U.S.R.

IL RETTORE

VISTO lo Statuto di Ateneo;

VISTO l'art. 15 del vigente Regolamento Didattico di Ateneo;

VISTO il Regolamento dei Corsi di Perfezionamento, emanato con D.R. n. 1954 del 25/05/2017;

VISTA la Delibera del 22/01/2021, Verbale n.1, con la quale il Consiglio del Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione ha proposto l'istituzione e l'attivazione, a decorrere dall'anno accademico 2020/2021, del *Corso di Perfezionamento in "Cybersecurity for Businesses and ORGANizations (CyBORG)"*;

VISTA la Delibera n. 07 del 24/02/2021, con la quale il Senato Accademico ha espresso parere favorevole all'istituzione e all'attivazione, a decorrere dall'anno accademico 2020/2021, del suddetto *Corso di Perfezionamento in "Cybersecurity for Businesses and ORGANizations (CyBORG)"* ed ha approvato il Regolamento del Corso, subordinatamente all'adeguamento ai rilievi formulati dal competente Ufficio;

VISTA la Delibera n. 46 del 24/02/2021, con la quale il Consiglio di Amministrazione ha approvato l'istituzione e l'attivazione, a decorrere dall'anno accademico 2020/2021, del Corso di Perfezionamento di cui sopra ed ha espresso parere favorevole in merito al Regolamento del Corso stesso, subordinatamente all'adeguamento ai rilievi formulati dal competente Ufficio;

VISTA la Nota prot. n.102580 del 19/10/2021 con la quale il Direttore del Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione ha trasmesso il testo del Regolamento del Corso di Perfezionamento di cui trattasi, opportunamente adeguato ai rilievi formulati dal competente Ufficio;

VISTA la Nota mail del 19/10/2021 con la quale il suddetto Dipartimento, per il tramite del Coordinatore dell'istituendo Corso di perfezionamento, ha chiesto di traslare la decorrenza della istituzione/attivazione del Corso di cui trattasi dall'a.a. 2020/21 all'a.a. 2021/2022;

DECRETA

A decorrere dall'anno accademico 2021/2022, è istituito, presso il Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione di questo Ateneo, il *Corso di Perfezionamento in "Cybersecurity for Businesses and ORGANizations (CyBORG)"* ed è autorizzata l'attivazione dello stesso Corso.

E' emanato, nel testo allegato al presente Decreto, di cui costituisce parte integrante, il Regolamento del Corso di Perfezionamento sopra citato.

IL RETTORE
Matteo LORITO

Ripartizione Affari Generali
Il Dirigente dott. Francesco BELLO
Unità organizzativa responsabile del procedimento:
Ufficio Statuto, Regolamenti e Organi Universitari
Responsabile del procedimento:
Il Capo dell'Ufficio dott. Antonio NASTI

REGOLAMENTO DEL CORSO DI PERFEZIONAMENTO IN “Cybersecurity for Businesses and ORGanizations (CyBORG)”

(in vigore dall'a.a. 2021/2022)

ORGANIZZATO DAL	Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI)		
IN COLLABORAZIONE CON	TIM S.p.A, CISCO Systems (Italy) S.r.l., CLARA S.c.a.r.l.		
SEDE DEL CORSO	Università degli Studi di Napoli Federico II		
DURATA:	Mesi: 6 / Ore: 750		
PERCENTUALE MINIMA DI FREQUENZA RICHIESTA:	80%		
CREDITI FORMATIVI UNIVERSITARI	30		
TITOLO DI STUDIO RICHIESTO PER L'ACCESSO	Laurea V.O., Laurea Triennale, Laurea Magistrale		
N. MASSIMO AMMISSIBILI	30	N. MINIMO ISCRITTI PER ATTIVAZIONE CORSO	20
MODALITA' DI SELEZIONE PER L'ACCESSO AL CORSO	Per titoli ed esami		
CONTRIBUTO DI ISCRIZIONE	€ 4.500,00		
EVENTUALI BENEFICI PER GLI ISCRITTI E/O PER COLORO CHE CONSEGUONO L'ATTESTATO DI FREQUENZA	È prevista l'attribuzione di borse di studio ad un numero selezionato di partecipanti afferenti alle organizzazioni partner dell'iniziativa, nonché ad enti/organizzazioni/aziende con cui esistano espliciti accordi di collaborazione, in ambito formativo, con la Federico II.		
ATTESTATO DI FREQUENZA	Al termine del Corso sarà rilasciato ai partecipanti, che abbiano superato la verifica finale, a cura del Dipartimento sede amministrativa del Corso di Perfezionamento, un attestato di frequenza firmato dal Coordinatore del Corso con indicazione della durata e dei C.F.U.		
INFO	Per informazioni contattare Prof. Simon Pietro ROMANO Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione, Università degli Studi di Napoli Federico II e-mail: spromano@unina.it		

OBIETTIVI FORMATIVI DEL CORSO

Il Corso si pone l'obiettivo di approfondire le principali tematiche relative alla sicurezza informatica, con particolare riferimento ai modelli, alle metodologie ed alle tecnologie per la protezione dei sistemi operativi, del software applicativo e delle infrastrutture di rete, sia in ambienti fisici che in architetture cloud basate sulla virtualizzazione e/o sulla cosiddetta "containerizzazione" delle risorse e dei servizi.

Il percorso formativo si articola in due fasi distinte, dedicate, rispettivamente, alla trattazione degli argomenti che rappresentano il bagaglio culturale fondamentale per un qualsiasi professionista nell'ambito della cybersecurity, ed all'approfondimento di alcune delle tematiche di maggior rilievo per la creazione di un profilo avanzato, con competenze di tipo specialistico in settori quali l'analisi forense in ambienti digitali, la cyber intelligence, il secure coding, il monitoraggio e la risposta agli incidenti di tipo informatico.

La platea di utenti del corso sarà dunque costituita sia da profili cosiddetti "junior", provenienti dalle organizzazioni partner dell'iniziativa e/o da PMI interessate alla costituzione di profili interni dotati di competenze in ambito cyber, sia da profili cosiddetti "senior", rappresentati da professionisti già impegnati in attività legate al contesto della sicurezza informatica, ma interessati a perfezionare/incrementare le proprie conoscenze, nell'ottica dell'aggiornamento e della formazione continua.

Per quanto riguarda gli argomenti di base, il corso toccherà i seguenti aspetti:

- *Principi base di crittografia;*
- *Sicurezza dei sistemi distribuiti, sia dal punto di vista della progettazione, che da quello della verifica del rispetto dei requisiti di sicurezza;*
- *Sicurezza di sistemi ed ambienti operativi;*
- *Sicurezza delle piattaforme (fisiche e virtualizzate) a supporto delle applicazioni di rete;*
- *Protezione della privacy;*
- *Cenni sugli aspetti normativi e legali (cfr. GDPR);*
- *Sicurezza nel mondo cloud, del mobile e delle reti;*
- *Security by design nella progettazione delle applicazioni di rete.*

Con riferimento, invece, agli aspetti avanzati, gli argomenti trattati sono elencati di seguito:

- *Tecniche di analisi in ambito Digital Forensics;*
- *Principi e metodologie per la Cyber Intelligence;*
- *Principi di Secure Coding;*
- *Modelli e tecniche di Security Monitoring;*
- *Tecniche e strumenti di Incident Response.*

ARTICOLAZIONE DEL PERCORSO FORMATIVO
LEZIONI – LABORATORI - ESERCITAZIONI
<ul style="list-style-type: none"> - Principi di base di crittografia: Introduzione. Cifratura. Funzioni di hash. Autenticazione. Firma digitale. Generazione e certificazione delle chiavi. Gestione dell'identità e degli accessi. Protocolli per l'identificazione e lo scambio delle chiavi. Cifrari a blocchi. Cifrari a flusso. Tecniche di crittoanalisi. Implementazioni sicure. Esempi pratici: Internet e wireless. Crittografia quantistica. Symmetric versus asymmetric algorithms and uses, Key management, Public key infrastructure (PKI) and hashing functions. Basic Cryptographic technologies and libraries. Symmetric, Asymmetric, Hash Algorithms. Attack methods and verification. - Laboratori ed esercitazioni su tutti gli argomenti sopra indicati.
<ul style="list-style-type: none"> - Sicurezza nel mondo delle reti (suddivisa in progettazione sicura e verifica di sicurezza delle reti): Sicurezza della rete. Vulnerability Assessment. Attack Graph. Visual Analytics. Data classification, Policies, procedures, standards and guidelines. Risk assessment and management. Personnel security, training, and awareness. OSI model: Protocols and Abstraction Layers. Local area network (LAN), metropolitan area network (MAN), and wide area network (WAN) technologies, Internet, intranet, and extranet issues. Network topologies and cabling: routers, bridges, and repeaters, Network Administration. Network Security: Firewall, IDS, IPS. Virtual private networks (VPNs), Proxies and Anonymization Overlays. Attack methods and Defense Strategies. Disaster recovery principles. Business resource identification and value assignment. Unit priorities and crisis management. Plan development, implementation, and maintenance. - Laboratori ed esercitazioni su tutti gli argomenti sopra indicati.
<ul style="list-style-type: none"> - Sicurezza di sistemi e ambienti operativi: Operating System Security. Malware Classification and Analysis. Threat Modeling. Security Review and Secure Coding. Web security. Mobile Application Security. Database Security. Various development practices and their risks. System storage and processing components. Security by Design. Distributed System Security and Blockchain. Security Assessment. - Laboratori ed esercitazioni su tutti gli argomenti sopra indicati.
<ul style="list-style-type: none"> - Sicurezza di piattaforme fisiche o virtualizzate su cui poggiano le applicazioni: Tecniche di virtualizzazione. Principi di cloud computing. Architetture di cloud computing. API (Application Programming Interfaces) per ambienti cloud. Virtualizzazione lightweight e container. Docker. Microservizi. Deployment di architetture virtuali. Approcci IaC (Infrastructure as Code). Vulnerabilità di ambienti virtualizzati. - Laboratori ed esercitazioni su tutti gli argomenti sopra indicati.
<ul style="list-style-type: none"> - Protezione della privacy: Privacy e cybersecurity. Tecniche di base per la protezione della privacy. Protocolli crittografici avanzati per la conservazione della privacy. Applicazioni. - Laboratori ed esercitazioni su tutti gli argomenti sopra indicati.
<ul style="list-style-type: none"> - Aspetti normativi e legali in ambito cyber: General Data Protection Regulation (GDPR)
<ul style="list-style-type: none"> - Sicurezza nel mondo del mobile e delle architetture IoT (Internet of Things) - Laboratori ed esercitazioni su mobile ed IoT hacking.
<ul style="list-style-type: none"> - Progettazione di applicazioni sicure: Un approccio olistico alla progettazione delle applicazioni con requisiti di sicurezza. - Digital forensics: Approcci per l'analisi "post-mortem" di applicazioni, sistemi, macchine ed apparati compromessi. - Laboratori ed esercitazioni su digital forensics analysis.
<ul style="list-style-type: none"> - Cyber Intelligence: Ricerca, acquisizione, analisi, utilizzo e scambio di informazioni su minacce cyber. Indicators of Compromise (IoC) ed approcci standard per la condivisione di informazioni sugli incidenti informatici. - Laboratori ed esercitazioni sugli argomenti sopra indicati
<ul style="list-style-type: none"> - Secure coding: Tecniche di scrittura sicura del codice. Architetture per la sicurezza delle applicazioni. - Laboratori ed esercitazioni sugli argomenti sopra indicati
<ul style="list-style-type: none"> - Security Monitoring e Incident Response: Eventi di sicurezza e gestione eventuali incidenti. - Laboratori ed esercitazioni sugli argomenti sopra indicati
ATTIVITA' FORMATIVE DI TIPO INDIVIDUALE
<p>Possibilità di TIROCINIO o STAGE presso alcune delle sedi delle aziende partner e/o degli eventuali stakeholder coinvolti nell'iniziativa (enti/organizzazioni/aziende con cui esistano espliciti accordi di collaborazione, in ambito formativo, con la Federico II).</p>
<p>SEMINARI a cura di esperti provenienti dalle aziende partner e/o eminenti esponenti del panorama cyber, provenienti anche dal mondo della Difesa.</p>
<p>VERIFICA FINALE basata anche sulla valutazione dei risultati di una "challenge" finale, di tipo sia progettuale che implementativo, condotta in gruppo.</p>

MODALITA' DI EROGAZIONE DEL CARICO DIDATTICO			
TIPOLOGIA ATTIVITA' FORMATIVA	N. ORE COMPLESSIVE	N. ORE DI IMPEGNO DOCENZA	N. ORE STUDIO INDIVIDUALE
DIDATTICA FRONTALE (Lezioni – Laboratori - Esercitazioni)	500	250	250
ATTIVITA' FORMATIVE DI TIPO INDIVIDUALE (Didattica Assistita: Seminari - Tirocini – Stage – Attività di studio per la preparazione della verifica finale)	250	50	200
TOT.	750	300	450

ARTICOLAZIONE DEL PERCORSO FORMATIVO CON INDICAZIONE DEI DOCENTI DEL CORSO		
INSEGNAMENTO	DOCENTE	ORE
Principi di base di crittografia	Prof.ssa Valentina Casola	18
Sicurezza nel mondo delle reti	Prof. Simon Pietro Romano	30
Sicurezza di sistemi e ambienti operativi	Prof. Domenico Cotroneo	18
Sicurezza di piattaforme fisiche o virtualizzate su cui poggiano le applicazioni	Prof. Simon Pietro Romano (6h) Prof. Roberto Natella (12h)	18
Protezione della privacy	Prof.ssa Valentina Casola	8
Aspetti normativi e legali in ambito cyber	Prof. Simon Pietro Romano	6
Sicurezza nel mondo del mobile e delle architetture IoT (Internet of Things)	Prof. Roberto Canonico (8h) Prof. Stefano Avallone (5h) Prof. Simon Pietro Romano (5h)	18
Progettazione di applicazioni sicure	Prof. Domenico Cotroneo (4h) Prof. Roberto Natella (8h)	12
Digital forensics	Prof. Simon Pietro Romano	12
Cyber Intelligence	Prof. Elio Masciari	12
Secure coding	Prof. Domenico Cotroneo (6h) Prof. Roberto Natella (6h)	12
Security Monitoring e Incident Response	Prof. Simon Pietro Romano (6h) Prof. Domenico Cotroneo (6h)	12
Contributi su molteplici moduli previsti nel programma formativo	Docenti Esterni TIM (E)	49
Contributi su molteplici moduli previsti nel programma formativo	Docenti Esterni CISCO (E) Docenti Esterni CLARA (E)	75
TOTALE ORE DIDATTICA DOCENTI INTERNI		176
TOTALE ORE DIDATTICA DOCENTI ESTERNI		124

CONSIGLIO DEL CORSO			
		<u>Membro Interno</u> Ateneo "Fed II"	<u>Membro Esterno</u> Ateneo "Fed II"
1	Prof. Simon Pietro Romano (Proponente/Coordinatore)	X	
2	Prof. Giorgio Ventre (Proponente)	X	
3	Prof. Roberto Canonico (Proponente)	X	
4	Referente TIM		X
5	Referente CISCO		X

PIANO FINANZIARIO DEL CORSO DI PERFEZIONAMENTO

ENTRATE:	Partecipanti minimi:	Partecipanti massimi:
Contributo iscrizione	€ 90.000,00	€ 135.000,00
Risorse del Dipartimento (ivi comprese eventuali economie derivanti da precedenti edizioni)	0	0
Finanziamenti pubblici esterni	0	0
Finanziamenti privati esterni	0	0
Totale entrate	€ 90.000,00	€ 135.000,00

USCITE:	Partecipanti minimi:	Partecipanti massimi:
5% del totale delle entrate del Corso da destinare al Bilancio di Ateneo	€ 4.500,00	€ 6.750,00
5% del totale delle entrate del Corso da destinare al Budget di Dipartimento	€ 4.500,00	€ 6.750,00
Spese per contratti per la didattica e seminari:	€ 40.000,00	€ 60.000,00
Spese per attrezzature e materiali a supporto della didattica:	€ 5.000,00	€ 10.000,00
Spese di gestione e funzionamento:	€ 11.000,00	€ 21.500,00
Spese per attività di promozione:	€ 25.000,00	€ 30.000,00
Altro (specificare):	0	0
Totale uscite	€ 90.000,00	€ 135.000,00