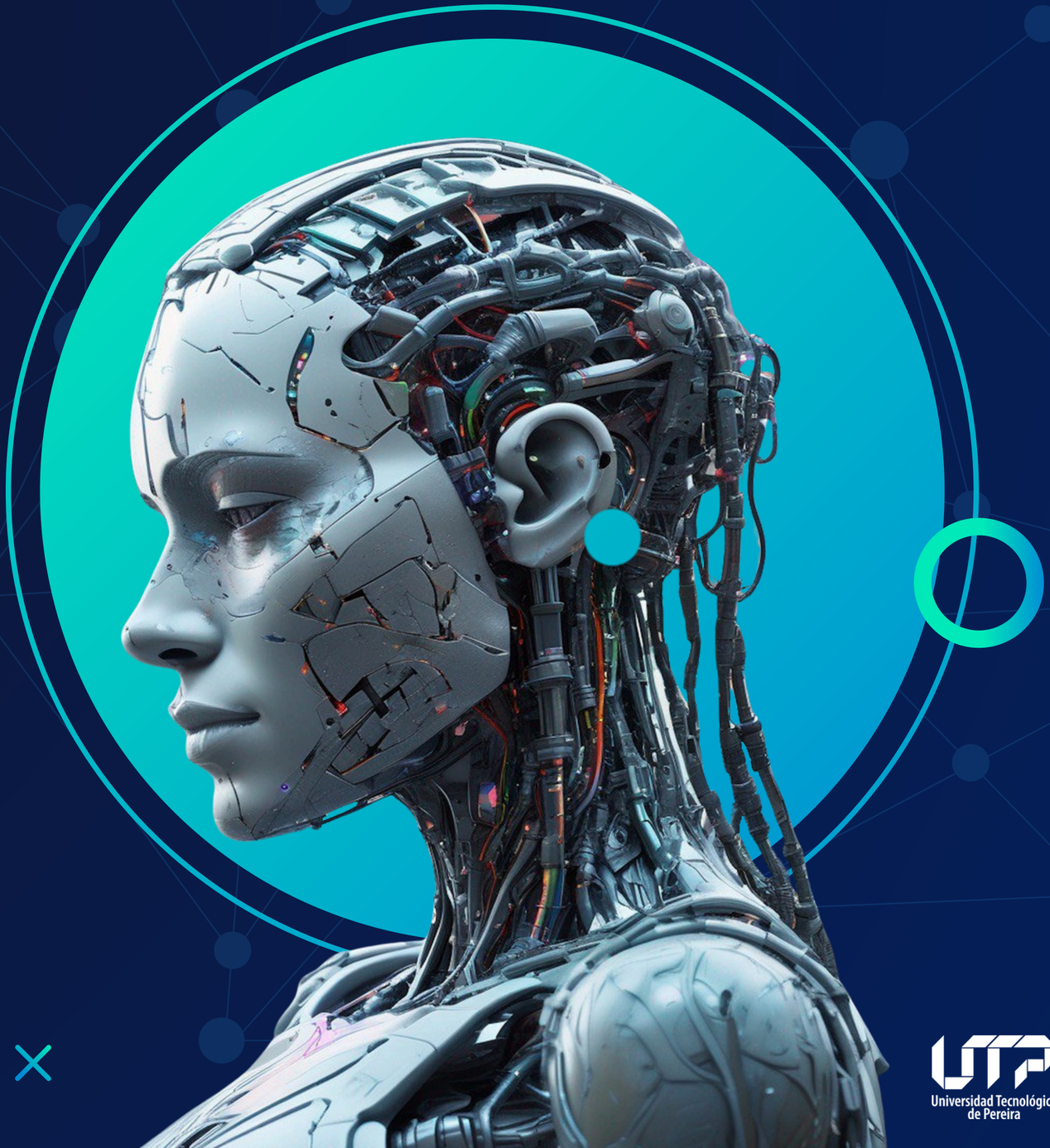
TALENTO TECH

REGIÓN 3
CAUCA - NARIÑO
LESSON 2 -UNIT 1



TIC

Universidad Tecnológica de Pereira

faceIT

Lesson 2: READING

TIC

Introduction to Cybersecurity: What Is It and Why DoesIt Matter?

What is cybersecurity?

Cybersecurity is a set of processes, tools, and frameworks designed to protect networks, devices, programs, and data from cyberattacks. Cybercriminals launch cyberattacks to gain unauthorized access to computer systems, disrupt business operations, modify, manipulate, or steal data, conduct industrial espionage, or extort money from victims.

Cyberattacks currently affect one in three Americans each year, with an attack occurring every 39 seconds. They often result in financial or reputational damage, damage to IT infrastructure, and regulatory fines. To protect their valuable assets and data from hackers, businesses and individuals need a strong cybersecurity posture.

TALENTO TECH

Universidad Tecnológica de Pereira | faceIT

Why is cybersecurity necessary?

In 2021, cybercrime cost the world US$6 trillion. By 2025, this cost will increase to US$10.5 trillion. Cybercrime is a growing problem, and to tackle it, a strong cybersecurity posture is essential.

Individuals, governments, businesses, nonprofits, and educational institutions are all at risk of cyberattacks and data breaches. The number of attacks will increase in the future, as digital technologies evolve, the number of devices and users increases, global supply chains become more complex, and data plays an increasingly strategic role in the digital economy. To minimize the risk of an attack and to secure systems and data, a strong cybersecurity posture becomes vital.

How are cybersecurity risks measured?

Cybersecurity risk is the potential for loss or harm resulting from damage to an IT asset, which can lead to intellectual property theft, financial loss, reputational damage, and legal
or regulatory fines. By measuring risk, organizations can optimize actions to better manage it, ensuring that business objectives are not hindered.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira | faceIT

Measuring cybersecurity risk typically involves all of the following steps:

Identify and prioritize assets. Assessing cybersecurity risk begins with understanding and prioritizing the assets of the organization, determining which assets could be impacted by loss, exposure, or damage.

Identify vulnerabilities. All vulnerabilities that could allow a threat to cause damage are identified using automated vulnerability scanning, penetration testing, or by using a vulnerability database such as the NIST National Vulnerability Database.

Assess the probability of a securityincident. The probability that a vulnerability could be exploited is assessed, and the vulnerability in question is then classified as high, medium, or low.

Calculate the threat impact. The probable impact or damage that a threat could cause to an asset is calculated and classified as high, medium, or low.

Calculate the risk. Risk = Threat x Vulnerability x Asset. From this equation, the organization can measure each risk.

TIC

Create a risk matrix for remediation planning. Finally, the risk matrix is established, with the two axes representing probability and impact.

Risk = Probability x Impact. From this value, each risk is classified as high, medium or low, after which appropriate reduction strategies are implemented.

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT