LEC4

Information security

- Types of information security

2025-2026
Second semester
2026-2-25

Alaa Y. Taqa

Definition of Information Security

Information Security (InfoSec) is the practice of **protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction** in order to ensure the **confidentiality, integrity, and availability of data**.

It is a key part of **Cybersecurity** and is closely related to **Cryptography**, which provides methods for protecting data.

Main Goals of Information Security (CIA Triad)

1.Confidentiality

Ensures that information is **accessible only to authorized users.**

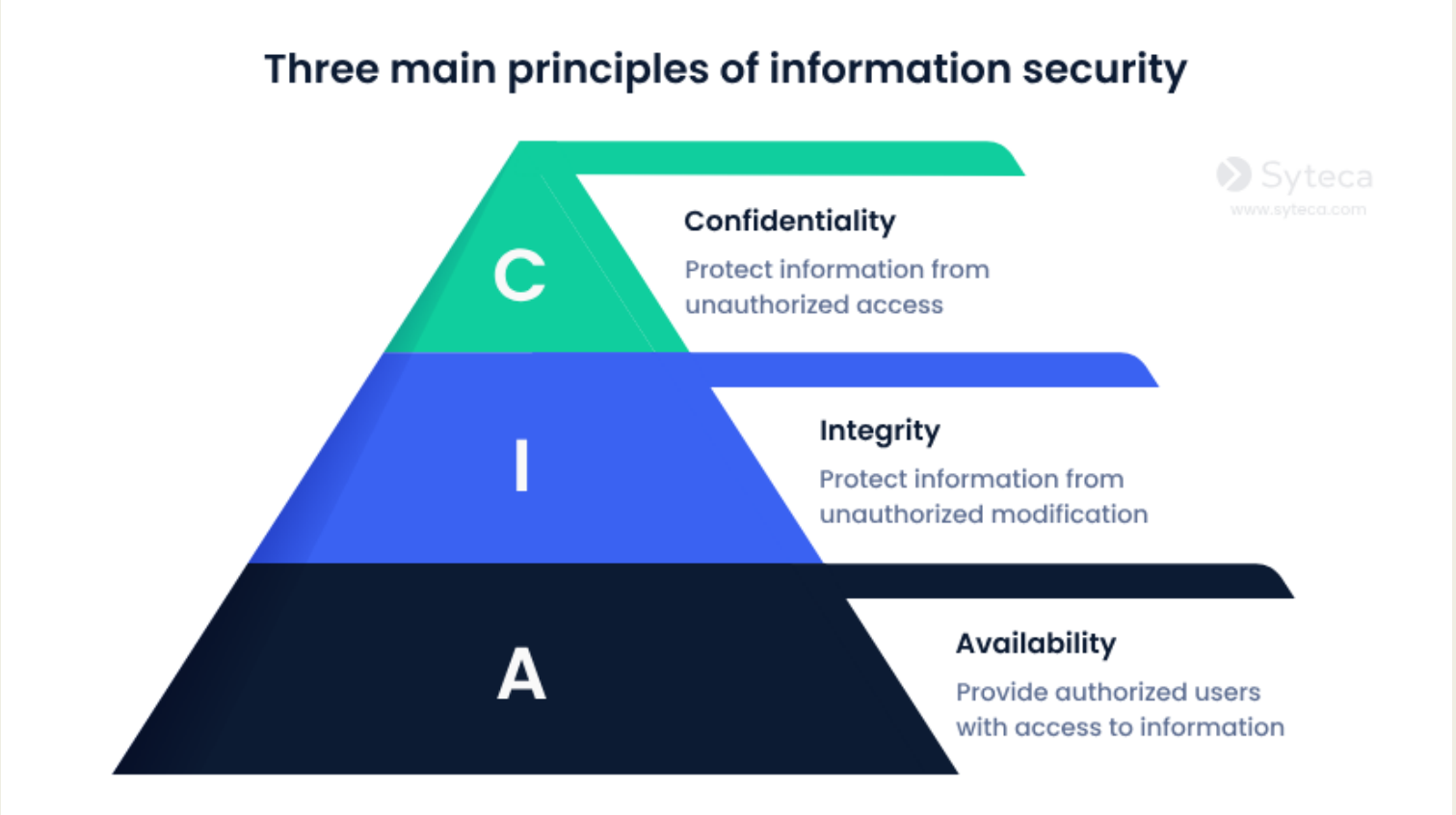
Example: Password-protected files or encrypted emails.

2.Integrity

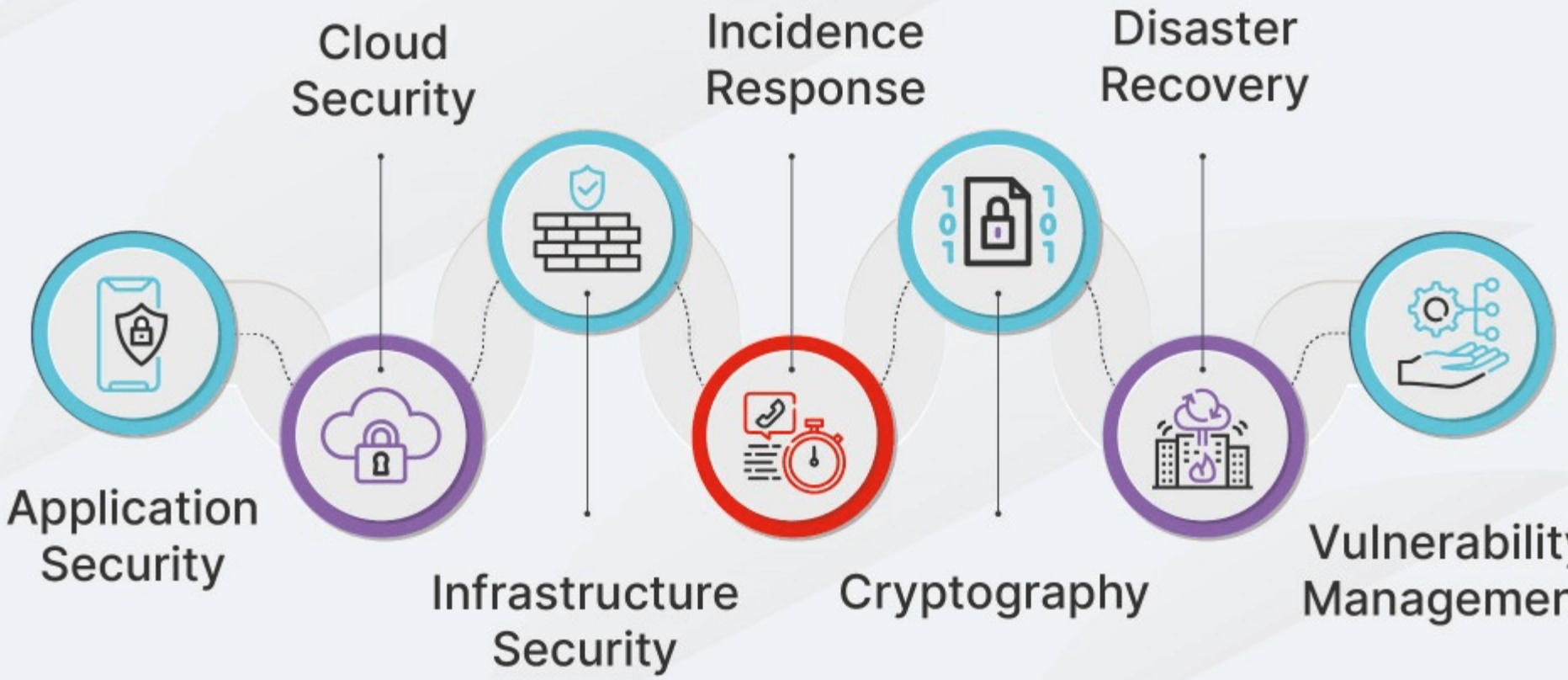
Ensures that data **remains accurate and is not altered by unauthorized users.**

3.Availability

Ensures that **authorized users can access information when needed.**



Types of Information Security



Need for Information Security

Information security is the practice of protecting information and information systems from **unauthorized access, use, disclosure, disruption, modification, or destruction**. It is a major part of **Cybersecurity** and **Information Security**.

Why Information Security is Needed

1.Confidentiality

1. Ensures that sensitive information is accessed **only by authorized people**.
2. Example: Protecting bank account details or medical records.

2.Integrity

1. Ensures that information is **not altered or modified** by unauthorized users.

3.Availability

1. Ensures that data and systems are **available when needed**.

4.Authentication

1. Verifies the **identity of users or systems**.

5.Non-repudiation

1. Prevents a sender or receiver from **denying a transaction** later.

These goals together form the **CIA Triad (Confidentiality, Integrity, Availability)** used in security design.

2. Examples of Security Violations

A **security violation** occurs when information security rules are broken and the system becomes compromised.

1. Unauthorized Access

When someone gains access to data without permission.

Example:

•A hacker logging into another person's email account.

2. Data Modification

Changing or altering information without authorization.

Example:

•An attacker changing bank account balances in a database.

3. Data Interception
Unauthorized users secretly access transmitted data.
Example:
•Someone capturing passwords over a public Wi-Fi network.

4. Denial of Service (DoS)
Attackers overload a system so that legitimate users cannot access it.
Example:
•Flooding a website with requests so it crashes.

5. Identity Theft
Someone uses another person's identity for fraudulent purposes.
Example:
•Using stolen credit card information for online purchases.

6. Malware Attacks
Malicious software used to damage or control systems.
Example:
•Viruses or ransomware encrypting files and demanding payment.

Security Mechanisms

Security mechanisms are techniques or tools used to **detect, prevent, or recover from security attacks**.

1. Encryption

Protects data by converting it into unreadable form using **Cryptography**.

Example:

- Secure communication on HTTPS websites.

2. Authentication Mechanisms

Verify the identity of users.

Examples:

- Passwords
- Biometrics (fingerprint, face recognition)
- Two-factor authentication

3. Access Control
Limits who can access certain data or resources.
Example:
•Only administrators can edit system settings.

4. Digital Signatures
Used to verify message authenticity and integrity.
Example:
•Secure online document signing.

5. Firewalls
Software or hardware systems that **monitor and control network traffic**.
Example:
•Blocking unauthorized connections from the internet.

6. Intrusion Detection Systems (IDS)
Systems that **monitor networks and detect suspicious activities**.


Questions


THANK
YOU