

## **DPS e Basilea II. Incombenze per ogni azienda.**

Quanti problemi hanno dato alla vostra azienda le tanto discusse direttive **BASILEA II** e il **DPS** più volte rinviato?

Alcuni analisti, tra il serio ed il faceto, paragonano il carico di lavoro derivante dalle incombenze relative a questi temi recentemente cadute fra capo e collo degli IT manager con gli aggiornamenti dovuti a suo tempo per il passaggio all'Euro o per il famoso "millenium bug".

Il DPS (che ora ha scadenza a fine 2005) richiede una serie di interventi ai fini di garantire i requisiti minimi aziendali in materia di sicurezza dei dati e protezione della privacy.

*Le direttive BASILEA 2, che sono essenzialmente orientate alla gestione dei rischi operativi e le relative raccomandazioni da parte della Banca d'Italia sono da tempo una fonte di grattacapi anche per le nostre aziende.*

Un dossier Microsoft è dedicato proprio a BASILEA 2 e ricorda che entro il 2007 saranno oltre cinque milioni le imprese italiane che, adeguandosi a quella normativa, dovranno predisporre, oltre a tante altre cose, anche un piano che garantisca una efficiente procedura di **Disaster Recovery**, peraltro richiesta anche dal DPS (Documento Programmatico della Sicurezza, da fare entro il 31/12/2005) e dalla certificazione standard ISO 17799 che a sua volta rientra negli standard richiesti per i sistemi informatici.

Vale la pena notare che tutte queste sigle hanno un denominatore comune: richiedono all'IT Manager una grande attenzione al problema della **business continuity** e alla prevenzione da eventi straordinari (disaster recovery). Alzi la mano chi almeno una volta, magari nel proprio ufficio, non ha visto svanire di colpo lavori, programmi, documenti vari e quant'altro. Ci sono aziende che hanno subito danni colossali e molte hanno rasentato il fallimento per aver trascurato questi temi.

In genere un precedente disastro, in informatica come per ogni altra cosa, spinge o meglio costringe a premunirsi per il futuro ed a valutare il rischio che corre l'azienda (risk assessment).

Per l'Azienda, mantenere costante la propria operatività, la Business Continuità, deve essere un dovere soprattutto in questo periodo di lavoro che scarseggia e con clienti sempre più esigenti.

Parlando con gli IT Manager emerge che non è certo la distrazione e la noncuranza il motivo principale per il quale non si predispongono un piano di Disaster Recovery blindato, ma i costi che non sono mai lievi per la piccola impresa, per cui è necessario trovare un buon compromesso.

E sono appunto i costi che preoccupano chi dovrà omologarsi a BASILEA 2.

**Vediamo come fare una valutazione dei rischi (risk assessment) per un progetto di questo tipo.**

Il modo migliore per giustificare la spesa di business continuity è capire esattamente quanto l'azienda perde durante un blocco dei sistemi, la cosiddetta business impact analysis, e confrontarlo con l'investimento necessario a evitare questa perdita. Le formule possibili possono essere abbastanza semplici.

Calcolata ad esempio la durata media di un blocco dei sistemi, la si moltiplica per il costo orario che l'azienda deve sopportare in casi simili.

Tale costo non deve comprendere solo il salario dei dipendenti che non possono lavorare proprio a causa del blocco, ma anche il fatturato perso e le eventuali penalità per contratti o accordi non rispettati.

***Insomma nella malaugurata ipotesi di un disastro l'investimento per garantire la propria continuità operativa si rivela sempre ben speso (nome in codice di tutto questo ROSI: Return of Security Investment).***