

# La guida Acronis<sup>®</sup> al backup e al ripristino per le PMI



Alan Stevens, giornalista freelance

Senza dubbio il duro lavoro ripaga ampiamente, ma sappiamo che non c'è nulla di più faticoso che creare e far funzionare una piccola impresa. Purtroppo però, indipendentemente da quanto tempo e impegno vi si sia dedicato, è vero che l'attività può subire danni rilevanti se si verificano eventi imprevisti nel reparto IT.

Non importa quali siano le cause del mancato funzionamento dei sistemi - un attacco virus, un bug del software o un guasto hardware -, le conseguenze sono quasi sempre le stesse: ore o perfino giorni di inattività e potenziale perdita di quantità incalcolabili di lavoro. Se, tuttavia, si dispone di un backup recente e di un piano di ripristino ben organizzato, l'impatto economico e produttivo può ridursi notevolmente.

Naturalmente, organizzare una strategia di backup e ripristino adeguata ha un costo in termini di tempo e denaro e spesso non viene considerata un'attività prioritaria, specialmente se si è occupati ad amministrare e a far crescere l'azienda. Poiché siamo a conoscenza di questo presupposto, l'intento su cui si fonda questa guida è il tracciare a grandi linee i passi da compiere, esaminando gli aspetti principali che devono essere considerati e analizzando le potenziali conseguenze di un'inattività del sistema rispetto all'azienda.

## Cosa proteggere?

Vanno definite in prima istanza le aree aziendali che necessitano della maggiore protezione e, soprattutto, quale sia il tempo massimo accettabile per riportare tali aree in attività qualora si verificasse un'emergenza. Se, ad esempio, ci fosse un guasto nel sistema dei pagamenti, potrebbero essere sufficienti - e accettabili - due giorni, ma qualora fosse il reparto di fatturazione e ricezione ordini a subire un danno, le conseguenze si ripercuoterebbero su tutto il flusso di cassa.

È bene poi analizzare quali sistemi proteggere nell'ambito di ogni funzione aziendale e dare la corretta priorità alle distribuzioni, in modo da ottimizzare i benefici. Ad esempio, si deve scegliere di effettuare il backup di tutto il reparto HR, o si può risparmiare tempo proteggendo soltanto i documenti e i file di dati, presupponendo che sia poi possibile reinstallare da zero Windows e ogni altra applicazione richiesta? Oppure, qualora gli utenti archivino i propri file su un server condiviso o un'applicazione di archiviazione (e se si esegue il backup di tali server), vale la pena pianificare anche il backup dei singoli PC?

Solo chi l'ha creata sa quali sono le migliori decisioni per la propria azienda. Come regola generale, tuttavia, è meglio un backup in più che uno in meno. Si può presupporre, ad esempio, che tutti salvino il proprio lavoro sul server, ma gli utenti avranno comunque delle copie in locale, che utilizzano ad esempio soprattutto se parte delle loro attività si svolge in viaggio. Anche i timori rispetto alle prestazioni, o una sorta di mancanza di fiducia nel server, possono far sì che gli utenti tengano copie locali del loro lavoro, che saranno quelle inevitabilmente più aggiornate e causeranno i maggiori problemi in caso di perdita. Le analisi degli analisti affermano infatti che oltre il 60% dei dati aziendali viene conservato sulle workstation; si tratta di un dato che vale la pena tenere a mente.

Occorre inoltre considerare il tempo che sarà necessario per effettuare il ripristino in caso di emergenza, ovvero quello che gli esperti del settore definiscono "obiettivo di ripristino in termini di tempo", o RTO (Recovery Time Objective). In alcuni casi la possibilità di ripristinare un sistema in pochi minuti è critica per l'azienda, quando ad esempio si verifica un guasto nel sito Web, nell'applicazione di posta elettronica o nel server principale dei database. È chiaro che il processo richiederà senz'altro tempi più lunghi se bisogna ricaricare il sistema operativo e poi il programma di backup per poter avviare il ripristino. È molto meglio disporre del backup dell'intero server, che sarà sempre pronto per essere ripristinato.

### Il costo reale dell'inattività

*Il costo dell'inattività non è facile da calcolare, ma è sempre alto e non solo in termini puramente finanziari. Considerate i tre esempi seguenti:*

- **Il server web si arresta, anche solo per un'ora:** gli ordini vanno persi, i clienti passano ai siti dei concorrenti e la reputazione aziendale si incrina.
- **Exchange va in crash e si perdono email importanti:** ci vogliono giorni per trovare e reimmettere le vecchie copie cartacee, ricostruire le mailing list e ripristinare il sistema esattamente al punto in cui si trovava prima dell'arresto. Clienti e partner sono infastiditi e i dipendenti frustrati perché non possono lavorare in modo efficiente.
- **Un virus trojan colpisce la cassa del negozio online, ed è necessario reinstallare il software** – lo staff del supporto deve fare gli straordinari per recuperare ed è costretto a tralasciare altre attività. I dipendenti sono obbligati a tornare ai sistemi manuali e la fedeltà del cliente è ridotta al limite.

*Backup non significa soltanto poter annullare l'eliminazione dei file accidentalmente spostati nel cestino. Significa poter ripristinare i sistemi dopo qualsiasi tipo di emergenza, sia essa un attacco virus, un errore del software o un guasto hardware, e ridurre al minimo l'impatto sulla produttività aziendale.*

## Glossario – Backup di un'immagine

*L'approccio classico al backup prevede la copia di ogni singolo documento e file dal server o dal PC sui quali risiedono al supporto di backup. Sebbene dipenda dal sistema di file host, è necessario un software speciale che gestisca i file utilizzati al contempo da altre applicazioni, e può rivelarsi molto esigente in termini di tempo.*

*La tecnologia di imaging del disco, originariamente concepita per "clonare" i PC, consente di superare queste problematiche acquisendo un'istantanea, o «immagine», del disco rigido. Poiché l'immagine viene creata a livello di blocco, non ha nessuna dipendenza a livello di file e può essere molto più veloce del tradizionale approccio file per file. Evita inoltre i problemi legati ai file aperti e può aiutare a semplificare il ripristino d'emergenza.*

*I backup basati su immagine sono una soluzione molto diffusa e offrono protezione senza limitare la flessibilità, consentendo anche il ripristino di un numero esiguo di documenti eliminati.*

Il ripristino di una singola workstation, d'altro canto, potrebbe non essere così importante, ma è sorprendente quanto tempo possa richiedere se non si dispone di un'adeguata protezione del backup. Per ricaricare solo Windows può essere necessaria almeno un'ora, senza contare la ricerca dei dischi che occorrono per reinstallare Office e le altre applicazioni, e il tempo che serve per ritrovare i codici di licenza, reimmettere le password dei vari account e modificare ogni altra impostazione. Il personale specializzato sarà tenuto per ore o addirittura giorni a dedicare il proprio tempo alla ricostruzione dei PC danneggiati, e tutto ciò avrà comunque un effetto domino, perché l'attività potrebbe rivelarsi costosa tanto quanto l'indisponibilità del server, senza parlare delle conseguenze in termini di inattività che tutto questo ha per il dipendente che per qualche giorno resterà senza PC.

## Con quale frequenza?

Quando si considera cosa sottoporre a backup, è bene riflettere anche sulla frequenza con cui sarà necessario eseguire l'attività. Da molti anni è ormai pratica comune effettuare un backup quotidiano, in genere durante la notte, quando l'utilizzo dei sistemi è ridotto, evitando così i conflitti tra file aperti e riducendo l'impatto su altre tipologie di elaborazione. Questo approccio si va rivelando

tuttavia inappropriato, poiché ormai i sistemi IT sono concepiti per lavorare quasi ininterrottamente. A questa considerazione va aggiunto il fatto che i backup notturni possono risultare obsoleti fino a 24 ore, e come conseguenza si rischia di perdere un intero giorno di lavoro, magari a causa di semplici inezie. I backup notturni non devono comunque essere trascurati perché rappresentano una forma di protezione basilare di cui è bene disporre. I più innovativi prodotti di backup integrano tecnologie che consentono di eseguire più spesso i backup, in genere con un impatto minimo in termini di prestazioni e di spazio necessario per archiviare le copie.

Ne è un esempio l'impiego della tecnologia che crea un'immagine del disco. Questa innovazione, se combinata con altre, può consentire l'esecuzione di backup orari.

## Da dove iniziare?

Non ci sono regole fisse e immutabili, ma esistono alcuni punti critici sui quali soffermarsi quando si progetta la strategia di backup per una piccola azienda.

**Risorse condivise** – Si inizia con i server e con le altre risorse condivise, quali i dispositivi di archiviazione. Anche se non sono critici per l'attività aziendale, la loro inattività può avere conseguenze su numerosi utenti, ed è pertanto fondamentale poter riportare in funzione questi dispositivi al più presto qualora si verifici qualsiasi tipo di problema. Ed è bene non prendere scorciatoie ed effettuare, se possibile, il backup dell'intero server o dispositivo, perché è questo che consente di risparmiare tempo prezioso quando si tratta poi di passare al ripristino.

**Desktop in rete** – Incoraggiare gli utenti a salvare i propri file nell'archivio condiviso, perché il processo di backup diventa molto più semplice da gestire. Si può inoltre considerare l'idea di incorporare i singoli desktop nella strategia di backup generale, preferibilmente utilizzando strumenti che possono essere amministrati e automatizzati centralmente, piuttosto che lasciare che siano gli utenti a gestirli da sé, poiché la maggior parte non lo farà.

Non c'è un'assoluta necessità di effettuare il backup di ogni elemento, ma questo potrebbe ridurre considerevolmente il tempo di ripristino. Se si sceglie un approccio selettivo, occorre prestare particolare attenzione alla protezione delle e-mail, in particolare nei casi in cui gli utenti scaricano la loro posta in un archivio dei messaggi locale nel disco rigido del proprio PC.

**Computer portatili** – Quando gli utenti trascorrono gran parte del loro tempo fuori dall'ufficio non è sempre pratico salvare ogni cosa in un archivio condiviso. In questo caso è importante individuare procedure che consentano di effettuare i backup e i ripristini conseguenti a delle emergenze in modalità non linea. Due aspetti importanti in questa situazione sono la semplificazione della gestione del processo per gli utenti dei notebook (teoricamente non dovrebbero essere affatto coinvolti e neanche consapevoli che questo avviene) e il supporto da utilizzare, aspetto questo che verrà analizzato in dettaglio a breve.

**Risorse virtuali** – Non sottovalutare la necessità di effettuare il backup di server e desktop virtuali. L’esecuzione del backup di un server host fisico è un buon punto di partenza, ma per offrire la protezione completa e per ripristinare singole macchine virtuali sono necessari strumenti appositamente progettati per funzionare con le tecnologie di virtualizzazione. Oltre a ciò, va ricordato che si tratta di risorse praticamente uguali a quelle reali e che pertanto è bene sottoporre a backup ogni loro elemento per ridurre il tempo e l’impegno necessario a completare il ripristino quando le cose non vanno come dovrebbero.

**Risorse su host** – Uno dei vantaggi dei servizi di hosting, ad esempio Google Apps o di un servizio Exchange, è che il backup dovrebbe essere effettuato automaticamente. Tuttavia, è bene non darlo per scontato. Occorre infatti verificare attentamente i termini dell’accordo sottoscritto per sapere cosa ci spetta, specialmente quando si tratta di effettuare un ripristino “nel migliore dei tempi possibili” rispetto agli impegni del provider del servizio, che potrebbero non corrispondere agli obiettivi RTO aziendali.

## A proposito dei supporti

A questo punto dovrete aver deciso quali sistemi proteggere con un backup e avere almeno un’idea generica del livello di dettaglio della protezione da applicare. Il passo successivo è quello di confrontare le varie soluzioni offerte e decidere quale è la più idonea alle proprie esigenze. È possibile scegliere tra diverse tecnologie e prodotti, ognuno con i suoi vantaggi esclusivi, che esamineremo più avanti. È sempre bene tenere comunque presente che un’offerta non è necessariamente appropriata in tutto e per tutto, e che l’approccio migliore potrebbe prevedere l’impiego di una combinazione delle diverse proposte. Questa considerazione è valida in modo esemplare per i supporti di backup. Sono ormai passati i tempi in cui il nastro era l’unica opzione disponibile. Questo supporto è ancora molto diffuso, ma è stato largamente superato dal disco, che non solo è più veloce, grazie all’accesso random e non lineare ai dati che contiene, ma è sempre meno costoso, non richiede una strumentazione complessa e offre la capacità necessaria per proteggere i server e le workstation moderne. Naturalmente, i dischi hanno vari formati ed esistono anche altri sistemi di backup. I pro e i contro di ognuno sono ripilogati nella tabella che segue:

**Tabella - Supporti di backup e ripristino a confronto**

Supporto	Pro	Contro	Funzionale per	Non funzionale per
<b>Nastro</b>	Le cartucce sono relativamente economiche. Non è facile sovrascriverle.	Accesso lento e lineare. Le librerie a nastro automatiche possono essere molto costose.	Backup automatico di file server di grandi dimensioni. Archiviazione a lungo termine.	Backup di singole workstation e PC. Ripristino rapido.
<b>CD/DVD</b>	Accesso random. Poco costoso. Praticamente ogni PC dispone di un masterizzatore CD/DVD.	Capacità limitata che obbliga a passare da un disco a un altro per effettuare il backup di grandi quantità di dati.	Backup offline di singoli PC e notebook. Dischi di ripristino avviabili. Archiviazione a lungo termine.	Backup di server.
<b>Scheda di memoria</b>	Facile da gestire e conservare. Non richiede altro hardware speciale oltre a porte USB o schede di memoria.	Facile da sovrascrivere, da danneggiare e perdere. Capacità limitata.	Backup ad hoc di documenti e file di dati importanti.	Backup di server dati di grandi dimensioni. Archiviazione a lungo termine.
<b>Disco rigido esterno</b>	Accesso random e rapido. Costo ridotto.	Facile da sovrascrivere. Non facile da trasportare.	Backup automatico di server e workstation in rete.	Backup of large data servers. Long term archiving.
<b>Archivio di rete</b>	Accesso random e rapido. Costo ridotto.	Facile da sovrascrivere.	Backup automatico di server e workstation in rete.	Archiviazione a lungo termine.
<b>Archivio online</b>	Risorsa gestita esternamente.	Prestazioni del backup e del ripristino limitate dalla larghezza di banda di Internet.	Backup di notebook di utenti mobili.	Backup/ripristino di server.

## Glossario – Deduplicazione dei dati

*Quando si parla di backup i compromessi sono inevitabili. Se si crea il backup di tutti gli elementi, lo spazio di archiviazione si esaurisce in breve tempo. Se si opera una selezione, si tralascerà senz'altro qualcosa di essenziale.*

*La compressione può essere d'aiuto, ma la tecnologia di cui oggi tutti parlano è la deduplicazione, che consente di archiviare una sola copia dei dati, indipendentemente da quanti doppioni vi siano. La maggior parte dei file necessari per Windows, ad esempio, è la stessa su ogni PC, perciò è abbastanza inutile fare il backup di ciascuna singola copia del programma. Ancora meglio se il software di backup può salvare una sola copia di ciascun file e impostare un puntatore a quella posizione valido per i backup successivi.*

*Un numero sempre maggiore di prodotti di backup supporta la deduplicazione a livello di file e in alcuni casi a livello di blocco, consentendo un notevole risparmio sui costi di storage e sul tempo necessario ad eseguire i backup, senza avere impatto sulla possibilità di ripristinare singoli file o sistemi completi nel caso in cui sia necessario.*

In questo senso un consiglio valido è quello di suddividere il rischio e di utilizzare per i backup più di un supporto. Una soluzione diffusa è quella di effettuare backup istantanei su dischi rigidi di rete o connessi in locale e quindi di utilizzare il nastro o altri supporti ottici (CD/DVD) per l'archiviazione a lungo termine. Un altro approccio prevede l'esecuzione simultanea dei backup su supporti doppi, ad esempio in archivi di rete e online, per garantire ulteriore protezione e flessibilità.

È bene inoltre fare in modo che i backup siano a portata di mano nel momento in cui sono necessari. Non riporre i nastri o i dischi di backup in un cassetto né lasciarli nel server che esegue il programma di backup. Occorre invece definire delle procedure per far sì che siano correttamente etichettati e archiviati in una posizione sicura, dove siano reperibili in modo rapido. Qualora sia possibile, far sì che le copie non vengano conservate in sede e, se i backup vengono salvati in un dispositivo di archiviazione, considerare l'idea di creare un secondo livello di backup, e di archivarlo altrove.

## Passaggi successivi

Nella fase finale vengono scelti i prodotti di backup da utilizzare. Ce ne sono molti in circolazione, ed è bene organizzare delle dimostrazioni o delle prove nella propria sede aziendale. In questo modo si può verificare esattamente quanto siano facili da utilizzare - tanto dagli esperti quanto dai principianti -, se forniscono il livello di protezione ricercato e se soddisfano o meno gli obiettivi RTO aziendali.

Dopo di che, si tratta solo (solo?) di installare e distribuire i prodotti selezionati. Ci sarebbero in realtà un paio di consigli finali, il primo dei quali è di testare i backup per essere sicuri che funzionino. Creare un backup non equivale ad essere in grado di ripristinarlo dopo un'emergenza, e non è insolito che alcune aziende eseguano quasi religiosamente tutte le attività di backup, giorno dopo giorno, solo per scoprire che i backup non sono utilizzabili o, peggio ancora, sono completamente vuoti quando arriva il momento di doverli utilizzare per effettuare il ripristino.

L'altro suggerimento è quello di documentare la strategia di backup e ripristino e tutte le procedure correlate. Non basta affidarsi a singole persone che "sanno" cosa fare. Se qualcosa deve andare male, lo farà, e succederà sempre quando la persona incaricata del ripristino è malata o in vacanza. È bene scrivere dettagliatamente le procedure, includendo il numero dei backup da eseguire, il supporto da utilizzare, le convenzioni di denominazione, l'organizzazione degli archivi e così via. Lo stesso vale per il ripristino, e bisogna anche accertarsi che le persone interessate leggano i documenti. Infine, le informazioni devono essere capillarmente diffuse e le procedure prontamente accessibili, su carta e in formato elettronico: insomma, non lasciatele in una cartella del server. In parte perché nessuno penserà di andarle a cercare lì, e in parte perché se il server si guasta... Ecco perché è indispensabile creare come prima cosa un piano di ripristino...

## Informazioni su Acronis®

Acronis è leader mondiale nella produzione di soluzioni per il backup in sede e in remoto, il ripristino d'emergenza e la sicurezza. La tecnologia brevettata per la gestione e l'imaging del disco consente alle organizzazioni e ai singoli utenti di proteggere le risorse digitali in ambienti fisici e virtuali. Grazie ai prodotti software di Acronis per il backup, il ripristino, il consolidamento del server e la migrazione delle virtualizzazioni, gli utenti proteggono le proprie informazioni digitali, favoriscono la continuità aziendale e riducono i tempi di inattività. I prodotti e le soluzioni Acronis sono distribuiti in oltre 180 paesi e disponibili in 13 lingue. Per ulteriori informazioni, visita <http://www.acronis.it>. Segui Acronis su Twitter: <http://twitter.com/acronis>.



Per ulteriori informazioni, visitare l'indirizzo <http://www.acronis.it>

Per acquistare i prodotti Acronis, visitare l'indirizzo [www.acronis.it](http://www.acronis.it) o cercare online un rivenditore autorizzato.

Altre informazioni sulle sedi Acronis sono reperibili all'indirizzo:  
<http://www.acronis.it/company/worldwide.html>

Copyright © 2000-2010 Acronis, Inc. Tutti i diritti riservati. "Acronis", "Acronis Compute with Confidence" e il logo Acronis sono marchi Acronis, Inc. Windows è un marchio registrato di Microsoft Corporation. Gli altri nomi menzionati possono essere marchi o marchi registrati dei rispettivi titolari. Soggetto a modifiche tecniche. Le immagini potrebbero non corrispondere al prodotto reale. Si declina qualsiasi responsabilità per possibili errori. 2010-03