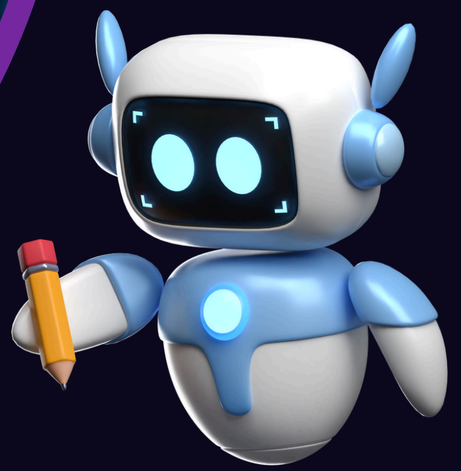
TALENTO TECH

TIC

REGIÓN 3
CAUCA – NARIÑO
LESSON 2



Universidad Tecnológica de Pereira | faceIT

LESSON 2: KEY WORDS

Socialize useful vocabulary before reading

ISO 27001: An international standard for information security management, providing a framework for organizations to protect sensitive data and ensure its confidentiality, availability, and security.

Information Security Management System (ISMS): A set of policies, procedures, and systems designed to securely manage and protect an organization's information from unauthorized access, damage, or loss.

Risk Assessment: The process of identifying potential risks to information, assessing their impact, and prioritizing actions to reduce vulnerabilities.

Security Controls: A set of 114 controls within ISO 27001 that are grouped into categories like access control, cryptography, and incident management. These controls guide organizations to improve security.

Compliance: The process of adhering to legal, regulatory, and contractual information security requirements.

Trust: The confidence customers and partners have in an organization's ability to protect sensitive data, especially when ISO 27001 is implemented.

Efficiency: The ability to manage risks and prevent costly security incidents through the application of ISO 27001 standards.

Reputation: The positive public image organizations gain by obtaining ISO 27001 certification, showing their commitment to security.

Certification: The process by which an organization proves it meets ISO 27001 standards through an external audit and assessment.

Cyberattacks: Malicious attempts to damage or disrupt information systems, which ISO 27001 aims to reduce by providing a structured approach to securing data.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT