BACKUP E DISASTER RECOVERY

Il salvataggio dei dati è uno degli adempimenti fondamentali di ogni azienda, anche in assenza degli obblighi stabiliti dal Codice Privacy, perché vi permette di avere, su un supporto esterno al vostro computer, l'ultima "fotocopia" in formato elettronico dei vostri dati. Ciò vi salvaguarda sia dal punto di vista economico che da quello lavorativo.
Quelle che conoscete meglio sono sicuramente le procedure di salvataggio periodiche (**Backup**) e le corrispondenti procedure di ripristino (**Restore**) ma, a fronte di gravi emergenze, siete obbligati a ricorrere a procedure che vi garantiscano l'erogazione dei servizi al più presto possibile (**Disaster Recovery**).
Ad esempio, se avete cancellato inavvertitamente un file, potrà essere sufficiente ripristinarlo dall'ultimo Backup tramite la procedura di Restore. Ma, se il vostro computer è guasto, attiverete la procedura di Disaster Recovery, che dovrà evidentemente prevedere cosa fare in queste occasioni.

BACKUP E RESTORE

Il **Backup** o copia di sicurezza è la procedura di salvataggio periodico dei dati, effettuata su un supporto diverso dalla memoria del vostro computer. Essa consiste normalmente nel lancio di un programma utente che può richiedere l'esecuzione di alcune operazioni manuali e/o automatiche.
Le principali funzionalità di un programma di backup sono:

- **copia immagine** (*disk image*): l'hard disk del computer o del server viene copiato integralmente, compreso il file system, su un altro disco fisico o virtuale, in modo tale da poter essere replicato su altri computer, ad esempio per un'installazione aziendale.
- **copia integrale** (*full backup*): vengono copiate tutte le directory ed i files dell'hard disk del computer o del server su un altro supporto, normalmente nastri magnetici o Cd-Rom;
- **copia selettiva** (*partial backup*): vengono copiate solo le directory e/o i files che rientrano nei parametri di selezione (nome, data, tipo, dimensioni, autore, ecc.) su un altro supporto, normalmente Cd-Rom o Pen-key;

Ogni copia integrale o selettiva può essere distinta in funzione della struttura dei dati salvati:

Struttura fisica

- **Copia normale** (*flat backup*): è utilizzata esclusivamente per il salvataggio di directory e/o files così come sono, senza riduzione di spazio occupato nei supporti di backup;
- **Copia compressa** (*compressed backup*): vengono creati e salvati in uno o più files in formato compresso le directory e/o i files, riducendo lo spazio occupato nei supporti di backup;
- **Copia sicura** (*security backup*): vengono copiate le directory e/o i files in formato crittografato con la possibilità di inserire una password per la successiva apertura in lettura e/o scrittura.

Struttura logica

- **Copia originale** (*real backup*): ogni copia è l'immagine dei files alla data del salvataggio
- **Copia differenziale** (*odds backup*): ogni copia, successiva al primo *full backup*, contiene le modifiche effettuate rispetto ad esso, con il vantaggio di ridurre i tempi di backup ma lo svantaggio di aumentare lo spazio ad ogni backup in caso di frequenti modifiche;
- **Copia incrementale** (*buildup backup*): ogni copia, successiva al primo *full backup*, contiene tutti i files che hanno subito modifiche, con il vantaggio, rispetto all'*odds backup*, di ridurre ulteriormente i tempi di backup ma lo svantaggio di aumentare i tempi di restore.

Ogni nuova copia integrale o selettiva, per salvaguardare la vita del supporto e quindi l'integrità dei dati, deve essere effettuata sostituendo il supporto fisico precedentemente utilizzato.
Esistono diversi metodi di sostituzione dei supporti, ma tutti si basano sulla rotazione dei supporti. Il più semplice è quello detto **parentale** o nonno, padre, figlio, che consiste nell'utilizzare tre supporti, uno per ciascuna copia: quando si deve sostituire la terza copia si ricomincia dalla prima. In questo modo, oltre alla copia più recente, avrete sempre a disposizione le due precedenti.

Il **Restore**, o ripristino, è la procedura di ripristino dei dati dai supporti salvati con la procedura di backup. Le sue funzionalità sono conseguenti al metodo adottato in fase di salvataggio e devono essere integrate nella procedura di **Disaster Recovery**.

La data e l'orario di salvataggio e di eventuale ripristino saranno decisi tenendo presente le esigenze organizzative dell'azienda, in modo tale da ridurre al minimo le interferenze con l'attività lavorativa. Se il backup è giornaliero l'esecuzione sarà serale o notturna, se settimanale avverrà di sabato o domenica, ecc. Esistono alcuni sistemi che effettuano una copia istantanea, cioè durante la fase di scrittura delle vostre modifiche: ciò non vi esenta dall'esecuzione periodica del backup.

Il Codice Privacy stabilisce, nell'Allegato B, che il Backup deve essere eseguito almeno con cadenza settimanale. Con il Provvedimento del 27 novembre 2008, il Garante ha stabilito che, per le sole aziende che trattano i dati personali esclusivamente per fini contabili ed amministrativi, il salvataggio può essere mensile e può riguardare le sole modifiche (copia differenziale o incrementale).

Il backup, qualunque sia la struttura fisica e/o logica delle copie di salvataggio ed il metodo di sostituzione dei supporti, dovrà essere il più possibile adatto alla realtà della vostra azienda e dovrà essere descritto in un apposito documento di qualità.

Se desiderate approfondire le vostre conoscenze sulle procedure di Backup e Restore, vi consigliamo di visitare i seguenti siti:

http://support.microsoft.com	per i sistemi Windows;
http://support.apple.com	per i sistemi Mac;
http://www.pluto.it	per i sistemi Linux.

DISASTER RECOVERY

Il **Disaster Recovery**, o ripristino del livello di servizio a seguito di gravi anomalie, è l'insieme delle misure tecnologiche ed organizzative atte a ripristinare dati, sistemi ed infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze. Esso è parte di un accordo, noto come ***SLA*** (***Service Level Agreement***), tra l'Information Tecnology o l'Amministrazione del Sistema e gli altri reparti aziendali od un'azienda esterna (*outsourcing*).
Lo *SLA* definisce i vari livelli di servizio fornito, relativi alla qualità delle linee di comunicazione interne ed esterne, all'efficienza dei server e dei client (i computer su cui lavorate), alla funzionalità del software installato, ecc. Per ognuno degli elementi precedentemente citati, sono riportati nello *SLA* i tempi medi e massimi di risoluzione delle emergenze a fronte di un intervento tecnico che, per le anomalie gravi, deve essere preceduto da un piano di Disaster Recovery.
Per definire un piano di Disaster Recovery occorre innanzitutto definire la criticità dei sistemi e delle applicazioni. La distinzione è, di norma, effettuata tra sistemi:

- **essenziali**: le funzioni possono essere eseguite solo su strumenti con le stesse caratteristiche, non possono essere sostituite da operazioni manuali ed i tempi di ripristino non possono essere superiori alla giornata lavorativa;
- **critici**: le funzioni possono essere eseguite su strumenti con le stesse caratteristiche oppure sono sostituibili con operazioni manuali a costi elevati ed il ripristino è effettuabile entro la settimana lavorativa;
- **non essenziali**: le funzioni possono essere eseguite su strumenti con caratteristiche analoghe oppure sono sostituibili con operazioni manuali a costi tollerabili ed il ripristino può avvenire entro le due settimane lavorative;
- **non critici**: le funzioni possono essere sostituite integralmente da operazioni manuali a basso costo ed i tempi di ripristino non sono superiori al mese lavorativo.

La stessa distinzione va fatta per ognuna delle applicazioni installate.

Successivamente è necessario analizzare le possibili anomalie gravi, iniziando da quelle conseguenti a possibili disastri ambientali, come terremoti, alluvioni, blackout energetici, terrorismo, ecc. e proseguendo con quelle più strettamente legate all'hardware ed al software.

A questo punto è possibile metter mano al piano di Disaster Recovery, tenendo presente che prevedere il ripristino delle funzionalità dell'Information Tecnology dell'azienda è una parte importante, ma non esclusiva, dello stesso.

Vediamo ora alcune delle possibilità che la tecnologia offre alle piccole e medie aziende ed ai professionisti che utilizzano almeno un server su cui salvare una copia (replica) di tutti i sistemi e le applicazioni che utilizzano normalmente.
Le tipologie sono essenzialmente:

Replica sincrona
La modifica effettuata su un client (un vostro computer) viene scritta nell'hard disk principale del server e, contemporaneamente, nell'hard disk secondario. Fino a quando il sistema non ha terminato di scrivere su entrambi i supporti, l'applicazione rimane sospesa.
L'hard disk secondario può essere fisicamente installato nello stesso server, o in un secondo server, dislocato nella stessa sede o in una sede secondaria. Dal punto di vista della sicurezza dei dati è evidente che la dislocazione in una sede secondaria offre maggiori garanzie rispetto a quelle offerte dalla dislocazione nella stessa sede, riducendo notevolmente eventuali rischi ambientali. La distanza massima tra i server deve essere compresa tra i 50 ed i 150 Km., per motivi di sincronismo.

Replica asincrona
La modifica effettuata su un client viene scritta nell'hard disk principale del server e quindi inviata all'hard disk secondario. Quando il sistema ha terminato di scrivere sul primo supporto, l'applicazione può continuare. Quando anche la scrittura sull'hard disk secondario è terminata il sistema riceve un messaggio di esito positivo o di errore. In quest'ultimo caso il sistema innesca la procedura di correzione dell'errore, riallineando le copie.
L'hard disk secondario è normalmente installato ad una distanza che può essere anche di diverse migliaia di Km., utilizzando una linea telefonica dedicata o Internet, rendendo minimi i rischi ambientali.

Replica a tecnica mista
Il sistema utilizza due o più server secondari: sul primo viene utilizzata la replica sincrona e sugli altri quella asincrona.
Quando esiste una rete nazionale, continentale o transcontinentale, utilizzando questo metodo si aumenta notevolmente la sicurezza del sistema.

Se non disponete di un server, preoccupatevi di definire una buona procedura di backup, di eseguirla con una frequenza adatta alle vostre esigenze e di conservare i supporti delle copie in un luogo sicuro, possibilmente lontano dalla vostra Sede Operativa.

Il Codice Privacy stabilisce, nell'Allegato B, che il piano di Disaster Recovery deve essere descritto in un documento aziendale, allegato al DPSS o al DSSS, se richiesto, controllato ed aggiornato periodicamente.

Qualunque sia la vostra struttura, è molto importante che esca dalle precedenti analisi un piano di Disaster Recovery che sia comunicato a tutte le persone coinvolte nello stesso, comprensibile ad ognuno di essi, ciascuno per le proprie competenze, e verificato periodicamente sul campo con serie simulazioni.

Se desiderate approfondire le vostre conoscenze sulle procedure di Disaster Recovery, vi consigliamo di visitare i seguenti siti:

www.cnipa.gov.it	per la sicurezza informatica nella Pubblica Amministrazione;
www.clusit.it	per la sicurezza informatica nelle aziende private;
www.csiaf.unifi.it	per il Service Level Agreement
www.disaster-recovery-guide.com	per il Disaster Recovery Plan (in lingua inglese).