CYBER SECURITY

Lezione 07 - Alcune Norme

LE NORME SULLA SICUREZZA

- ***L'ISO/IEC 17799 presenta una serie di linee guida e di raccomandazioni compilata a seguito di consultazioni con le grandi aziende.***
- Il documento sottolinea l'importanza della gestione del rischio e chiarisce che non è indispensabile implementare ogni singola linea guida, ma solo quelle che sono rilevanti.
- Lo standard copre tutte le forme d'informazione, incluse la voce, la grafica e i media come fax e cellulari.
- Esso riconosce anche i nuovi metodi di business, come l'e-commerce, Internet, l'outsourcing, il telelevoro e il mobile computing.

Le dieci aree delle linee guida dello standard ISO/IEC 17799

1. **Security Policy.** Fornire le linee guida e i consigli per la gestione, allo scopo di migliorare la sicurezza delle informazioni.
2. **Organizational Security.** Facilitare la gestione della sicurezza delle informazioni all'interno dell'organizzazione.
3. **Asset Classification and Control.** Eseguire un inventario dei beni e proteggerli efficacemente.
4. **Personnel Security.** Minimizzare i rischi di errore umano, furto, frode o uso illecito delle attrezzature.
5. **Physical and Environment Security.** Prevenire la violazione, il deterioramento o la distruzione delle attrezzature industriali e dei dati.
6. **Communications and Operations Management.** Assicurare il funzionamento adeguato e affidabile dei dispositivi di elaborazione delle informazioni.
7. **Access Control.** Controllare l'accesso alle informazioni.
8. **Systems Development and Maintenance.** Assicurare che la sicurezza sia incorporata nei sistemi informativi.
9. **Business Continuity Management.** Minimizzare l'impatto delle interruzioni dell'attività aziendale e proteggere da avarie e gravi disastri i processi aziendali essenziali.
10. **Compliance.** Evitare ogni violazione delle leggi civili e penali, dei requisiti statutari e contrattuali e dei requisiti di sicurezza.

LO STANDARD **BS 7799-2**

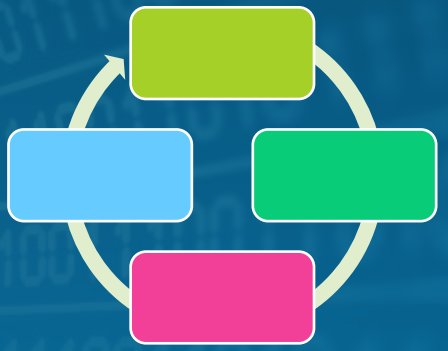
- *lo standard* **BS 7799-2** *fornisce le direttive per istituire un sistema di gestione della sicurezza delle informazioni (ISMS, Information Security Management System) da sottoporre alla certificazione di un ente accreditato.*
- L'applicazione del BS 7799-2 permette all'azienda di dimostrare ai suoi partner che il proprio sistema di sicurezza è conforme allo standard e risponde alle esigenze di sicurezza determinate dai propri requisiti.

LO STANDARD BS 7799-2

Il modello di ISMS definito dallo standard BS7799-2 comprende quattro fasi in un loop ciclico, analogo a quello dell'ISO 9001. Il modello è detto PDCA dalle iniziali delle quattro fasi:

LO STANDARD BS 7799-2

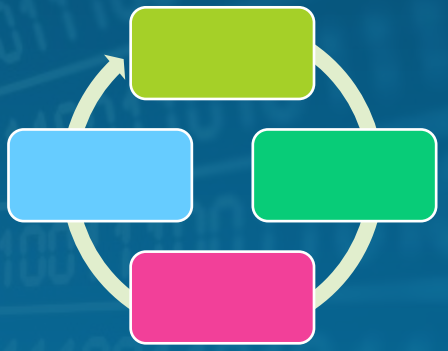
Le quattro fasi dell'ISMS: 1) Plan



- definizione dell'ambito di applicazione dell'ISMS
- definizione di una politica di sicurezza di alto livello
- definizione di un approccio sistematico per l'analisi del rischio
- identificazione dei rischi
- valutazione dei rischi
- identificazione delle opzioni per il trattamento dei rischi (eliminazione, cessione e riduzione)
- selezione delle contromisure per il controllo dei rischi
- redazione della dichiarazione di applicabilità, comprendente l'esplicitazione delle ragioni che hanno portato alla selezione delle contromisure e alla non applicazione di misure indicate nell'appendice A della norma.

LO STANDARD BS 7799-2

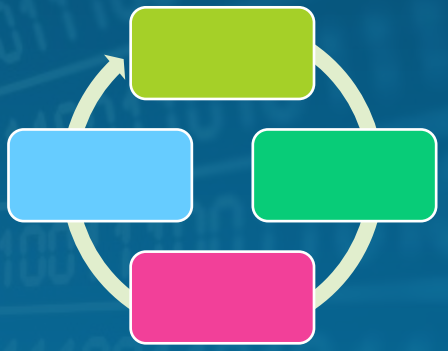
Le quattro fasi dell'ISMS: 2) Do



- formulazione di un piano di trattamento dei rischi
- implementazione del piano
- implementazione delle contromisure selezionate
- svolgimento di programmi d'informazione e di formazione
- gestione delle operazioni connesse alla fase Do
- gestione delle risorse connesse alla fase Do
- implementazione di procedure e altre misure che assicurino rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza

LO STANDARD BS 7799-2

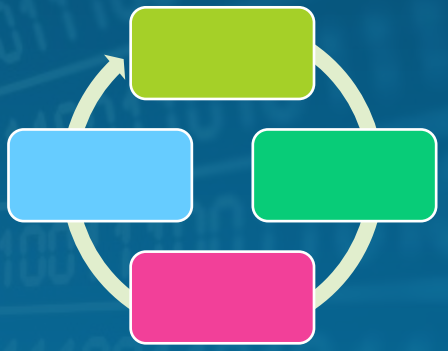
Le quattro fasi dell'ISMS: 3) Check



- esecuzione delle procedure di monitoraggio dell'ISMS
- esecuzione di revisioni del rischio residuo
- conduzione di audit interni all'ISMS
- conduzione di review al massimo livello dirigenziale dell'ISMS
- registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni dell'ISMS

LO STANDARD BS 7799-2

Le quattro fasi dell'ISMS: 4) Act



- implementazione delle azioni migliorative dell'ISMS identificate
- implementazione delle azioni correttive e preventive
- comunicazione dei risultati
- verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base