1 Introduction

the terms information, computer and network security get confused, but the difference is important

- information security regards all the the prevention of any damage involving data, in any format
- Computer security regards the protection of the phisical machine and the data it contains
- Network security regards the protection of the network and infrastructure of a company

cybersecurity is the ability to protect the use of cyberspace (internet, private networks,...) from cyber attacks

1.1 Remarks on security

Adversaries

Security is characterized by protection against malicious adversaries, with different motivations (money or glory), different capabilities and objectives. This details compone the modelling of a malicious adversary

Mitigation

To mitigate a threat, various strategies are aviable, reguarding people, processes and technologies. This controls are classified in preventive, detective and corrective.
What conditionates which tactic to select is risk management, or the process to identify the probability of an attack and the extention of the subsequent damage

Trust

A library, or dependency, or every third party product to a software, requires trust and dependability, also known as the ability to avoid failures.

Residual Risks

All security controls can mitigate an attack, but do not avoid it completely. In some cases they can contain more vulnerabilities

1.2 Cia Triad

The most important security properties are Confifentiality, Integrity and Availability

Confidentiality

The main objective of confidentiality is to protect personal privacy and proprietary information from unauthorized indiviaduals. Confidentiality covers data in storage, during processing and while in transit

Integrity

In this case our objective is to avoid unauthorized modification or destruction of data, including the authenticity and non-repudiation

Availability

Ensuring timely and reliable access to data and services by authorized users

1.3 Risk

Vulnerability

A vulnerability is a weakness or flaw in a system, procedure, design or network that can be exploited by a threat source. They are characterized by the difficulty in identifying and exploiting them

Threat

A threat is any circumstance or event that could impact organiazational operations or assets via unauthorized access, destruction and modification of data or denial of service. They are characterized by the propensity to attack (intent) and the ability to successfully do it (capability)

Risk

the probability that a threat will exploit a system vulnerability is called risk, and it's calculated in function of the impact and the likelihood of occurrence.

The risk is anilized though a matrix $5x5$ which uses the the severity of the impact and the likelihood to happen as axis and gives point based on the multiplication of the axes

1.4 Secutity policy, service and mechanism

This three things are, in order, the rules set by an organization to protect data, the capabilities to support one or more security requirements and the devices and functions used to protect data and provide security services