Ad esempio, per valutare l'impatto in termini di riservatezza, integrità e disponibilità delle informazioni, ci si sofferma sugli aspetti economico/finanziario, operativo, reputazionale e legale (compliance).

Le fasi che costituiscono la gestione del rischio effettuato con Cyber Risk Management di AgID sono le seguenti:

1) Analisi del contesto. Vengono identificati i servizi erogati e i servizi trasversali utilizzati in ambito pubblica amministrazione. Di ogni servizio viene descritto un profilo di criticità.
2) Valutazione di ciascun servizio erogato e da ciascun servizio trasversale in termini d'impatto su riservatezza, integrità e disponibilità delle informazioni trattate.
3) Calcolo del rischio attuale, sulla base dei valori di probabilità di accadimento e d'impatto, per ogni minaccia identificata. La fase di Risk Assessment prevede anche l'identificazione delle contromisure da implementare per un'efficace mitigazione del rischio.
4) Applicazione delle contromisure previste dal piano di trattamento del rischio, volte a mitigare, accettare o trasferire i rischi individuati.
5) Analisi del rischio residuo, cioè la valutazione del rischio che permane, nonostante l'applicazione del piano di trattamento del rischio.
6) Fase di monitoraggio dell'intero processo, con eventuale adeguamento in seguito a modifiche del contesto o in presenza di nuove minacce alla sicurezza delle informazioni.

Il tool AGID di Risk Management è gratuito ed a completa disposizione di tutte le Pubbliche Amministrazioni: www.sicurezzait.gov.it

6.3 Requisiti

La fase di analisi e specifica dei requisiti è fondamentale nel ciclo di vita dello sviluppo software.

Di seguito si riportano i linguaggi e gli strumenti utili alla fase di definizione dei requisiti di sicurezza del software.

6.3.1 Linguaggi per la specifica dei requisiti

Un linguaggio di specifica in ambito sicurezza può essere considerato:

- un linguaggio di specifica software utilizzato per indicare gli attacchi (AsmL e UML state charts),
- l'estensione di un linguaggio di specifica software utilizzato per rappresentare gli attacchi (Misuse Cases , Abuse Cases, AsmLSec e UMLintr) e i requisiti di sicurezza (UMLsec, SecureUML, Secure Tropos e Misuse Cases),
- un linguaggio per la specifica degli attacchi (*attack specification language), per esempio* STATL e Snort Rules.

UMLsec[17] è un'estensione di UML per lo sviluppo di sistemi sicuri e usa stereotype, tag e constraint per specificare i requisiti di sicurezza. Gli stereotype servono come etichette per gli elementi del modello UML allo scopo di introdurre informazioni al modello e specificare i vincoli che devono essere soddisfatti da questo. I tag sono associati con gli stereotype e sono utilizzati per specificare in modo esplicito una

[17] https://en.wikipedia.org/wiki/UMLsec