L'angolo dell'informatica

Una tecnica indispensabile per quanto ancora scarsamente diffusa

Il backup per non perdere le informazioni digitali

di Marco Manenti

Il nostro lavoro ci porta, ogni giorno, a dover gestire informazioni digitali di ogni genere. Testi, fogli di calcolo, dati contabili, immagini, e-mail. Buona parte del nostro mondo, non ultimo il nostro "patrimonio aziendale", è ormai immateriale, volatile. Possiamo usufruirne ovunque siamo, trasportarlo su microscopiche chiavette USB. Trattandosi di una rivoluzione abbastanza recente però non abbiamo ancora avuto la possibilità di abituarci a gestire la conservazione di queste informazioni. A differenza dei contenuti cartacei, fisici, riguardo ai quali siamo preparati alla (o almeno consci della) eventualità di subire danni irreparabili (abbiamo da poco ricordato i 50 anni dell'alluvione di Firenze), per l'informazione digitale non abbiamo ancora preso le dovute cautele. Non abbiamo ancora la necessaria sensibilità.

Marco Manenti

Il rischio di perdere le fotografie dal proprio telefono è all'ordine del giorno, basta una distrazione o un click di troppo, mentre pochi anni fa sarebbe stato necessario bruciare un negativo oppure stracciare un foglio. Gesti totalmente differenti ma dai risultati identici, con la differenza che una fotografia stracciata può essere incollata, mentre una memory card cancellata è potenzialmente persa[1].

Come difendere il patrimonio "informazione"?

Analizziamo prima le varie casistiche nelle quali possiamo rischiare di perdere le nostre informazioni: errore umano (file cancellato o peggio, sovrascritto con informazioni diverse), errore informatico (file corrotto dal software causato da un errore di programmazione; file cancellato o perso o sovrascritto dal software), danno hardware (supporto di memorizzazione rotto), evento atmosferico (blackout, scariche elettriche, allagamento), dolo (virus, malware o ramsonware [2]).

1. Nel caso dovesse succedere, mettetela da parte e portatela da uno specialista o provate a recuperare i dati. L'importante è non usarla per scattare altre foto. Cancellare la memoria solitamente significa cancellare l'indice delle foto (dei file) memorizzati, non i file stessi. http://www.cgsecurity.org/wiki/PhotoRec_Passo_Dopo_Passo

2. software malevolo particolarmente infame, non cancella l'informazione ma la codifica, chiedendo un riscatto per la decodifica. Si rimane in possesso dei propri dati, ma non si possono utilizzare.

L'unico metodo per evitare di perdere le nostre informazioni è il backup, ovvero la replicazione dei dati. Questa tecnica purtroppo però è ancora scarsamente diffusa perché - erroneamente - ritenuta inutile, dispendiosa, dispersiva. Spendere (leggasi: investire) qualche centinaio di euro per duplicare dati è tuttora considerato opzionale, fino al momento in cui si rende necessario spenderne migliaia per tentare di recuperare i dati persi o dover pagare gli straordinari ai propri dipendenti per ricaricare bolle, fatture o dichiarazioni dei redditi.

Esiste anche una normativa che rende necessaria la pianificazione di misure minime di sicurezza e l'obbligo del loro utilizzo nel trattamento dei dati (Il D.L. 30 giugno 2003 n. 196).

E' quindi doveroso sottolineare a chi ha scarsa dimestichezza con il computer che dovrà essere consigliato ed assistito da un tecnico esperto. Il faida-te, in questi casi, è sconsigliato. Darebbe solo una falsa sensazione di sicurezza, creando potenziali danni.

Esistono poche ma chiare regole per i backup. Devono essere periodici, verificati e separati.

Periodici: i salvataggi devono essere effettuati con tempistiche programmate. Occorre che ad intervalli regolari i propri dati siano messi al sicuro. Una volta al giorno, almeno.

Verificati: non sappiamo se i backup siano stati effettivamente eseguiti fino a quando non ne verifichiamo l'integrità. A intervalli regolari occorre controllare la corretta esecuzione della copia di riserva, perché bisogna aver fiducia dei propri salvataggi [3].

Separati: i salvataggi non servono solamente a preservare i dati in seguito ad errori umani. Senza scomodare eventi catastrofici, basta un corto circuito o un furto per rischiare di perdere i supporti contenenti i back-up. Buona regola é salvare i dati e conservare le copie in luoghi diversi.

Come fisicamente effettuare i back-up? Le vecchie modalità sono ancora attuali: i salvataggi su nastro possono garantire senza particolari difficoltà il rispetto delle tre precedenti caratteristiche, con costi attualmente contenuti. Utilizzare un nastro diverso per ogni giorno della settimana più uno completo da tenere in un altro luogo (a casa, magari) è una buona idea. Possibilmente con la verifica dei dati scritti sul supporto ad ogni salvataggio eseguito.

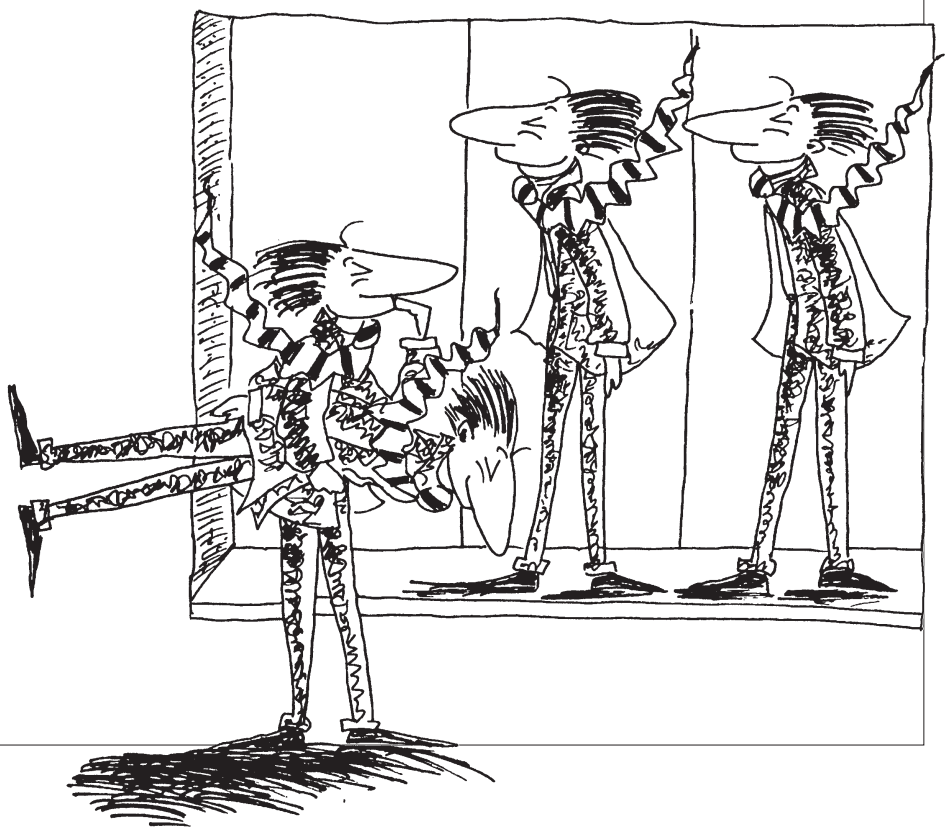
Esiste inoltre il backup remoto: archiviare i propri documenti su un supporto dislocato in un altro locale oppure su internet può essere utile, ma attenzione alla velocità del collegamento e al rispetto della normativa sulla privacy (i contenuti dovranno essere codificati) [4].

Usare con la dovuta cautela i supporti estraibili: sono molto fragili (non sono nati per questo), meglio solo come backup secondario (oppure per poter conservare l'archivio in altro luogo).

Una cosa da evitare assolutamente è salvare i dati sullo stesso supporto dei dati stessi, men che meno se i salvataggi sono visibili in tutta la rete dell'ufficio. Lasciarli sullo stesso disco fisso, sullo stesso pc è quantomeno pericoloso.

Volendo utilizzare al meglio le soluzioni a nostra disposizione è possibile, tramite la virtualizzazione [5], effettuare la copia dell'intero sistema operativo, per poter recuperare immediatamente il server contenente tutte le informazioni, in caso di bisogno, in pochissimo tempo. Non protegge solamente dalla perdita dei dati ma anche dalla rottura fisica del server. In poco tempo è possibile recuperare e rendere operativo il server defunto, dati compresi.

L'utilizzo della virtualizzazione in-



3. Predisporre un piano di disaster recovery, ovvero: cosa fare se improvvisamente dovesse guastarsi un computer? Possiamo permettercelo? Contiene informazioni recuperabili?

4. Tra i vari software rsnapshot (open source / solo per linux) è uno strumento comodo. Permette l'archiviazione remota dei file, aggiornando solo i documenti modificati per velocizzarne il trasferimento. Particolarmente comoda la possibilità di archiviare ad intervalli regolari, potendo recuperare i dati a seconda dei momenti in cui è avvenuto il salvataggio.

5. Tramite la virtualizzazione un software rappresenta virtualmente un elaboratore nel quale far funzionare un sistema operativo. Un singolo computer è quindi in grado di ospitare più sistemi operativi contemporaneamente, di duplicarli (e pertanto salvarli) e trasferirli molto più agevolmente rispetto ai sistemi non virtualizzati.

troduce un nuovo metodo di backup, anzi un nuovo metodo di operatività. La virtualizzazione in cluster, oppure in cloud. Semplificando, ed esemplificando: due o più server fisici ospitano il gestionale ed effettuano ogni sera un salvataggio completo. Nel caso di un guasto fisico di un server, l'altro manterrà in linea il gestionale, senza perdita di dati o di tempo-lavoro. Nel caso di un problema sui dati, sarà immediatamente possibile rimettere in funzione l'ultimo salvataggio disponibile (e considerato valido). Nel momento in cui risulta necessario rinnovare i server sarà possibile farlo, sempre senza fermo macchine e problemi, aggiungendo al cluster (gruppo) i nuovi server e - terminata la migrazione - rimuovendo i vecchi. Questa struttura potrà essere gestita presso lo studio oppure presso un soggetto terzo, che curerà la manutenzione hardware (attenzione sempre alla normativa sulla privacy!).

Diverso è il cloud (nuvola). Con il cloud si perde la proprietà dell'hardware e si passa al noleggio di "unità di elaborazione". Il gestionale sarà ospitato in una infrastruttura per cui serve decidere solamente la potenza di calcolo che si vuole utilizzare, possono trattarsi di 10 server come di 1.000, pagando in base al consumo, come il noleggio dell'auto. Non occorre neppure preoccuparsi dell'obsolescenza dell'infrastruttura. Tramite il cloud è possibile accedere ai propri dati esclusivamente online. Attenzione però, occorre valutare caso per caso, non è consigliabile per tutti (si pensi agli studi dislocati in zone scarsamente coperte da decenti collegamenti ad internet). Ulteriore "salto di fede", si perde il controllo dei propri dati e, anche per quanto riguarda la riservatezza, occorre scegliere con giudizio chi offre il servizio di cloud.

Alcune raccomandazioni finali:

Programmare i salvataggi in modo tale da eseguirli una volta al giorno (possibilmente la notte) e conservare tali salvataggi per almeno 7 giorni. Conservare un backup giornaliero affinché diventi un salvataggio settimanale, ogni settimana, ottenendo quindi 4 salvataggi settimanali. Infine conservare un salvataggio settimanale affinché diventi un salvataggio mensile, ogni mese, ottenendo quindi 12 salvataggi mensili.

Se possibile evitare soluzioni proprietarie oppure poco diffuse. Nel caso di rottura del supporto fisico (es. lettore del nastro) potrebbe un domani risultare impossibile trovare ricambi, oppure nel caso di malfunzionamento del software (o aggiornamento del sistema operativo) potrebbe risultare impossibile accedere ai dati archiviati.

Se possibile "congelare" gli archivi ad intervalli regolari, anche ogni 3-6 mesi, masterizzandoli su dvd. Un domani poter recuperare un documento che, modificato, è stato sostituito anche nei salvataggi periodici, potrebbe essere utile.

In ultimo, prevedere una copia di tutto ciò che necessariamente dobbiamo avere sempre a portata di mano. L'ambiente entratel ed intraweb, ad esempio.

Ma soprattutto, come sempre, tanto, tanto buonsenso. Perché, secondo la ben nota legge di Murphy, se qualcosa può andar male, lo farà. E solitamente sempre a ridosso di una importante scadenza.

Marco Manenti
Dottore Commercialista