

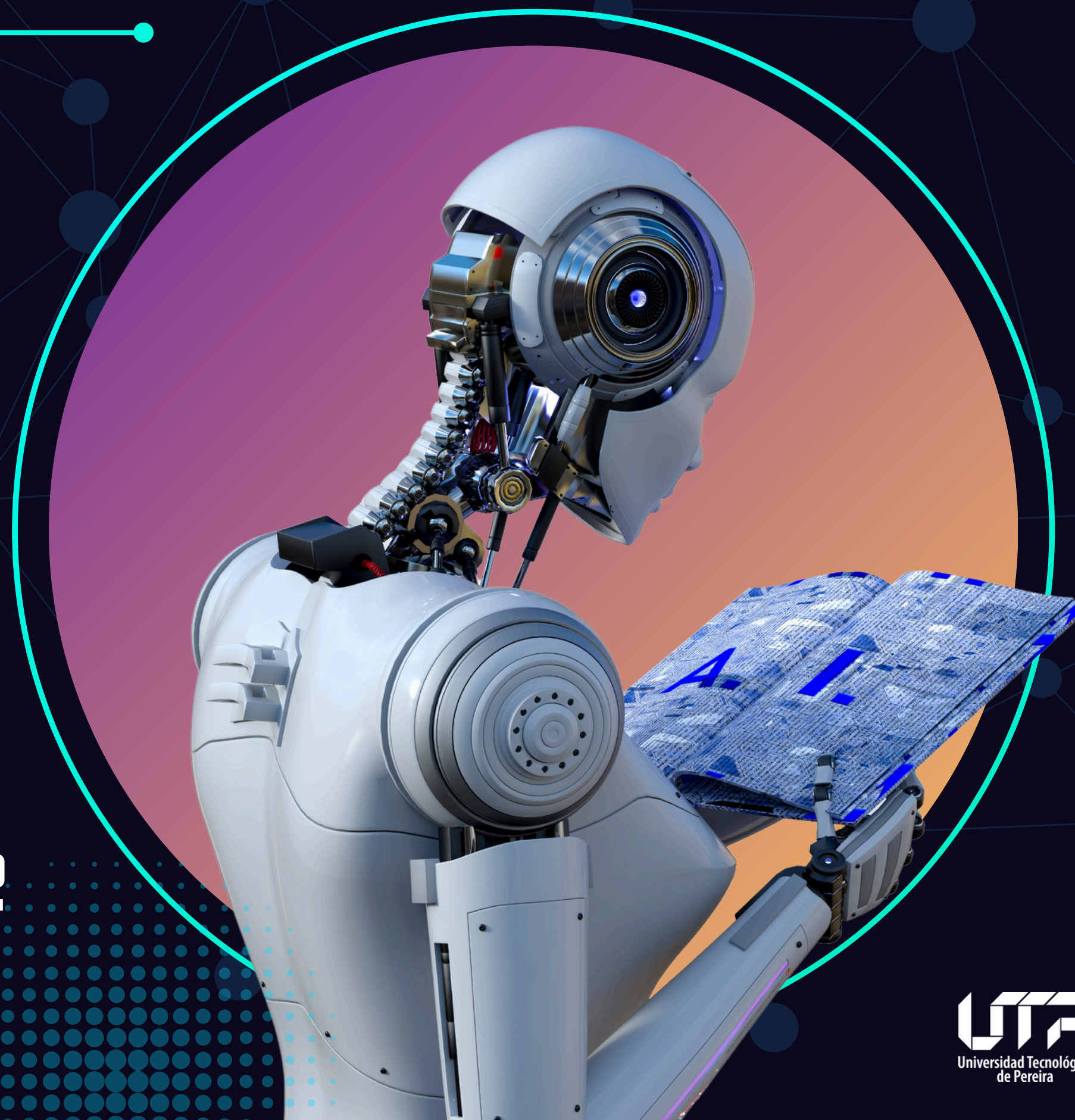


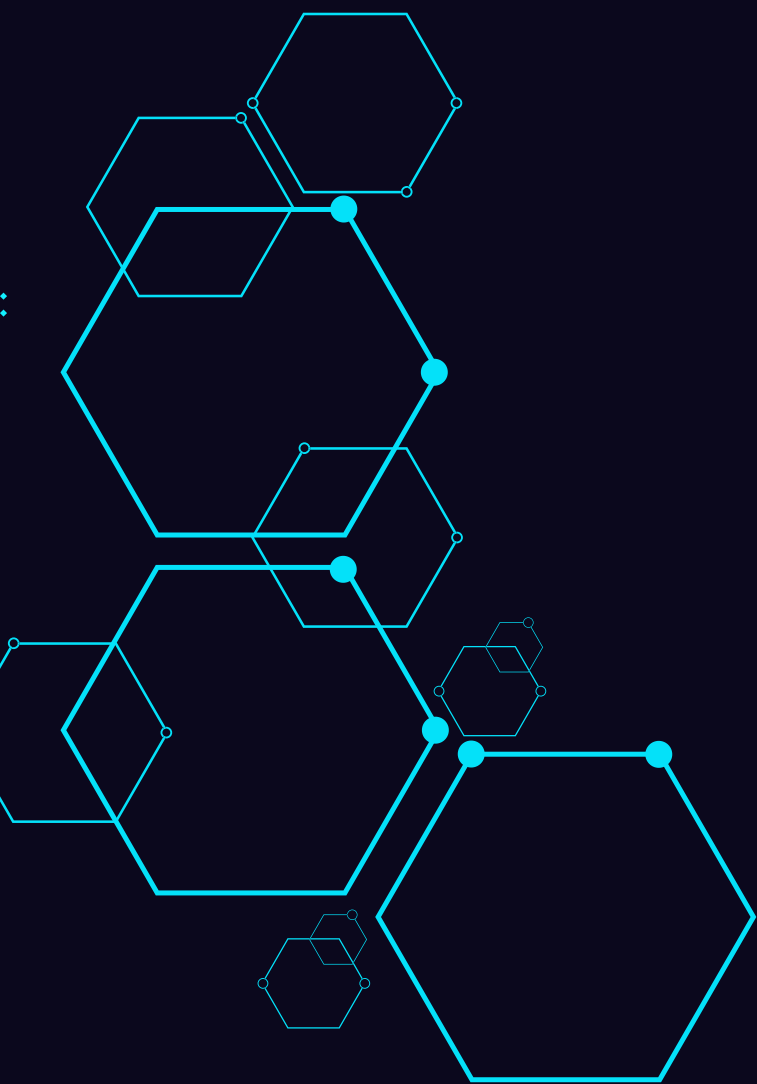
TIC



▶ TALENTO TECH

REGIÓN 3
CAUCA - NARIÑO
MODULE 2- UNIT 2





Unit 2: Identifying and Mitigating Vulnerabilities based on OWASP Top 10.

GENERAL OBJECTIVES:



Recognize the most common vulnerabilities in web applications and how to solve them.



Identify the list of vulnerabilities and risks compiled by the OWASP.



TIC



Linguistic competence: Use effective language, key concepts, and vocabulary to discuss topics related to cybersecurity, vulnerabilities, and system risks.

Pragmatic competence: Develop practical skills in applying cybersecurity principles, particularly those influencing identifying vulnerabilities and risks.

01

04

Topical Competence: Get a deep understanding of important cybersecurity concepts, terminologies, and the historical context of OWASP, aligning with exploring vulnerabilities and risks..

02

03

Sociolinguistic competence: Gain insights into the fundamentals and concept of OWASP and understand its societal implications, vulnerabilities, and risks to systems.



Competencies
to Develop



Time available: 4 hours

Lesson cybersecurity

- 1) Idiom of the day
 - 2) Activity 1. Warm-up activity - "Spot the Vulnerability"
 - 3) Lesson 1. Socialize keywords before reading.
 - 4) Lesson 2. Reading - OWASP Top 10 Vulnerabilities
 - 5) Activity 2. Complete the sentences
 - 6) Lesson 3. Video- OWASP Top 10 2021 - The List and How You Should Use It
 - 7) Activity 3. True or false questions about the previous video
 - 8) Reading: "Identifying Vulnerabilities and Fixing Them: A Practical Guide"
- Quizziz game about the previous reading



Learning materials.

<https://www.veracode.com/security/owasp-top-10>
<https://www.youtube.com/watch?v=hryt-rCLJUA>
<https://view.genially.com/6768634299f80ca1e7f6fef1/interactive-content-true-or-false-questions-about-video>
<https://quizizz.com/admin/quiz/6768dc3781d8eb5d0625cbd4>