Learning Content phase	Learning outcome	Teaching /Learning objectives	Learning Activities (actions and teaching methods to meet the objectives)	Communication and Collaboration form	Resources, tools, and media
Introduction and orientation **20 minutes**	Understand the concepts and types of Internet of Things Attacks at basic level	-Define Internet of Things Attacks and its basic characteristics. -Identify different types of Internet of Things Attacks - -Explain how Internet of Things Attacks - Basics can be used to manipulate individuals and organizations into taking specific actions or divulging sensitive information	-Use Learning Videos to watch the basics Internet of Things Attacks -Discussion (Questions and Answers, brainstorming) -Ask students to share any recent incidents or news they have heard about Internet of Things Attacks	Verbal and guided	LMS
Lesson Execution -15 minutes	Analyze the impact and behavior of Internet of Things Attacks at basic level. Evaluate the effectiveness of Internet of Things Attacks detection and prevention strategies at basic level	- Analyze real-world examples of Internet of Things Attacks and their consequences - Study the propagation methods of different types of Internet of Things Attacks - Evaluate the impact of Internet of Things Attacks - on Individuals and Organizations at basic level - Analyze how individuals and organizations can be protected against Internet of Things Attacks and how these attacks can be detected (discuss the role of a strong cybersecurity strategy in dealing with these attacks)	-Discussion (Questions and Answers, brainstorming)	Verbal and Guided	LMS
Evaluation – 10 minutes	Assessment of students/lesson	Evaluate students' understanding of Internet of Things Attacks at basic level and their ability to apply this knowledge in a practical context.	Students will answer an online evaluation assessment/lesson feedback in the LMS and they will get the results	Written Evaluation	LMS/Quiz