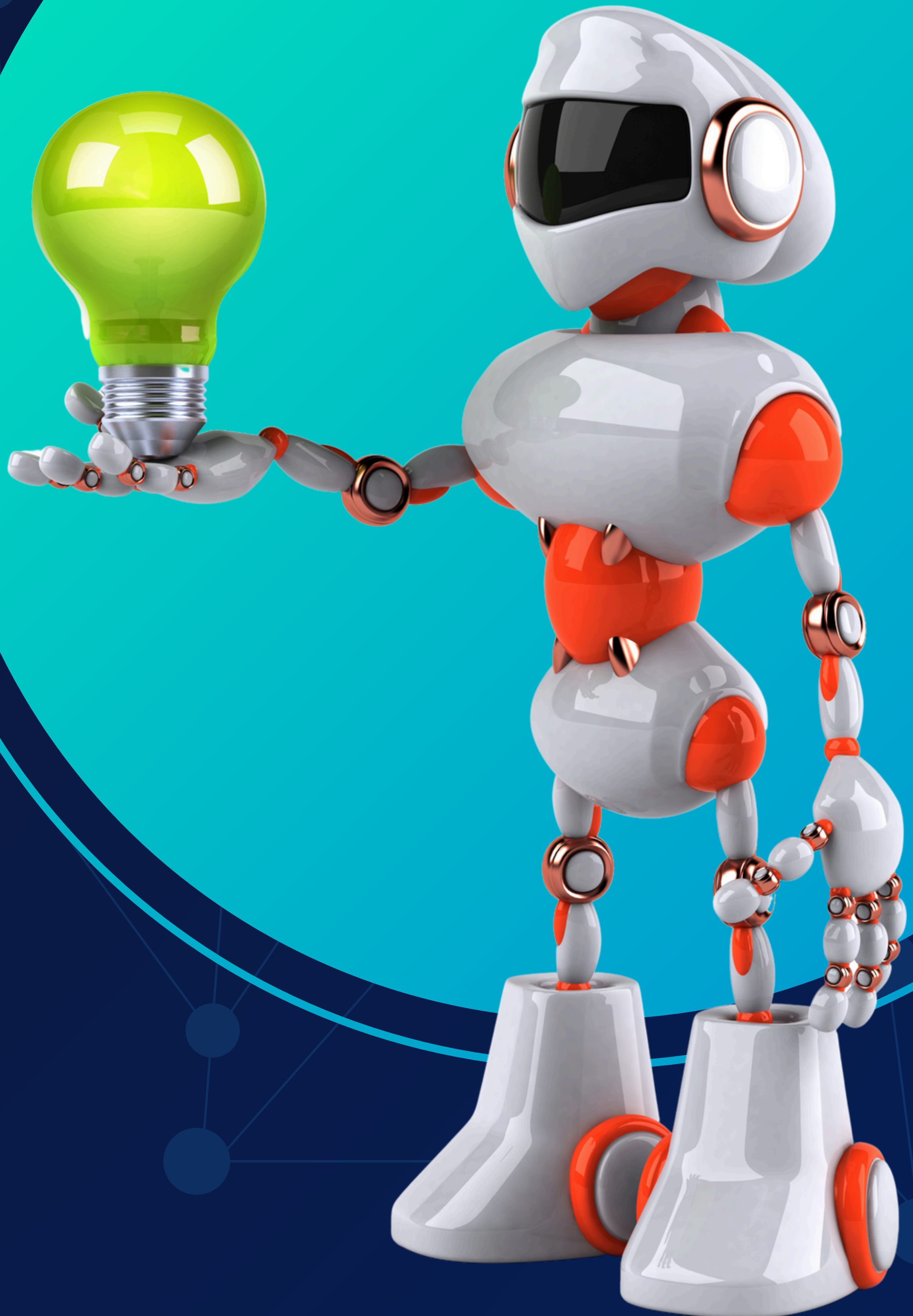
TALENTO TECH

REGIÓN 3
CAUCA - NARIÑO
LESSON 1 -UNIT 1



TIC

Universidad Tecnológica de Pereira

faceIT

Lesson 1: Digital Forensic Analysis

1)Idiom of the day

"Lock it down!": To implement strong security measures to protect a system or data.

Example: "After the data breach, the IT team decided to lock down the network with stricter access controls."

2) Activity: Warm-up activity "Spot the Digital Clue"

Objective:
To introduce students to Digital Forensic Analysis simply and engagingly by helping them identify "digital clues" in everyday situations.
Materials needed:

- A list of everyday digital activities or scenarios (examples provided below).
- A whiteboard or projector for discussion.

Instructions:

1.Start by asking: "Have you ever noticed how much information your devices keep about what you do daily? For example, your phone knows your location, your browser remembers websites you visit, and even your photos have hidden data!"

Explain briefly: "Digital forensic analysis is about finding these 'digital clues' to solve problems or answer questions."

1. Activity Setup:

- Present the following scenarios (you can write them on the board or share them verbally).
- Ask participants to identify the possible "digital clues" that might be found in each scenario.

Example Scenarios:

1.Scenario: A stolen smartphone.
Digital Clues:

- GPS location history.
- Recent app usage or messages.
- Last Wi-Fi connection.

2.Scenario: A social media account hacked.
Digital Clues:

- Login timestamps and IP addresses.
- Suspicious changes in account settings.
- Messages sent to contacts.

3.Scenario: A fake email claiming to be from a bank.
Digital Clues:

- Email header information (e.g., sender's IP address)
- Links in the email (phishing attempts).
- Misspellings or unusual formatting.

5.Scenario: A photo uploaded online reveals too much.

Digital Clues:

- Metadata (e.g., location, time, device used).
- Background details in the image.
- Who shared or liked the photo?

6.Scenario: An employee suspected of leaking files.

Digital Clues:

- File access logs on a computer.
- USB drive usage history.
- Email attachments sent from work accounts.

Group Discussion:

- After discussing the scenarios, ask:

"What tools or skills might be needed to analyze these clues?"

"Why do you think it's important to handle digital evidence carefully?"

1. Debrief:

- Emphasize that digital forensic analysis is like being a detective but in the digital world.
- Transition to the main lesson:
- "Today, we'll learn how experts analyze these types of clues to solve real-world problems."