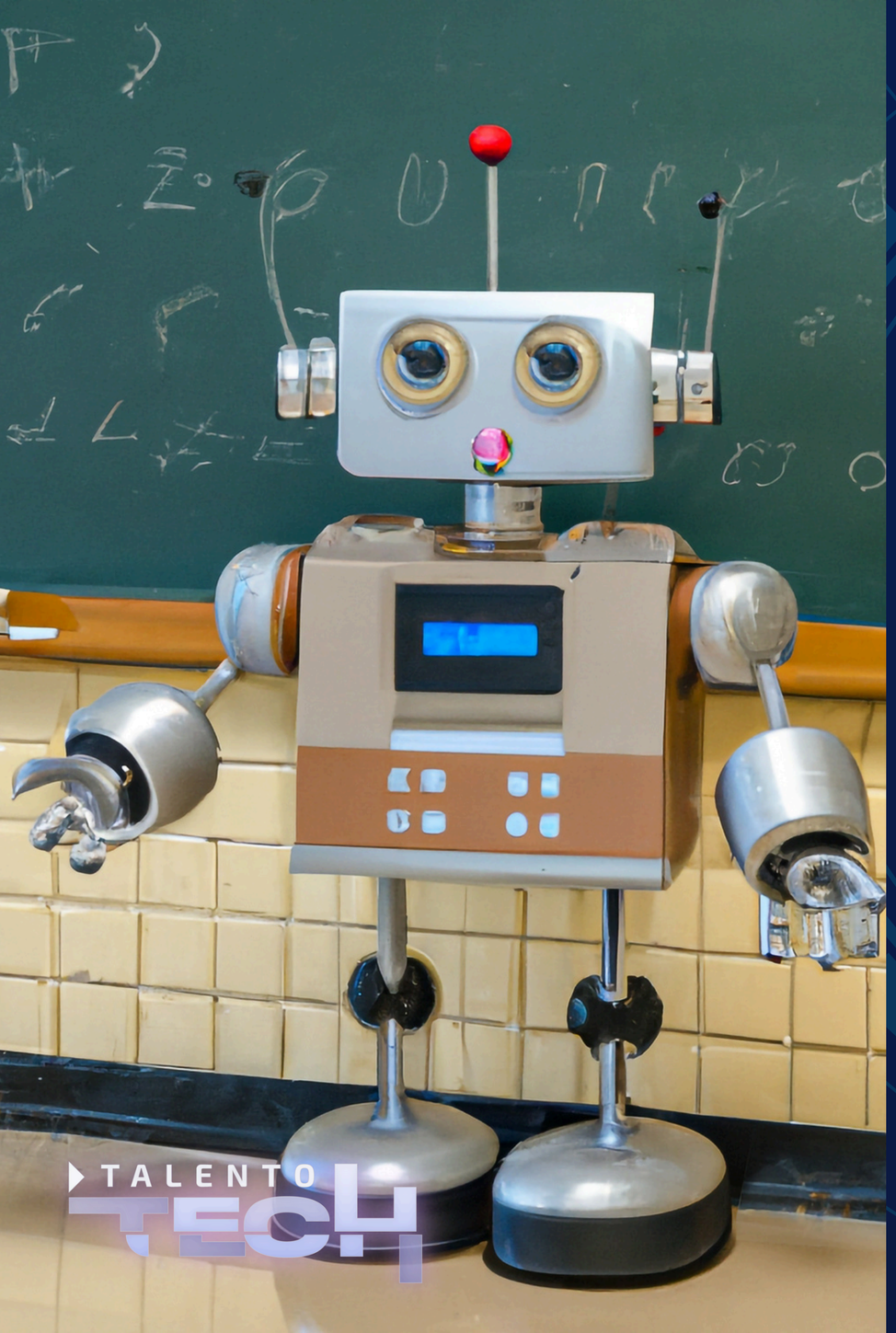
TALENTO TECH

REGIÓN 3
CAUCA – NARIÑO
LESSON 1- UNIT 3

TIC

Universidad Tecnológica de Pereira

faceIT



Lesson 1: Information Security Framework

1)Idiom of the day

"Red flag"
A "red flag" is a warning sign or a signal of possible danger when something raises one. This expression can be used in computer security to characterize questionable behavior or irregularities that need to be addressed right away. An abrupt increase in network traffic, for instance, maybe a "red flag" signaling a potential cyberattack.

2)Warm-up activity "The Security Shield Game"

Objective:
Introduce the concept of an Information Security Framework by having students collaborate to build a "security shield" to protect an imaginary organization.
Materials Needed:

- A whiteboard or virtual collaboration tool (e.g., Jamboard, Miro, or a shared Google Doc).
- Sticky notes (if offline) or digital text boxes.
- A basic scenario or story about an organization facing security challenges.

TIC

Universidad Tecnológica de Pereira | faceIT

Instructions:

1.Set the Scene:

Begin with a short scenario:

"Imagine you're the security team of a company that stores valuable customer data. Hackers, malware, and accidental data breaches threaten the company every day. Your mission is to create a strong shield to protect the company's information."

2. Brainstorm Key Components:

Divide the class into small groups. Then, ask each group to brainstorm 2–3 strategies, tools, or principles they think are necessary for building this "security shield." (Examples: passwords, firewalls, policies, training). Write each idea on sticky notes or add them as digital text boxes.

3.Build the Shield:

- Have groups come forward (or collaborate virtually) to add their ideas to a large "shield" outline on the board or screen.
- Encourage them to briefly explain why they chose each component.

4.Facilitate Discussion:

- After the shield is built, discuss how their suggestions align with the key elements of an Information Security Framework.
- Introduce the core pillars: confidentiality, integrity, availability, policies, monitoring, and risk management.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

5.Reflection Question: Ask the class: "What would happen if one piece of our shield was missing or weak? How might this impact the organization?"

Explain that the "security shield" they built represents the foundation of an Information Security Framework. Each piece plays a critical role in protecting data, preventing breaches, and ensuring smooth operations.

3) Keywords

Information Security Framework: A set of rules and guidelines designed to protect sensitive information from cyber threats, ensuring that data is secure and accessible only to authorized individuals.
Security Policies: Official documents that establish rules and procedures for managing and protecting information within an organization. These policies guide employees on how to handle sensitive information and how to respond to security incidents.
Sensitive Data: Information that must be protected due to its value or confidential nature, such as personal, financial, or medical data.
Cyber Threats: Risks and attacks that affect computer systems, including viruses, malware, hacking, and other forms of virtual attacks.
Password Policy: Rules defining how employees should create and manage passwords, such as requiring passwords to be sufficiently long and secure, and to be changed regularly.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

Data Protection Policy: Strategies and rules for protecting sensitive information, ensuring that only authorized personnel have access and that data is stored and disposed of securely.
Access Control Policy: Rules that define who can access different types of information and systems, ensuring that only necessary employees can view or manipulate sensitive data.
Incident Response Policy: Procedures established to handle and respond to security incidents, such as data breaches or cyberattacks, to mitigate damage and restore security.
Acceptable Use Policy: Guidelines that define acceptable use of company devices and networks, including restrictions on visiting dangerous websites or using unauthorized software.
Compliance: The process of ensuring that the organization adheres to relevant laws, regulations, and standards related to information protection and cybersecurity.

4) Reading: Information Security Framework and Security Policies

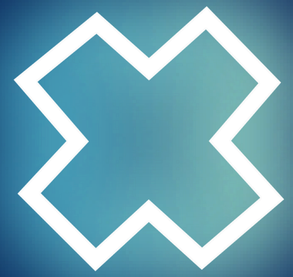
In today's world, protecting information is a top priority for businesses and organizations. An Information Security Framework is a system of rules and guidelines designed to help protect sensitive data from cyber threats. This framework ensures that the right measures are in place to protect data and keep it safe from unauthorized access, theft, or loss.

What Are Security Policies?

Security policies are official documents that outline the rules and procedures for managing and protecting information in an organization. They provide guidance on how to handle sensitive data, ensure that employees are aware of security risks, and define the actions to take in case of a security incident. These policies are part of the Information Security Framework and help organizations maintain a strong security posture.

Examples of Security Policies

- Password Policy: This policy defines how employees should create and manage passwords. For example, it might require that passwords be at least eight characters long and include a mix of letters, numbers, and special characters. The policy could also require that passwords be changed every few months.
- Data Protection Policy: This policy outlines how sensitive data, such as personal information or financial records, should be protected. It may include guidelines for encrypting data, restricting access to authorized personnel only, and securely disposing of old data.
- Access Control Policy: This policy defines who has access to different types of data and systems. It ensures that employees can only access the information necessary for their job. For example, a manager might have access to employee records, but a cashier would not.



- Incident Response Policy: This policy outlines the steps to follow in case of a data breach or cyberattack. It includes instructions for reporting incidents, investigating the breach, and recovering any lost or compromised data.
- Acceptable Use Policy: This policy sets guidelines for how employees should use company devices and networks. It may include rules about not visiting certain websites, not downloading unsafe software, and not sharing passwords.

Why Are Security Policies Necessary?

Security policies are necessary because they provide a clear framework for managing risks and responding to threats. Without policies, employees may not know how to properly handle sensitive information or how to react in case of a cyberattack. By setting clear rules and guidelines, organizations can:

- Protect sensitive data from theft or unauthorized access.
- Ensure compliance with legal and industry standards.
- Help employees understand their roles in maintaining security.
- Minimize the impact of security incidents through proper response procedures.

Information Security Frameworks and policies ensure that organizations can identify, prevent, and respond to potential security threats. By implementing clear rules and practices, businesses can protect their assets and maintain trust with customers and partners.