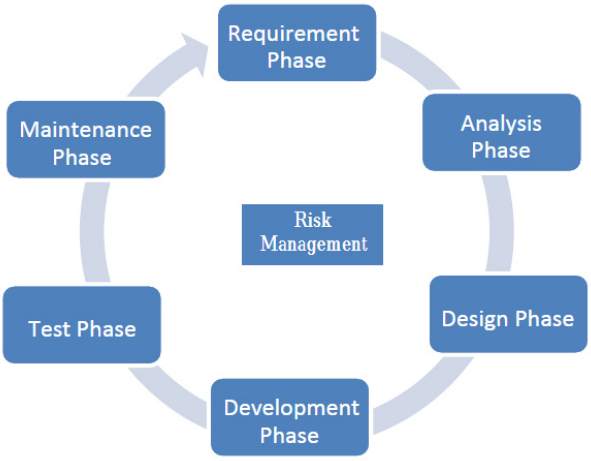

Figura 11 - Gestione del rischio nel ciclo di vita del Software

- Avvio del progetto/Requisiti. La valutazione preliminare del rischio è volta a definire l'ambiente di minaccia in cui opererà il prodotto o il sistema. Questa valutazione è seguita da una prima identificazione dei controlli di sicurezza richiesti che devono essere soddisfatti per proteggere il sistema nell'ambiente operativo previsto.
- Disegno. I requisiti di sicurezza del sistema vengono identificati attraverso un processo formale di Risk Assessment. L'analisi parte dalla valutazione del rischio effettuata nella fase precedente di avvio/inizializzazione e viene approfondita per il contesto specifico. Durante questa fase vengono rivisti attentamente i requisiti e le aspettative di sicurezza e privacy al fine di identificare problemi di sicurezza e rischi per la privacy. In questo passaggio vengono identificate le vulnerabilità presenti nell'ambiente software o derivanti dall'interazione con altri sistemi (Security Assessment). Una volta identificati i rischi, devono essere valutati in merito alla loro potenziale gravità dell'impatto e alla probabilità che si verifichino (Risk Assessment). Nel processo di valutazione è necessario definire le priorità per l'attuazione del piano di gestione dei rischi. La mitigazione del rischio (Risk Mitigation) è il piano delle azioni volte a ridurre o eliminare le priorità più alte. Lo scopo è di valutare la progettazione del sistema, i requisiti dichiarati e i requisiti minimi di sicurezza derivanti dal processo di categorizzazione della sicurezza al fine di determinarne l'efficacia delle azioni di mitigazione per i rischi previsti. I risultati dovrebbero mostrare come i controlli di sicurezza specifici forniscono la protezione appropriata o evidenziare le aree in cui è necessaria un'ulteriore pianificazione. La valutazione del rischio deve essere eseguita prima dell'approvazione delle specifiche progettuali (design specifications) poiché potrebbe fornire specifiche aggiuntive o ulteriori elementi da valutare per le specifiche identificate (ad esempio si dovrebbe considerare come il sistema potrebbe influenzare altri sistemi a cui sarà direttamente o indirettamente collegato; ciò implica che ci potrebbero essere controlli comuni che devono essere ereditati dall'applicazione in oggetto o ulteriori rischi che devono necessariamente essere mitigati).
- Implementazione. In questa fase è necessario determinare i rischi residui accettabili (le specifiche possono imporre oneri e costi eccessivi se i rischi residui accettabili non sono conosciuti). L'obiettivo del processo di valutazione della sicurezza è verificare che il sistema sia conforme ai requisiti funzionali e di sicurezza e operi all'interno di un livello accettabile di rischio residuo per la sicurezza.
- Monitoraggio continuo. L'obiettivo finale del monitoraggio continuo è determinare se i controlli di sicurezza continuano a essere efficaci nel tempo alla luce degli inevitabili cambiamenti che si potrebbero verificare nel sistema e nell'ambiente in cui opera. La valutazione del potenziale