Sicurezza

Alessandro Savioli

Marzo 2025

Contents

1 Introduzione

Secondo il **NIST** (National Institute of Standards and Technology) il termine *sicurezza informatica* può essere definito come:

> Misure e controlli che assicurino **confidenzialità, integrità e disponibilità** di asset del sistema informatico che includono hardware, software, firmware e informazioni processate, memorizzate e comunicate.

2 CIA e Livelli di impatto

2.1 CIA

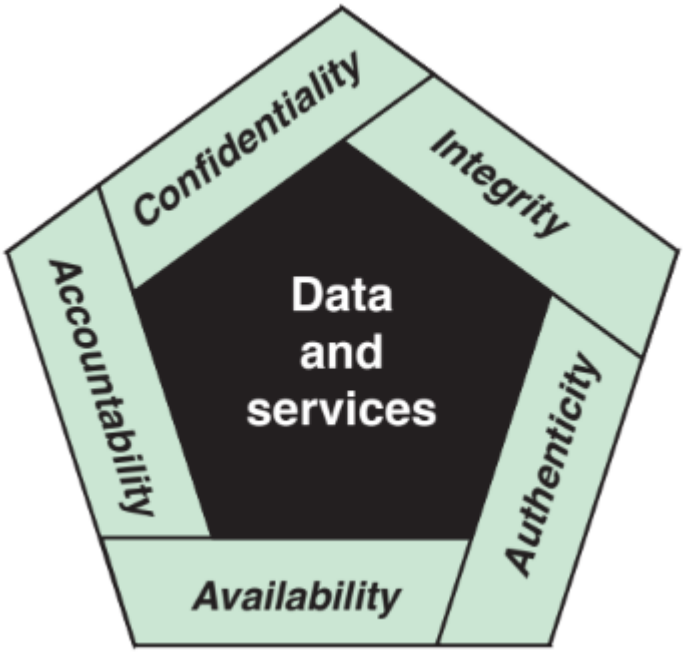
Nel campo della sicurezza informatica possiamo trovare tre obiettivi o requisiti principali:

- **Confidentiality**, ovvero preservare l'accesso autorizzato e prevenire la divulgazione di informazioni, come dati sensibili o proprietari;
- **Integrity**, ovvero la prevenzione contro la modifica o la distruzione impropria di informazioni, assicurando anche che un informazione non possa essere ripudiata oltre che quest'ultima sia autentica;
- **Availability**, ovvero assicurare l'accesso ad una determinata informazione.

A questi tre obiettivi principali se ne possono accostare ulteriori due, così da formare un quadro completo di tutto ciò che serve ad un sistema per essere sicuro:

- **Authenticity**, ovvero la proprietà di un utente di essere verificato e affidabile. Questo significa verificare che gli utenti siano chi dicono di essere e che gli input del sistema derivino sempre da una fonte affidabile;

- **Accountability**, ovvero la capacità di tracciare le attività di una qualsiasi entità all'interno del sistema, così da poter ricondurre un attacco ad un responsabile e tenere traccia di cosa sia successo per andare poi a migliorare la sicurezza del sistema.



2.2 Livelli d'impatto

Analizziamo ora i diversi livelli d'impatto che un attacco può procurare ad una organizzazione:

1. **Impatto basso**, causa una degradazione lieve alle funzioni dell'organizzazione, che risulta ancora in grado di svolgere le sue funzioni principali ma con efficacia ridotta. Può causare danni **minori** ad assets, finanze o danni agli individui;

2. **Impatto moderato**, causa una degradazione significativa alle funzioni dell'organizzazione, che risulta ancora in grado di svolgere le proprie funzioni ma con efficacia nettamente ridotta. Può causare danni **significativi** ad assets e finanze o agli individui, senza includere perdite di vite;

3. **Impatto elevato**, causa una degradazione severa alle funzioni dell'organizzazione, che non risulta più in grado di svolgere una o più delle sue funzioni primarie. Può causare danni **severi o catastrofici** ad assets e finanze o agli individui, includendo anche perdite di vite.