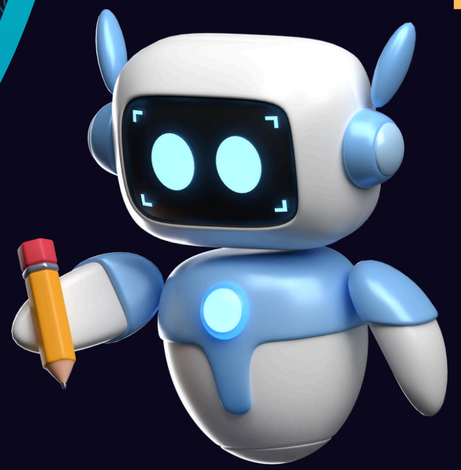
TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LESSON 2



Universidad Tecnológica de Pereira | faceIT

Lesson 2: READING

What Is Network Security? How to Keep Networks Safe

What is network securityand how does it work?Overall, network securityincludes the use of rules, techniques, and other security controls to safeguard crucial computer networks and their sensitive data against cyberattacks, malicious malware, and data breaches.

VPNs, NACs, and the Logic Behind Network Security Solutions

Network security relies on binary logic to allow or prohibit access, depending on security criteria. Who may see or utilize network resources is regulated by network access control (NAC).
Virtual Private Networks (VPNs) protect distant users, while powerful behavioral analytics detect and react to questionable activity. Network segmentation secures business networks, while antivirus software prevents cyber attacks.

Every component of network security is important from network security tools to security policies, incoming and outgoing traffic monitoring and application security to prevent application layer assaults. Even though network users depend on email security to protect them from phishing, security professionals work hard behind the scenes, using advanced security information systems to optimize network performance and protection.

Network security analysts, network administrators, and security architects work together to create a safe and secure environment. Strategies and solutions to secure networksand ensure their integrity in the face of evolving cyber threats change with the cyber environment.

Network Access Control

Network access control is a key component of network security and controls computer network data access. With today's complex network traffic from mobile devices and computers, a strong network security solution is essential for securing an organization’s critical information.

NAC checks and enforces security regulations on all devices connecting to an organization's network. These security rules restrict harmful software and unauthorized users, allowing only authorized users with system-compliant devices to access.
Network access controlalso protects sensitive data from externalthreats and breacheswhen it is combined with intrusion prevention systems, DLP software, and VPNs.

Too many security solutions might be daunting. Application security protects against application layer assaults, whereas wireless security ensures data integrity in wireless setups. Network segmentation isolates business networks, reducing cybersecurity risks.

Network Traffic

Network traffic is the data that flows over a network,such as a company's local area network (LAN) or the internet. Data streams power everything from corporate transactions to social interactions in the digital environment. This connection makes network security a constant issue.

Network ManagersAre Traffic Cops for a Network

Network traffic monitoring and control are key to network security. Network managers use security tools and application security procedures to keep data flowing while restricting malicious components. Every incoming and outgoing network bit and byte is monitored.

Virtual Private Network

Our connected digital world demands privacy, security, and access control. Networksecurity solutions employ VPNs to link remote users to constrained resources and secure data.

VPNs provide secure internet tunnels between computers to safeguard public network data. Computers and mobile devices might exchange data across shared or public networks like private networks. Remote users accessing their corporate network need this design.

VPNs improve network security in numerous ways and affect different types of network security. They protect important data, offer remote access, and prevent unauthorized access. VPNs also encrypt data packets for protection against malicious software and organizations.

A VPN isn't a universal security solution. Network security involves understanding of security controls and security technologies and their application to safeguard assets. A VPN combined with an intrusion prevention system detects and prevents threats in real time, improving network security.

The Important Role of VPNs in Modern Security

Like any security solution, VPNs need frequent updates. Security teams must outperform cybercriminals, and they need better security to resist new threats. VPNs are effective, but they are just one component of cybersecurity.

VPNs may improve company networks in the era of remote work and globalization because they offer secure, effective means to connect global network components or supply remote users with company resources.

However, VPNs are not perfect. The cyber environment is dynamic and constantly evolving, so effective network security needs to evolve as well. Organizations need VPNs and other security measures to protect their networks and valuable data.

VPNs are crucial to modern security. They represent the technology and strategy needed to traverse today's complicated digital environment by securing connections, protecting data, and allowing remote access.