

organizzativa in cui il sistema di servizi opera e che giustifichi ciascuna contromisura in un quadro complessivo.

1.3. Il contesto internazionale

A livello internazionale il tema sicurezza è affrontato in modo sistematico dal 1995 (norme BS7799). Le norme introducono nel settore della sicurezza il concetto di “Sistema di Gestione” che permette di tenere sotto controllo nel tempo i processi legati alla sicurezza, tramite la definizione di ruoli, responsabilità, di procedure formali e di canali di comunicazione.

Principale obiettivo di un sistema di sicurezza è la salvaguardia delle informazioni. A tal proposito è fondamentale individuare quali informazioni proteggere e quale livello di protezione assegnare a ciascuna di esse.

Lo standard BS7799 individua tre aspetti fondamentali relativi alla sicurezza delle informazioni:

- **Confidenzialità** solo gli utenti autorizzati possono accedere alle informazioni necessarie.
- **Integrità** protezione contro alterazioni o danneggiamenti; tutela dell’accuratezza e completezza dei dati.
- **Disponibilità** le informazioni sono rese disponibili quando occorre e nell’ambito di un contesto pertinente.

Fra le risorse (asset) da tutelare rientrano certamente:

- dati digitali,
- documenti cartacei,
- flussi informativi,

nonché componenti materiali come:

- computer,
- reti,

ma anche:

- il personale,

e non ultimo:

- gli edifici,
- gli uffici.

L’approccio alla sicurezza deve avvenire in una logica di prevenzione (risk management) piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.

L’architettura per rispondere alle esigenze di sicurezza è costituita da 3 elementi fondamentali:

- le politiche dell’organizzazione,
- gli strumenti organizzativi e tecnologici,
- gli atteggiamenti individuali.