ACTIVITY 2:

1. **Kahoot game:**

https://create.kahoot.it/details/9ef31aee-bc6b-481a-805a-0d1421d85a12

2. **Practical activity "Security and Vulnerability Management"**

Objective: Create and evaluate an effective security policy for a small fictional business that addresses key points such as passwords, access, and backups.

Steps to follow:

*1) **Form Teams:** Divide the class into groups of 3 to 5 people. Each group will work on creating a security policy for a fictional company.*

*2) **Define the Scenario:** Each group should imagine a fictional company and answer the following questions to define its context:*

- What is the name of the company?
- What type of products or services does it offer?
- What kind of sensitive data does it manage (e.g., customer information, financial records)?

3) Create the Security Policy:

Each group must create a security policy that includes the following key points:

1. **Password Policy:**
- What requirements should passwords meet (length, complexity, frequency of change)?
- **Example:** Passwords must be at least 12 characters long and include uppercase letters, lowercase letters, numbers, and symbols.

2. **Access Control:**

- How will access to sensitive information be granted and restricted?
- **Example**: Employees will only have access to the systems necessary for their job roles.

3. **Data Backup Policy:**

- How often will backups be performed?

- **Example:** Automated backups will be performed weekly and stored on an encrypted server.

4. **Incident Response:**

- What steps should staff follow if a security issue is detected?

4) Group Review

Each group will share their policy with another team to receive feedback. During the review, teams should analyze:

- Does the policy cover all key points (passwords, access, backups)?
- Is it clear and practical for employees?
- Does it include specific examples to facilitate understanding?

5) Final Presentation

One representative from each group will present their security policy to the rest of the class.