

I COSTI DELLA SICUREZZA INFORMATICA IN AMBITO AZIENDALE

Best Practices di Organizzazione
per la Sicurezza delle Informazioni

Roberto Gattoli



Associazione Italiana per la
Sicurezza Informatica



A scanso di equivoci



- La sicurezza delle informazioni non coincide, ma include la sicurezza informatica
- Nella maggior parte dei casi i **costi della non sicurezza** non dipendono da attacchi esoterici, ma da "banali" virus, dall'indisponibilità delle risorse o da personale poco attento e consapevole del valore delle informazioni
- L'indisponibilità dei sistemi e la loro cattiva gestione sono spesso trasparenti al management per mancanza di consapevolezza o di verifica
- ... per paradosso, spesso per poterli usare i Veri Hacker gestiscono i sistemi meglio del personale preposto
- I Pen Test, che puntualmente arrivano al cuore dei sistemi, servono soprattutto a evidenziare il livello qualitativo della gestione e quindi tutelarsi dagli errori e incidenti più comuni
- Alcuni provvedimenti tecnici siano irrinunciabili, ma Gengis Khan ci ricorda che non basta affidarsi alle sole "difese perimetrali" sebbene lunghe 10.000 li...



Lo standard di riferimento

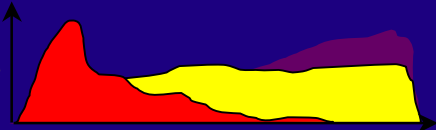
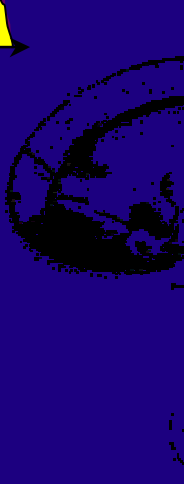
- Lo standard **BS7799** oggi standard internazionale **ISO/IEC 17799:2000**

È un - **codice di Pratica** - rivolto ad **ogni tipo di organizzazione**
che nasce da un Gruppo di lavoro dell'industria nel Gennaio 1993

indica: 10 Paragrafi dettagliati sui controlli
 36 Obiettivi di controllo
 127 Controlli

- suggerisce set di controlli e contromisure per assicurare che i rischi siano ridotti ad un livello accettabile
- Individuati i provvedimenti e i controlli necessari si implementano in modo che generino opportuni log per monitorarli
- Un SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) permette infine di gestire e mantenere i provvedimenti organizzativi adottati verificandone l'efficacia

Il processo di base

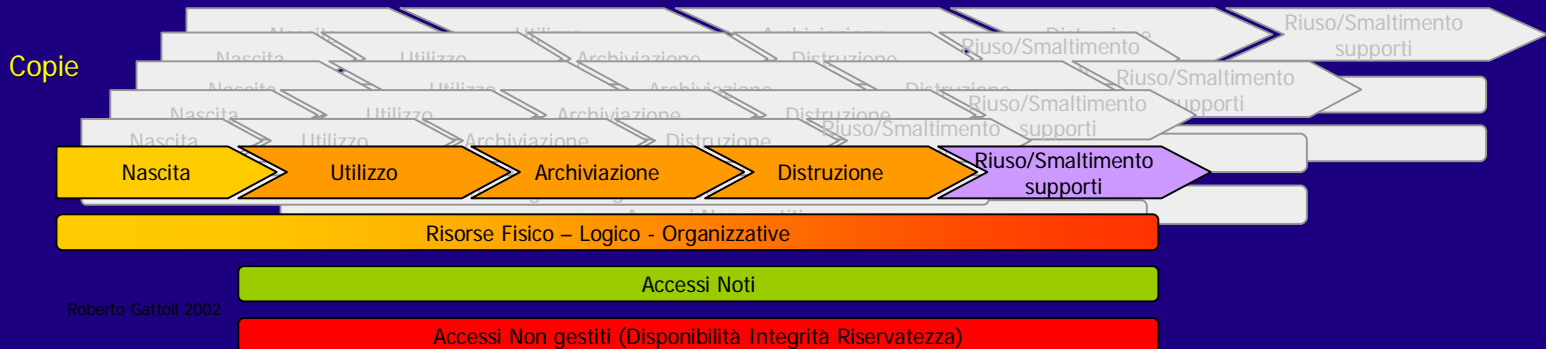
- Primo fondamentale elemento è l'impegno della direzione
- Identificare le caratteristiche delle informazioni da tutelare
- Definire le necessità di protezione degli asset fisico-logici
- Definire il piano di investimento possibile 
- Scegliere il mix e la proporzione di provvedimenti da adottare considerando che, a parità di efficacia, ciascuna combinazione (ad esempio: tecnici – organizzativi – formazione – consulenza) ha un costo diverso in relazione a:
 - Cultura dell'ambiente dell'organizzazione
 - Risorse dell'ambiente in cui insiste l'organizzazione
 - Costi di implementazione
 - Costi di gestione
- Verificare e mantenere nell'ottica del miglioramento continuo di efficacia e adeguatezza, non di investimento incrementale 

Ciclo di vita delle Informazioni

- Trasversalità e pervasività delle informazioni nell'organizzazione

- prevenzione nella generazione -

le informazioni sono trasmesse e memorizzate secondo modalità note e non...
e hanno un "ciclo di vita" per ciascuna di queste



Chi Come Quando Perché usa le informazioni o le risorse dell'Organizzazione

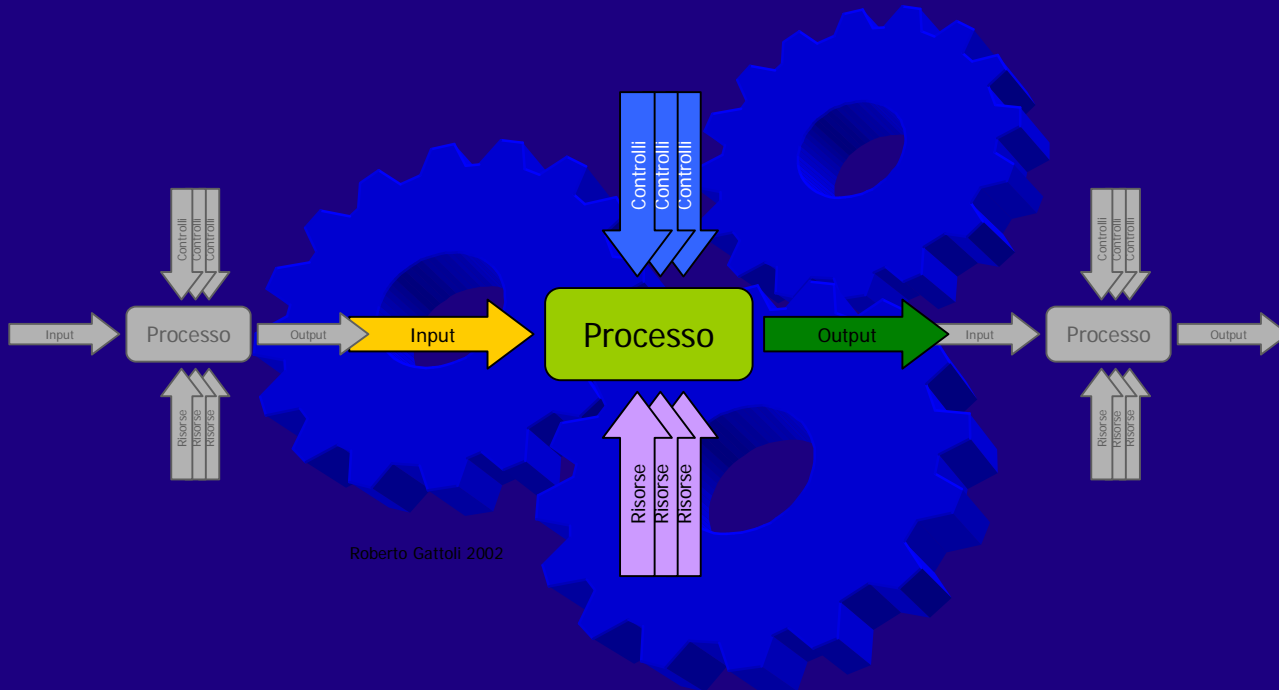


Ignoti - trattamenti - **Noti**

Informazioni, CPU, Spazio su disco, Connettività

Approccio Sistemico

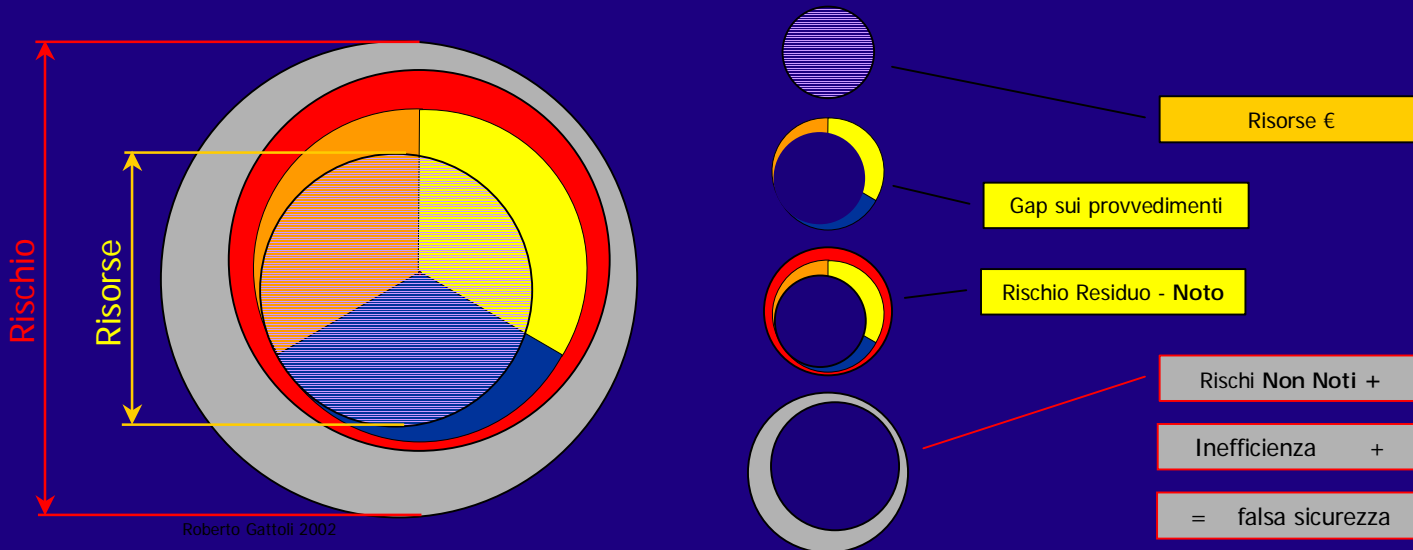
- approccio sistemico verso aspetti tecnici, organizzativi, legali, manageriali e di formazione
- lungo tutto il “percorso” dell’informazione da proteggere nell’ambito dei processi interessati nel suo ciclo di vita



L'analisi dei rischi

$$\text{Rischio} = \text{Valore} \times \text{Minaccia} \times \text{Vulnerabilità}$$

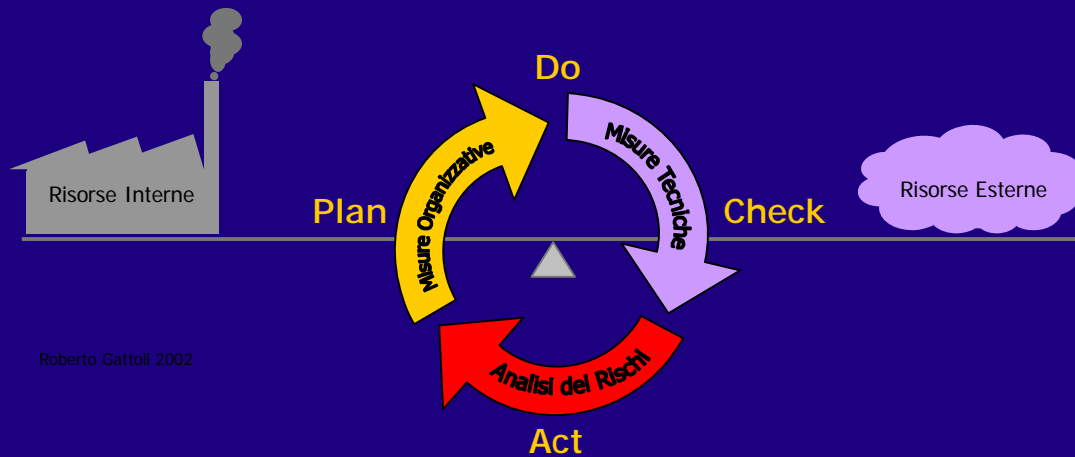
- Ossia: realistica analisi e definizione dei bisogni e del gap anche in un'ottica di benchmarking



Provvedimenti adeguati all'ambiente e alla cultura dell'organizzazione

individuare il mix di provvedimenti più idoneo

- alla cultura dell'organizzazione
- ai costi adeguati e sostenibili
- alla disponibilità degli skill interni/esterni necessari



Consulenza per la sicurezza

Per individuare, Implementare, Verificare
i provvedimenti più idonei per la sicurezza

uno dei passaggi chiave è la scelta di consulenti
in grado di bilanciare proposte e bisogni
perché la migliore ed effettiva sicurezza è polifonica

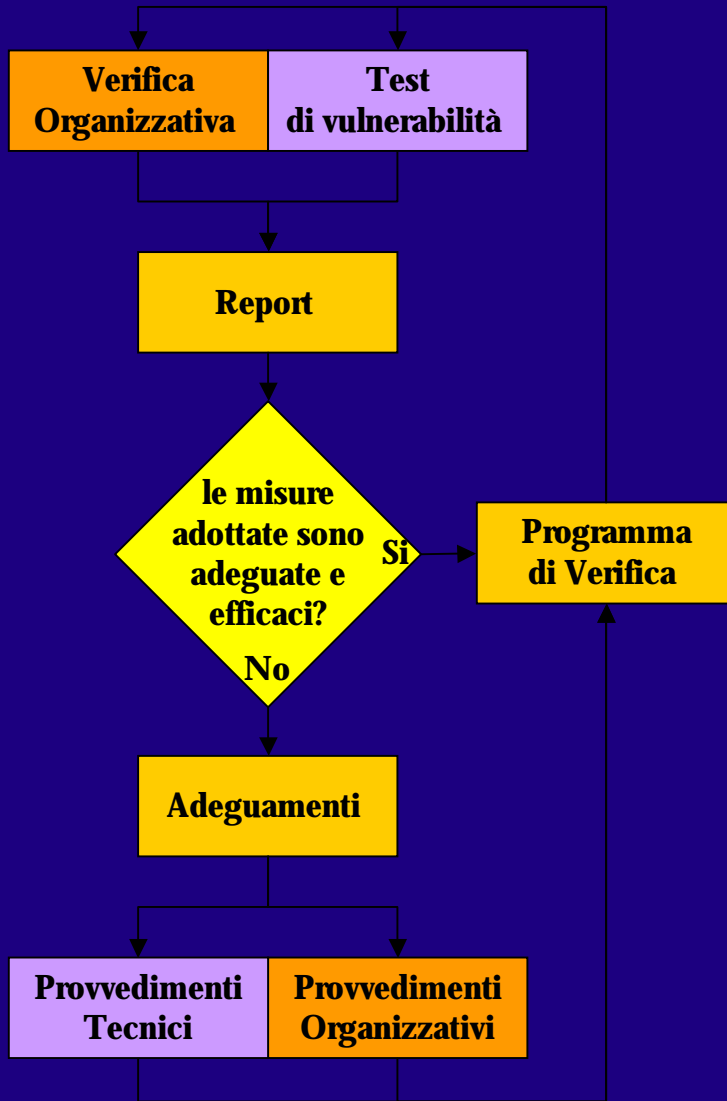


Esperienza e Formazione



tutto il personale che interagisce ad ogni livello e funzione
è la risorsa più preziosa e insieme critica per la sicurezza

Verifiche cicliche



I provvedimenti in atto definiti o meno nell'ambito di un sistema di gestione (BS7799 o DPS ex DPR 318/99) e a prescindere dalla loro complessità o sviluppo, devono essere oggetto di verifiche cicliche, senza le quali non è possibile non solo il migliorarli, ma neppure mantenerli nel tempo.

Gli elementi critici

- Centralità dell'impegno della Direzione
- Analisi dei carichi di lavoro del personale addetto all'amministrazione dei sistemi e alla sicurezza
- Progressività
- Aggiornamento continuo sia del personale che del software...
- Consapevolezza e consenso per conciliare usability e security
- Analisi dei Rischi ripetute e basate su un Asset inventory aggiornato
- Verifiche e Test indipendenti e ripetuti

- *Perseguire obiettivi realistici, perché spesso il meglio è nemico del bene*

Grazie per l'attenzione