solarwinds msp

E-book

# Backup e disaster recovery dopo l’entrata in vigore del GDPR

## INTRODUZIONE

*Il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) è stato ideato per favorire ulteriormente la tutela della privacy e dell'integrità dei dati personali per i cittadini residenti in Unione Europea. Una delle disposizioni principali del regolamento prevede diritti estesi per gli individui i cui dati sono oggetto di trattamento, vale a dire che essi avranno accesso ai propri dati personali, potranno richiederne il trasferimento e limitarne il trattamento. Gli MSP dotati di un'opportuna soluzione gestita per backup e ripristino potranno rispondere al meglio alle richieste dei soggetti interessati.*

Per fortuna, la maggior parte degli MSP considera già come prioritari i backup giornalieri e incrementali e sa come implementare un piano di continuità operativa aziendale. Anche in assenza di problematiche relative a conformità e sicurezza, includere nei propri contratti di servizi standard una robusta soluzione di backup hybrid cloud è decisamente sensato.


*Gli MSP dotati di un'opportuna soluzione gestita per backup e ripristino potranno rispondere al meglio alle richieste degli individui i cui dati sono oggetto di trattamento.*

## AVVERTENZE

Gli MSP che desiderano erogare un servizio di backup come parte dell'offerta SECaaS o CaaS dovranno scegliere con cura il prodotto per il backup per assicurarsi che garantisca le tutele fondamentali previste dal GDPR.

Ad esempio, il prodotto deve sottoporre i backup a crittografia: non è giustificabile che i dati presenti nei backup non siano crittografati. La crittografia andrà utilizzata anche per qualsiasi supporto rimovibile utilizzato come speed vault o repository per il backup in locale. Per garantire l'integrità dei backup, il software deve prevedere un efficace algoritmo di crittografia per proteggere tutti i dati, quelli a riposo e anche quelli in fase di trasferimento all'infrastruttura di hosting.

In caso di perdita di un backup non sottoposto a crittografia, a seguito di un attacco informatico, di una configurazione non ottimale o di un furto fisico, potrebbe essere necessario segnalare la cosa alle autorità competenti e/o pagare multe potenzialmente ingenti, in base al GDPR. Ecco perché è necessario che una soluzione di backup offra un'opportuna crittografia.

## VERIFICA DEI BACKUP

Gli MSP di successo probabilmente eseguono già backup quotidiani e persino un test occasionale del ripristino, ma, avendo a disposizione una soluzione di backup all'avanguardia, potranno altresì automatizzare un ripristino di prova per assicurarsi che i backup a disposizione funzionino correttamente quando è il momento di utilizzarli. Potrebbe essere davvero un problema per la vostra impresa e rappresentare un danno per i vostri clienti se durante un incidente serio un backup risultasse non funzionante. Controllando con regolarità i report dei backup e quelli dei ripristini di prova, sarete più sicuri durante un incidente (e darete prova ai vostri clienti di una gestione responsabile dei backup, anche qualora il ripristino non riuscisse). Inoltre, tali report potrebbero tornare utili per dimostrare alle autorità GDPR di aver agito in buona fede.

*Avendo a disposizione una soluzione di backup all'avanguardia, potrete automatizzare un ripristino di prova per assicurarvi che i backup a disposizione funzionino correttamente quando è il momento di utilizzarli.*

Gli MSP sono messi a dura prova quando un incidente di sicurezza richiede il ripristino di diversi sistemi o se le workstation hanno configurazioni complesse o inusuali. In questo, i servizi cloud possono davvero tornare utili. Se i vostri clienti si avvalgono di servizi aziendali di fornitori di terze parti tramite applicazioni Web, potranno preoccuparsi di meno in caso di incidenti di sicurezza che mettono a repentaglio la disponibilità.

## SUGGERIMENTI PER I PIANI DI RIPRISTINO

Ecco alcuni aspetti da prendere in considerazione durante la stesura di un piano di continuità operativa aziendale con disaster recovery da proporre ai clienti.

1. *Stabilite le aspettative con il cliente prima che si verifichino incidenti.*

   È fondamentale stabilire un piano e i costi legati a circostanze straordinarie e catastrofiche. Anticiparsi su questo punto può ridurre drasticamente l'ansia per tutti durante un incidente. Ad esempio, se il ripristino dipende da attrezzature specifiche, diverse configurazioni uniche o chiavi di licenze software, i tempi potrebbero essere significativamente maggiori rispetto alle aspettative dei clienti. È importante stabilire in anticipo cosa sarete in grado di fare durante un incidente.

2. *Se le workstation sono state personalizzate dagli utenti, dovrete sottoporre a backup sia le workstation sia i server.*

   Nelle piccole e medie imprese, molte applicazioni potrebbero dipendere da configurazioni specifiche degli endpoint. Anche sui laptop potrebbe risiedere una quantità elevata di dati importanti copiati sulle unità locali. Un efficace piano di continuità operativa aziendale con disaster recovery deve tenere in considerazione i dati dei profili utente presenti sugli endpoint: se ripristinare elementi banali come i collegamenti degli utenti può sembrare inutilmente dispendioso, non vi dispiacerà disporre di una protezione degli endpoint qualora dobbiate ripristinare invece importanti documenti finanziari di un CFO. Anche se molti MSP insistono sul fatto che le informazioni debbano risiedere sul server per il backup, i vostri clienti saranno molto più soddisfatti se riuscirete a sottoporre a backup anche i loro dati importanti presenti sugli endpoint.

### 3. *Provate a virtualizzare i server ed erogate i servizi aziendali da servizi di hosting di terze parti.*

Una delle principali problematiche legate agli ambienti di piccole e medie imprese è rappresentata dall'hardware esistente. Non è infrequente, infatti, che queste aziende utilizzino server vecchi di cinque anni (o più). Se questo è il vostro caso, reperire rapidamente hard disk obsoleti, schede di interfaccia proprietarie o anche moduli di alimentazione compatibili potrebbe essere difficile se non impossibile durante un disastro, soprattutto se il server è prossimo al termine del suo ciclo di vita o non è più in garanzia. Se l'azienda o l'MSP non dispone di componenti hardware sostitutivi, il ripristino potrebbe subire ritardi.

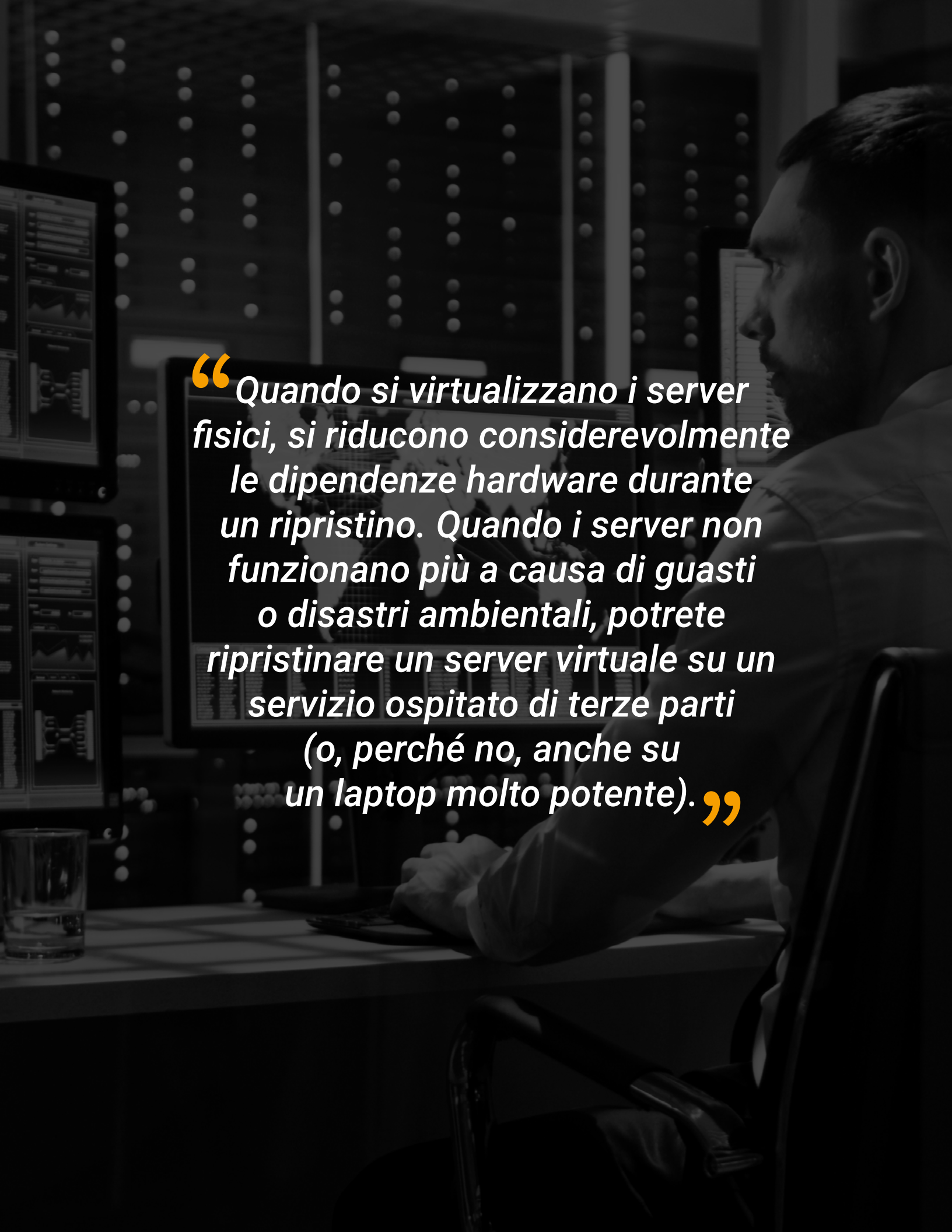
Ecco dove entra in gioco la virtualizzazione. Quando si virtualizzano i server fisici, si riducono considerevolmente le dipendenze hardware in fase di ripristino. Quando i server non funzionano più a causa di guasti o disastri ambientali, potrete ripristinare un server virtuale su un servizio ospitato di terze parti (o, perché no, anche su un laptop molto potente).

Ancora meglio sarebbe se i clienti trasferissero i servizi critici su un servizio di hosting di terze parti o a un provider SaaS. Se i sistemi di comunicazione tramite e-mail o gli strumenti CRM rappresentano i servizi aziendali più importanti, trasferirli all'esterno dell'ambiente aziendale fisico potrebbe accelerare considerevolmente eventuali ripristini (ammesso che si rivelino effettivamente necessari).

### 4. *Le unità SSD potrebbero costituire la soluzione ottimale se utilizzate come spazio di archiviazione o repository dei dati di backup.*

Se la vostra strategia di backup e ripristino include snapshot di database e/o file ogni ora, le unità SSD rappresentano una soluzione di ripristino eccellente in caso di attacchi ransomware. L'incredibile velocità in lettura/scrittura di queste unità offre elevati ritmi di backup per le copie in locale. Tali copie in locale potranno poi essere trasferite all'infrastruttura di hosting al termine della giornata lavorativa al fine di ridurre i colli di bottiglia per la larghezza di banda durante gli orari di lavoro.

I sistemi con elevata attività su disco (quali i server dei database, i server di posta o i server Microsoft® Exchange™ o SharePoint®) solitamente gravano sulle risorse durante le ore di lavoro. Trasferire le snapshot per il backup su un'unità SSD tramite interfaccia iSCSI o USB-3 vi permetterà di ridurre le risorse necessarie per l'attività di backup che influiscono sulla reattività dei server.



*“Quando si virtualizzano i server fisici, si riducono considerevolmente le dipendenze hardware durante un ripristino. Quando i server non funzionano più a causa di guasti o disastri ambientali, potrete ripristinare un server virtuale su un servizio ospitato di terze parti (o, perché no, anche su un laptop molto potente).”*

## UTILIZZO DEL BACKUP PER GLI UPGRADE

Un prodotto per il backup efficace è anche in grado di semplificare gli upgrade dei server e il funzionamento dei prodotti per la migrazione. Gli MSP dovrebbero avvalersi dei prodotti per il backup che consentono di catturare immagini complete del sistema e di trasformarle in un server virtuale autoavviante. In questo modo sarà più semplice effettuare l'upgrade di un server utilizzando le immagini virtuali create da un prodotto per il backup ed eseguire l'implementazione nel nuovo host. Di fatto, le funzionalità di backup e ripristino semplificano il trasferimento dei server dall'hardware esistente su host hypervisor o VMware® ESXi.

*Gli MSP dovrebbero avvalersi dei prodotti per il backup che consentono di catturare immagini complete del sistema e di trasformarle in un server virtuale autoavviante.*

In casi estremi, l'immagine è eseguibile da una struttura di hosting su cloud o da un hard disk portatile collegato a un laptop all'avanguardia (che ci crediate o no, quelli adatti ai giochi sono perfetti in questi casi). Le unità SSD USB-3 da 250 GB o 500 GB sono facilmente reperibili, mentre il software VMware Workstation Player è scaricabile gratuitamente (ma è necessario acquistarne la licenza per utilizzare il prodotto a scopi commerciali). Grazie a questi due strumenti, potrete garantire la continuità operativa aziendale con disaster recovery utilizzando un laptop all'avanguardia dotato di molta RAM e qualche unità SSD portatile.

Il GDPR prevede molti diritti per gli individui i cui dati sono oggetto di trattamento, inclusi il diritto di cancellazione, noto anche come diritto all'oblio, che consente di richiedere l'eliminazione dei propri dati personali. Questo aspetto naturalmente presenta alcune complicazioni per l'erogazione di servizi di backup.

Dovrete discutere con i clienti in modo da pianificare opportunamente il da farsi qualora pervenga questo tipo di richieste. Il GDPR contiene alcune disposizioni per la conservazione dei dati per il trattamento secondo la legge e altri interessi legittimi, inclusi leggi e statuti esterni all'Unione Europea, che potrebbero imporre la conservazione dei documenti aziendali. Come sempre, vi suggeriamo di rivolgervi al vostro consulente legale in merito alla questione prima di finalizzare qualsiasi piano.

## REQUISITI DEL GDPR IN MATERIA DI RACCOLTA E ARCHIVIAZIONE DEI DATI

In base al GDPR, uno dei mezzi per il trattamento dei dati personali in conformità alle leggi vigenti è ottenere l'esplicito consenso dagli individui prima di raccogliere o trattare i loro dati. Questo implica che le imprese, sia degli MSP sia dei loro clienti, debbano dichiarare le categorie di dati raccolti, la finalità di tale raccolta e il periodo di conservazione previsto per tali dati.

Ad esempio, in base ad alcune leggi, le fatture contabili vanno conservate per almeno sette anni. Per quanto riguarda i tribunali o il settore sanitario, in alcuni casi per i documenti è previsto un periodo di conservazione a vita o indefinito. Invece, i dati con finalità di marketing delle liste di distribuzione possono essere eliminati a seguito di una esplicita richiesta da parte dei soggetti interessati. È essenziale impostare un periodo di conservazione dei dati seguendo i suggerimenti del vostro consulente legale o, nel migliore dei casi, del responsabile della sicurezza dei dati (DPO, Data Protection Officer), in conformità ai requisiti del GDPR.

Gli MSP che erogano servizi di backup dovranno collaborare con le aziende per agevolare le richieste provenienti dai cittadini dell'UE. Collaborando con un consulente legale o un DPO in anticipo, risparmierete tempo e assicurerete procedure più efficienti, stabilendo in anticipo come rispondere alle richieste più comuni. Ad esempio, potreste preparare alcune risposte predefinite per eventuali richieste di cancellazione, di accesso o altre richieste in base al GDPR. In caso di richieste di cancellazione, ad esempio, chiedete al vostro consulente legale di aiutarvi a fornire ai vostri clienti una spiegazione relativa ai dati che non è possibile eliminare a causa dei periodi di conservazione previsti dalla legge.

## GDPR E BACKUP

Il regolamento generale sulla protezione dei dati introduce alcune problematiche per gli MSP che erogano servizi di backup. A seconda della complessità e della natura dei dati personali raccolti, archiviati, elaborati o trasmessi, i piani di backup devono bilanciare i requisiti legali previsti per la conservazione dei dati, rimanendo tuttavia flessibili per garantire il rispetto dei diritti dei cittadini dell'UE, in base alla nuova legge. Pare proprio che l'epoca di sottoporre a backup e archiviare i dati in modo illimitato stia per giungere al termine.

In qualità di MSP che erogano servizi di backup, dovrete gestire le aspettative dei vostri clienti, stilare un piano per gli incidenti di sicurezza che mettono a repentaglio la disponibilità e predisporre servizi critici che garantiscano ridondanza e resilienza.