# *Sicurezza dei Sistemi Informatici: Requisiti e Soluzioni*

**Rebecca Montanari**
rmontanari@deis.unibo.it
DEIS- Università di Bologna

# *Requisiti di Sicurezza*

- **confidenzialità**

  "E' possibile proteggere i dati da letture non autorizzate?"
- **autenticazione dell'utente nell'accesso ad un sistema e durante la comunicazione attraverso reti pubbliche**

  "E' possibile garantire a ciascun comunicante che l'altro e' proprio quello che dice di essere?"
- **integrita'**

  "E' possibile garantire il messaggio da modifiche non autorizzate quando memorizzato e/o trasmesso?"
- **non ripudio**

  "E' possibile garantire che l'autore di un messaggio non potrà disconoscerne la paternità e a chi trasmette un messaggio che non gli venga attribuita la paternità di un messaggio che in realtà non ha mai spedito?"
- **controllo dell'accesso**
- **disponibilità**

# *Cosa Occorre Conoscere?*

Fondamentale per il responsabile della sicurezza di un'organizzazione è la conoscenza di quali sono:

❒ attacchi alla sicurezza

❒ modelli e tecnologie di sicurezza

Occorrono metodi sistematici per la definizione dei requisiti di sicurezza e per l'analisi e la scelta degli approcci da adottare per il soddisfacimento di tali requisiti

# *Proteggere le Informazioni: Quali Domande?*

Quanto valgono le informazioni?

Come si può quantificare il rischio di subire un attacco?

Come si può valutare il danno subito da perdite di informazioni rispetto al costo da sostenere per evitare tali perdite?

⇩

metodologia di progettazione, realizzazione e manutenzione della sicurezza che a partire dalle politiche e dai vincoli di un'organizzazione metta in atto un piano per la sicurezza

# *Fasi Metodologiche (1.)*

❒ **analisi del contesto** => struttura dell'organizzazione e finalità (distribuzione geografica delle sedi, unità organizzative, ruoli, competenze, responsabilità)

❒ **analisi del sistema informatico** => analisi risorse fisiche, logiche, dipendenze tra risorse

❒ **classificazione degli utenti** => assegnazione di una classe di appartenenza

❒ **definizione dei diritti di accesso** => a quali servizi e informazioni può accedere una tipologia di utenti

# *Fasi Metodologiche (2.)*

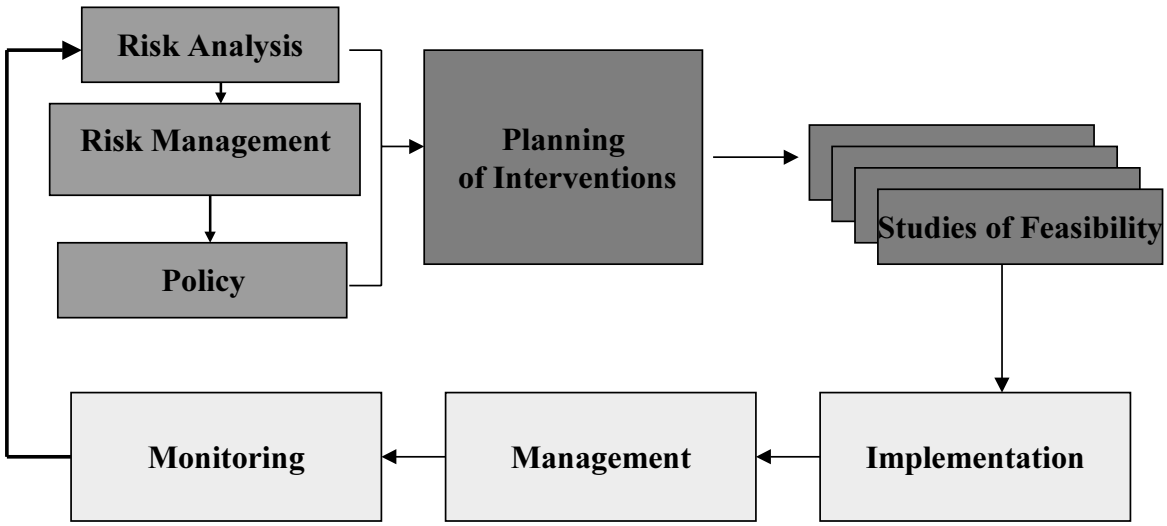
❒ **catalogazione degli eventi indesiderati** (attacchi indesiderati, eventi)

❒ **valutazione del rischio** =>associare un rischio a ciascuno degli eventi indesiderati individuati. Rischio esprime la probabilità che un evento accada e il danno che arreca al sistema se accade

❒ **individuazione delle contromisure** =>analisi di standard e modelli, valutazione del rapporto costo/efficacia, contromisure di carattere sia organizzativo sia tecnico

❒ **integrazione delle contromisure** => individuare sottoinsieme di costo minimo che soddisfi vincoli di completezza, omogeneità, ridondanza controllata, effettiva attuabilità

# *Progettazione della Sicurezza*






# *Le Tecnologie*