



# Privacy: i costi

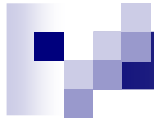


# Il costo per chi detiene i dati: la sicurezza

Da un punto di vista generale il termine sicurezza indica la situazione che vede la predisposizione di misure di protezione idonee a contrastare il verificarsi di eventi accidentali o intenzionali che possano produrre danni a determinati beni

Salvaguardare la sicurezza delle informazioni significa conseguire prefissati obiettivi in termini di:

- riservatezza
- integrità
- disponibilità



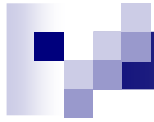
# Riservatezza delle informazioni

- Salvaguardare la riservatezza delle informazioni significa ridurre a livelli accettabili il rischio che:
  - un'entità possa, volontariamente o involontariamente, accedere alle informazioni stesse senza esserne autorizzata



# Integrità delle informazioni

- Salvaguardare l'integrità delle informazioni significa ridurre a livelli accettabili il rischio che:
  - possano avvenire cancellazioni o modifiche a seguito di interventi di entità non autorizzate, o di fenomeni non controllabili



# Disponibilità delle informazioni

- Salvaguardare la disponibilità delle informazioni significa ridurre a livelli accettabili il rischio che:
  - entità autorizzate non possano accedere alle informazioni a causa di interventi di altre entità non autorizzate, o del verificarsi di fenomeni non controllabili



# Come soddisfare gli obiettivi?

- Il problema della sicurezza delle informazioni dovrebbe essere sempre analizzato in senso ampio, non limitato alla sfera tecnologica
- Ogni organizzazione dovrebbe proteggere le informazioni che tratta mediante misure di sicurezza di tipo:
  - ☐ logico
  - ☐ fisico
  - ☐ organizzativo



# Misure di tipo logico

## ■ Alcuni esempi:

- tecniche di protezione contro virus e worm per impedire che questi programmi possano compromettere dati e sistemi
- meccanismi crittografici, per garantire la riservatezza dei dati, per assicurare l'integrità e la paternità dei documenti
- (firma digitale)
- meccanismi di controllo accessi (user ID/password) e per limitare la possibilità di intrusioni illecite

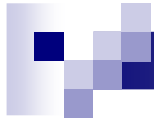


# Misure di tipo fisico

## ■ Alcuni esempi:

- ☐ guardiana
- ☐ sistemi di allarme anti-intrusione
- ☐ sistemi di allarme anti-incendio
- ☐ controllo accesso ai locali (badge, sistemi biometrici)
- ☐ custodia dei supporti (casseforti, armadi blindati)
- ☐ gruppi di continuità elettrica





# Misure di tipo organizzativo

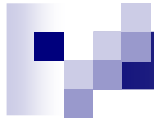
## ■ Alcuni esempi:

- ☐ istituzione dell'infrastruttura organizzativa incaricata della gestione di tutti gli aspetti della sicurezza
- ☐ distribuzione di ruoli e responsabilità
- ☐ definizione e implementazione delle politiche di sicurezza
- ☐ piani formativi e informativi rivolti al personale



## Come si scelgono le misure di sicurezza?

- Tenendo conto degli obiettivi di sicurezza (definiti in relazione alla missione) e della normativa occorre:
  - analizzare i rischi in termini di minacce,
  - vulnerabilità e danni potenziali ai beni
  - implementare misure di sicurezza (logiche, fisiche e di tipo organizzativo) commisurate ai rischi



## Un vero e proprio sistema: il Sistema di Gestione della Sicurezza delle Informazioni

- il complesso dei ruoli, delle responsabilità, delle procedure e delle tecniche per la gestione della sicurezza (SGSI)
- definito, attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento degli obiettivi di sicurezza

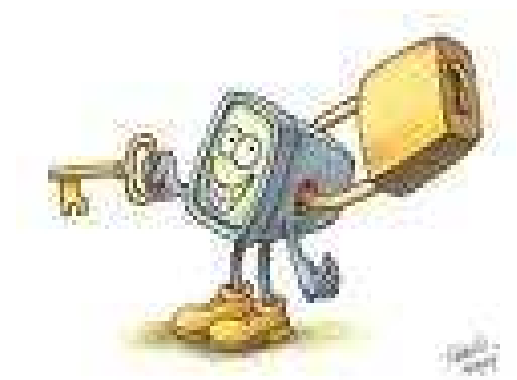


# Il decreto legislativo 196/2003

- Contiene importanti innovazioni che tengono conto della “giurisprudenza” del Garante e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche

# Misure di sicurezza (Art.31)

- Il Codice obbliga ad adottare le misure di sicurezza idonee a garantire:
  - ☐ l'integrità dei dati
  - ☐ la disponibilità dei dati
  - ☐ la riservatezza dei dati
- Ciò al fine di prevenire i rischi di:
  - ☐ Distruzione/perdita
  - ☐ Trattamento illecito
  - ☐ Accesso non autorizzato





# Misure Minime di Sicurezza (Artt.33-36)

- Il Codice, oltre a prescrivere un generico obbligo di adozione di misure di sicurezza, individua anche le misure minime da adottare che vengono definite come “quell'insieme di misure tecniche, informatiche, organizzative, logistiche e procedurali, in grado di configurare il livello minimo per la protezione del sistema informativo” .
- L'adozione di tali misure deve essere effettuata secondo:
  - la tipologia dei dati stessi (personali, sensibili o giudiziari)
  - l'automatizzazione (o meno) del trattamento



## Allegato B: ***Disciplinare tecnico in materia di misure minime di sicurezza***

- Trattamenti con strumenti elettronici
  - ☐ Sistema di autenticazione informatica
  - ☐ Sistema di autorizzazione
  - ☐ Altre misure di sicurezza
  - ☐ Documento Programmatico sulla Sicurezza
  - ☐ Misure di tutela e garanzia
  - ☐ Ulteriori misure **in caso di trattamento di dati sensibili** o giudiziari

Trattamenti senza l'ausilio di strumenti  
elettronici