Principali informazioni sull'insegnamento	
Titolo insegnamento	Organizzazione Aziendale
Corso di studio	Laurea Magistrale in Sicurezza Informatica
Crediti formativi	6
Denominazione inglese	Business Organization
Obbligo di frequenza	NO
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo Mail
	Vita Santa Barletta	vita.barletta@uniba.it

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Caratterizzante	SECS-P/10	6

Modalità di erogazione	
Periodo di erogazione	II semestre
Anno di corso	I
Modalità di erogazione	E-learning

Organizzazione della didattica	
Ore totali	150
Ore di corso	48
Ore di studio individuale	102

Calendario	
Inizio attività didattiche	01 Marzo 2021
Fine attività didattiche	04 Giugno 2021

Syllabus	
Prerequisiti	Prerequisiti definiti dal manifesto del corso di studi
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, riportati nei quadri A4a, A4b e A4c della SUA, compreso i risultati di apprendimento trasversali)	• *Conoscenza e capacità di comprensione* Conoscenze e competenze relative ai principali aspetti di organizzazione aziendale orientati alla sicurezza, ai processi di divisione e coordinamento del lavoro in un SOC (Security Operations Center) e CSIRT (Computer Security Incident Response Team) e all'organizzazione dei processi per la sicurezza dell'infrastruttura. • *Conoscenza e capacità di comprensione applicate* Saper definire ed organizzare i processi ed i servizi dell'impresa nella direzione della difesa e protezione delle proprie reti ed informazioni per poter garantire la business continuity di una organizzazione e renderla capace di rilevare attacchi di natura cibernetica e

	preservare, o ripristinare quando necessario, i servizi eventualmente coinvolti e danneggiati. • *Autonomia di giudizio* Capacità di formulare giudizi autonomi, nonché di esprimere valutazioni collegiali con riferimento alle politiche gestionali e scelte tecnico-progettuali degli enti nei quali potrà operare e sempre con riferimento agli aspetti connessi alla sicurezza. Capacità di proporre, valutare e giudicare soluzioni volte al miglioramento della sicurezza dell'organizzazione e dei suoi processi e servizi. • *Abilità comunicative* Comunicare ed esprimere verbalmente in modo chiaro ed efficace le conoscenze apprese, presentare i casi applicativi ed esempi illustrativi. Discutere le soluzioni adottate adeguando il contenuto al target professionale. Redigere elaborati scritti chiari, sintetici e coerenti. Lavorare in team con diverse professionalità. • *Capacità di apprendere* Individuare, elaborare e organizzare informazioni appropriate per soluzioni di problemi connessi all'organizzazione della sicurezza in una impresa. Elaborare e organizzare idee e soluzioni a problemi organizzativi connessi alla sicurezza in modo critico e sistematico.
Contenuti di insegnamento	Introduzione all'organizzazione aziendale • L'organizzazione • Le principali teorie dell'organizzazione • Le variabili dell'organizzazione • Le strutture organizzative L'organizzazione, i processi e i ruoli • La progettazione organizzativa • I processi di impresa • I ruoli chiave • I sistemi di gestione di impresa Introduzione alla Sicurezza Informatica • Sicurezza Organizzativa • Sicurezza Applicativa • Sicurezza in Rete L'organizzazione per la sicurezza • Metodi di attacco • Tecniche di Difesa • Controlli di sicurezza • SOC: Security Operations center • CSIRT: Computer Security Incident Response Team

	I processi per la Sicurezza
	• Processi SOC
	  ○ Incident analysis
	  ○ Security Information and Event Management
	  ○ Log Management
	  ○ Risk Management
	  ○ Vulnerability Management
	  ○ Controllo remoto delle workstation
	  ○ Analisi Forense
	  ○ Interfaccia all'Incident Analysis and Response
	  ○ Interfaccia al processo di Change Management
	• Processi CSIRT
	  ○ Incident triage
	  ○ Incident response
	  ○ Patch management
	  ○ Altri processi e funzioni del CSIRT
	
	I processi di controllo della Sicurezza
	• Verifica vulnerabilità
	• Protezione dei dati e Data Privacy
	• Altri controlli di sicurezza

Programma	
Testi di riferimento	• Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: A condensed field guide for the Security Operations team (Volume 2). ISBN-13: 978-1726273985 • Foundations of Information Security: A Straightforward Introduction. Jason Andress, October 2019, 248 pp. ISBN-13: 9781718500044
Note ai testi di riferimento	• ORGANIZZAZIONE AZIENDALE, 3ed 8838615284 · 9788838615283 di Giovanni Costa, Paolo Gubitta, Daniel Pittino. © 2015 | Data di Pubblicazione: 15 Dicembre 2015
Metodi didattici	• N° 16 ore di lezioni in modalità e-learning • N° 16 ore di esercitazione in piattaforma dedicata • N° 16 ore di ricevimento e approfondimento tecnico
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	La verifica dei risultati formativi raggiunti avviene durante l'esame, che prevede un colloquio orale in cui si presenta e si discute una tesina inerente gli argomenti trattati a lezione.

Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	• *Conoscenza e capacità di comprensione*
	  ○ Lo studente deve conoscere le principali strutture organizzative aziendali e saper correttamente collocare in esse i processi connessi ad un SOC e CSIRT.
	
	• *Conoscenza e capacità di comprensione applicate*
	  ○ Lo studente deve saper definire ed organizzare i

	processi ed i servizi dell'impresa nella direzione della difesa e protezione delle proprie reti ed informazioni. o Lo studente deve saper definire e strutturare operativamente il SOC ed il CSIRT. • *Autonomia di giudizio* o Lo studente deve saper formulare giudizi autonomi e fare valutazioni circa l'organizzazione dei processi connessi alla sicurezza di una impresa. o Lo studente deve saper valutare e giudicare soluzioni volte al miglioramento della sicurezza dell'organizzazione e dei suoi processi e servizi • *Abilità comunicative* o Lo studente deve saper esporre, comunicare ed esprimere in modo chiaro ed efficace le conoscenze apprese, presentare i casi applicativi e d esempi illustrativi. o Lo studente deve saper discutere le soluzioni adottate inerenti la sicurezza dell'organizzazione. o Lo studente deve saper redigere elaborati scritti chiari, sintetici e coerenti. o Lo studente deve saper comunicare con le diverse professionalità operanti in un SOC e un CSIRT. • *Capacità di apprendere* o Lo studente deve dimostrare attraverso lo svolgimento di piccoli esercizi pratici di saper elaborare soluzioni a problemi connessi all'organizzazione della sicurezza in una impresa. o Lo studente deve sapere elaborare e organizzare idee e soluzioni a problemi organizzativi connessi alla sicurezza.
Altro	