Università degli Studi di Cagliari
FACOLTA' DI INGEGNERIA E ARCHITETTURA

CORSO DI LAUREA MAGISTRALE IN COMPUTER ENGINEERING, CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

PERCORSO FORMATIVO COORTE 2018/19

1° anno

Sem	Insegnamento	SSD	TAF	CFU	Ore
1	Industrial Software Development	ING-INF/05	B	8	80
1	Supervisory control and monitoring	ING-INF/04	B	9	90
	Corso integrato: Intelligent Systems				
1	- Modulo: Artificial Intelligence	ING-INF/05	B	6	60
2	- Modulo: Machine Learning	ING-INF/05	B	6	60
2	Cybersecurity Technologies and Risk Management	ING-INF/05	B	10	100
2	Fault diagnosis and estimation in dynamical systems	ING-INF/04	B	5	50
	Un corso a scelta tra:				
	Corso integrato: Smart Grid and Critical Infrastructures				
2	- Modulo: Industrial Informatics for energy storage systems	ING-IND/32	C	2	20
2	- Modulo: Critical infrastructures for innovative power distribution	ING-IND/33	C	2	20
2	- Modulo: Measurements and Cybersecurity for Smart Grid	ING-INF/07	C	2	20
2	Physical-layer techniques for Wireless communication security	ING-INF/02	C	6	60

2° anno

Sem	Insegnamento	SSD	TAF	CFU	Ore
1	Operating Systems	ING-INF/05	B	7	70
	Corso integrato: Embedded Systems				
1	- Modulo: Advanced Embedded Systems	ING-INF/01	C	8	80
1	- Modulo: Internet of Things	ING-INF/03	C	6	60
	Corso integrato: Computer Forensics				
1	- Modulo: Computer Forensics Techniques	ING-INF/05	B	5	50
2	- Modulo: Computer Law	IUS/20	C	5	50
2	Web security and malware analysis	ING-INF/05	B	6	60
	Un corso a scelta tra:				
2	Biometric Technologies and Behavioural Security	ING-INF/05	B	5	50
2	Economics of Security and Human Factors	ING-INF/05	B	5	50
2	Fault tolerant and secure control systems	ING-INF/04	B	5	50
2	Stochastic Models	ING-INF/04	B	5	50

Ulteriori crediti da acquisire

Sem	Attività formativa	SSD	TAF	CFU	Ore
	Altre Attività		F	3	
	A scelta libera[1]		D	10	
	Prova Finale		E	15	

TOTALE COMPLESSIVO DEI CREDITI 120

(1) La scelta dei relativi crediti formativi deve essere coerente con il percorso formativo dello studente e deve avere l'approvazione vincolante del Consiglio di Corso di Studio.

Per gli ulteriori dettagli relativi all'organizzazione del Corso di Studio si rimanda al regolamento didattico.

Università degli Studi di Cagliari
FACOLTA' DI INGEGNERIA E ARCHITETTURA

Risultati di apprendimento attesi, espressi tramite i Descrittori Europei del titolo di studio

DESCRITTORI EUROPEI **Scheda formulata con riferimento al Corso di** **Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence**	Industrial Software Development	Supervisory control and monitoring	Cybersecurity Technologies and Risk Management	Fault diagnosis and estimation in dynamical systems	Operating Systems	Web security and malware analysis	Computer Forensics Techniques	Computer Law	Artificial Intelligence	Machine Learning	Advanced Embedded Systems	Internet of Things	Industrial Informatics for energy storage sytems	Critical infrastructures for innovative power distribution	Measurements and Cyber Security for Smart Grid	Physical-layer Techniques for Wireless Communication Security	Biometric Technologies and Behavioural Security	Economics of Security and Human Factors	Fault tolerant and secure control systems	Stochastic models	Prova finale
A1) Conoscere e comprendere le metodologie di sviluppo software in diversi ambiti aziendali, e, in particolare, in ambienti distribuiti.	X		X		X	X					X	X									X
B1) Conoscere e comprendere le architetture di calcolo e le metodologie di comunicazione caratteristiche dei sistemi embedded e della Internet of Things.					X						X	X				X					X
C1) Conoscere e comprendere le metodologie per la modellazione di sistemi complessi, e le tecnologie per il loro governo, con particolare riferimento agli aspetti legati alla sicurezza informatica.		X		X									X	X	X				X	X	X
D1) Conoscere e comprendere gli aspetti relativi alla sicurezza logica e fisica di sistemi complessi, le tecnologie informatiche e le metodologie organizzative e gestionali per la mitigazione del rischio e l'analisi dei sistemi in caso di violazione.			X		X	X	X								X	X	X	X	X		X
E1) Conoscere e comprendere gli aspetti economici e giuridici legati alla sicurezza informatica.			X				X	X										X			X
F1) Conoscere e comprendere gli approcci alla base degli algoritmi utilizzati per l'apprendimento automatico e l'intelligenza artificiale, e la loro applicazione alla realizzazione di meccanismi di protezione fisica e logica.									X	X							X				X
A2) Capacità di applicare le conoscenze relative alla progettazione, sviluppo e verifica del software in ambiti complessi.	X		X		X	X					X	X									X
B2) Capacità di applicare le conoscenze relative alle architetture di sistemi embedded e Internet of Things finalizzate allo sviluppo software in ambito distribuito e alla analisi di sicurezza dal punto di vista del rischio derivante da attacchi informatici.	X		X		X						X	X				X					X
C2) Capacità di applicare le conoscenze relative alla modellazione e gestione di sistemi complessi, con particolare attenzione agli aspetti di sicurezza e di gestione del rischio.		X		X					X				X	X	X				X	X	X
D2) Capacità di formulare e applicare soluzioni all'avanguardia per la mitigazione del rischio nel campo della cybersecurity, sia in fase di progettazione, sia in fase di esercizio, in diversi contesti applicativi, e per la gestione dei sistemi in presenza di violazione.			X		X	X	X		X	X					X	X	X	X	X		X
F2) Capacità di implementare soluzioni algoritmiche originali adeguate ottenute o derivate dalla conoscenza delle metodologie di intelligenza artificiale, anche con applicazione alla sicurezza fisica e logica dei sistemi.						X			X	X							X				X