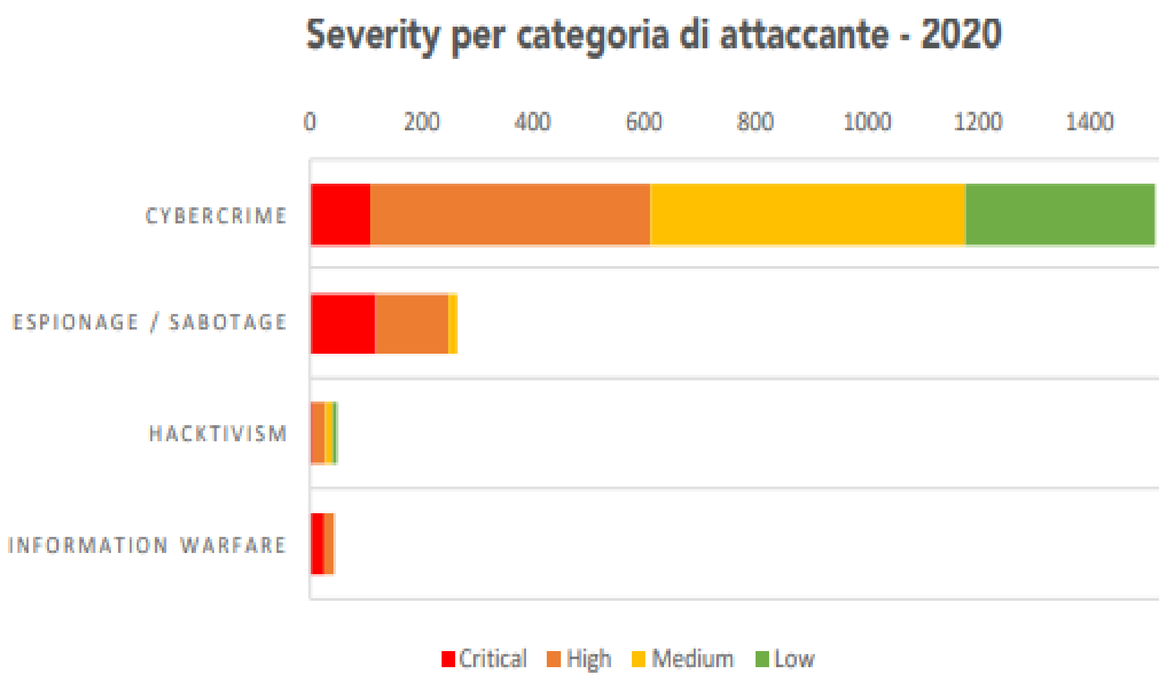
Dati da rapporto 2021 del CLUSIT sulla sicurezza ICT in Italia

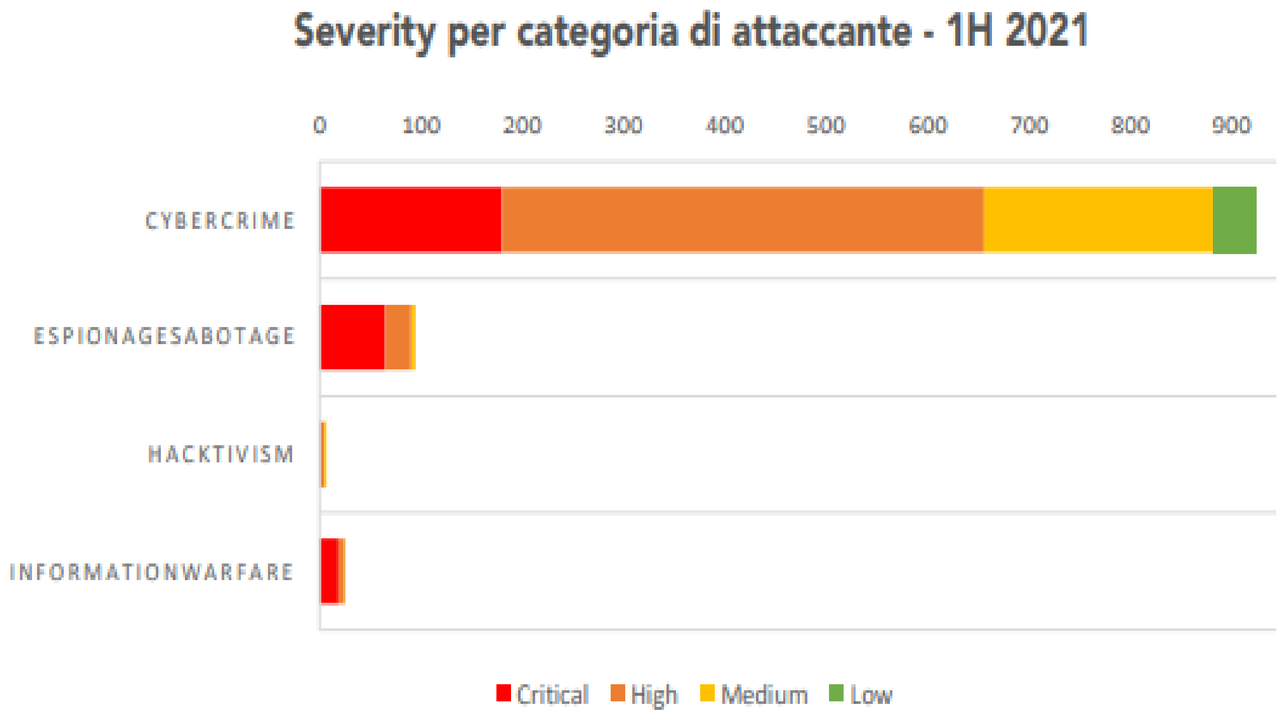
Il fenomeno più preoccupante è rappresentato dall'**incremento dell'attività dei ransomware**.

Nel **2021** si evidenzia una crescita dell'attività di questa tipologia di attacco di circa il **350%** rispetto allo stesso periodo del 2020.

Gli attacchi **ransomware** hanno finalità di estorsione di denaro alle vittime e costituiscono la categoria di **Cybercrime** con il maggiore incremento di attacchi con severity Critical o High.

Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici





Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici

Dati da rapporto 2021 del CLUSIT sulla sicurezza ICT in Italia

Nel 2020 circa **un'azienda italiana su tre*** ha subito un **attacco ransomware.**

Il principale motivo risiede, probabilmente, in un cambiamento nelle tecniche usate dai cybercriminali che sono passati **da attacchi generici automatizzati** su larga scala **ad attacchi più complessi e mirati** con maggiori potenzialità di danni, sia in termini di costi necessari per ripristinare l'operatività che di ammontare del riscatto richiesto.

Difficile è avere dati oggettivi su quantità e ammontare reali dei riscatti pagati per aver indietro i dati sottratti o resi inutilizzabili. I dati statistici sul campione che ha fornito informazioni a riguardo indicano che almeno **una vittima su quattro ha perso informazioni in modo definitivo.**

*Fonte ricerca Sophos

Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici

Non esiste nulla come un attacco ransomware per farti rimpiangere di non aver investito meglio nei backup.

Un sistema che non preveda, all'interno delle proprie procedure, una attività di **disaster recovery** è un sistema intrinsecamente destinato al fallimento ed uno dei sistemi migliori per **garantirsi un corretto recovery** è appunto il **backup.**

Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici

Main Best Practice – Backup / DR e piani di continuità

- **Valutare la possibilità di essere colpiti**. Cyberattacchi e ransomware restano fortemente diffusi. Nessun settore, Paese o azienda ne è immune. È meglio essere preparati e non venire colpiti che viceversa.

- **Effettuare i backup**. I backup sono il primo metodo usato dalle aziende per recuperare i loro dati dopo essere state colpite da cyberattacchi. Raramente si riesce a tornare in possesso dei dati pur avendo pagato il riscatto, per cui i backup sono fondamentali.

- **Implementare una protezione a strati**. Gli attacchi a puro scopo di estorsione sono raddoppiati passando dal 3% nel 2019 al 7% nel 2020. Diventa fondamentale riuscire a tenere gli avversari al di fuori del proprio perimetro utilizzando una protezione a strati per bloccare gli attaccanti nel maggior numero di punti possibili.

Il valore dei dati e delle configurazioni come obiettivo emergente degli attacchi informatici

Main Best Practice – Backup / DR e piani di continuità

- **Combinare gli esperti con la tecnologia anti-ransomware**. Per bloccare le cyberminacce occorre una difesa che combini tecnologia anti-ransomware con attività di threat hunting condotte da personale esperto.

- **Non pagare i cybercriminali.** Versare un riscatto è un metodo inefficace per riottenere i dati ed ha spesso impatti di tipo legale. Inoltre, chi decide di pagare, deve comunque tenere in considerazione la possibilità di veder ripristinati in media solo 2/3 dei file.

- **Preparare un recovery plan dal malware**. Il modo migliore per evitare che un cyberattacco si trasformi in una violazione completa è quello di prepararsi per tempo con un piano di risposta agli incidenti.

Il backup come approccio professionale alla gestione operativa e come presidio di continuità

Un processo di gestione controllata e sicura delle modifiche ad ogni piattaforma ICT prevede tra le misure essenziali:

1. La **valutazione degli impatti** architetturali ed applicativi delle modifiche introdotte in termini di funzionalità, sicurezza e performance.
2. L'identificazione di **procedure di rollback** per il **ripristino di configurazioni e dati** allo stato precedente all'implementazione delle modifiche in caso di anomalie.
3. Il **test tecnico ed il collaudo** delle funzionalità su ambienti non di produzione.
4. Il trasferimento in produzione delle modifiche una volta superati test e collaudo.

Il backup come approccio professionale alla gestione operativa e come presidio di continuità

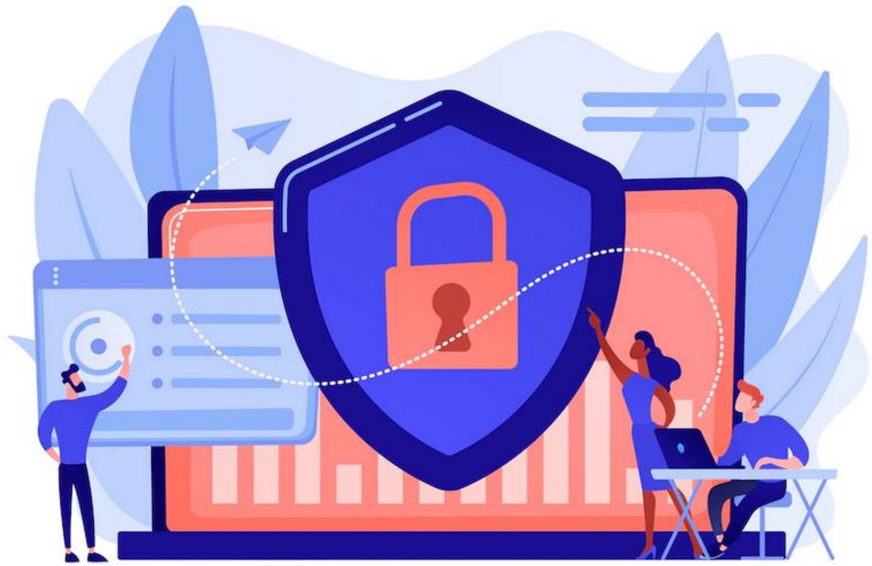
Presidi di sicurezza CORE che garantiscono un "rollback" completo continuità di servizio

- Disponibilità di strumenti/sistemi e **servizi di Backup** che, ad intervalli predefiniti o a fronte di determinate modifiche, creino, archivino e aggiornino su sistemi distinti da quelli di produzione copie di:
  - file core dell'applicazione
  - media e archivi caricati
  - documenti caricati
  - dati e struttura del Database
  - plugin e temi
- Disponibilità di processi, strumenti/sistemi e servizi di **gestione della continuità operativa** e di **Disaster Recovery** che permettano l'attivazione tempestiva di procedure e di risorse alternative, infrastrutturali ed organizzative, per garantire la continuità del funzionamento del servizio.

Il backup come approccio professionale alla gestione operativa e come presidio di continuità

Il **Disaster Recovery** comprende l'insieme delle misure atte a ripristinare i sistemi, i dati e le infrastrutture necessarie all'erogazione di servizi di business, a fronte di gravi emergenze che ne intacchino la regolare attività.

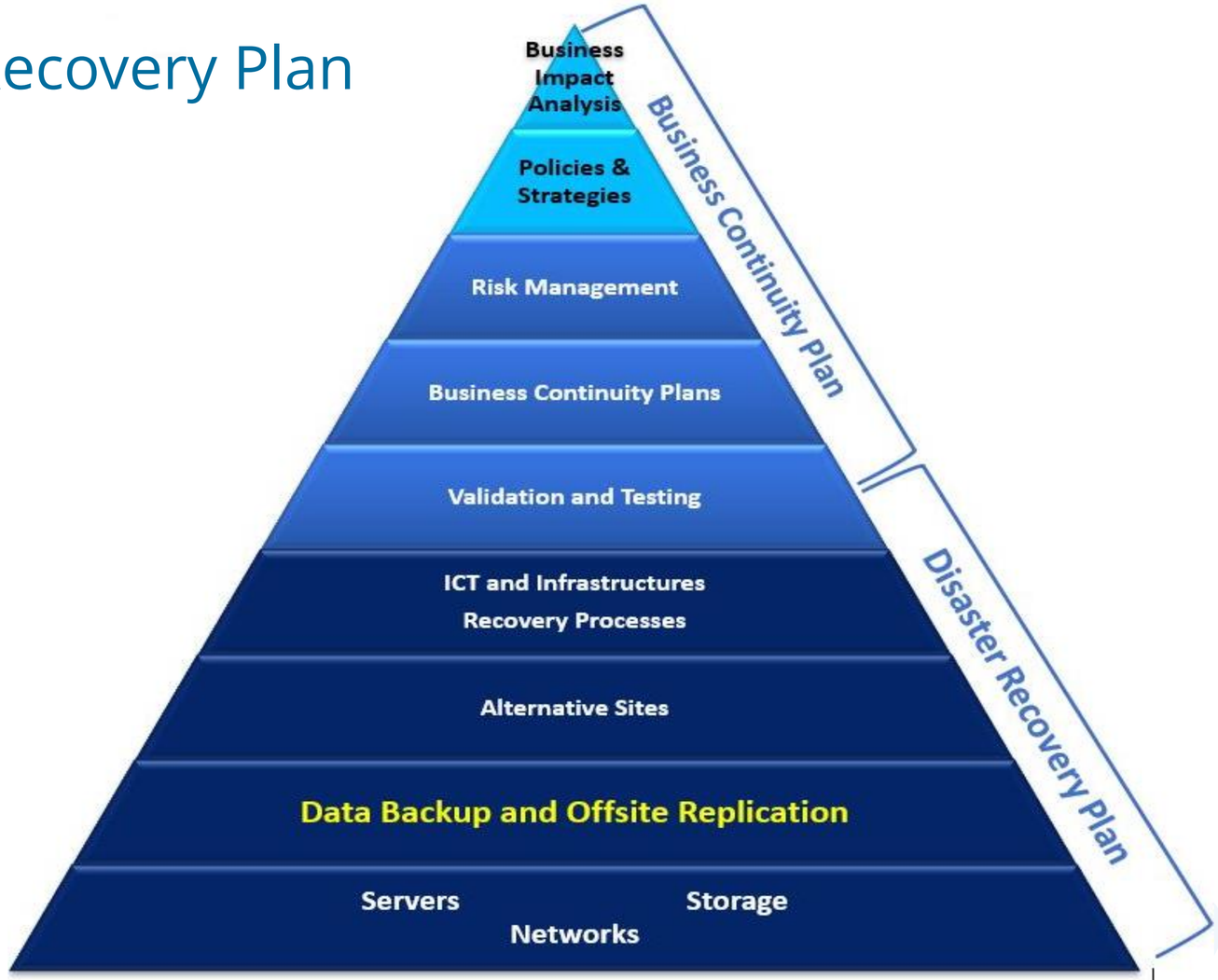
La gestione della **continuità operativa** e del **Disaster Recovery** rappresentano presidi importanti anche nel caso di discontinuità o anomalie causate da attacchi esterni che spesso, oltre a minacciare la disponibilità e integrità delle informazioni, possono rendere indisponibili o malfunzionanti le architetture e le applicazioni primarie che elaborano i dati.



Il backup come approccio professionale alla gestione operativa e come presidio di continuità

Business Continuity Plan e Disaster Recovery Plan

- Livello Strategico e Procedurale
- Livello di Gestione e Organizzazione
- Livello Infrastrutturale



Il backup come approccio professionale alla gestione operativa e come presidio di continuità

Business Continuity Plan e Disaster Recovery Plan

Tipologie di Backup e modalità di gestione

Rischi nella gestione manuale del Backup senza strumenti automatizzati

- **Errori nel processo di copia** e corruzione delle copie.
- **Dimenticanze** nel selezionare manualmente gli oggetti da copiare:
    - File core dell'applicazione.
    - Media e archivi caricati.
    - Documenti caricati.
    - Dati e struttura del Database.
    - Plugin e temi.
- Potenziale **inefficienza operativa** rispetto alla dinamicità dei siti web che condiziona la frequenza di backup.
- **Aumento di effort** per:
    - Lo svolgimento dell'attività di copia.
    - La verifica dell'integrità delle copie.
    - L'organizzazione/indicizzazione delle copie.
    - L'effettuazione periodica di verifiche di restore dei dati.
- Necessità di **strutturare autonomamente dei piani d'intervento** efficaci e tempestivi in caso di necessità di ripristino dei dati.

Tipologie di Backup e modalità di gestione

Backup automatico gestito dal provider del servizio di hosting

Il **servizio di gestione del Backup** fornito dagli hosting provider fa parte dei servizi " Server Managed" in cui il provider, oltre a fornire la gestione di tutte le componenti architetturali ed infrastrutturali CORE su cui su è in esecuzione l'applicazione, fornisce anche **servizi customizzati per il singolo cliente** finalizzati alla gestione professionale della continuità operativa.

Questo tipo di servizio permette di lasciare la **gestione delle attività operative** di backup di dati, configurazione, verifica di integrità e test di restore **al provider del servizio di hosting** attivando strumenti di pianificazione e monitoraggio delle attività che permettono:

- Un controllo continuo dello stato e della configurazione del servizio.
- Un controllo continuo delle copie dei propri dati/configurazioni.
- Una comunicazione ed un intervento tempestivo nel caso di necessità di ripristino di dati/configurazioni inutilizzabili o inaccessibili a fronte di attacchi esterni o di errori interni.

Tipologie di Backup e modalità di gestione

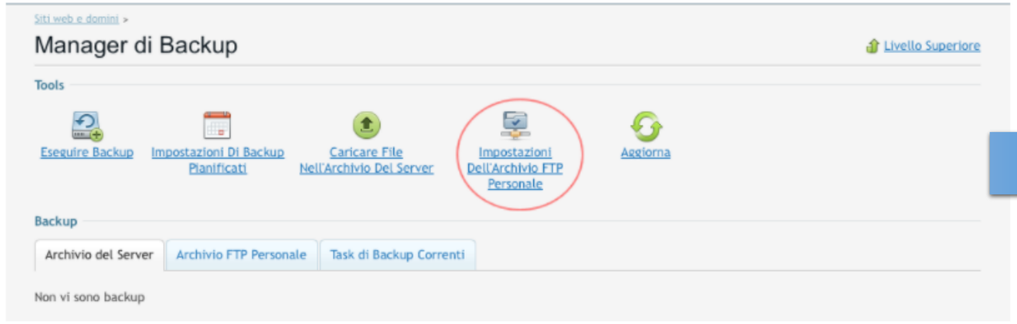
Backup automatico gestito dal provider del servizio di hosting - Pannello Plesk 1/3

1

Effettua il login nel pannello di gestione Plesk, poi entra nel Backup Manager.

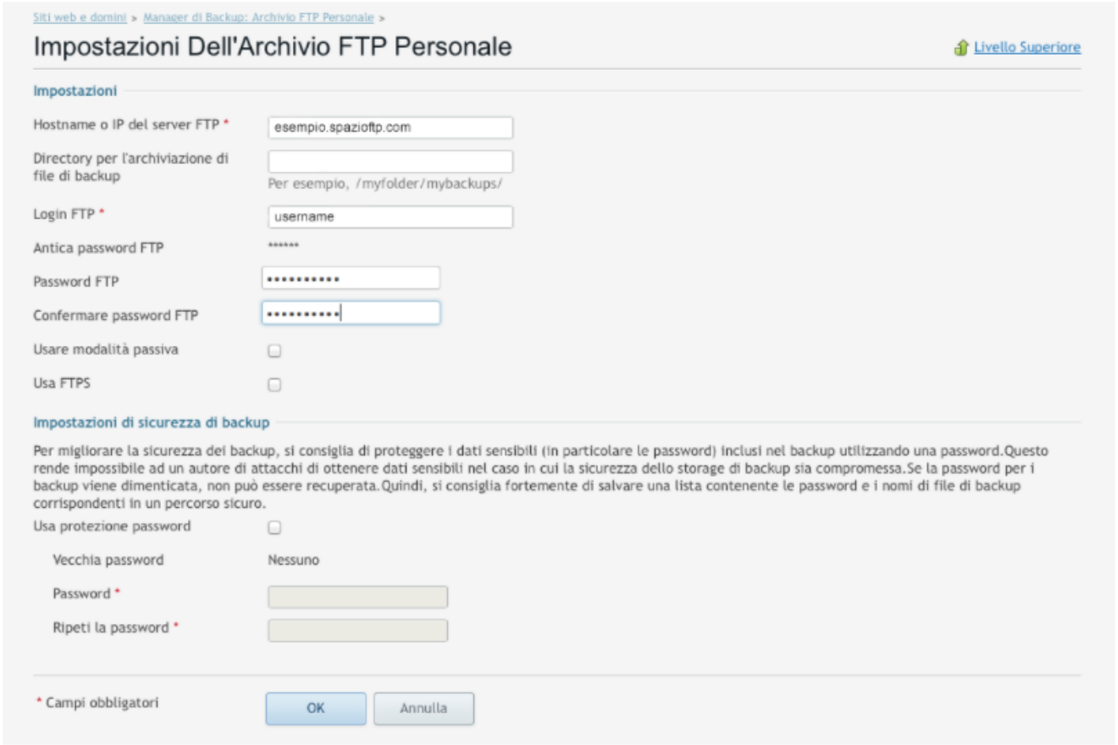
2

Clicca su Impostazioni Dell'Archivio FTP Personale per impostare un archivio FTP da utilizzare per i tuoi backup, che ti permetterà di utilizzare le funzionalità di programmazione dei backup.



3

Nella pagina che segue inserisci i dati dell'archivio FTP a cui collegare Plesk.
Se usi uno Spazio Backup (puoi acquistarlo dalla pagina di gestione del tuo server, nel Pannello di controllo), inserisci nei campi di questa pagina i dati dello Spazio Backup come mostrato qui sotto:



Tipologie di Backup e modalità di gestione

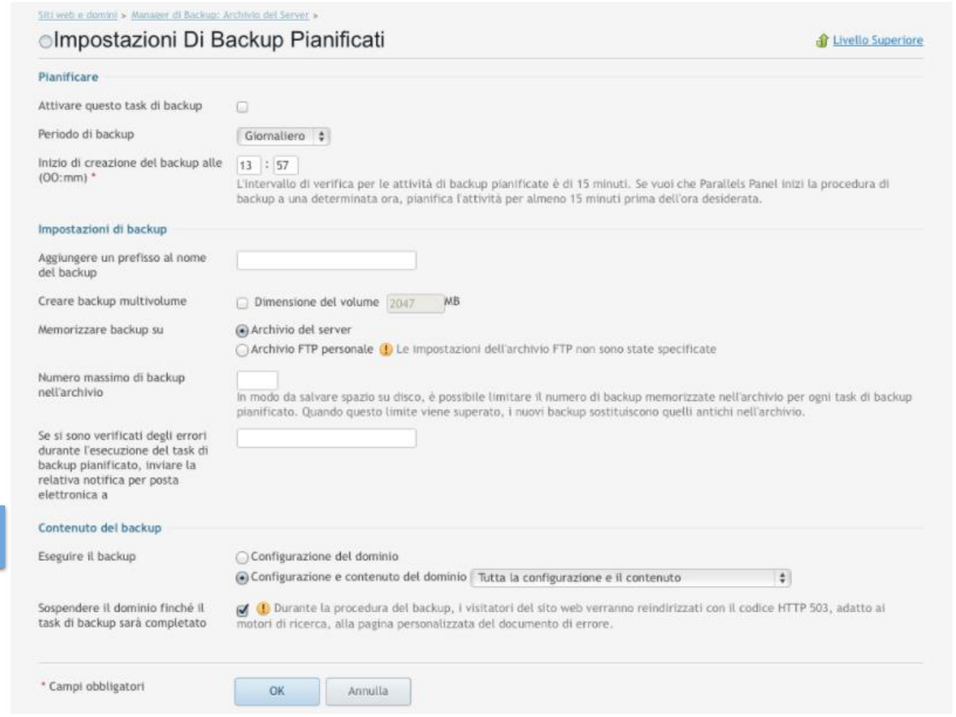
Backup automatico gestito dal provider del servizio di hosting - Pannello Plesk 2/3

4

Dopo aver inserito i dati per l'uso di un archivio FTP, puoi procedere a impostare la pianificazione dei tuoi backup:

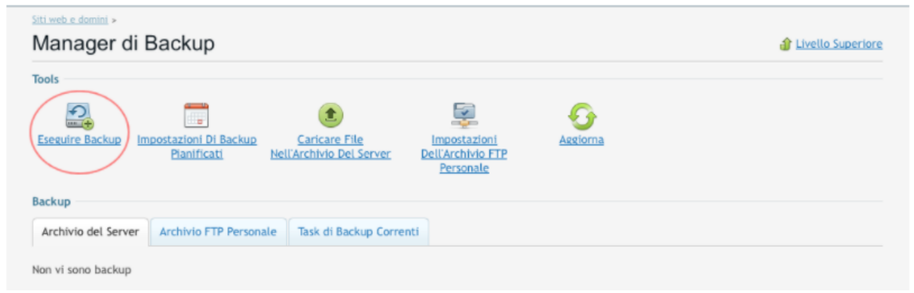
5

Gli intervalli disponibili sono: giornaliero, settimanale e mensile.
Un'opzione importante da attivare è quella che prevede di eseguire il backup del contenuto e della configurazione del dominio: questo permetterà di ripristinare un server in caso di disaster recovery alla configurazione dell'ultimo backup, senza doverlo reimpostare.



6

Adesso puoi eseguire il tuo backup.
Ricorda: l'opzione "Archivio del server" salverà il backup sul server stesso; seleziona "Archivio FTP personale" per utilizzare lo Spazio Backup che hai precedentemente impostato.
Premi infine il tasto Esegui backup per avviare l'operazione.



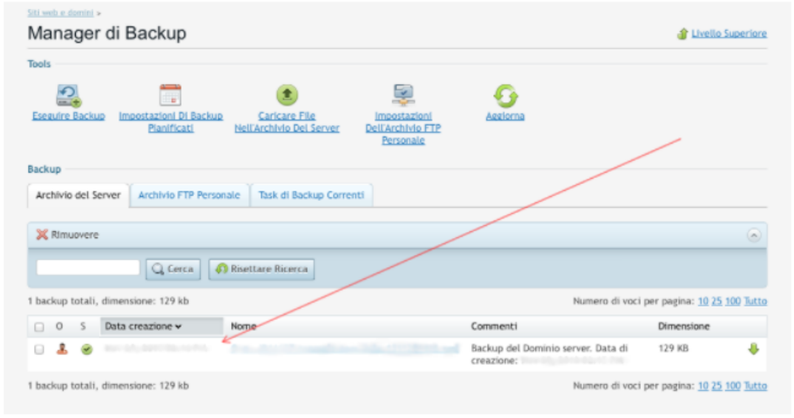
Tipologie di Backup e modalità di gestione

Backup automatico gestito dal provider del servizio di hosting - Pannello Plesk 3/3

7

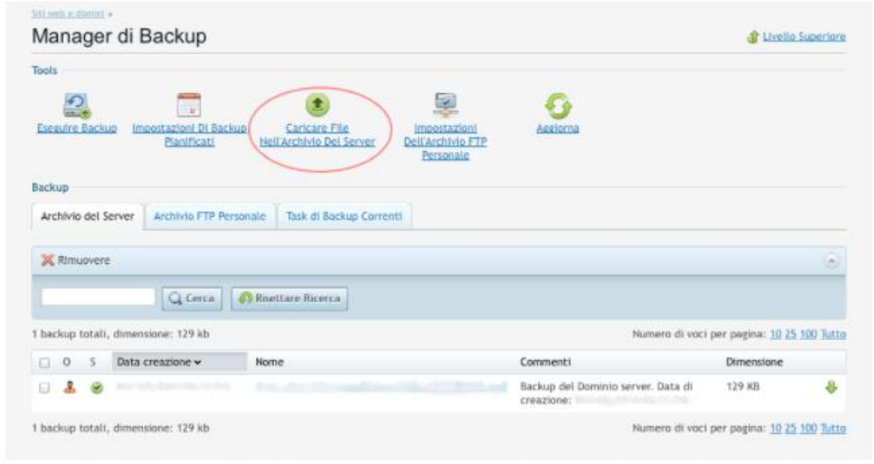
Al termine del salvataggio, il tuo backup (o i tuoi backup, se ne hai eseguiti più di uno) apparirà elencato nella pagina del Manager di backup da cui abbiamo iniziato.

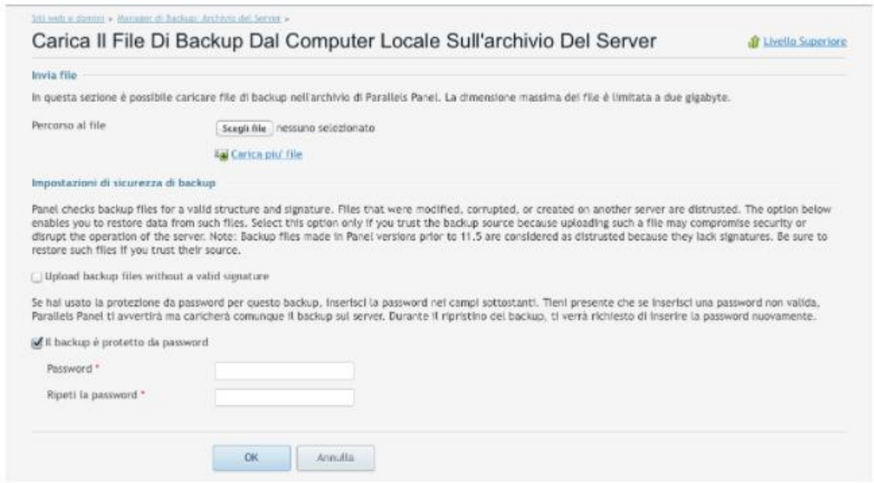
Cliccando sul nome del backup avrai accesso a una pagina in cui visualizzare i dettagli relativi al backup e, se lo desideri, ripristinare quanto salvato in precedenza.



8

Se già disponi di un archivio di backup che desideri salvare sul tuo server, la funzione Caricare File Nell'Archivio Del Server ti permetterò di importarlo per poterlo utilizzare ed eventualmente ripristinare.





Tipologie di Backup e modalità di gestione

Tipologie di Backup per modalità di memorizzazione - Backup Completo

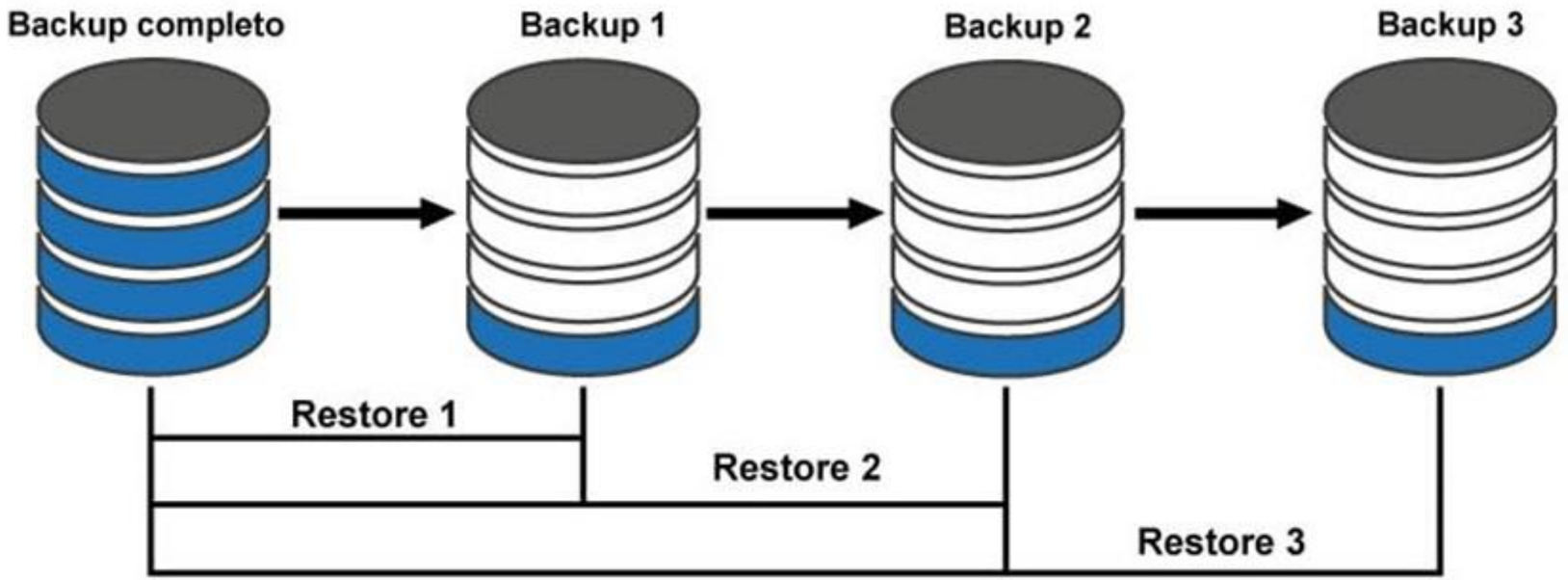
Un **backup completo prevede la replica di tutti dati** e, ripristinando l'ultima copia eseguita, ne consente il totale recupero.

Il processo di copia dei dati e quello di ripristino di un backup completo richiedono però **più tempo e spazio** di archiviazione delle altre modalità di backup.
È questo il motivo per cui di solito i backup completi vengono eseguiti insieme ad altre tipologie di backup ma con una frequenza inferiore.

Tipologie di Backup e modalità di gestione

Tipologie di Backup per modalità di memorizzazione - Backup Incrementale

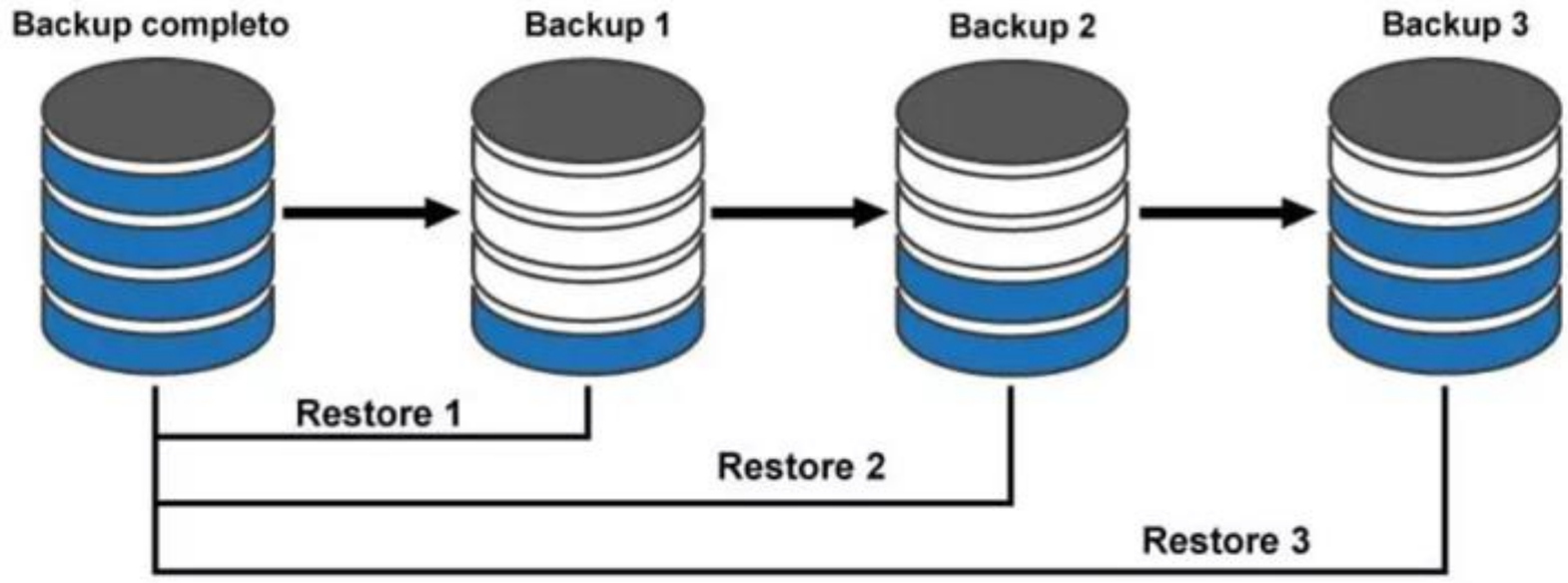
Il backup incrementale prevede una **copia dei soli dati che risultano modificati rispetto al backup incrementale precedente.** Consente una maggiore efficienza temporale e nell'uso di spazio in fase di realizzazione della copia è meno veloce nella fase di restore perché per il recupero di tutti i dati richiede il ripristino di tutta la serie di backup incrementali eseguiti.



Tipologie di Backup e modalità di gestione

Tipologie di Backup per modalità di memorizzazione - Backup differenziale

Il backup differenziale è una forma di backup incrementale che, partendo da un backup completo effettuato con una determinata periodicità, effettua **copie dei soli dati che sono stati modificati dall'ultimo backup completo**, fino al successivo backup completo schedulato.



Tipologie di Backup e modalità di gestione

Tipologie di Backup per localizzazione dei dati - Backup fisico on-premise

Il backup fisico on-permise prevede **l’archiviazione locale** su sistemi/apparati/dispositivi di memoria all’interno del proprio data center.

Questo tipo di backup **è molto veloce nella processazione dei dati** ma risente di tutti i rischi dovuti alla "guastabilità" e ai possibili danneggiamenti da eventi accidentali o malevoli delle componenti fisiche dell’architettura di memorizzazione.

Tipologie di Backup e modalità di gestione

Tipologie di Backup per localizzazione dei dati – Backup in Cloud

Il Backup in Cloud prevede l'invio e l'**archiviazione dei dati in un Data Center** su architetture costituite da cluster di sistemi che, secondo tecnologie avanzate e a vari livelli architetturali, offrono livelli di sicurezza mediamente molto superiori alle architetture fisiche on-premise in termini di resilienza, ridondanza e tolleranza al guasto.

Tipologie di Backup e modalità di gestione

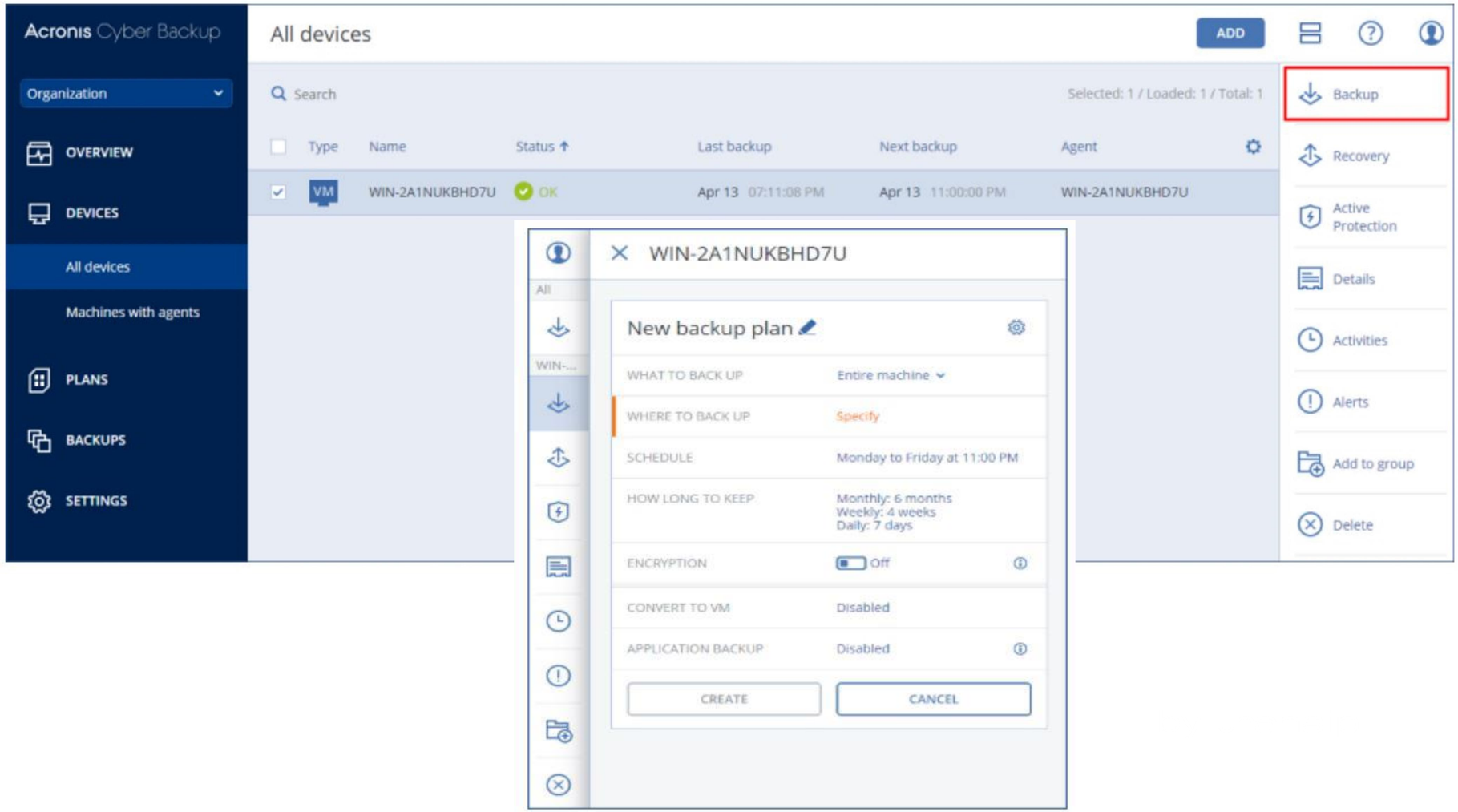
Tipologie di Backup per localizzazione dei dati – Backup in Cloud

- Il **backup in Cloud privato** è ospitato da una infrastruttura IT on-premise, presso il proprio Data Center o presso il Data Center del fornitore del servizio, in cui l'infrastruttura fisica di elaborazione, trasmissione e memorizzazione su cui è realizzato l'ambiente Cloud è **dedicata al singolo cliente**. Si tratta di una soluzione che comporta importanti costi tecnici/organizzativi per la manutenzione e la gestione dell'infrastruttura. Questo è il motivo per il backup in Cloud è solitamente adottato da **aziende medio-grandi**.

- I **backup in Cloud pubblici** archiviano le copie dei dati in architetture cloud in cui le risorse/componenti fisiche sono **condivise con altre aziende/utenti**, a fronte di opportune misure di sicurezza per la segregazione logica degli ambienti. Questo tipo di soluzione si adatta meglio alle esigenze di **aziende di piccole dimensioni o privati** che non hanno l'esigenza di investire in hardware dedicato per il backup ma intendono comunque adottare soluzioni efficaci, sicure e di semplice gestione.

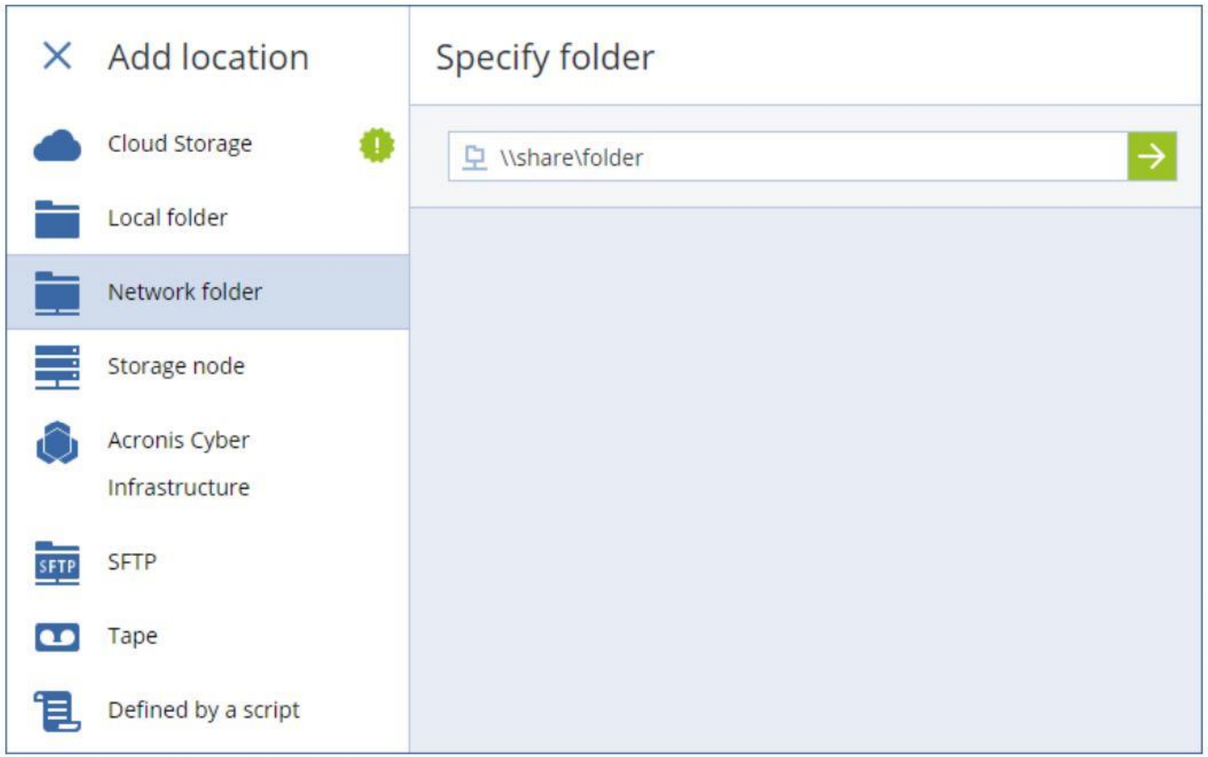
Soluzioni professionali di backup - Acronis Cyber Backup

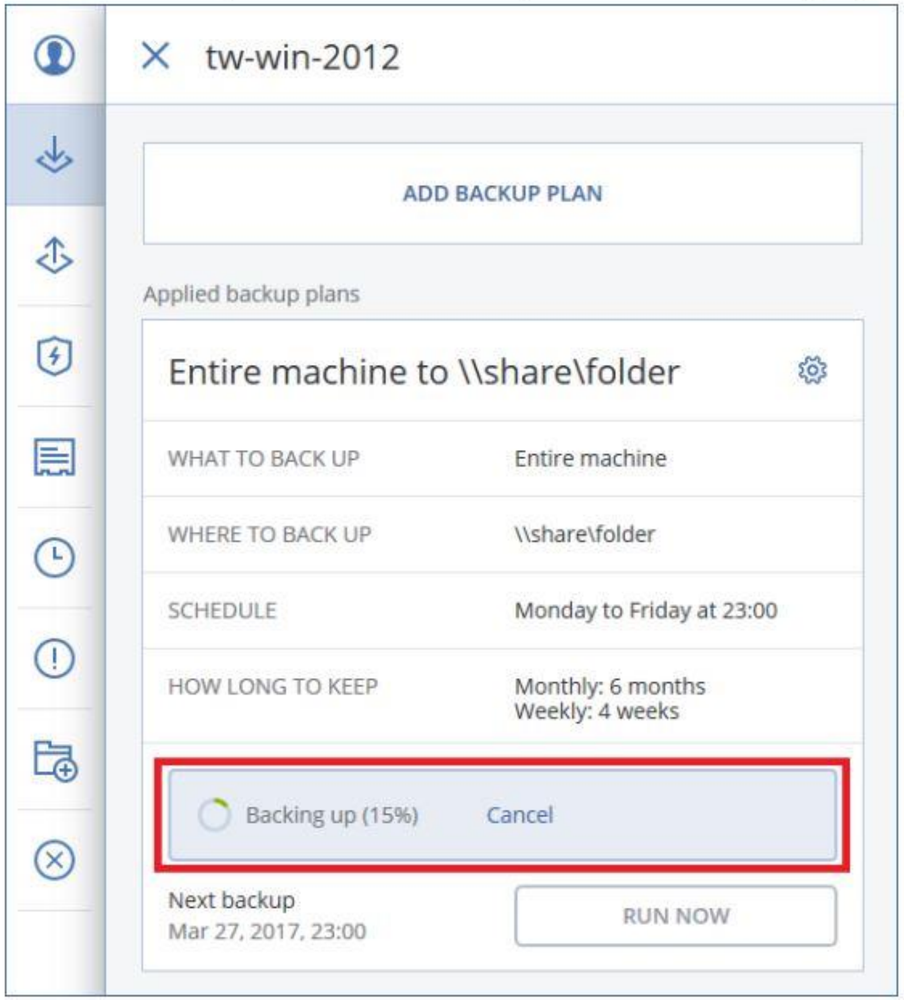
Backup dell’interna macchina 1/2



Soluzioni professionali di backup - Acronis Cyber Backup

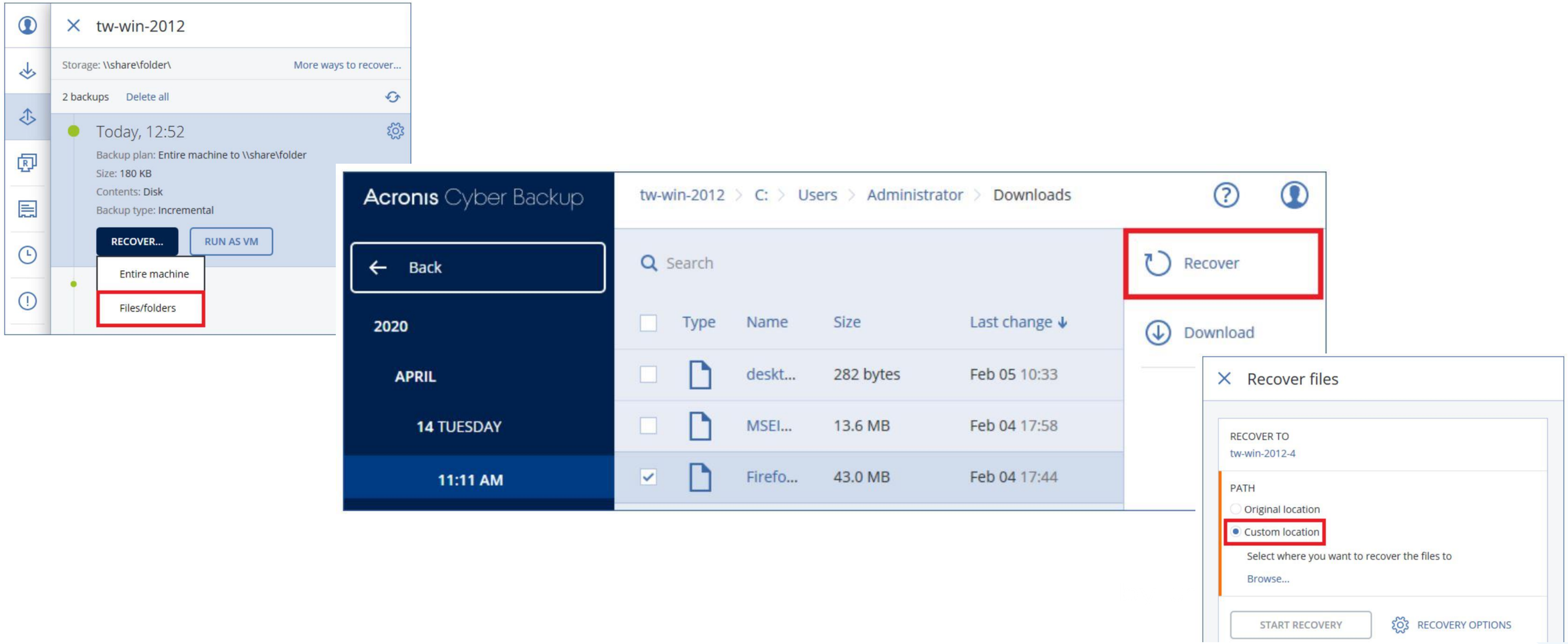
Backup dell'interna macchina 2/2





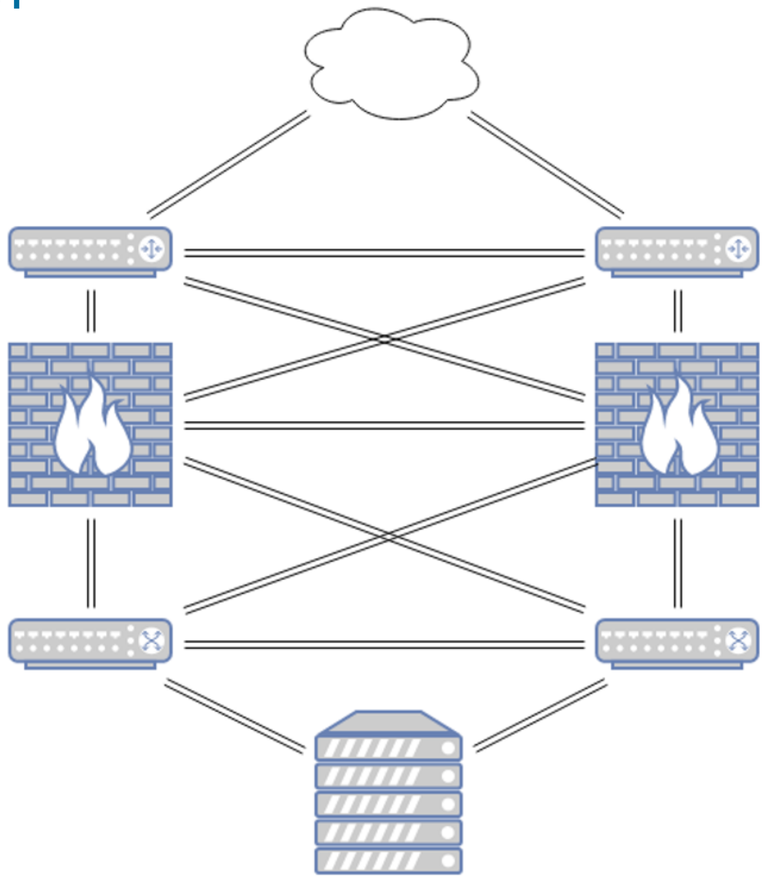
Soluzioni professionali di backup - Acronis Cyber Backup

Funzionalità di recovery granulare dei singoli file



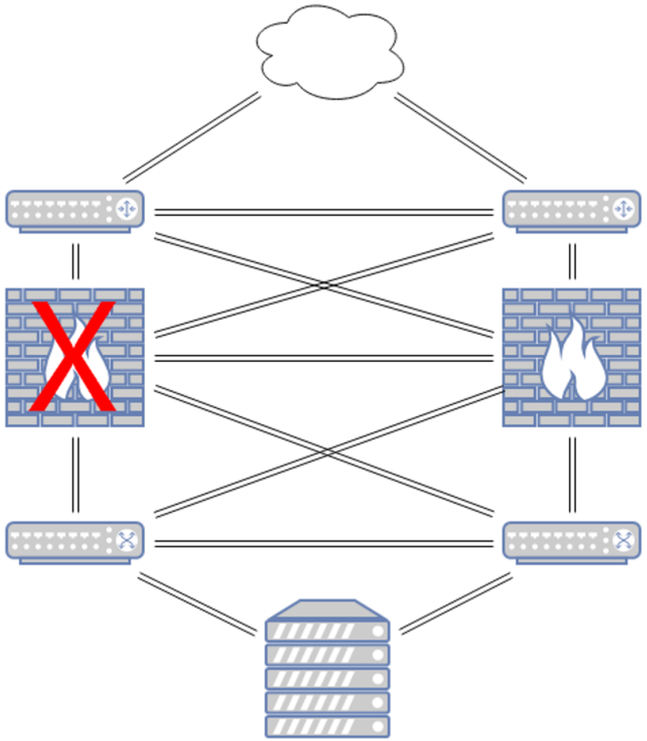
Procedure e gestione dei Backup in Register.it

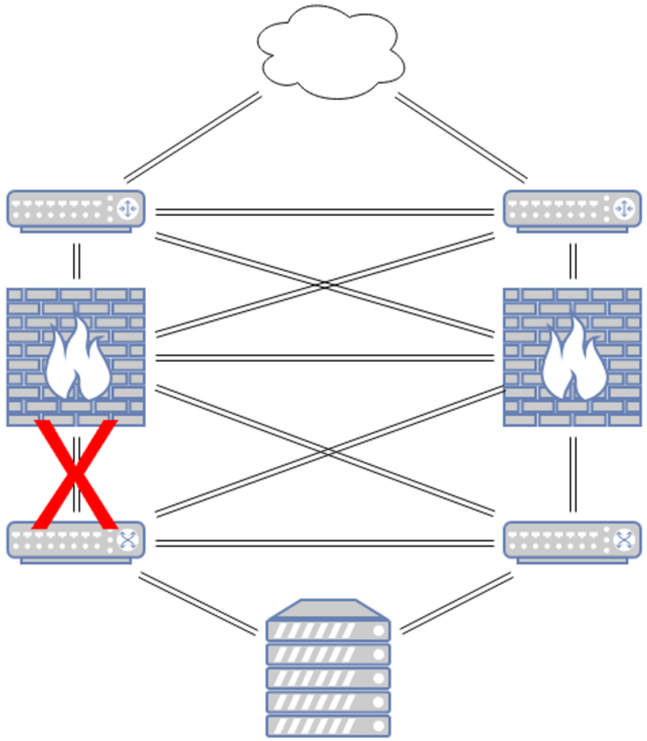
Ridondanza dei dispositivi

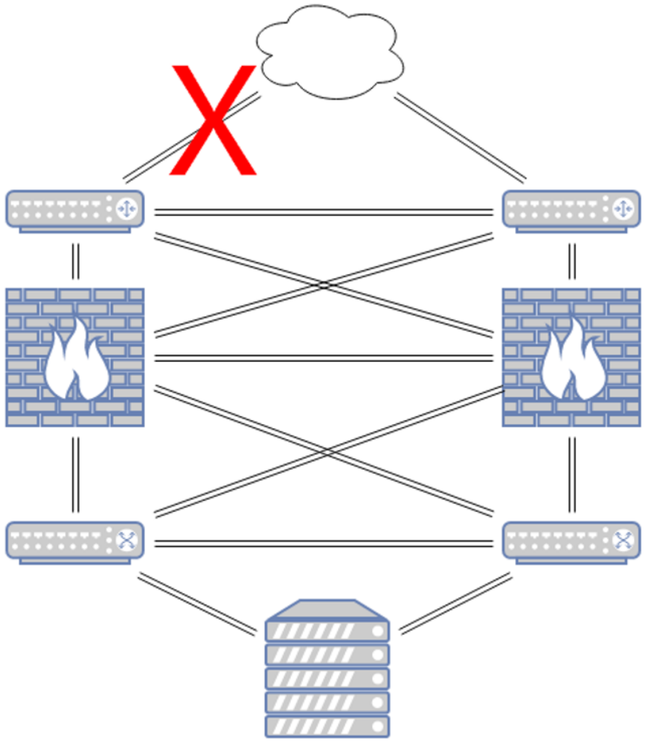


Procedure e gestione dei Backup in Register.it

Ridondanza dei dispositivi

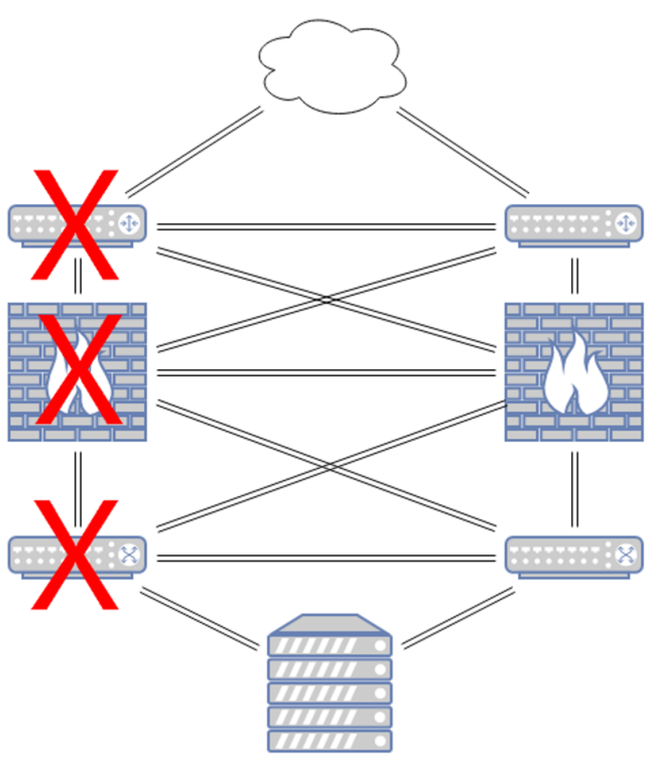


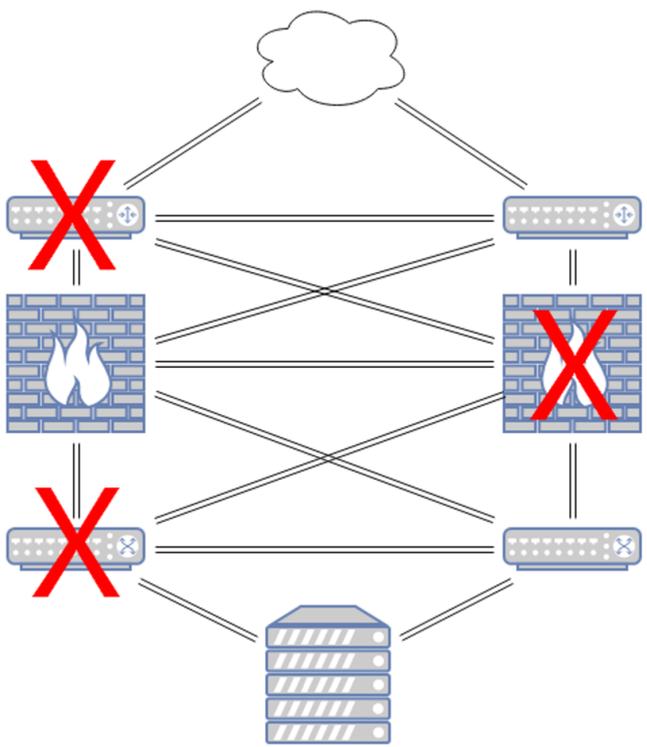


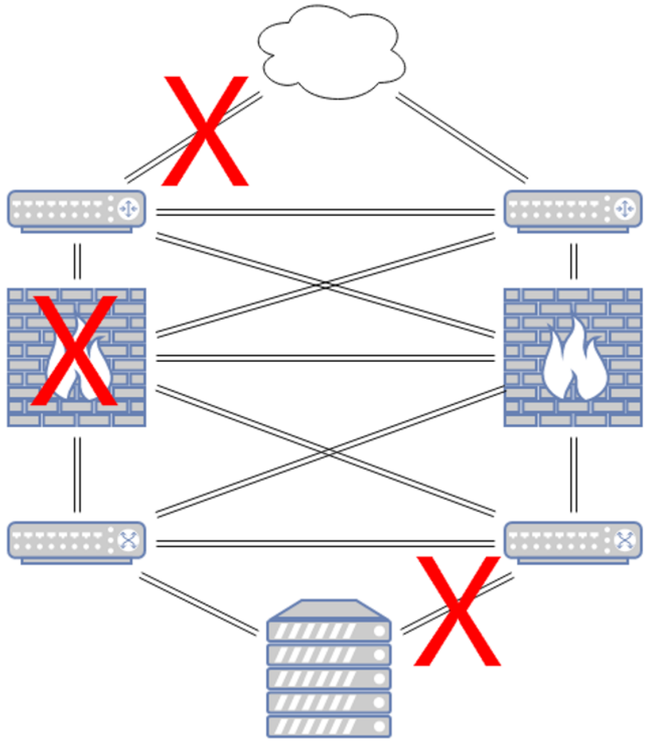


Procedure e gestione dei Backup in Register.it

Ridondanza dei dispositivi







Procedure e gestione dei Backup in Register.it

Regole generali

- Il codice sorgente viene salvato su **software di controllo di versione** (git, github, gitlab, svn, crucible, cvs).
- Il software di controllo di versione esegue un **backup periodico su un datacenter diverso**.
- Viene usato un software di configuration management (ansible, puppet, chef, ecc.) le cui configurazioni risiedono su software di controllo di versione.
- Gli **storage** eseguono **2 tipi di backup:** dei backup periodici tenuti all'interno dello storage (per proteggere da eventuali cancellazioni accidentali della configurazione) e dei backup periodici trasferiti su un datacenter diverso da quello di produzione (per proteggere i dati da eventuali problemi al datacenter principale).
- I database eseguono dei **backup periodici** che vengono salvato su un datacenter diverso.
- I **backup vengono periodicamente testati** per assicurarsi che siano consistenti e per valutare i tempi di ripristino.

Questions and Answers

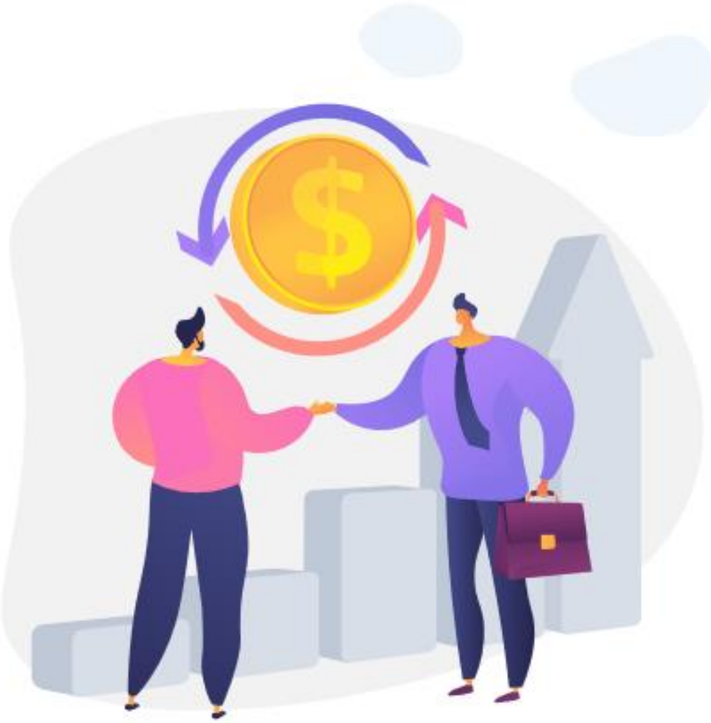
.Thanks

Finanziamenti PNRR per PMI

- Fino al 31 maggio 2022 è possibile presentare **domande di finanziamento** per accedere alle risorse europee stanziate nell'ambito del PNRR, il Piano Nazionale di Ripresa e Resilienza.

- Register.it può aiutarti a sviluppare il tuo sito di e-commerce per usufruire dei finanziamenti agevolati.

- Per maggiori informazioni contatta il tuo commerciale di riferimento o **chiamaci al 035 57 87 900** dalle 10:00 alle 18:00



Il prossimo webinar

register.it

part of team.blue