DiGiTAL academy

by register.it

Cyber Security

BACKUP, IL VALORE DELLA DISPONIBILITÀ DEI DATI

Argomenti del corso

- 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.

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

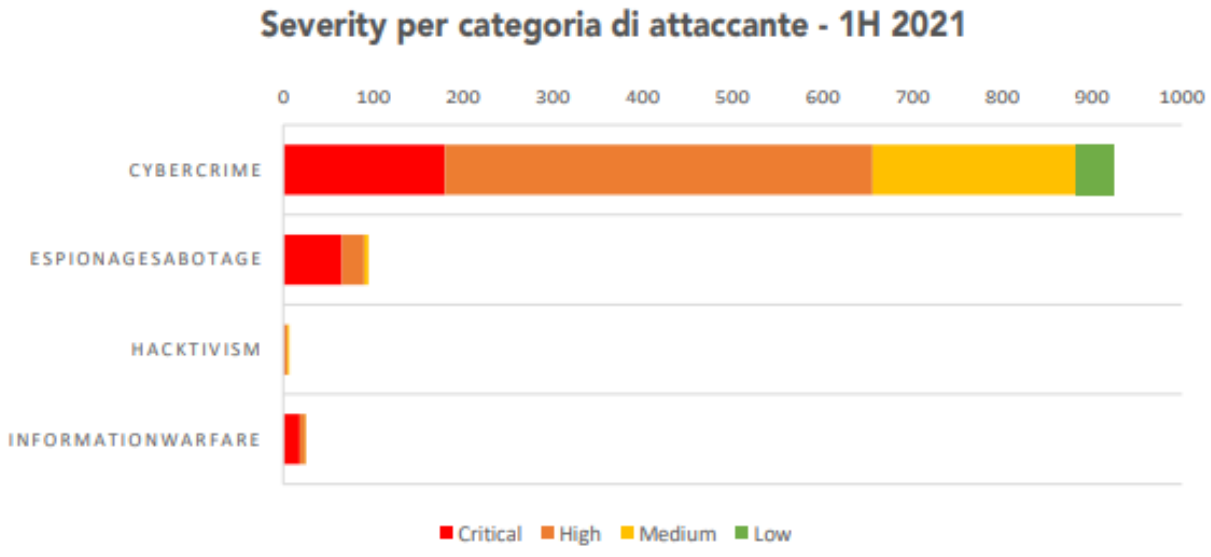
Iniziamo fornendo qualche dato che possa dare un quadro statistico oggettivo e indipendente della situazione in termini di **minacce reali per la disponibilità e l'integrità delle informazioni** e la conseguente continuità dei servizi informatici che le utilizzano.

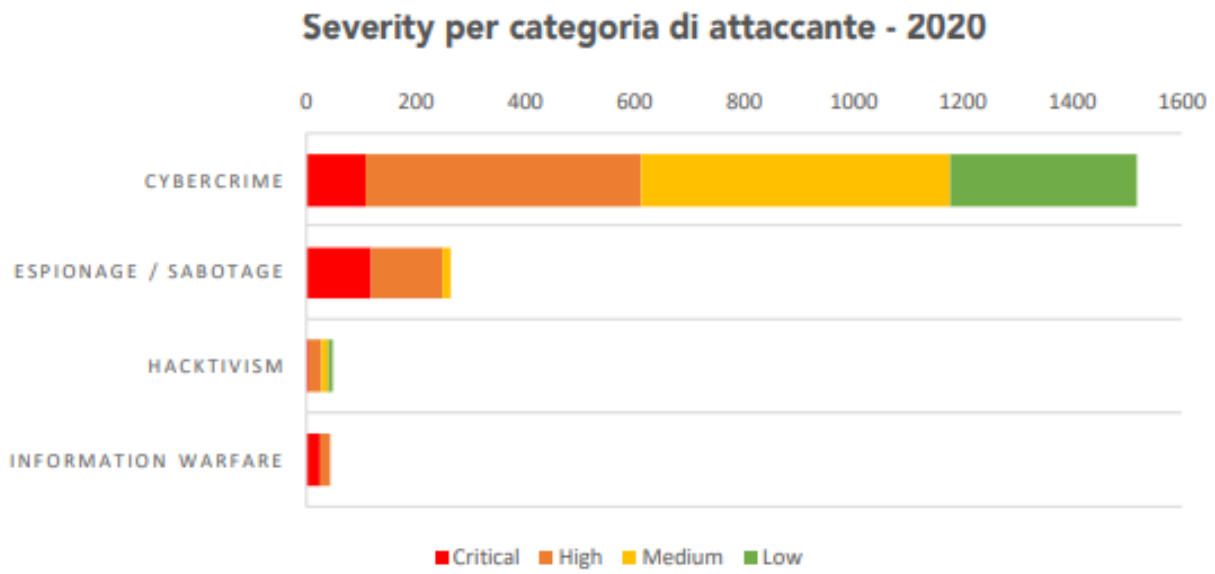
Secondo l'ultimo **rapporto 2021 del CLUSIT** sulla sicurezza ICT in Italia i dati relativi alla severity degli attacchi subiti, valutata considerando impatto geopolitico, sociale, economico (diretto e indiretto) e di immagine, evidenziano il seguente andamento:

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

Nel 2021 il campione osservato evidenzia una crescita dell'attività di questa tipologia di attacco di circa il **350%** rispetto allo stesso periodo del 2020. Tali tipologie di attacchi rientrano nella categoria **Cybercrime** con finalità di **estorsione di denaro alle vittime** e costituiscono la categoria per la quale si è osservato il maggiore incremento degli attacchi con severity Critical o High come mostrato nei grafici seguenti.



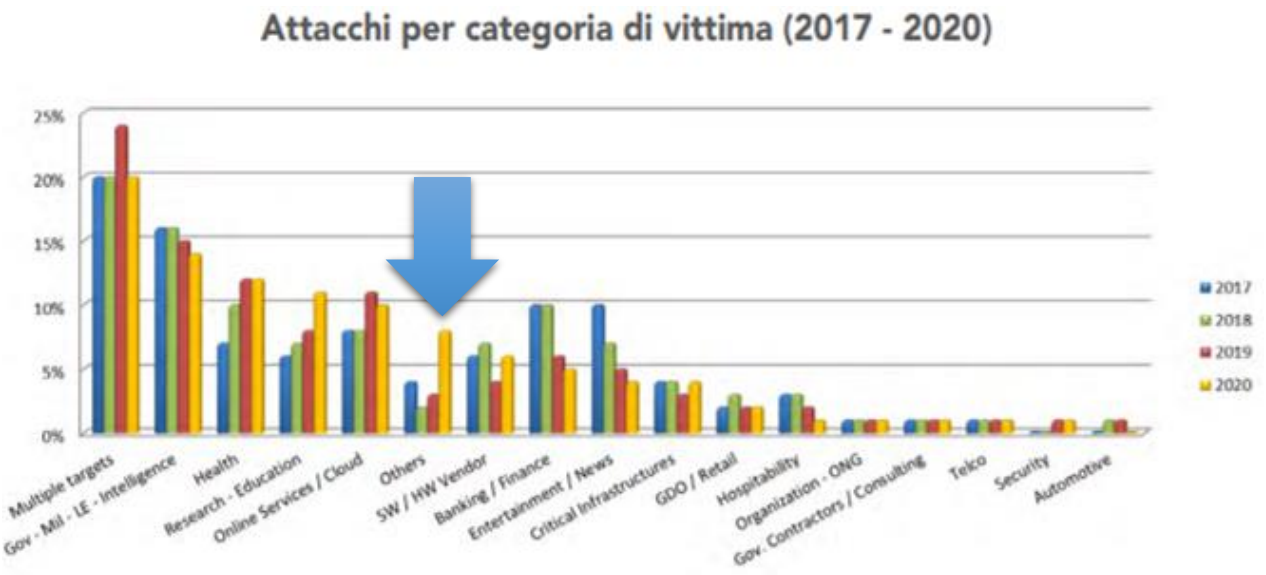


Fonte Rapporto 2021 sulla Sicurezza ICT in Italia

L'efficacia di questa tipologia di attacchi si basa principalmente sulla capacità degli attaccanti di **rendere i dati indisponibili o inutilizzabili da parte delle vittime** a meno che non vengano corrisposte somme di denaro o a fini di sabotaggio o comunque finalizzato ad acquisire vantaggio commerciale o fornirlo ad altri soggetti.

Oltre ad una maggiore frequenza, ad una severity media più alta di questi attacchi negli ultimi anni è cresciuta molto anche la categoria **"Others"** in cui rientrano le PMI e i soggetti privati non inquadrabili nelle altre macro-categorie di osservazione, indice di un aumento indiscusso di attacchi rivolto a questa categoria di utenti.

"*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 base per garantirsi un corretto recovery è appunto il backup*"



Fonte Rapporto 2021 sulla Sicurezza ICT in Italia

L'osservazione di queste dinamiche il cambiamento epocale nei livelli globali di cyber-insicurezza avvenuto negli ultimi anni è causato:

- dall'evoluzione rapidissima degli attori attaccanti o aventi interesse nell'attacco;
- dal cambiamento delle modalità di attacco;
- dall'aumento di pervasività ed efficacia degli attacchi cui non è corrisposto un incremento sufficiente delle contromisure adottate.

Nel 2020 circa **un'azienda italiana su tre ha subito un attacco ransomware** (Fonte ricerca Sophos) che ne ha aggirato le difese. Il principale motivo di questo dato 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 per ripagarsi dell'effort maggiore di preparazione e gestione dell'attacco.

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

Main Best Practice raccomandate – Backup / DR e piani di continuità.

Alla luce degli elementi presentati e dall'analisi condotta dal CLUSIT, con particolare focus sul ransomware, si possono sintetizzare le raccomandazioni nelle seguenti best practice:

1. **Valutare la possibilità di essere colpiti.** Cyberattacchi e ransomware in particolare restano fortemente diffusi. Nessun settore, Paese o azienda è immune da questo rischio. È meglio essere preparati e non venire colpiti che viceversa.

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

3. **Implementare una protezione a strati**. Gli attacchi a puro scopo di estorsione sono raddoppiati passando dal 3% di tutti gli incidenti del 2019 al 7% del 2020. Di fronte a questo considerevole incremento diventa più importante che mai riuscire innanzitutto 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.

4. **Combinare gli esperti con la tecnologia anti-ransomware.** Un elemento essenziale per poter bloccare le cyberminacce come il ransomware è la presenza di difese approfondite che combinano tecnologia anti-ransomware dedicata con attività di threat hunting condotte da personale esperto. La tecnologia fornisce l'automazione e i tool che occorrono, mentre gli esperti riescono a identificare le tattiche, le tecniche e le procedure che segnalano il tentativo di accesso nel proprio perimetro da parte di un abile attaccante.

5. **Non pagare i cybercriminali.** Difficile quando l'azienda è totalmente ferma a causa di un attacco ransomware. Al di là di qualsiasi considerazione etica, versare un riscatto è un metodo inefficace per riottenere i dati ed ha spesso se non sempre impatti di tipo legale. Chi decide di pagare, considerati i suddetti impatti legali che ciò può comportare, deve comunque tenere in considerazione la possibilità di veder ripristinati in media solo 2/3 dei file.

6. **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. Le aziende che cadono vittima di un attacco si rendono spesso conto che avrebbero potuto evitare parecchi costi, fastidi e problemi se solo avessero avuto un piano di risposta agli incidenti.

Circostanziando tali raccomandazioni alla gestione sicura di un sito web:

- I punti 3 e 4, si basano su attività e misure di sicurezza implementate dall'hosting provider o del gestore del sito web
- Tutti i restanti punti focalizzano le misure di sicurezza nell'adozione di sistemi, servizi e strumenti di **Backup & Recovery,** di pianificazione e gestione della continuità operativa e di attivazione di sistemi, infrastrutture e processi di Disaster Recovery che permettano il recupero quanto più possibile completo e tempestivo di dati, file, contenuti, record o interi database e configurazioni resi indisponibili o inutilizzabili.

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

La disponibilità di strumenti, servizi e processi di backup e rispristino in grado di garantire la disponibilità delle informazioni nel caso di compromissione rappresenta anche il **giusto presidio** professionale **per la gestione a regime di tutti i cambiamenti**, miglioramenti, evoluzioni o fix che fanno parte del ciclo di vita di un sito web duraturo.

Parliamo in questo caso di situazioni di compromissione non dovute ad attacchi o attività malevole ma principalmente ad errori nella gestione dei suddetti cambiamenti, commessi da utenze autorizzate ad effettuarli.

Un processo di gestione controllata e sicura delle modifiche ad ogni piattaforma ICT prevede sempre, 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. I 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.

Si tratta quindi di adottare strumenti e processi strutturati e con un costo tecnologico ed organizzativo che può risultare notevole per privati o piccole aziende.

Tuttavia, anche in assenza di processi strutturati di pianificazione e gestione controllata dei cambiamenti, dovendo affrontare il **rischio di intervenire direttamente sui sistemi di produzione**, i presidi di sicurezza **CORE** che garantiscono un "rollback" completo e continuità di servizio in caso di malfunzionamenti, regressioni o perdite di dati sono costituiti da:

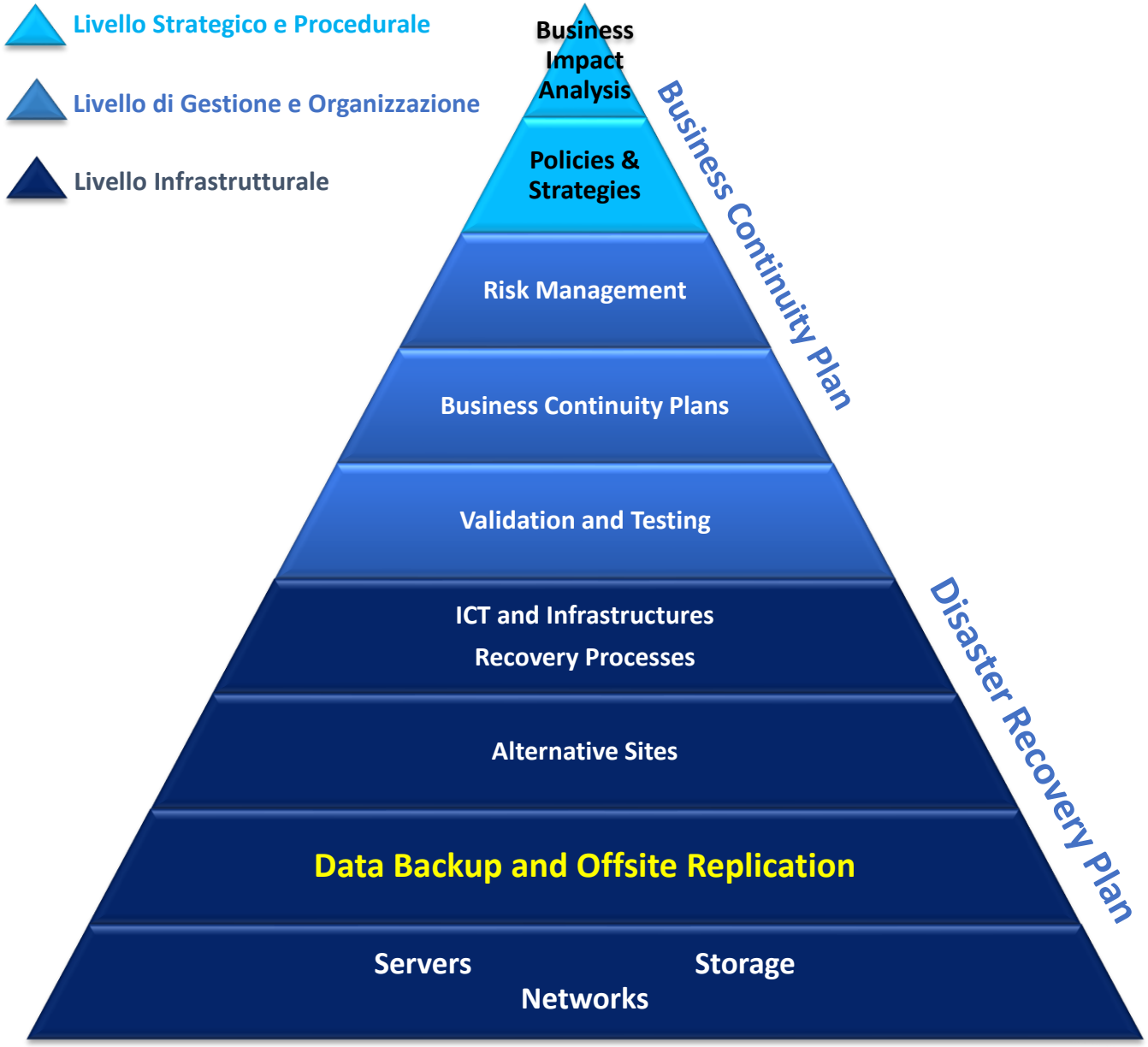
- La disponibilità di strumenti/sistemi e/o servizi di **Backup** che, ad intervalli predefiniti o a fronte di determinate modifiche, creino, archivino e aggiornino su sistemi distinti da quelli di produzione copie di:
    - file core dell'applicazione
    - media e archivi caricati
    - documenti caricati
    - dati e struttura del Database
    - plugin e temi.

- La 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, eventualmente a livelli degradati ma accettabili.

Il **Disaster Recovery** comprende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e 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, di cui il Backup costituisce una componente, anche nel caso di discontinuità o anomalie causate da attacchi esterni che spesso, oltre a minacciare la disponibilità e integrità delle informazioni, possono contemporaneamente rendere indisponibili o malfunzionanti le architetture e le applicazioni primarie che elaborano tali dati.

Si riporta di seguito una descrizione sintetica dei livelli tecnico/organizzativi di un piano di gestione della continuità operativa (**Business Continuity Plan**) e di un piano di attivazione e gestione delle risorse architetturali secondarie per la gestione delle situazioni critiche (**Disaster Recovery Plan**)


Livello Strategico e Procedurale
Livello di Gestione e Organizzazione
Livello Infrastrutturale
Business Impact Analysis
Policies & Strategies
Risk Management
Business Continuity Plans
Validation and Testing
ICT and Infrastructures
Recovery Processes
Alternative Sites
Data Backup and Offsite Replication
Servers
Storage
Networks
Business Continuity Plan
Disaster Recovery Plan

La predisposizione, verifica e test periodico dei suddetti piani impegna notevoli risorse tecniche ed organizzative.

Nella gestione di un sito web la maggior parte di questi processi vengono o possono essere gestiti dall'hosting provider nel caso cui:

1. l'utente abbia attivato con il provider anche uno specifico servizio di backup
2. l'hosting provider disponga piani di gestione della continuità e di Disaster Recovery per il servizio fornito.

Tuttavia, la gestione del Backup di cui al punto 1 può essere effettuata anche con modalità alternative di cui discuteremo nei prossimi paragrafi.

Per quanto riguarda il secondo punto è invece fondamentale ricordare che la disponibilità da parte dell'hosting provider di piani di gestione della continuità e di Disaster Recovery per il servizio di hosting è una delle caratteristiche che può essere accertata verificando, il **possesso di certificazioni per il sistema di gestione della sicurezza** delle informazioni secondo standard internazionali di settore (ISO 27001 / 27017 / 27018) che hanno fra i loro requisiti la definizione, il test periodico e l'aggiornamento continuo di tali piani e ne prevedono la regolare verifica da parte di organismi indipendenti.

Tipologie di soluzioni di backup e modalità di gestione

Una forma basilare e manuale di Backup può essere realizzata in modo molto semplice dotandosi di uno spazio separato nello stesso hosting provider del sito o anche altrove, dove manualmente copiare file, documenti e dump dei db.

Non utilizzando strumenti automatizzati o servizi gestiti tramite architetture dedicate si può ovviamente andare incontro a rischi dovuti a:

- Errori nel processo di copia e corruzione dele 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 con cui è necessario effettuare il backup.
- Aumento di effort per:
    - Lo svolgimento dell'attività di copia.
    - La verifica dell'integrità delle copie effettuate.
    - 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.

Riportiamo un utile link per la gestione manuale dei backup su piattaforme Linux o Windows usufruendo del servizio **Spazio Backup** che Register.it offre ai propri utenti per l'acquisto sia con i nuovi server dedicati e virtuali che separatamente dalla pagina di gestione dei nel Pannello di controllo.

I suddetti rischi possono essere in parte mitigati con un'adeguata pianificazione delle attività e la definizione di procedure/istruzioni operative da seguire nello svolgimento delle attività ma per una gestione strutturata, più affidabile e sicura, del processo di backup è opportuno affidarsi a servizi e strumenti professionali come:

- L'attivazione di un servizio di **Backup automatico** gestito dal provider del servizio di hosting, di cui descriveremo a seguire le caratteristiche.
- L'adozione di tool o soluzioni professionali di Backup per poter autonomamente pianificare, configurare e gestire le copie e gli eventuali restore, come ad esempio Acronis Cyber Backup, di cui descriveremo features e caratteristiche nel paragrafo successivo.

Backup automatico gestito dal provider del servizio di hosting

Il servizio di gestione del backup fornito dai provider di servizi di hosting fa parte delle tipologie di servizi Server Managed in cui l'hosting 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 specifici e customizzati per il singolo cliente** finalizzati alla gestione professionale della continuità operativa, come ad esempio il **Backup automatico e gestito.**

Questo tipo di servizio permette, secondo diverse formule configurabili a seconda delle esigenze e dei requisiti di business, di lasciare la gestione delle attività operative di backup di dati, configurazione, verifica di integrità e test di restore alla gestione del provider del servizio di hosting, attivando strumenti di pianificazione e monitoraggio delle attività, come ad esempio le funzionalità di gestione backup offerte dal **pannello di gestione di Plesk** (vedi step operativi nelle immagini successive) e di tracciatura delle richieste, 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 e professionale nel caso di necessità di ripristino di dati/configurazioni inutilizzabili o inaccessibili a fronte di attacchi esterni o di errori interni.

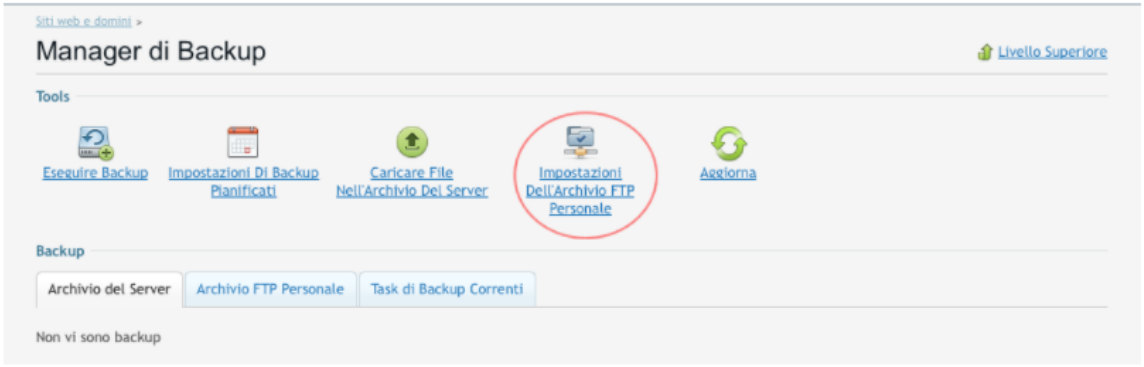
Step operativi del pannello di gestione Plesk

1

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

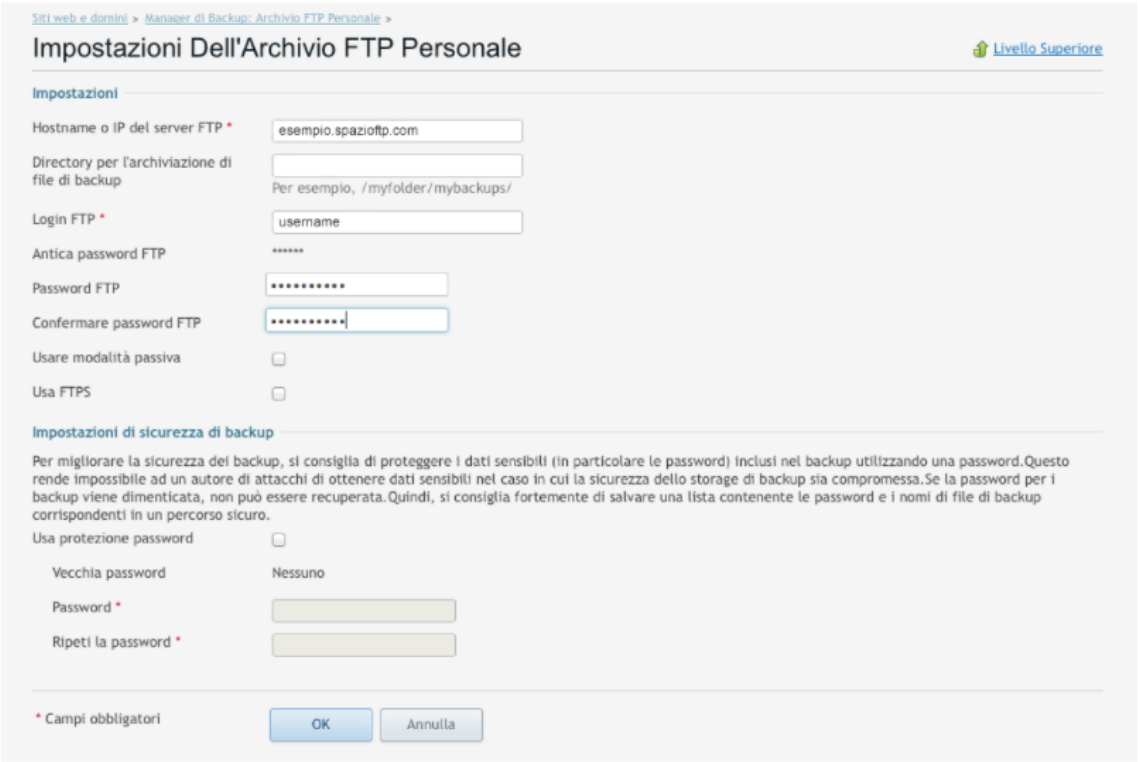
2

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:

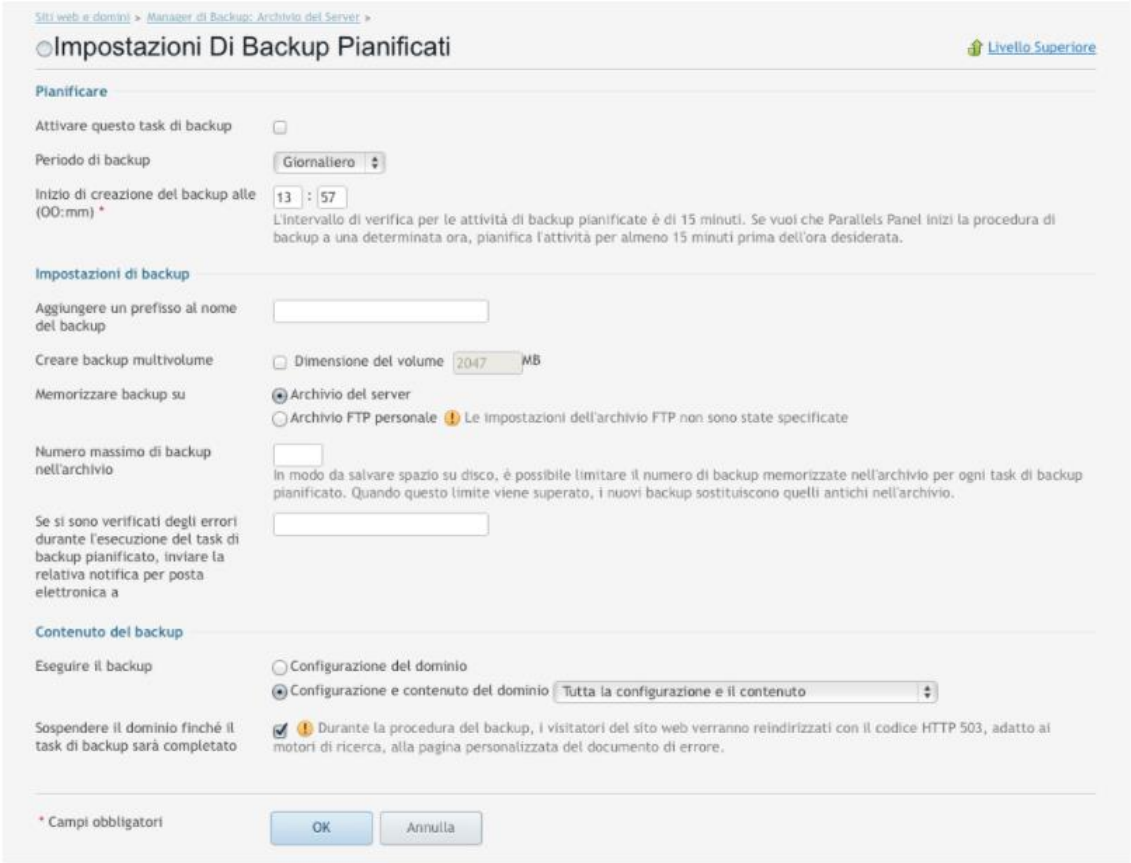


4

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.



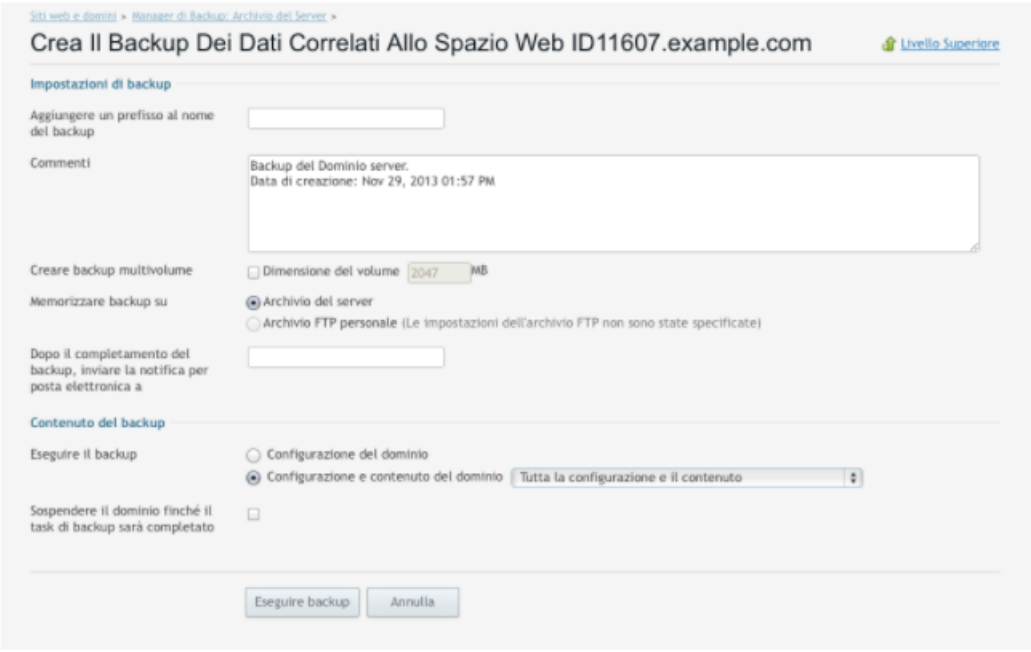
6

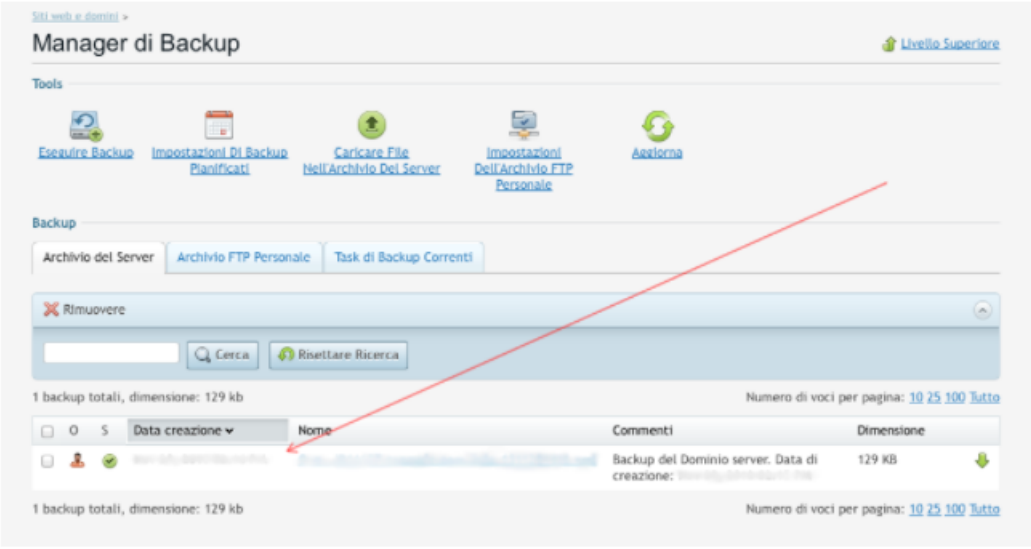
Adesso puoi eseguire il tuo backup.
Ricorda: l'opzione "Archivio del server" salverà il backup sul server stesso; seleziona "Archivio FTP personale" per utilizzare lo Spazio Backup che hai precedentemente impostato.
Premi infine il tasto Esegui backup per avviare l'operazione.

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.

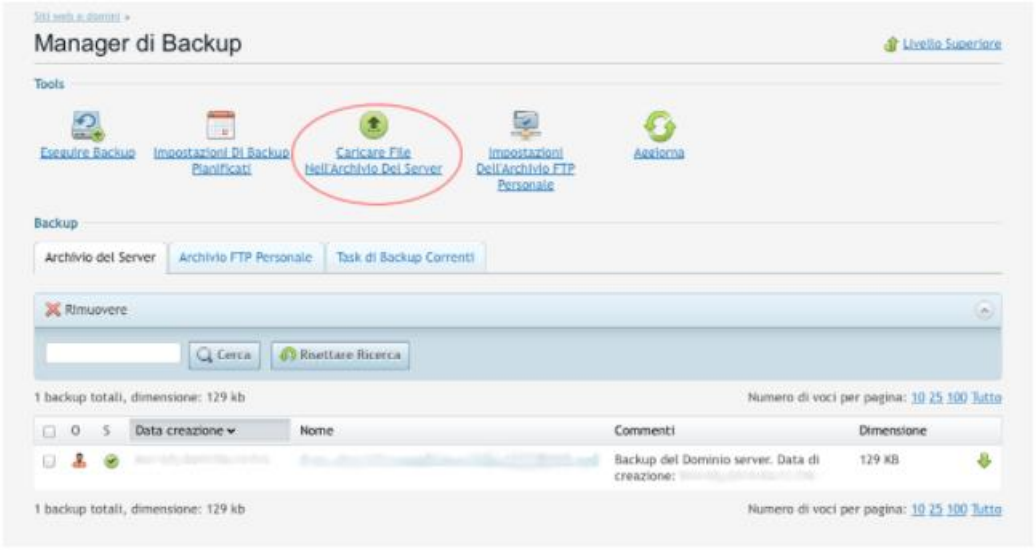
Cliccando sul nome del backup avrai accesso a una pagina in cui visualizzare i dettagli relativi al backup e, se lo desideri, ripristinare quanto salvato in precedenza.

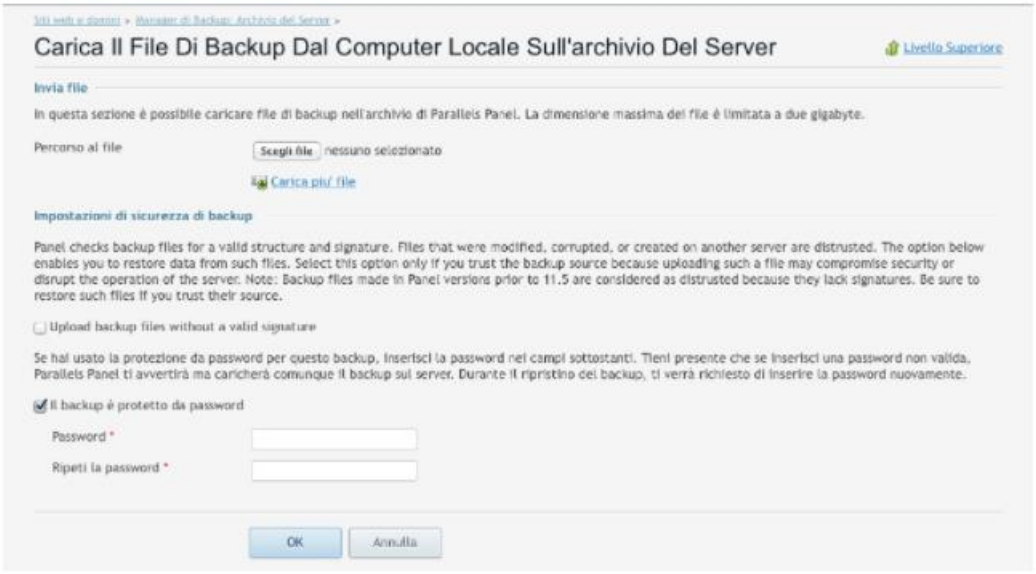




8

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

Le diverse tipologie di Backup si differenziano essenzialmente per:

- modalità di memorizzazione dei dati
- localizzazione dei dati

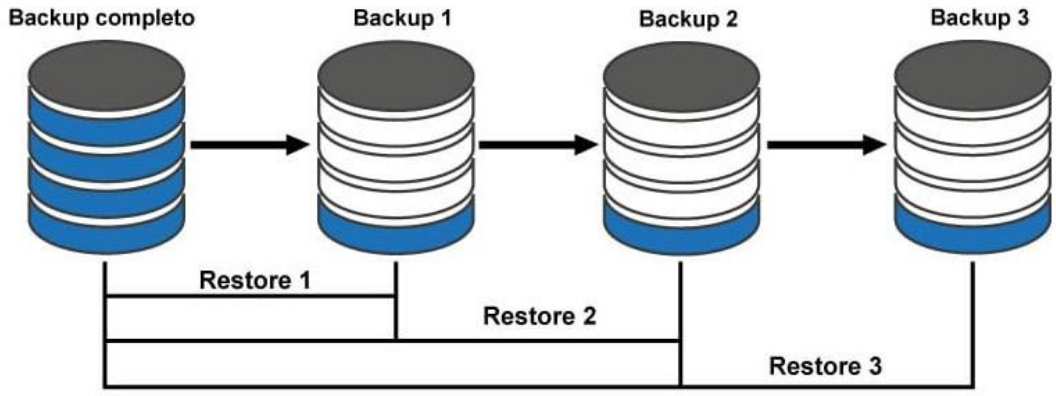
e vengono poi implementate secondo:

- specifiche tecniche e modalità di accesso ai file, salvataggio delle configurazioni di sistema e dei dump dei database.
- tipologia di supporti di memorizzazione utilizzati che possono variare a seconda delle caratteristiche architetturali dell'infrastruttura e dei requisiti di perimetro, frequenza, capacità, rapidità di ripristino e livelli di ridondanza definiti con il service provider.

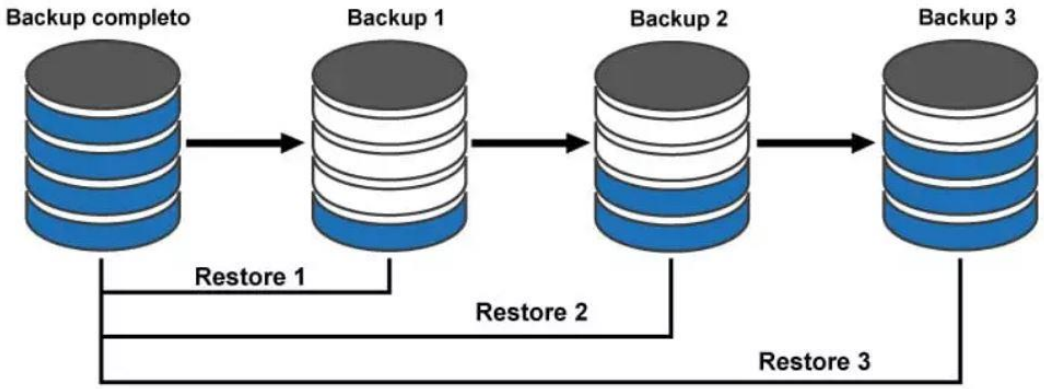
Backup per modalità di memorizzazione:

- Il **backup completo** prevede la replica di tutti dati e, ripristinando l'ultima copia eseguita, permette di recuperare interamente tutti i dati. 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. Per via di queste motivazioni capacitive e prestazionali di solito i backup completi vengono eseguiti insieme ad altre tipologie di backup ma con una frequenza inferiore.

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



- 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.



Backup per localizzazione dei dati:

- Il **backup fisico on-premise** prevede l'archiviazione locale su sistemi, apparati e dispositivi di memoria all'interno del proprio data center. Questo tipo di backup è molto veloce nella processazione dei dati ma, di contro, risente di tutti i rischi dovuti alla "guastabilità" e ai possibili danneggiamenti da eventi accidentali o malevoli delle componenti fisiche di tutta l'architettura di memorizzazione.

- 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, 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.

  Il backup in cloud può essere implementato come servizio cloud privato o servizio cloud pubblico:

  - Il **backup in Cloud privato** è ospitato da una infrastruttura IT on-premise, di proprietà presso il proprio Data Center o presso il Data Center del fornitore del servizio, in cui **l'infrastruttura fisica** di elaborazione, trasmissione e memorizzazione (Server, Rete e Storage) su cui è realizzato l'ambiente Cloud **è dedicata al singolo cliente**. Si tratta di una soluzione che comporta un particolare effort e costi tecnici/organizzativi per la manutenzione e la gestione dell'infrastruttura da parte del fornitore del servizio, motivo per il quale tali soluzioni sono solitamente adottate **da aziende medio-grandi.**

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

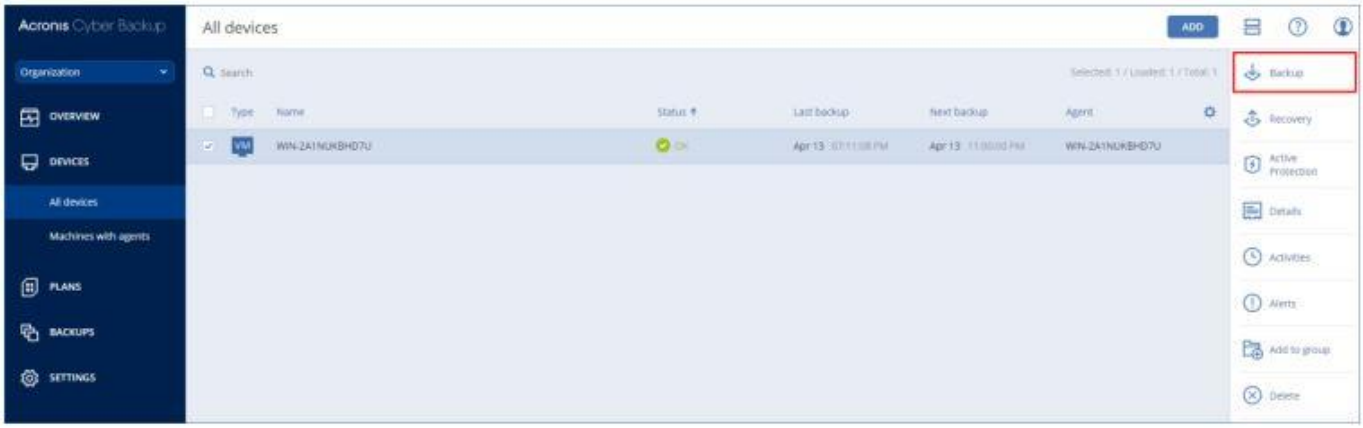
Soluzioni professionali di backup - Acronis Cyber Backup

In quest'ultima parte vi introdurremo le funzionalità offerte da strumenti professionali di gestione del Backup presentando alcune delle principali funzionalità della soluzione Acronis Cyber Backup, offerta da Register.it.

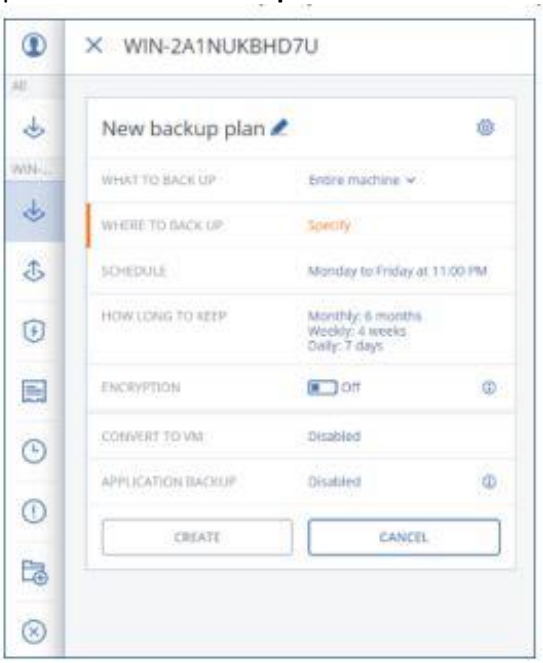
Backup dell'interna macchina e funzionalità di recovery granulare dei singoli file

In questo scenario di utilizzo l'utente può effettuare tramite le consolle di gestione il backup di contenuti e configurazioni dell'intera macchina su cui è in funzione il sito e poi a discrezione recuperare singolarmente i singoli file o, con una procedura analoga, volumi, dischi o l'intero contenuto delle immagini delle macchine salvate.

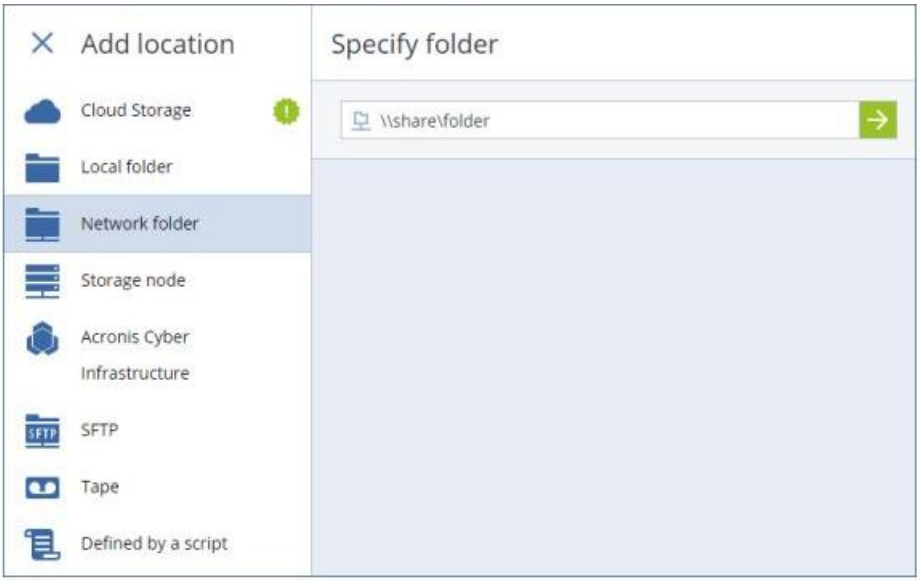
La procedura di backup della macchina si avvia selezionando quest'ultima dall'elenco presente nella dashboard della consolle di backup e cliccare sull'opzione a destra **↓ Backup**



Viene quindi presentato un template di **Piano di Backup**

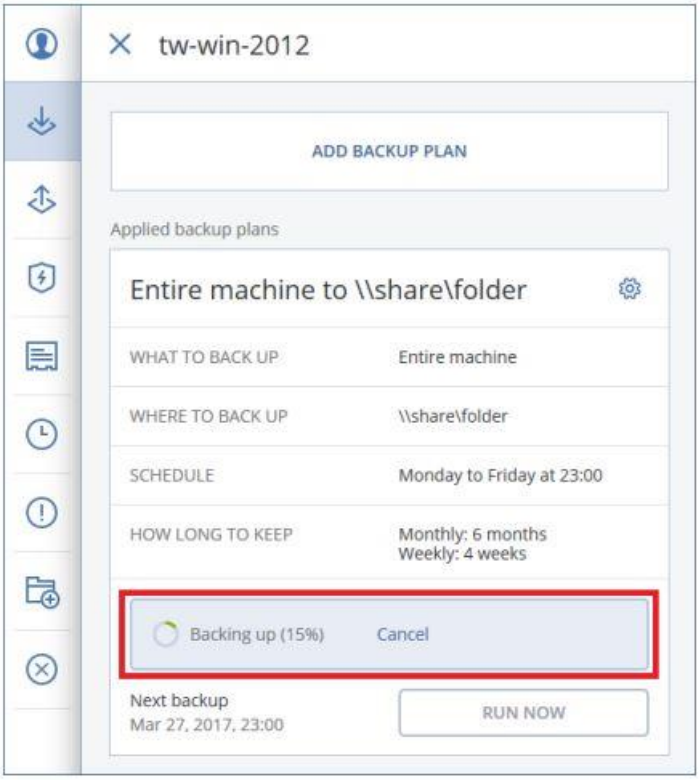


Selezionando le opzioni **Where to backup -> Network folder**, si potrà navigare nel filesystem per selezionare la cartella, precedentemente creata, dove realizzare il backup oppure inserirne direttamente il percorso, cliccando infine l'opzione **Add.**

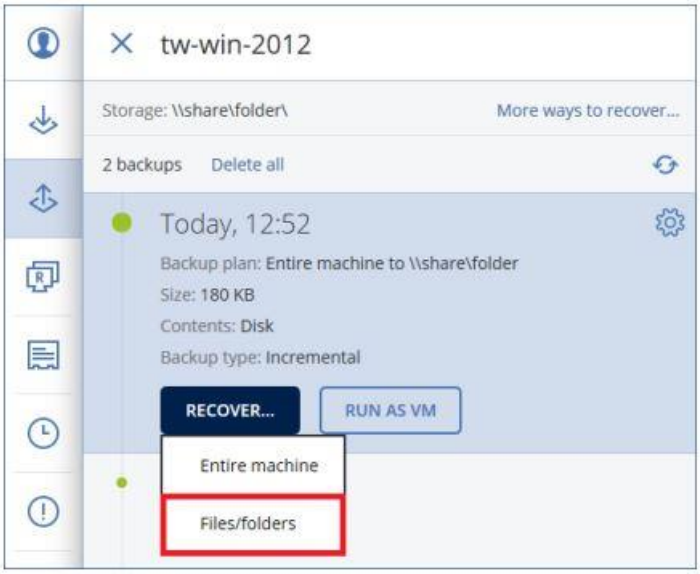


Successivamente cliccando sul pannello di backup **Create-> RUN NOW** verrà avviato il backup completo e il form mostrerà lo stato di avanzamento %.

Qualora sia già stato effettuato un backup completo è possibile effettuare un backup incrementale utilizzando la freccia che appare di fianco al tasto RUN NOW e cliccando su **INCREMENTAL**.

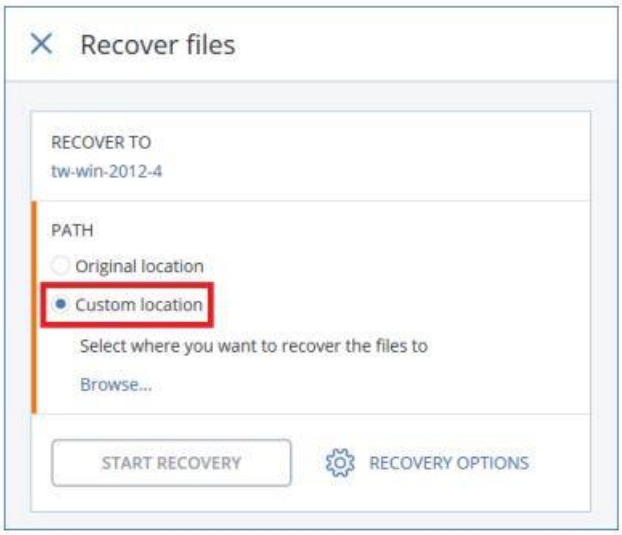


Per effettuare il recovery di un file dal backup e necessario selezionare, come per la procedura precedente, la macchina di riferimento dal pannello di Backup e cliccare e poi nel menù a destra sull'opzione **Recovery**, selezionare il backup da cui si vuole effettuare il recupero e selezionare le opzioni **Recover -> Files/folders**



Navigare fino al file che si intende recuperare, eventualmente utilizzando la funzione di ricerca, selezionare il file e cliccare a destra su **Recover**

Selezionare **Custom location** nel tab PATH



Cliccare su **Browse** e specificare un percorso di destinazione per i file recuperati, cliccare su **Start Recovery**

Selezionare una delle opzioni proposte per l'eventuale sovrascrittura dei file recuperati:

- **Overwrite existing files**
- **Overwrite an existing file if it is older**
- **Do not overwrite existing files**

Cliccare su **Proceed** per avviare Recovery il cui avanzamento % verrà mostrato nel tab Activities.