SYLLABUS: Security and high availability	CREDITS: 6

COMPETENCES
AFTER COMPLETING THIS COURSE, STUDENTS WILL BE ABLE TO: C1: Optimize system performance by configuring the hardware devices. C2: Evaluate the performance of hardware devices and identify opportunities for improvement. C3: Implement high availability solutions, analyzing different options, to protect and restore the system to unforeseen situations. C4: Monitor physical security to prevent disruptions in service delivery system. C5: Ensure the system and data to prevent failures and external attacks. C6: Diagnose malfunctioning of the system and take corrective measures to restore its functionality. C7: Manage and maintain the resources based on workloads and maintenance plan.

COMPETENCES DISTRIBUTION		
COMPETENCE	ESSENTIAL 80% TIME 90% MARK	IDEAL 20% TIME 10% MARK
C1.1: Optimize system performance. C1.2: Configure hardware devices according to operational requirements.	X	
C2.1: Evaluate the performance of hardware devices.	X	
C2.2: Identify opportunities for improvements in hardware devices.	X	
C3.1: Implement high availability solutions.	X	
C3.2: Analyze different options of the market.		X
C3.3: Protect and restore the system of unforeseen situations.	X	
C4.1: Monitoring physical security as specified by the manufacturer.	X	
C4.2: Monitoring physical security as the security plan.	X	
C4.3: Avoid interruptions in service delivery system.	X	
C5.1: Ensure system and data according to usage needs.	X	
C5.2: Ensure system and data according to established security conditions.	X	
C5.3: Prevent failures and external attacks.	X	
C6.1: Diagnose the system malfunctions.	X	
C6.2: Adopt corrective measures.	X	
C6.3: Restore functionality.	X	
C7: Manage and maintain the resources based on workloads and maintenance plan.	X	

CONTENTS
Adoption of safe practices guidelines and information processing: - Reliability, confidentiality, integrity and availability. - Vulnerable elements in the computer system. Hardware, software and data. - Analysis of the main vulnerabilities of a computer system.

- Threats. Types. Physical and logical threats.
- Physical and environmental security.
- Location and physical protection of computers and servers.
- Uninterruptible power supply.
- Logical security.
- Cryptography.
- Access Control Lists.
- Establishing password policies.
- Storage policies.
- Backup and backup images.
- Storage Media.
- Forensic analysis in computer systems.

Implementation of active safety mechanisms:
- Attacks and Countermeasures in personal computers.
- Classification of attacks.
- Anatomy of attacks and malware analysis.
- Preventive tools.
- Mitigation tools.
- Updating systems and applications.
- Security in connection with public networks.
- Guidelines and safe practices.
- Security in the corporate network.
- Monitoring network traffic.
- Safety protocols for wireless communications.
- Potential risks of network services.
- Attempted penetration.

Implementation of remote access techniques. Perimeter security:
- Basic elements of perimeter security.
- Network perimeters. Demilitarized zones.
- Weak screened subnet architecture.
- Strong screened subnet architecture.
- Virtual Private Networks. VPN.
- Benefits and disadvantages over dedicated lines.

Encryption techniques. public key and private key.
- VPN network level. SSL, IPSec.
- VPN application level. SSH.
- Remote Access Servers.
- Authentication protocols.
- Access parameter settings.
- Authentication Servers.

Installing and configuring firewall:
- Using firewall.
- Filtering data packets.
- Types of Firewalls. Characteristics. Principal functions.
- Installing firewall. Location.
- Firewall filtering rules.
- Funcionality test. Probe.
- Event logs firewall.

Installing and configuring proxy servers:
- Types of proxy. Features and functions.
- Installation of proxy servers.
- Installing and configuring proxy clients.
- Configuration of caching proxy.
- Setting up filters.
- Authentication methods in a proxy.

Implementation of high availability solutions:
- Definition and objectives.
- Analysis of high availability configurations.
- Continuous operation.
- Data integrity and recovery of service.
- Redundant servers.
- Systems clusters.
- Load Balancer.
- Installation and configuration of high availability solutions.
- Virtualization systems.
- Possibilities of system virtualization.
- Tools for virtualization.
- Setting up and using virtual machines.
- High availability and virtualization.
- Simulation of virtualization services.

Legislation and regulations on safety and data protection:
- Legislation on data protection. Legal figures in the treatment and maintenance of data files.
- Legislation on services of the information society and email.