



Il modello di security governance di Business-e e ANGQ

Costantino Imbrauglio
ICT Security Advisor
costantino.imbrauglio@business-e.it



Governo del rischio

Le attività di governo del rischio associate ad un particolare insieme di risorse devono essere considerate in un'ottica di processo.

Trattasi di un processo ciclico che deve accompagnare l'intero ciclo di vita delle risorse e che si compone di due fasi principali:

- > Analisi del rischio (risk analysis)
- > Riduzione del rischio (risk mitigation)



Analisi del rischio (risk analysis)

- > Caratterizzazione del sistema (asset analysis)
- > Identificazione delle minacce e delle vulnerabilità
- > Analisi dei meccanismi di controllo in essere
- > Valutazione d'impatto
- > Valutazione del rischio



Riduzione del rischio (risk mitigation)

- > Determinazione del livello di rischio accettabile
- > Analisi di scostamento (gap analysis)
- > Piano di rientro e meccanismi di controllo
- > Rischio residuo e rischio imponderabile

Efficacia di un programma di gestione del rischio

Le chiavi per il successo di un programma di gestione del rischio sono:

- > Supporto da parte del management
- > Supporto e partecipazione da parte dello staff IT
- > Competenza del team di supporto alle attività di gestione del rischio (sia esso interno all'organizzazione o preso dall'esterno)
- > Consapevolezza e partecipazione da parte delle utenze, le quali devono operare nel rispetto delle politiche, delle procedure e delle linee guida definite nonché rispettare i meccanismi di controllo posti in essere a protezione delle infrastrutture
- > Una periodica attività di valutazione del rischio e del suo impatto sulla missione dell'organizzazione