Backup e Disaster Recovery: Obbligo di legge

L'era digitale è l'era dei **dati**. I nuovi protagonisti sono spesso custodi di importanti informazioni che rivestono per una qualsiasi azienda un'importanza spesso vitale.

Altrettanto vero e concreto è il rischio di perdere o vedersi danneggiati i sistemi fisici preposti alla **memorizzazione**. Basta un virus, un guasto o un semplice **attacco informatico** perché milioni di dati possono essere per sempre resi inaccessibili.

Lo scenario che allora si prospetterebbe potrebbe essere più o meno drammatico a seconda del danno. Provate a pensare alla vostra azienda che ha appena perso dati essenziali relativi a un progetto, a dei clienti o addirittura all'amministrazione.

Per evitare queste spiacevoli quanto probabili circostanze è bene effettuare sempre un backup dei dati con una certa **periodicità** , in corrispondenza delle necessità aziendali.

Diversi sono i fattori che possono concorrere alla **pianificazione** dello storage di sicurezza delle informazioni digitali aziendali. Sicuramente bisogna partire da una stima abbastanza dettagliata della **quantità di dati** in gioco e dei centri aziendali che maggiormente contribuiscono al loro **incremento**.

Il backup può quindi essere progettato in aderenza a queste specifiche. Oltre questo è bene pensare al tipo di **supporto** da utilizzare, dall'**importanza relativa** dei dati, ai **costi di perdita e a quelli di memorizzazione** sia in termini economici che tempistici.

Fin qui ben poche le novità se non un semplice **monito** che ogni tanto è bene fare. L'aspetto che può, invece, più facilmente sfuggire alle aziende italiane sono gli obblighi di legge imposti a chiunque abbia dati in forma digitale da gestire. In particolare le prescrizioni riguardano i dati personali e sensibili, entrambi molto frequenti e diffusi. L'art. 31 del D.lgs 196/2003 dice infatti:

I dati personali oggetto del trattamento sono custoditi e controllati [...] in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di **distruzione o perdita, anche accidentale**,*…*

I chiari riferimenti all'adozione di misure specifiche per la memorizzazione preventiva (back-up) dei dati non si concludono in questa norma di carattere generale. Infatti l'art. 34 comma 1-f del codice autorizza il trattamento con strumenti elettronici solo se sono previste una serie di **misure minime di sicurezza** tra cui:

l'adozione di procedure per la custodia di copie di sicurezza, il **ripristino di disponibilità dei dati** *e dei sistemi.*

Al semplice backup si aggiungono prescrizioni anche sul Disaster Recovery, con riferimento – per i dettagli tecnici – all'allegato B al codice. L'art. 18 del documento impone che il salvataggio abbia almeno frequenza settimanale e l'art. 23 obbliga ad adottare misure di ripristino idonee a rendere i dati nuovamente accessibili nell'arco massimo di sette giorni dal Disaster.

Tutti i provvedimenti presi dall'azienda devono inoltre essere riportati, secondo l'art.19, nel **documento programmatico sulla sicurezza**.

Per concludere questo excursus legislativo è bene ricordare che le misure richieste sono improntate sulla **tutela dei diritti di privacy**, ma per quanto detto è evidente che incontrano anche gli **interessi di tutte le aziende**.