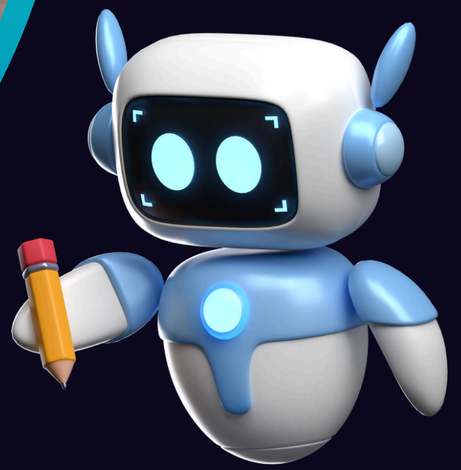
TIC

TALENTO TECH

REGIÓN 3
CAUCA – NARIÑO
LESSON 6



Universidad Tecnológica de Pereira | faceIT

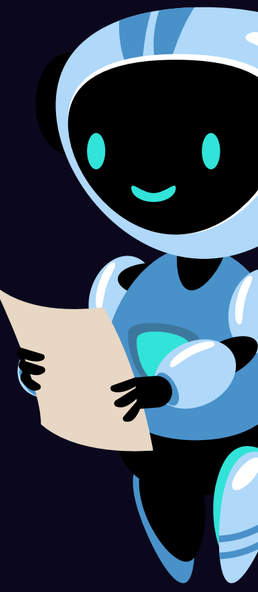
LESSON 6: Reading

Establish basic security policies

Creating effective security policies is essential for protecting an organization's information, systems, and employees. Security policies are written documents that outline rules and procedures for managing and safeguarding data, ensuring everyone understands their roles in maintaining security.

What Are Security Policies?

A security policy is a formal set of rules and guidelines that define how information and assets should be protected. These policies ensure compliance with legal and industry standards, protect against cybersecurity threats, and establish a clear framework for responding to incidents.



Key Points of Security Policies

1. **Purpose and Scope**

- Clearly define why the policy exists and what it covers.
- For example, a password policy might explain the need for strong, unique passwords for all systems.

2. **Responsibilities**

- Assign roles to specific individuals or teams, such as IT staff for technical controls and employees for following best practices.

3. **Definitions**

- Provide clear explanations of key terms, such as “sensitive data” or “access control.”

4. **Enforcement**

- Explain how compliance will be monitored and what consequences exist for violations.

5. **Review and Updates**

- Policies must be reviewed regularly to adapt to evolving threats and organizational changes.

How to Create Basic Security Policies

- **Identify Risks:** Conduct a risk assessment to understand potential threats, such as data breaches, phishing attacks, or insider threats.
- **Set Clear Objectives:** Define what you aim to achieve with the policy. For instance, a data protection policy might aim to prevent unauthorized data sharing.
- **Collaborate with Stakeholders:** Involve employees, management, and IT staff to ensure the policy is practical and comprehensive.
- **Use Simple Language:** Write policies in clear, non-technical language so all employees can understand them.
- **Include Real-Life Examples:** Provide examples to clarify expectations, such as how to handle suspicious emails or create strong passwords.

Examples of Basic Security Policies

- **Password Policy**

➔ Employees must use passwords with at least 12 characters, including letters, numbers, and symbols.

➔ Passwords should be changed every 90 days.

➔ Passwords must not be shared or written down in insecure places.

Rule: Use a password with at least 12 characters, including numbers, symbols, and uppercase letters.

Example: A strong password: "D@t@123Safe!"

Explanation: This rule prevents easy guessing or brute-force attacks.

- Email Usage Policy

➔ Only use company-approved email systems for work-related communication.

➔ Do not open attachments or click on links from unknown senders.

➔ Report any suspicious emails to the IT department immediately.

Rule: Only use company-approved email systems for work.

Example: Employees should report emails from unknown senders with subject lines like "Congratulations, you've won!"

Explanation: This prevents phishing attacks that target employees' emails.

- Data Protection Policy
  - → Sensitive data must be encrypted when stored or transmitted.
  - → Access to sensitive data should be limited to authorized personnel.
  - → Employees must lock their computers when leaving their desks.

Rule: Encrypt sensitive files during transmission.

Example: Use tools like Secure File Transfer Protocol (SFTP) instead of regular email for sharing files.

Explanation: Encryption ensures data remains secure even if intercepted.

Why Security Policies Are Important

- Protect Data: Prevent loss or theft of sensitive information.
- Ensure Compliance: Meet legal and industry requirements like GDPR or HIPAA.
- Build Trust: Show customers and partners that security is a priority.
- Reduce Risks: Minimize vulnerabilities and prepare for potential threats.