fine di fornire l'adeguato supporto nella valutazione dell'impatto di qualsiasi vulnerabilità durante il processo di analisi dei rischi[13].
Ad alto livello, il processo dovrebbe prevedere:

1) l'identificazione delle minacce, dei rischi e dei requisiti di conformità a cui l'applicazione è soggetta;
2) l'individuazione degli adeguati requisiti di sicurezza capaci di fronteggiare le minacce e i rischi di cui sopra;
3) la comunicazione dei requisiti di sicurezza agli appropriati team operativi;
4) la convalida dell'attuazione di ciascun requisito di sicurezza;
5) l'audit, se necessario, al fine di dimostrare la conformità a qualsiasi politica o regolamento applicabile.

5.5.1 Introduzione e concetti base

Nella sua forma più elementare la modellazione delle minacce è un approccio strutturato che identifica le potenziali minacce alla sicurezza, valutandone il rischio e fornendo le più opportune contromisure.
La modellazione delle minacce comporta l'identificazione degli asset in un processo strutturato, individuando le possibili minacce che insistono su tali asset, categorizzandole e determinando le appropriate strategie di mitigazione.
Quando si approccia con la modellizzazione delle minacce, è importante avere una corretta comprensione della terminologia di base:

- **Asset**, è qualcosa di valore su cui un avversario pone particolare interesse. I dati presenti in un database sono un esempio di Asset.
- **Threat Agent**, un individuo o un gruppo di individui che possono manifestare una minaccia.
- **Superfice di attacco**, l'insieme dei diversi punti (i vettori di attacco) in cui un utente non autorizzato (l'aggressore) può tentare di introdurre dati in un ambiente o di estrarre dati da un ambiente.
- **Probabilità**, possibilità che si verifichi un evento ostile in cui un attore minaccioso sfrutta la presenza di una debolezza. La probabilità di eventi di minaccia che si traducono in impatti negativi determina la possibilità che un evento di minaccia si traduca in un risultato effettivo.
- **Impatto**, danno potenziale (fisico, logico, finanziario, ecc.) dovuto a un evento di minaccia.
- **Controllo**, protezione o contromisura per prevenire, rilevare, contrastare o ridurre al minimo i rischi per la sicurezza delle informazioni, dei sistemi informatici o di altri beni.
- **Mitigazione**, riduzione sistematica del rischio o dell'impatto su un asset.
- **Minaccia** (threat), è un evento che può o non essere dannoso all'origine ma che possa danneggiare o compromettere un'attività a seguito di un attacco.
- **Vulnerabilità**, è un difetto nella sicurezza di una o più parti di un sistema che rende possibile una minaccia.
- **Attacco**, è un tentativo da parte di un avversario di sfruttare una vulnerabilità.
- **Rischio**, è la probabilità di essere bersaglio di un attacco.
- **Contromisura**, è un'azione o uno strumento che contrasta una minaccia e mitiga il rischio.

La modellazione delle minacce può essere definita come la "revisione sistematica delle caratteristiche e dell'architettura dell'applicazione da un punto di vista della sicurezza". Tale processo fornisce un approccio strutturato per identificare e classificare le minacce basate sui componenti del software, sui flussi di dati e sui confini di fiducia (confini entro i quali esistono dei criteri di sicurezza).

[13] Per l'attività di Risk Assessment si deve far riferimento alla metodologia e al tool adottato da AGID a tale scopo (**Cyber Risk Management** - **https://www.sicurezzait.gov.it/Home**).