Progettazione di un Sistema di Gestione per la Sicurezza delle Informazioni

Cesare Gallotti

Agenda

- I principi della sicurezza delle informazioni
- La metodologia
- Alcune considerazioni
- Conclusioni

I principi della Sicurezza delle Informazioni

Informazione - Definizione

- L'**informazione** è l'insieme di uno o più dati memorizzati, organizzati, messi in relazione o interpretati nell'ambito di un contesto in modo da avere un significato. Equivalentemente, si può definire come informazione un insieme di dati che è stato sottoposto ad un processo che lo ha reso significativo per il destinatario e realmente importante per il suo processo decisionale presente e futuro.

- Il processo di produzione delle informazioni si compone di tre fasi:
  - acquisizione di dati elementari,
  - elaborazione dei dati elementari in dati sintetici,
  - emissione dell'informazione finale in funzione del destinatario.

Il Sistema Informativo

- **Sistema Informativo (S.I.):** insieme di procedure e documenti utilizzati dall'azienda per svolgere la propria attività.
- **Sistema Informatico:** parte del S.I. che coinvolge risorse tecnologiche, comprendendo elaboratori, periferiche ed infrastruttura di rete.
- **Sistema non Informatico:** comprende archivi fisici, sedi, locali e gestione del personale.

Sicurezza - Definizione

Per **sicurezza delle informazioni** si intende quell'attività volta a definire, conseguire e mantenere le seguenti proprietà delle informazioni (nel seguito indicate come **parametri RIDAN**):

- **Riservatezza**: capacità di non rendere disponibili o divulgare ad individui, entità o processi non autorizzati, le informazioni;
- **Integrità**: impossibilità di alterare o distruggere, da parte di individui, entità e processi non autorizzati, le informazioni;
- **Disponibilità**: garanzia di accesso ed utilizzo delle informazioni da parte di chi ne è autorizzato secondo i tempi richiesti;
- **Autenticità**: garanzia della provenienza di un'informazione;
- **Non ripudio**: le informazioni devono essere protette da falsa negazione di ricezione, trasmissione, creazione, sottomissione, trasporto, consegna, ricevuta.

Sicurezza - Osservazioni

- Non esiste la sicurezza assoluta: nuove modalità di attacco ed eventi inaspettati possono sempre verificarsi.
- Un sistema informativo può quindi considerarsi *sicuro* quando difende *adeguatamente* le proprie informazioni. Per questo è necessario progettare un Sistema di Gestione per la Sicurezza delle Informazioni che sia:
  - coerente al valore delle informazioni stesse,
  - uniforme in tutta l'azienda,
  - efficace,
  - aggiornato ed aggiornabile.

Obiettivi dell'azienda

- Gli obiettivi che un'impresa si propone con la salvaguardia della sicurezza delle informazioni sono:
  - adempiere agli obblighi normativi,
  - agevolare il conseguimento della propria missione aziendale,
  - salvaguardare la propria immagine,
  - gestire correttamente le proprie risorse (umane, economiche, logistiche).

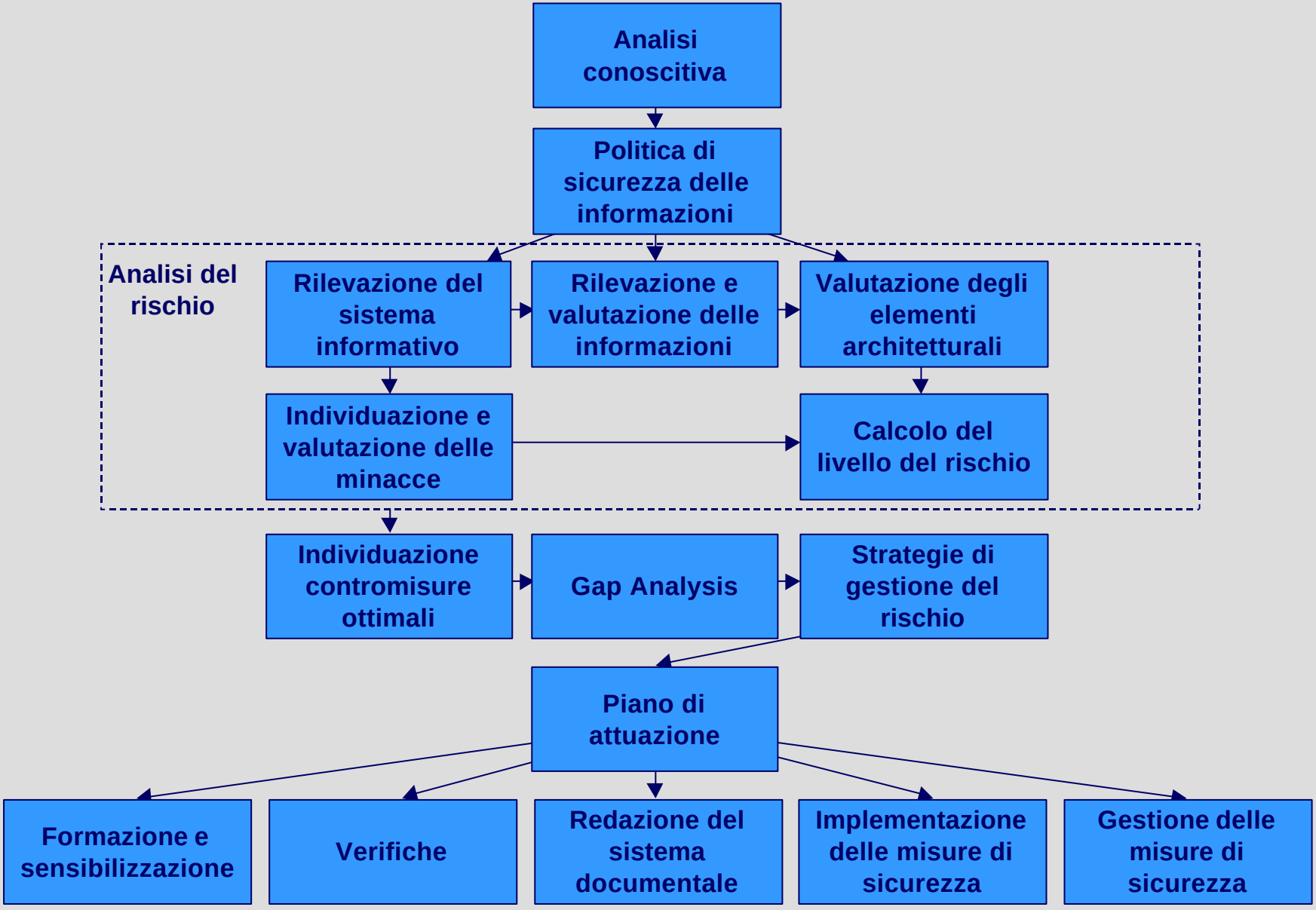
La metodologia

Un approccio all’analisi e alla gestione del rischio

Introduzione

- Una metodologia per la progettazione di un Sistema di Gestione per la Sicurezza delle Informazioni deve essere:
  - facilmente realizzabile;
  - conforme alla Politica Generale, agli obiettivi di sicurezza e all'organizzazione preesistenti nell'azienda cliente;
  - in grado di fornire la giusta garanzia, sia all'interno dell'azienda cliente che a terze parti, che quanto realizzato sia corretto e che siano effettivamente salvaguardati i diritti della proprietà, dei dipendenti e dei terzi che vengono in relazione con la società;
  - coerente con gli obblighi normativi;
  - flessibile, per essere adattabile ai business emergenti e alle nuove tecnologie (stabilità del modello);
  - in grado di tenere in considerazione il rapporto costi-benefici.

Le fasi di lavoro



Analisi conoscitiva

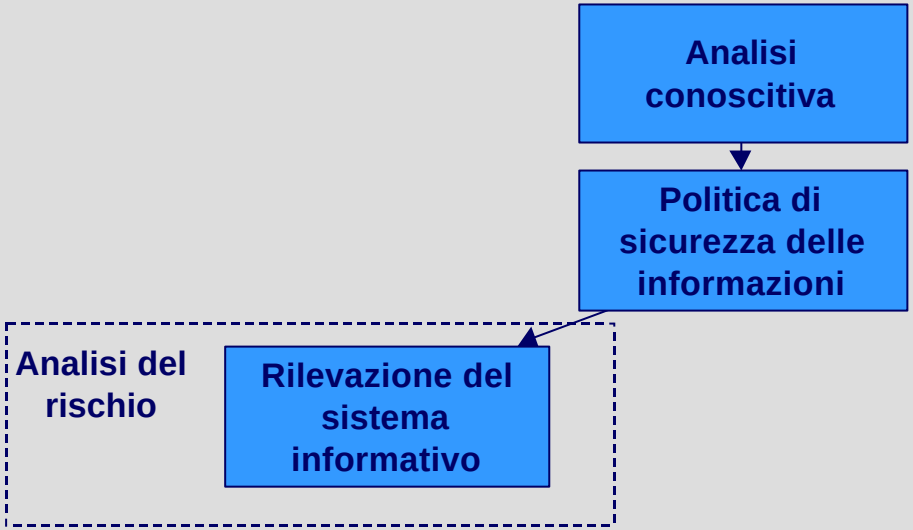
Analisi conoscitiva

- L’unico modo per comprendere quali informazioni sono rilevanti per la società è dato da uno studio della stessa e dei suoi processi:
  - osservazione dell’**organigramma aziendale**,
  - descrizione della **missione** e **dell’attività aziendale**,
  - indicazione dei **vincoli** (normativi, contrattuali, strategici) ai quali l’azienda deve sottostare,
  - individuazione **delle risorse e dei processi critici** per un’analisi del Rischio relativa all’intera attività aziendale e all’elaborazione di una Politica Generale di Sicurezza delle Informazioni coerente con la strategia aziendale,
  - **analisi del mercato**, per stabilire al meglio i bisogni di sicurezza delle informazioni in relazione agli aspetti strategici e ai piani futuri.

Politica di sicurezza delle informazioni

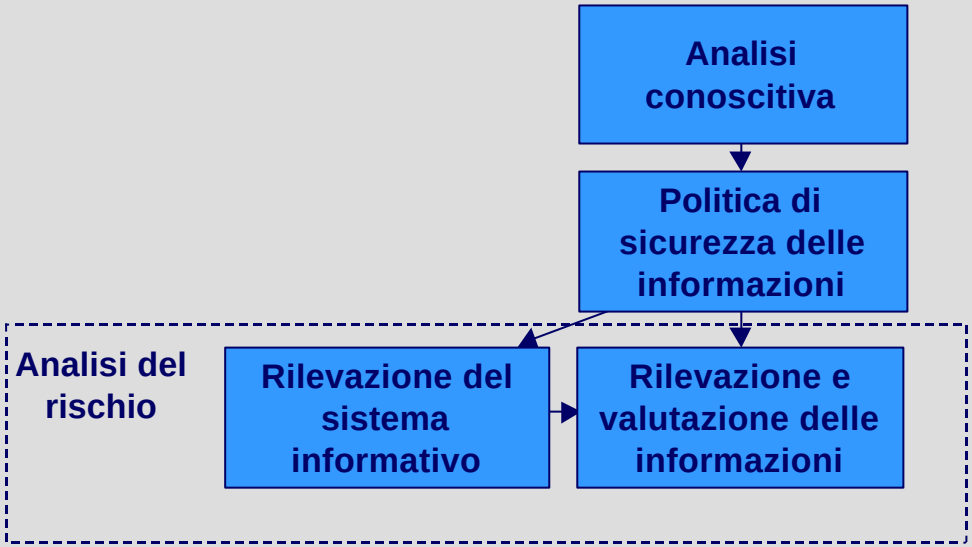
- Definisce ad alto livello gli obiettivi da perseguire per la difesa da minacce ed illeciti in grado di ledere i fattori chiave del successo, la capacità competitiva e di generazione del valore.
- Deve essere approvata dalla Direzione aziendale, pubblicata e comunicata, secondo le appropriate modalità, al personale.
- La Direzione aziendale deve garantire inoltre pieno sostegno alle attività collegate alla Sicurezza delle Informazioni.
- Deve indicare ruoli e responsabilità relativi alla sicurezza:
  - Responsabile per la sicurezza delle informazioni
  - Funzione per la gestione della sicurezza
  - Forum per la sicurezza delle informazioni
  - Amministratori di Sistema e di applicazioni
  - Responsabili delle informazioni
  - Funzione di Audit.

Rilevazione del sistema informativo



- In questa fase sono individuati e descritti gli *elementi architetturali* che compongono il sistema informativo dell'azienda cliente. In particolare, sono rilevate le sedi, i locali critici, gli archivi fisici, le applicazioni in uso, gli elaboratori e la struttura della rete aziendale.

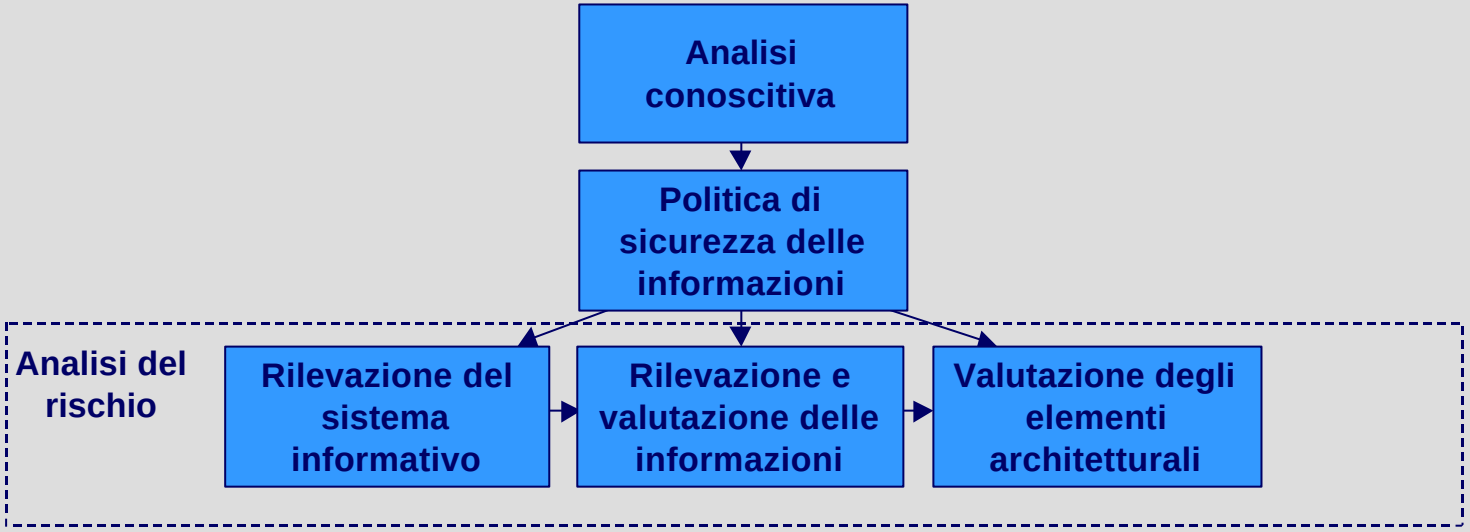
Rilevazione e valutazione delle informazioni



- Sono rilevate le informazioni utilizzate dall'azienda e sono quindi correlate agli elementi architetturali che le trattano (posizionamento) .

- Le informazioni così aggregate vengono successivamente valutate, su una scala predeterminata, in termini di criticità rispetto ai parametri di sicurezza RIDAN.
- Le attività sono svolte con i **Responsabili di processo** e con il supporto di questionari.

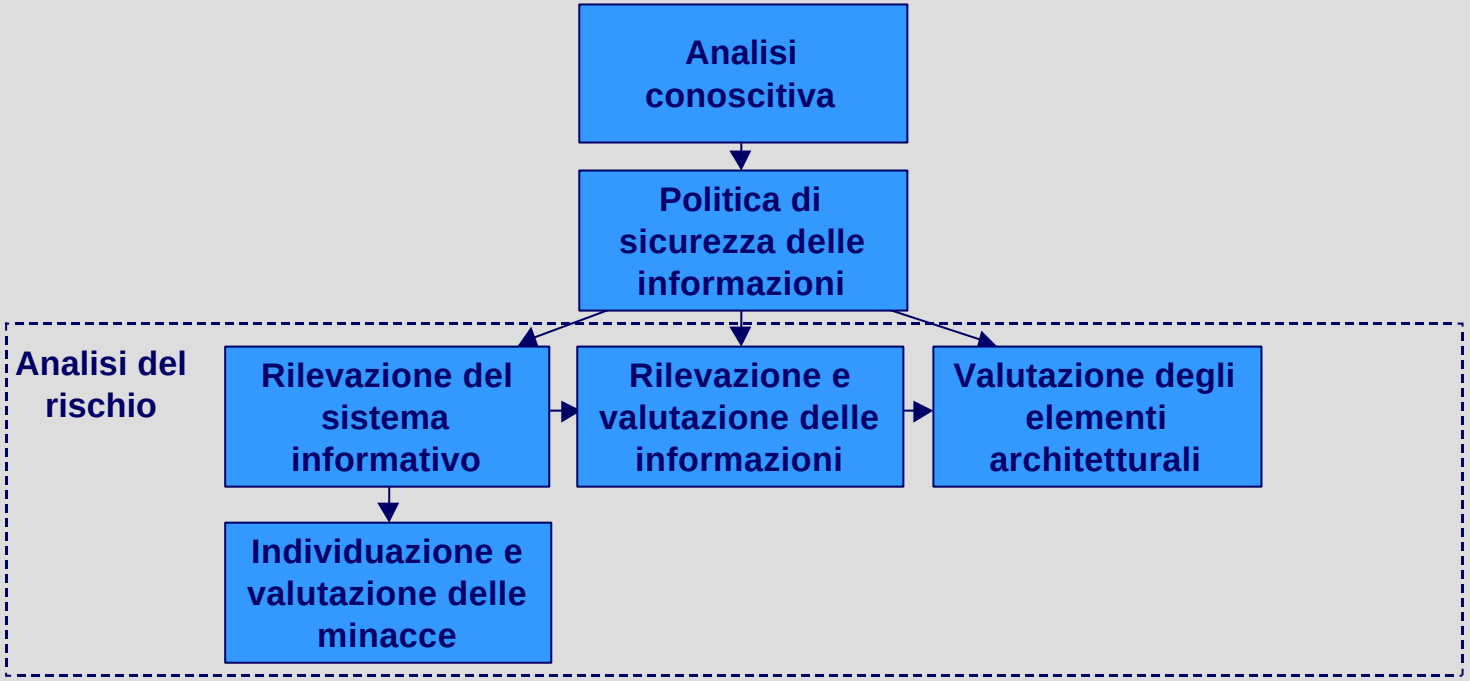
Valutazione degli elementi architetturali



- Il valore degli elementi architetturali verrà determinato in maniera induttiva in base al valore delle informazioni che sono gestite da tali elementi.
- Ovviamente,

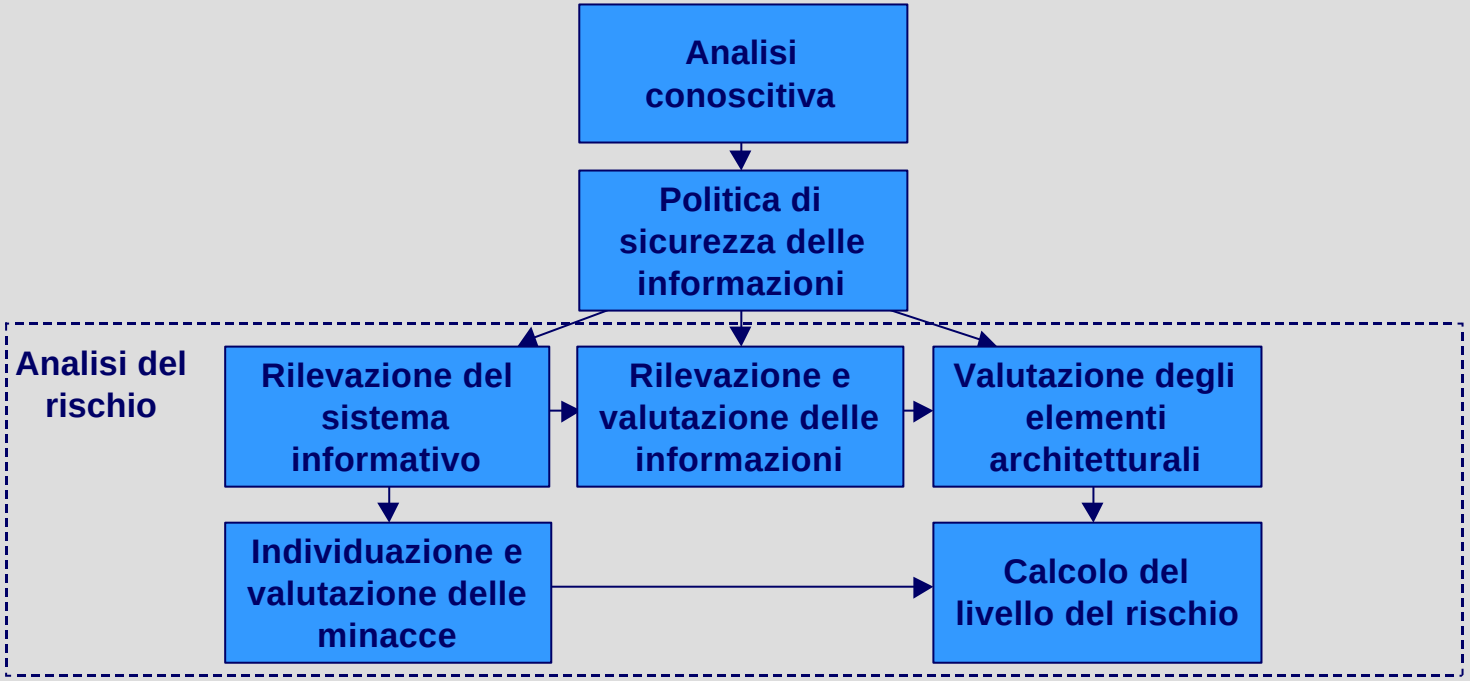
  Valore elemento architetturale μ *Valore informazioni gestite*

Individuazione e valutazione delle minacce



- Per la valutazione delle minacce si considerano le serie storiche e le vulnerabilità “intrinseche” al sistema informativo analizzato. Non sono pertanto qui considerate le contromisure già implementate perché si devono determinare le misure di sicurezza ottimali e non quelle residue (quest’ultima fase è coperta dalla Gap Analysis).

Calcolo del livello del rischio (1)

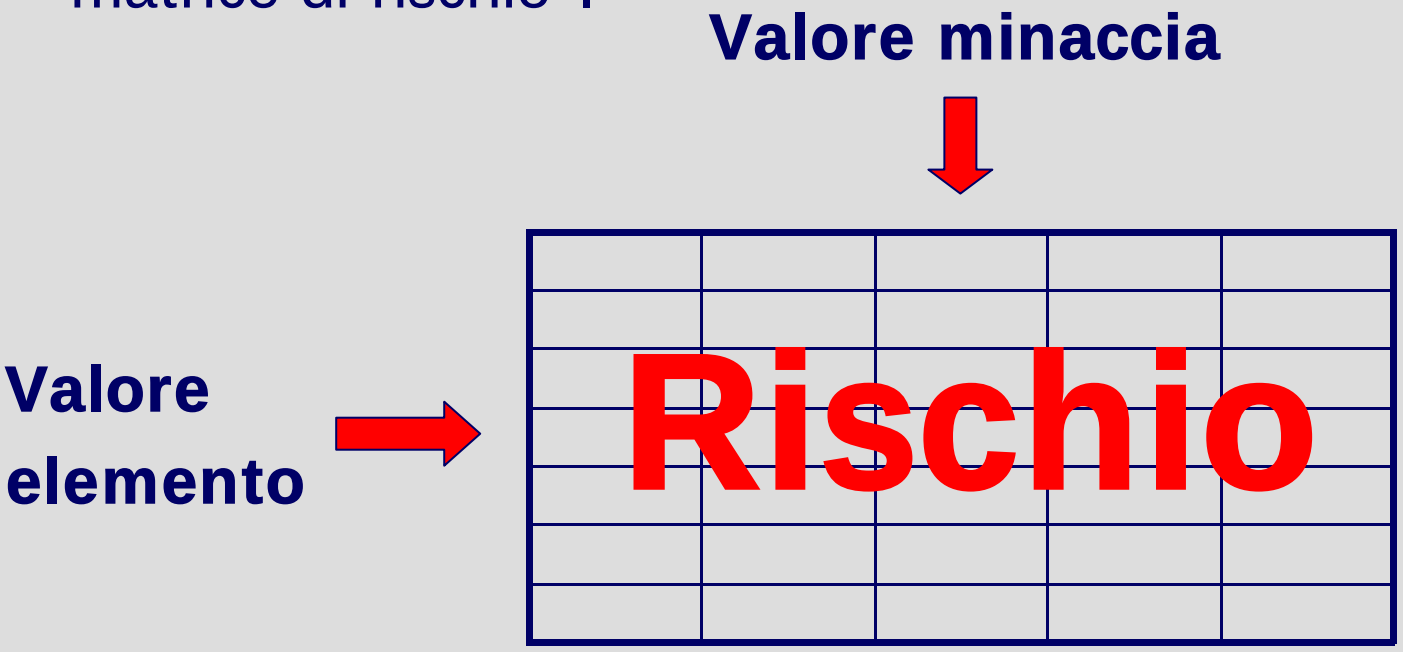


- Il livello di rischio viene calcolato per ogni elemento architetturale e per ogni minaccia ad esso pertinente:

$$\textit{Livello di Rischio} = \mu \left(\textit{Valore elemento architetturale} \cdot \textit{Valore Minaccia} \right)$$

Calcolo del livello di rischio (2)

- Per il calcolo viene generalmente utilizzata la cosiddetta “matrice di rischio”.



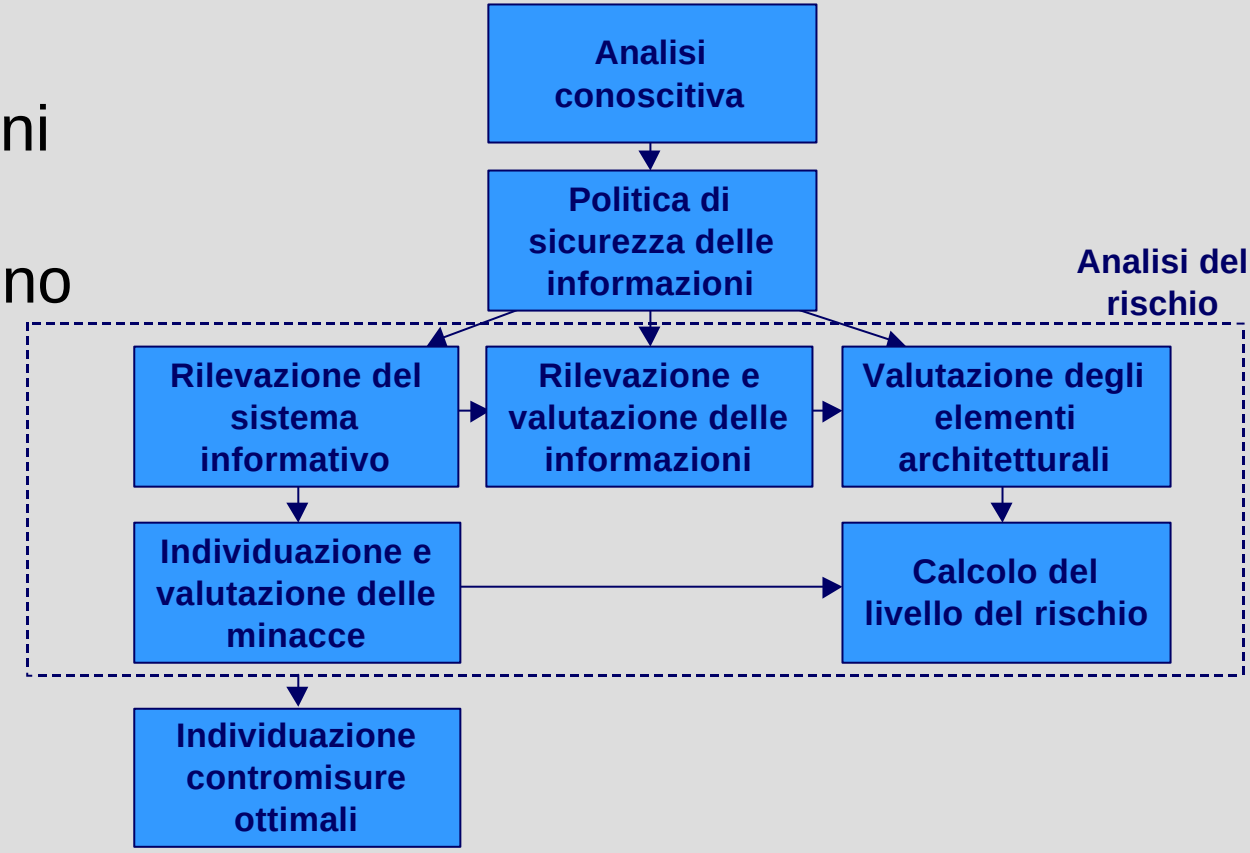
- Al posto del “Valore minaccia” alcuni usano

$$\frac{\textit{Valore minaccia}}{\textit{Contromisure presenti}}$$

oppure *Val. minaccia* · *Liv. vulnerabilità*

Individuazione delle contromisure ottimali

- Efficacia: per ogni elemento architetturale sono selezionate le contromisure ottimali per contrastare le minacce.

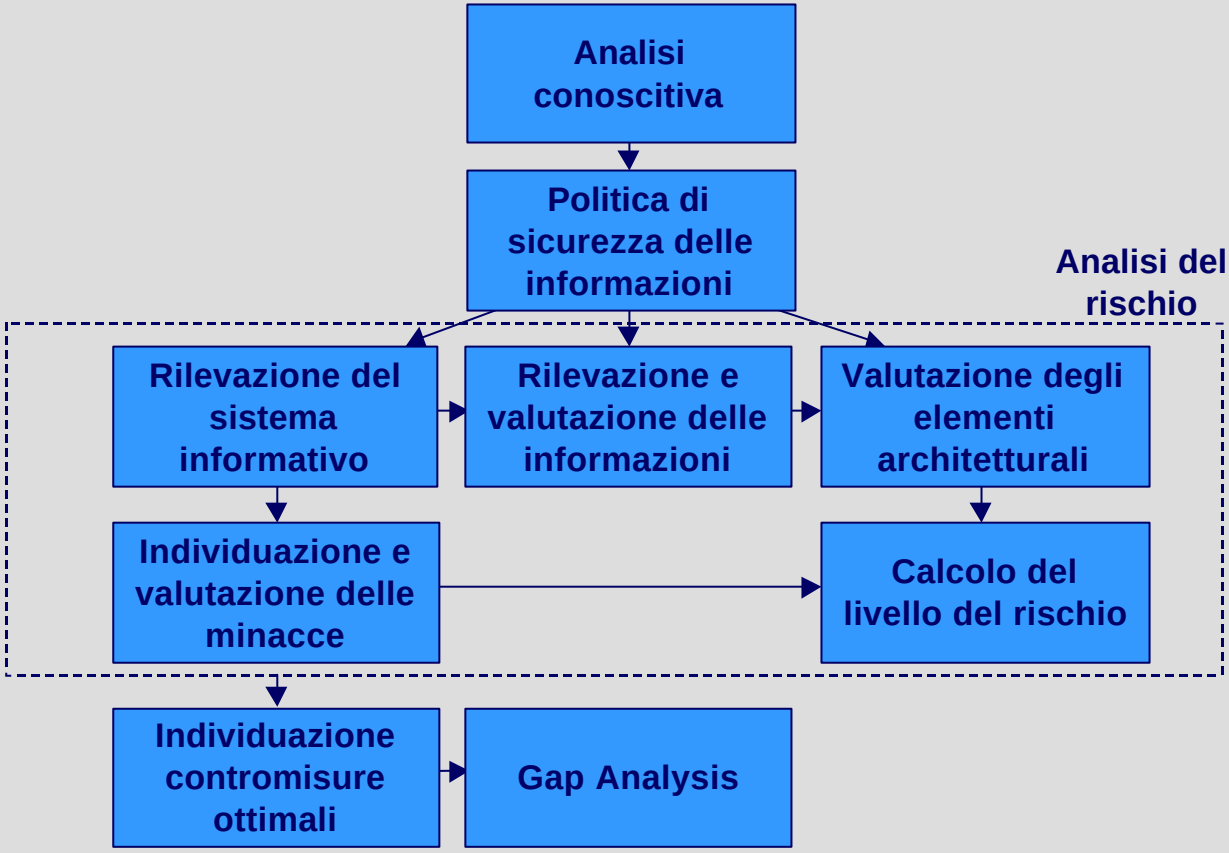


- Efficienza:

Costo implementazione, adeguamento, manutenzione μ *Livello del rischio* μ *Valore elemento architetturale*

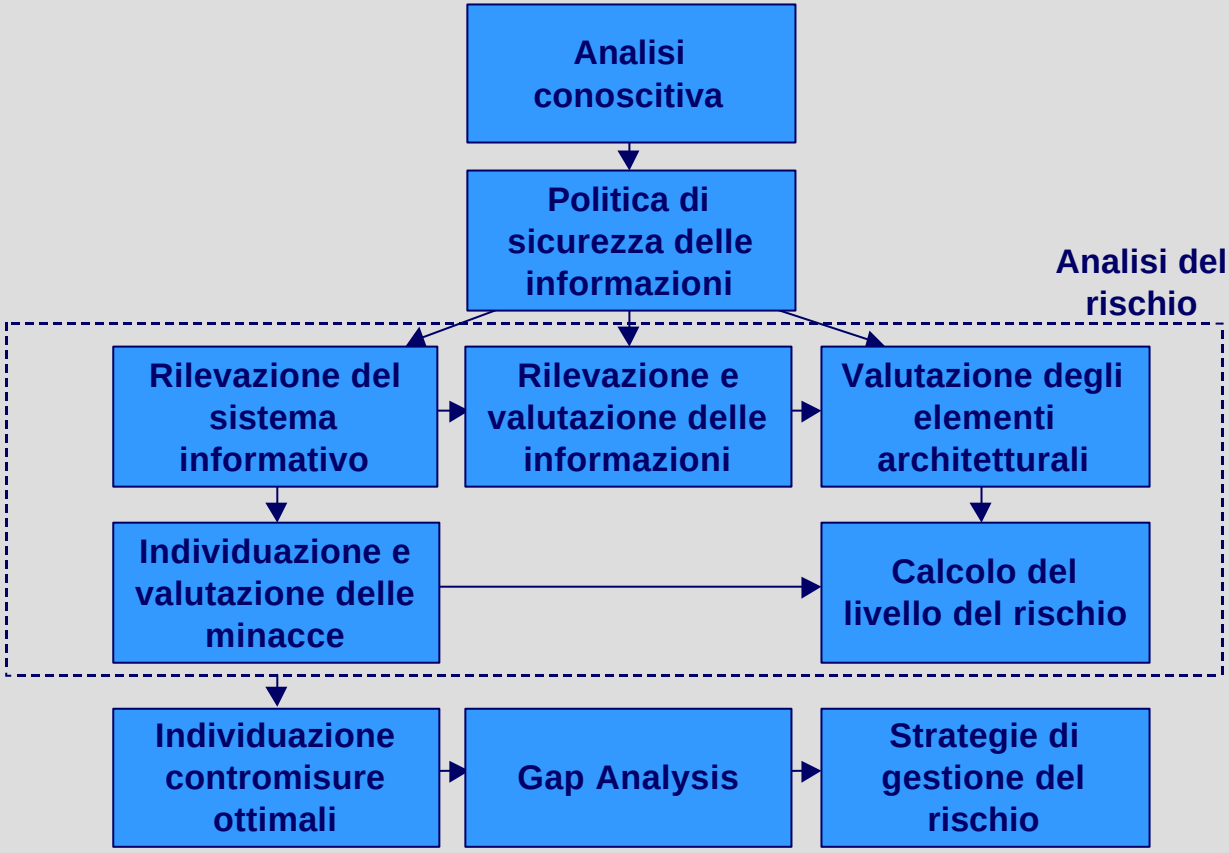
Gap Analysis

- Per ogni contromisura individuata si dovrà verificare se quest'ultima è già stata implementata (completamente o parzialmente)



- Alcune contromisure non potranno essere implementate per ragioni tecniche particolari: si valuteranno misure alternative.

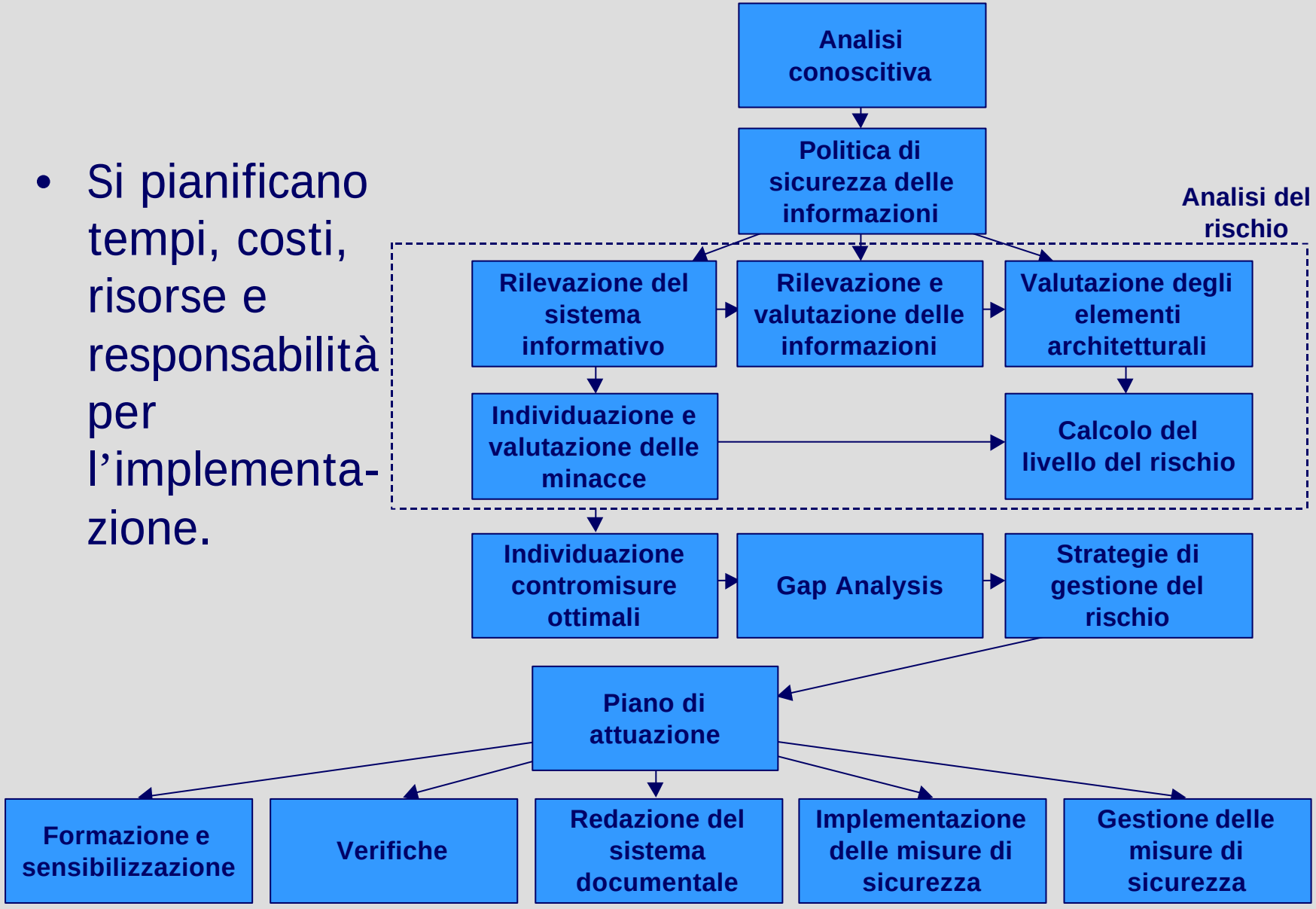
Strategie di gestione del rischio



- **contrastare il rischio**: si implementano le contromisure individuate;
- **trasferire il rischio**: stipulazione di polizze assicurative o affidamento della gestione di attività ad outsourcer;
- **ritenere il rischio**: qualsiasi forma di investimento nei livelli di sicurezza non è ritenuta giustificabile.

Piano di attuazione

- Si pianificano tempi, costi, risorse e responsabilità per l'implementa-zione.



Alcune considerazioni

Perché una nuova metodologia?

- Per estendere la copertura dei parametri RID a quelli più caratteristici di problematiche di rete (Autenticazione e Non ripudio) -> RIDAN
- Necessità di disporre di uno strumento completo che tenga conto
  - ✓ della sicurezza come sistema e non come semplice insieme di strumenti
  - ✓ delle competenze dei consulenti
  - ✓ della necessità di offrire servizi modulari
  - ✓ di condurre attività con il corretto grado di approfondimento

Conoscere l'azienda

Complessità e sintesi

- Un'azienda può avere un sistema informativo estremamente complesso:
  - un'organizzazione molto ramificata,
  - una forte dislocazione sul territorio,
  - parecchie tipologie di ambienti informatici (dal mainframe, al pc con Windows o Macintosh).
- Sulla base dell'esperienza è necessario e possibile operare una sintesi che tenga conto di ogni peculiarità ma che non renda il progetto impossibile da realizzare.
- Se i tempi sono troppo lunghi, i risultati del progetto potrebbero non essere più validi.

Minacce

Statistica e “nasometria”

- Non esistono statistiche accurate sulla frequenza di accadimento delle minacce.
- Le assicurazioni non rilasciano le informazioni in loro possesso.
- Le informazioni a disposizione delle assicurazioni non sono sempre significative perché non sono tenute a considerare ogni evento.
- Le aziende tendono a non coinvolgere i CERT e forze dell’ordine per evitare danni all’immagine (?).
- Molte aziende non sono consapevoli degli attacchi a cui sono sottoposte.
- Rimane solo la “nasometria”.

Vulnerabilità

Audit e progettazione

- Le vulnerabilità sono, sostanzialmente, delle contromisure non presenti o non correttamente implementate.
- Quando si svolge un'attività di progettazione è corretto individuare quale dovrebbe essere la situazione ottimale.
- Una volta stabilita la possibile situazione ottimale, è possibile effettuare delle scelte.
- Gli audit sono svolti con l'intento di verificare la coerenza e la correttezza di quanto fatto. In questo ambito è corretto individuare le vulnerabilità.
- Molte società svolgono sia l'analisi delle vulnerabilità che la Gap Analysis, duplicando così il lavoro (e le fatture...).

Individuazione delle misure

Massimalismo e flessibilità

- Le misure di sicurezza non devono essere eccessive: immaginate una società dove non ci sono armadi ma solo casseforti a combinazione…
- La sicurezza deve adattarsi alle attività operative svolte in funzione del business aziendale. Se ciò non fosse:
  - l'operatività subirebbe rallentamenti non giustificabili,
  - il personale escogiterebbe metodi per superare le misure di sicurezza.
- In tutti i casi, la Direzione Aziendale deve garantire l'appoggio alle attività relative alla sicurezza.
- Le attività relative alla sicurezza possono (o meglio, devono) essere immaginate su più anni e sulla base della progressiva "maturazione" dell'azienda.