

<b>Principali informazioni sull'insegnamento</b>	
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

<b>Docente responsabile</b>	Nome Cognome	Indirizzo Mail
	Vita Santa Barletta	vita.barletta@uniba.it

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

<b>Modalità di erogazione</b>	
Periodo di erogazione	Il semestre
Anno di corso	I
Modalità di erogazione	E-learning

<b>Organizzazione della didattica</b>	
Ore totali	48
Ore di corso	48
Ore di studio individuale	

<b>Calendario</b>	
Inizio attività didattiche	24 Febbraio 2020
Fine attività didattiche	31 Maggio 2020

<b>Syllabus</b>	
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)	<ul style="list-style-type: none"> <li>• <i>Conoscenza e capacità di comprensione</i> 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.</li> <li>• <i>Conoscenza e capacità di comprensione applicate</i> 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</li> </ul>

	<p>preservare, o ripristinare quando necessario, i servizi eventualmente coinvolti e danneggiati.</p> <ul style="list-style-type: none"> <li>• <i>Autonomia di giudizio</i> 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.</li> <li>• <i>Abilità comunicative</i> 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.</li> <li>• <i>Capacità di apprendere</i> 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.</li> </ul>
<p>Contenuti di insegnamento</p>	<p>Introduzione all'organizzazione aziendale</p> <ul style="list-style-type: none"> <li>• L'organizzazione</li> <li>• Le principali teorie dell'organizzazione</li> <li>• Le variabili dell'organizzazione</li> <li>• Le strutture organizzative</li> </ul> <p>L'organizzazione, i processi e i ruoli</p> <ul style="list-style-type: none"> <li>• La progettazione organizzativa</li> <li>• I processi di impresa</li> <li>• I ruoli chiave</li> <li>• I sistemi di gestione di impresa</li> </ul> <p>Introduzione alla Sicurezza Informatica</p> <ul style="list-style-type: none"> <li>• Sicurezza Organizzativa</li> <li>• Sicurezza Applicativa</li> <li>• Sicurezza in Rete</li> </ul> <p>L'organizzazione per la sicurezza</p> <ul style="list-style-type: none"> <li>• Metodi di attacco</li> <li>• Tecniche di Difesa</li> <li>• Controlli di sicurezza</li> <li>• SOC: Security Operations center</li> <li>• CSIRT: Computer Security Incident Response Team</li> </ul>

	<p>I processi per la Sicurezza</p> <ul style="list-style-type: none"> <li>• Processi SOC <ul style="list-style-type: none"> <li>○ Incident analysis</li> <li>○ Security Information and Event Management</li> <li>○ Log Management</li> <li>○ Risk Management</li> <li>○ Vulnerability Management</li> <li>○ Controllo remoto delle workstation</li> <li>○ Analisi Forense</li> <li>○ Interfaccia all'Incident Analysis and Response</li> <li>○ Interfaccia al processo di Change Management</li> </ul> </li> <li>• Processi CSIRT <ul style="list-style-type: none"> <li>○ Incident triage</li> <li>○ Incident response</li> <li>○ Patch management</li> <li>○ Altri processi e funzioni del CSIRT</li> </ul> </li> </ul> <p>I processi di controllo della Sicurezza</p> <ul style="list-style-type: none"> <li>• Verifica vulnerabilità</li> <li>• Protezione dei dati e Data Privacy</li> <li>• Altri controlli di sicurezza</li> </ul>
--	--

Programma	
Testi di riferimento	<ul style="list-style-type: none"> <li>• 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</li> <li>• Foundations of Information Security: A Straightforward Introduction. Jason Andress, October 2019, 248 pp. ISBN-13: 9781718500044</li> </ul>
Note ai testi di riferimento	<ul style="list-style-type: none"> <li>• ORGANIZZAZIONE AZIENDALE, 3ed 8838615284 · 9788838615283 di Giovanni Costa, Paolo Gubitta, Daniel Pittino. © 2015   Data di Pubblicazione: 15 Dicembre 2015</li> </ul>
Metodi didattici	<ul style="list-style-type: none"> <li>• N° 16 ore di lezioni in modalità e-learning</li> <li>• N° 16 ore di esercitazione in piattaforma dedicata</li> <li>• N° 16 ore di ricevimento e approfondimento tecnico</li> </ul>
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)	<ul style="list-style-type: none"> <li>• <i>Conoscenza e capacità di comprensione</i> <ul style="list-style-type: none"> <li>○ Lo studente deve conoscere le principali strutture organizzative aziendali e saper correttamente collocare in esse i processi connessi ad un SOC e CSIRT.</li> </ul> </li> <li>• <i>Conoscenza e capacità di comprensione applicate</i> <ul style="list-style-type: none"> <li>○ Lo studente deve saper definire ed organizzare i</li> </ul> </li> </ul>

	<p>processi ed i servizi dell'impresa nella direzione della difesa e protezione delle proprie reti ed informazioni.</p> <ul style="list-style-type: none"> <li>○ Lo studente deve saper definire e strutturare operativamente il SOC ed il CSIRT.</li> </ul> <ul style="list-style-type: none"> <li>● <i>Autonomia di giudizio</i> <ul style="list-style-type: none"> <li>○ Lo studente deve saper formulare giudizi autonomi e fare valutazioni circa l'organizzazione dei processi connessi alla sicurezza di una impresa.</li> <li>○ Lo studente deve saper valutare e giudicare soluzioni volte al miglioramento della sicurezza dell'organizzazione e dei suoi processi e servizi</li> </ul> </li> <li>● <i>Abilità comunicative</i> <ul style="list-style-type: none"> <li>○ Lo studente deve saper esporre, comunicare ed esprimere in modo chiaro ed efficace le conoscenze apprese, presentare i casi applicativi e d esempi illustrativi.</li> <li>○ Lo studente deve saper discutere le soluzioni adottate inerenti la sicurezza dell'organizzazione.</li> <li>○ Lo studente deve saper redigere elaborati scritti chiari, sintetici e coerenti.</li> <li>○ Lo studente deve saper comunicare con le diverse professionalità operanti in un SOC e un CSIRT.</li> </ul> </li> <li>● <i>Capacità di apprendere</i> <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ Lo studente deve sapere elaborare e organizzare idee e soluzioni a problemi organizzativi connessi alla sicurezza.</li> </ul> </li> </ul>
Altro	