sicurezza. Un esempio di obiettivo di sicurezza potrebbe essere "Il sistema deve mantenere la riservatezza di tutti i dati classificati come riservati".
I requisiti di sicurezza possono essere distinti in quattro diverse tipologie:

1. **Requisiti funzionali sicuri**: che descrivono i criteri di sicurezza integrati in ciascun requisito funzionale. Tipicamente indicano anche ciò che non deve accadere. Questi possono ad esempio essere derivati da casi di uso improprio.
2. **Requisiti di sicurezza funzionale**: definiscono i servizi di sicurezza che devono essere implementati nel sistema sottoposto ad analisi. Alcuni esempi sono l'autenticazione, l'autorizzazione, il backup, il server-clustering, ecc. Questi possono essere derivati dalle best-practices di sicurezza, dalle politiche adottate e dalle eventuali norme che il sistema stesso deve rispettare.
3. **Requisiti di sicurezza non funzionali**: trattasi di requisiti architetturali legati alla sicurezza, come “la robustezza" o "le prestazioni minime e la scalabilità". Questa specifica tipologia di requisiti è tipicamente derivata dai principi architetturali di secure-design e dagli standard in tale ambito.
4. **Requisiti di sviluppo sicuro**: descrivono le attività richieste durante lo sviluppo del sistema al fine di garantire che il sistema stesso nella sua versione finale sia esente da vulnerabilità. Alcuni esempi possono essere la "classificazione dei dati", le "linee guida di sviluppo sicuro” o la “metodologia di test”. Tali requisiti sono derivati da framework metodologici basati su best-practices come "CLASP".

Tutti i requisiti di sicurezza devono essere identificati dall'analista e analizzati dal team di sicurezza come parte dei requisiti funzionali e quindi aggiunti nel documento "Specifica dei requisiti di sicurezza", in una sezione dei requisiti di sistema o dei requisiti software. Di seguito si riportano alcune delle voci che dovrebbero essere presenti nel documento in questione:

- **Descrizione del prodotto** o sistema e relativo scopo. Definisce il perimetro del prodotto, in termini generali, sia in modo fisico sia logico.
- **Ambiente operativo**: definizione dei vincoli di sicurezza previsti per l'ambiente operativo al fine di facilitare l'identificazione e la formulazione delle premesse sull'uso previsto del prodotto. L'analista deve valutare l'uso dell'ambiente in cui opera il prodotto per verificare se il comportamento dell'utente può in qualche modo compromettere la sicurezza del prodotto stesso. A volte sarebbe necessario definire i criteri di protezione del prodotto e del suo ambiente operativo da adottare.
- **Funzioni di sicurezza di base**: descrizione delle features essenziali per implementare le necessarie politiche di sicurezza organizzativa.
- **Livello di garanzia della sicurezza**: tutti i prodotti devono avere un “Software Security Assurance” e questo, deve necessariamente essere incluso nel documento di specifica dei requisiti di sicurezza.
- **Requisiti normativi**: definizione dei requisiti normativi che il prodotto, lì dove applicabile, deve rispettare.

9.1 Definizione dei requisiti di sicurezza

I principali obiettivi di sicurezza da definire sono:

- **Riservatezza e Integrità.** I due più importanti aspetti della sicurezza sono Riservatezza e Integrità. La Riservatezza significa che le risorse possono essere utilizzate solo dalla parte legittima. L'integrità dei dati significa che devono essere modificabili solo dalle persone autorizzate.
- **Autenticità.** Il terzo requisito di sicurezza principale è l'Autenticità: *Message authenticity* (o *data* origin authenticity) ed *entity authenticity*.

- **Non-ripudio.** Garantisce che qualsiasi azione sul sistema non possa essere in seguito rinnegata.
- **Flusso Informativo**. Il livello di sicurezza può avere regole diverse. Generalmente si considerano due livelli: alto (altamente sensibile o altamente attendibile) e basso (meno sensibile o meno attendibile). Laddove componenti di sistema considerati di alto livello interagiscono con parti meno attendibili, si deve garantire che non vi sia alcuno scambio di dati dall'alto verso il basso (vale invece il contrario ossia ci può essere lo scambio di dati dal basso verso l'alto *non up-flow*).
- **Controllo Accessi**. Uno dei requisiti di sicurezza principali è il controllo degli accessi, il che significa che solo un utente fidato può avere accesso a un sistema sicuro. Il **Role-Based Access Control (RBAC)** assicura un meccanismo di controllo degli accessi per tutelare i beni. I privilegi di accesso alle risorse dipendono dal ruolo che assumono nel tempo gli individui all'interno dell'Organizzazione. Ai ruoli sono associati profili che definiscono comandi, transazioni e accessi ai dati. L'assegnazione dei ruoli è centralizzata. **ABAC** (Attribute Based Access Control) fornisce i diritti di accesso in base agli attributi dell'utente, delle risorse a cui si accede e dell'ambiente (contesto operativo, tecnico e persino situazionale in cui si verifica l'accesso alle informazioni). Gli attributi sono insiemi di etichette o proprietà che possono essere utilizzati per descrivere tutte le entità che devono essere considerate ai fini dell'autorizzazione. Le regole di sicurezza possono essere definite per una qualsiasi combinazione di attributi, offrendo la possibilità di creare regole specifiche per particolari risorse. Questa caratteristica rende ABAC particolarmente indicato per essere adottato nei sistemi che richiedono un controllo di accesso granulare come l'Internet of Things.

Le principali azioni di sicurezza da attuare sono:

- **Definizione degli elementi di sicurezza applicativa**, finalizzata alla valutazione dei requisiti relativamente a**:**
  - Integrità,
  - Autenticità,
  - Riservatezza,
  - Disponibilità,
  - Non-ripudio,
  - Autorizzazione.
- **Definizione dei requisiti di privacy**, attraverso la raccolta strutturata delle seguenti categorie di informazioni:
  - Dati personali,
  - Servizi di terze parti,
  - Policy.
- **Risk assessment**, finalizzato alla valutazione del rischio (vedi Paragrafo6.2). In questa fase viene definito un profilo di rischio per l'applicazione che include: aree sensibili del software e aree che presentono superfici di attacco suscettibili a determinate minacce; aree del codice ad alto rischio che possono essere vulnerabili a diverse minacce. Viene condotta quindi, una fase critica di comprensione, analisi e classificazione dei vari rischi per l'applicazione. Durante questo processo è utile classificare i vari rischi utilizzando diversi framework di sicurezza quali: OWASP Top 10, SANS CWE Top 25 o OWASP ASVS.
  - **Consolidamento dei Requisiti**, review dei requisiti di sicurezza e privacy a seguito del Risk Assessment;