

1. Descrizione delle norme relative alla “sicurezza”

1.1. Ambiti relativi alla sicurezza

Gli ambiti normativi relativi alla sicurezza, sono classificati nel modo seguente:

- Norme funzionali relative ai prodotti, aventi come scopo principale la ricerca dell'interoperabilità dei sistemi informatici;
- Criteri di valutazione della fiducia riposta nella sicurezza (assurance) di specifici sistemi e prodotti informatici;
 - TCSEC (Applicato in ambito USA);
 - ITSEC (Applicato in Europa);
 - ISO /IEC 15408;
 - Direttiva “Stanca” sulla sicurezza ITC;
- Norme relative al sistema di gestione della sicurezza;
 - ISO/IEC TR 13335 (parti 1,2,3,4);
 - BS7799 (parti 1 e 2);
 - ISO/IEC 17799:2000 (recepisce la parte 1 delle BS7799);
- Vigenti normative nazionali ed europee.

1.2. La sicurezza nell'ITC (Tecnologie dell'Informazione e della Comunicazione)

Con il termine “sicurezza” s'intende l'insieme di misure, di carattere organizzativo e tecnologico, tese ad assicurare a ciascun utente autorizzato (e a nessun altro) esclusivamente i servizi previsti per l'utente stesso, nei tempi e nelle modalità stabilite. Più formalmente, secondo la nota definizione ISO, la sicurezza è “l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite” e dunque l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco.

Gli incidenti di sicurezza possono essere causati da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi,
- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc.),
- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc.),
- persone interne all'organizzazione.

e possono essere identificati come:

- accidentali,
- deliberati.

Rendere sicuro un sistema informatico non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma significa, in particolare, collocare ciascuna delle contromisure individuate in una politica organica di sicurezza che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed