U N I V E R S I T À D E G L I S T U D I D I G E N O V A
AREA INTERNAZIONALIZZAZIONE, RICERCA E TERZA MISSIONE
SERVIZIO RAPPORTI CON IMPRESE E TERRITORIO
SETTORE APPRENDIMENTO PERMANENTE

D.R. 2873 del 01.07.2022

IL RETTORE

- Visto il Decreto del Ministero dell'Università e della Ricerca Scientifica e Tecnologica n. 270 del 22/10/2004 "Modifiche al regolamento recante norme concernenti l'autonomia didattica degli atenei, approvato con decreto del Ministero dell'Università e della Ricerca Scientifica e Tecnologica del 03/11/1999 n. 509", ed in particolare l'art. 3, comma 9;
- Visto il Regolamento dei Corsi di Perfezionamento, di aggiornamento professionale e di formazione permanente e dei corsi per Master Universitari di primo e secondo livello dell'Università degli Studi di Genova emanato con D.R. n. 551 del 10/02/2015;
- Viste le disposizioni del Ministero dell'Università e della Ricerca relative alle Procedure per l'ingresso, il soggiorno e l'immatricolazione degli studenti stranieri/internazionali ai corsi di formazione superiore in Italia per l'a.a. 2021/2022 (http://www.studiare-in-italia.it/studentistranieri);
- Visto il Regolamento per la disciplina dei contratti di ricerca, di consulenza e di formazione per conto terzi (D.R. n. 5321 del 31/10/2018);
- Vista la delibera del Consiglio di Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni - DITEN del 13.05.2022 con la quale è stata proposta la IV edizione del Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" per l'a.a. 2021/2022;

D E C R E T A

Art. 1
Norme Generali

È attivato per l'anno accademico 2021/2022 il **Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - IV edizione** presso il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni - DITEN. Il corso è realizzato in collaborazione con Area Internazionalizzazione, Ricerca e Terza missione, Servizio Rapporti con imprese e territorio - Settore apprendimento permanente.
Collaborano alla realizzazione del corso:
Strutture Università di Genova: Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi – DIBRIS e Area Internazionalizzazione, Ricerca e Terza missione (Servizio Rapporti con imprese e territorio).
Enti esterni: Centro di competenza per la sicurezza e l'ottimizzazione delle infrastrutture strategiche - Start 4.0

Art. 2
Finalità del Corso e destinatari

Finalità del Corso:
Il Corso si propone di formare la figura di un esperto nella progettazione e gestione dei sistemi basati sull'Information and Communications Technology (ICT) e di Cybersecurity (Mobile, Web, Cloud, SCADA, ...) preposti alla tutela della sicurezza e alla protezione del patrimonio informativo ed architetturale di un'azienda, una Infrastruttura Critica o un'organizzazione.

Obiettivi formativi, risultati di apprendimento *(learning outcomes)* attesi:
Il Corso si pone i seguenti obiettivi formativi:

- Fornire un insieme completo di nozioni fondamentali di Cybersecurity a laureati magistrali in materie legate all'ICT, al fine di incrementare la preparazione dei laureati su tali tematiche emergenti.
- Fornire competenze sulla governance della Cybersecurity e delle relative procedure a livello aziendale o di Infrastruttura Critica, in modo da potenziare la formazione professionale degli studenti anche con conoscenze approfondite sulle "best practice", con l'obiettivo di agevolare un inserimento rapido ed efficace degli studenti stessi in un contesto aziendale.
- Fornire nozioni in ambito legale sulla Cybersecurity, affinché lo studente sappia prendere decisioni in tale contesto non solo dal punto di vista tecnico ma anche considerando l'impatto legale che le scelte fatte possano avere sull'azienda nelle sedi legali.
- Fornire capacità pratiche e padronanza operativa di soluzioni e prodotti allo stato dell'arte nello scenario moderno di Cybersecurity. A tal fine, molti insegnamenti del Corso includono parti pratiche finalizzate ad incrementare le capacità pratiche dello studente. Lo scopo di questa dimensione operativa è di colmare il gap con l'attuale preparazione universitaria che tende, anche in ambito Cybersecurity, ad essere sbilanciata verso la teoria a scapito della applicazione pratica. Anche in questo caso la preparazione su strumenti e tool allo stato dell'arte ha lo scopo di migliorare la facilità di inserimento in azienda.
- Fornire conoscenze e competenze sulla protezione delle Infrastrutture Critiche in termini sia teorici sia pratici. Questo ambito include aspetti emergenti quali le tecnologie SCADA, Web Security, Mobile Security, IoT Security, ecc. Lo scopo è rendere lo studente operativo in un elevato e svariato numeri di scenari attuali, in modo che sia flessibile e facilmente inseribile nella realtà aziendale in cui verrà coinvolto.

Il raggiungimento dei precedenti obiettivi formativi permette di colmare il gap di formazione e preparazione delle attuali corsi di studi, permettendo, con un solo anno di formazione aggiuntiva, di creare professionisti di Cybersecurity pronti all'inserimento in un contesto aziendale, alleviando le aziende o le Istituzioni dalla necessità di formare internamente le persone, con costi aggiuntivi e spesso tempi di formazione insostenibili.

Il Corso è rivolto a:
Laureati o diplomati con un background informatico che intendano approfondire la preparazione su tematiche verticali nell'ambito della cybersecurity e della protezione delle infrastrutture critiche.

Titoli di studio richiesti per l'ammissione al Corso

- Laurea in Ingegneria Civile e Ambientale (classe 8), Ingegneria dell'Informazione (classe 9), Ingegneria Industriale (classe 10), Scienze e Tecnologie Fisiche (classe 25), Scienze e Tecnologie Informatiche (classe 26) Scienze Matematiche (classe 32) conseguita secondo l'ordinamento vigente o titoli equipollenti (ai sensi del D.I. del 09/07/2009)

Eventuali altri requisiti
Possono accedere altresì coloro che, in possesso di un titolo di studio universitario diverso da quello specificato o del solo diploma di scuola media superiore, abbiano conoscenze e comprovata esperienza professionale ritenute affini al profilo del Corso. Il Comitato di Gestione si riserva di decidere l'ammissione sulla base dell'analisi del curriculum formativo e professionale che i candidati dovranno presentare con la domanda di ammissione al Corso.
Occorre in ogni caso essere in possesso di diploma di scuola secondaria superiore.

È possibile iscriversi all'intero corso oppure ai singoli insegnamenti.

Art. 3
Organizzazione didattica e contenuti

Il Corso prevede 1080 ore di formazione, articolate come segue:

- 432 ore di attività formative d'aula e laboratori;
- 648 ore di studio individuale e verifiche di apprendimento;

Al Corso sono attribuiti 43,2 CFU.

Programma didattico:

PARTE I – FORMAZIONE CULTURALE	Ore	CFU	SSD
Introduction to Cybersecurity	8	0.8	ING-INF/01
Computer Security	24	2.4	INF/01

Information Security Management and Legals	24	2.4	ING-INF/01
Network Security	28	2.8	ING-INF/03
Cryptography	24	2.4	INF/01
PARTE II – FORMAZIONE PROFESSIONALE			
Security and Threats to Critical Infrastructure	12	1.2	ING-IND/31
Cryptographic Protocols	16	1.6	ING-INF/05
Blockchain Tecnologies	16	1.6	ING-INF/05
Web Security	20	2	ING-INF/05
Information Security & Risk Management	28	2.8	ING-INF/01
Business Continuity and Crisis Management	16	1.6	ING-INF/05
Informatica Legale, Privacy and Cyber Crime	36	3.6	IUS/01
Fundamentals of Computer Forensics	8	0.8	ING-INF/05
Cyber Security in Financial and Credit Systems	4	0.4	ING-INF/05
Cybersecurity in SCADA Systems, Industry, Power, and Energy	32	3.2	ING-INF/01, ING-INF/03
IoT Security	20	2	ING-INF/05
Defense-in-Depth Strategies for Critical Infrastructures	12	1.2	ING-INF/05
Standards and Best Practices for Security and Safety	16	1.6	ING-IND/31
Social Engineering and Intelligence for Cybersecurity	16	1.6	ING-INF/01
Parziale ore	*360*	*36*	

PARTE III SPECIALIZZAZIONI – INDIRIZZO I: Cyber Defence of IT/OT systems	**Ore**	**CFU**	**SSD**
Incident Response and Forensics Analysis	24	2.4	ING-INF/05
Malware Analysis	24	2.4	INF/01
Mobile Security	12	1.2	ING-INF/05
Cloud Security	12	1.2	ING-INF/05
Parziale ore	*72*	*7.2*	
PARTE III SPECIALIZZAZIONI – INDIRIZZO II: GRC for Critical Infrastructure Protection and the Enterprise			
Cyber Defense and Cyber Intelligence	24	2.4	ING-INF/01
Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301	24	2.4	ING-INF/05, ING-IND/31
Physical Security	12	1.2	ING-INF/01
Risk Propagation in Interconnected Infrastructures	12	1.2	ING-IND/31
Parziale ore	*72*	*7.2*	
TOTALE ORE DIDATTICA	***432***		

Il Corso si svolgerà da settembre 2022 a luglio 2023 con un impegno indicativo 16 ore alla settimana divise tra il giovedì pomeriggio (4h), il venerdì (8h) ed il sabato mattina (4h).
Assenze consentite: 34%.
La lingua di insegnamento e di verifica del profitto: ITALIANO.
È richiesto livello di certificazione B2 della lingua italiana per gli studenti stranieri.

Sede di svolgimento dell'attività didattica: il corso sarà erogato online tramite la piattaforma Microsoft Teams.

Art.4
Valutazione

Alla fine di ogni insegnamento sarà effettuato un esame con votazione in trentesimi, utile a valutare e monitorare l'apprendimento e le competenze acquisite dagli allievi e valido per l'acquisizione dei corrispondenti CFU.

Art. 5
Presentazione delle domande e selezione

La domanda di ammissione all'intero corso deve essere presentata mediante la procedura on-line disponibile all'indirizzo http://servizionline.unige.it/studenti/post-laurea/corsiperfezionamentoformazione/domanda **entro le ore 12:00 del 23.09.2022**

La data di presentazione della domanda di partecipazione al corso è certificata dal sistema informatico che, allo scadere del termine utile per la presentazione, **non permetterà più l'accesso e l'invio della domanda**.
Al primo accesso, è necessario richiedere le credenziali UNIGE cliccando sulla voce *Registrazione utente*. Ottenute le credenziali, si potrà accedere alla pagina della domanda.

Alla domanda di ammissione al Corso devono essere allegati, mediante la procedura online e in formato pdf:
1. copia fronte/retro del documento di identità;
2. curriculum vitae.

Nel caso di titolo di studio conseguito all'estero

Qualora il titolo non sia già stato riconosciuto equipollente, l'interessato deve chiederne l'equipollenza ai soli fini del concorso, allegando alla domanda i seguenti documenti:
- titolo di studio tradotto e legalizzato dalla competente rappresentanza diplomatica o consolare italiana del paese in cui è stato conseguito il titolo;
- "dichiarazione di valore" del titolo di studio resa dalla stessa rappresentanza.

Il provvedimento di equipollenza sarà adottato ai soli fini dell'ammissione al concorso e di iscrizione al Corso. Nel caso in cui la competente rappresentanza diplomatica o consolare italiana non abbia provveduto a rilasciare tale documentazione in tempo utile per la presentazione della domanda di ammissione, è necessario allegare alla domanda tutta la documentazione disponibile. L'eventuale provvedimento di equipollenza sarà adottato sotto condizione che la traduzione legalizzata e la "dichiarazione di valore" siano presentate entro il termine previsto per l'iscrizione ai corsi da parte dei candidati ammessi. Il rilascio della suddetta documentazione e dell'eventuale permesso di soggiorno per la partecipazione alle eventuali prove di selezione e per la frequenza del Corso ai cittadini stranieri è disciplinato dalla nota del Ministero dell'Università e della Ricerca relative alle procedure per l'accesso degli studenti stranieri richiedenti visto ai corsi di formazione superiore per l'a.a. 2021/2022

Ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, alle dichiarazioni rese nella domanda di ammissione, nel caso di falsità in atti e dichiarazioni mendaci si applicano le sanzioni penali previste dall'art. 76 del decreto n. 445/2000 sopra richiamato. Nei casi in cui non sia applicabile la normativa in materia di dichiarazioni sostitutive (D.P.R. n. 445/2000 e ss.mm.ii), il candidato si assume comunque la responsabilità (civile, amministrativa e penale) delle dichiarazioni rilasciate.

L'Amministrazione si riserva di effettuare i controlli e gli accertamenti previsti dalle disposizioni in vigore. I candidati che renderanno dichiarazioni mendaci decadranno automaticamente dall'iscrizione, fatta comunque salva l'applicazione delle ulteriori sanzioni amministrative e/o penali previste dalle norme vigenti.
L'Amministrazione universitaria non assume alcuna responsabilità per il caso di smarrimento di comunicazioni dipendente da inesatte indicazioni della residenza e del recapito da parte dell'aspirante o da mancata oppure tardiva comunicazione del cambiamento degli stessi, né per eventuali disguidi postali o telegrafici non imputabili a colpa dell'Amministrazione medesima.

Al Corso sono ammessi al massimo 20 allievi. Il numero minimo per l'attivazione è pari a 1.
Il Comitato di Gestione valuterà la possibilità di ridurre i costi di gestione ad un livello corrispondente a quello dei proventi, come condizione per svolgere il Corso.

L'ammissione dei candidati verrà effettuata sulla base della valutazione del curriculum vitae et studiorum.

Il Comitato di Gestione provvederà alla valutazione adottando i seguenti criteri di valutazione:

Valutazione esperienze formative e professionali (max 25 punti)
Valutazione della laurea:
- 5 punti per il voto di laurea pari a 110 e lode
- 4 punti per il voto di laurea compreso tra 110 e 107
- 3 punti per il voto di laurea compreso tra 106 e 103
- 2 punti per il voto di laurea compreso tra 102 e 100
- 1 punto per il voto di laurea pari o inferiore a 99

Massimo 7 punti per altre esperienze formative pertinenti
Massimo 3 punti per il possesso di ulteriori certificazioni (es. conoscenza dell'inglese e competenze informatiche di base)
Valutazione delle esperienze professionali (max 10 punti)
- 5 punti per le competenze specifiche acquisite attraverso attività professionali/di ricerca/ stage
- 5 punti per la pertinenza del settore di attività e/o il ruolo professionale per le persone occupate

La graduatoria finale dei candidati idonei sarà stilata sulla base della somma dei punteggi riportati nella valutazione delle diverse voci. Saranno ammessi al Corso i primi candidati in graduatoria fino a un massimo di 20 candidati.

Sarà inoltre possibile iscriversi a uno o più singoli insegnamenti del Corso.
In questo caso le domande saranno accettate in ordine di arrivo e fino al raggiungimento del numero massimo di allievi ammissibili, previa verifica del possesso di uno dei titoli di studio richiesti per l'ammissione al Corso. Eventuali domande pervenute dopo il raggiungimento del numero massimo di iscritti verranno considerate a riserva nel caso di rinunce e/o esclusioni.

La graduatoria di ammissione all'intero Corso, redatta a seguito degli esiti della selezione, sarà pubblicata a cura della Segreteria organizzativa del Corso sul sito internet https://www.perform.unige.it/corsi/corso-cybersecurity-iv-edition.html **entro il 26.09.2022**
L'Università può adottare, anche successivamente alla pubblicazione della graduatoria di ammissione, provvedimenti di esclusione nei confronti dei candidati privi dei requisiti richiesti.

Art. 6
Modalità e quota d'iscrizione

I candidati ammessi all'intero Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" devono perfezionare l'iscrizione mediante la procedura on-line disponibile all'indirizzo https://servizionline.unige.it/studenti/post-laurea/confermaPL (cliccando su "conferma iscrizione post-laurea" e scegliendo il Corso la cui iscrizione deve essere confermata)
entro **il 27.09.2022 alle ore 12:00.**

Coloro i quali intendano iscriversi a uno o più singoli insegnamenti devono presentare domanda entro le scadenze previste (e pubblicate alla pagina web del corso https://www.perform.unige.it/corsi/corso-cybersecurity-iv-edition.html) e perfezionare l'iscrizione mediante la procedura on-line disponibile all'indirizzo https://servizionline.unige.it/studenti/post-laurea/confermaPL (cliccando su "conferma iscrizione post-laurea" e scegliendo il Corso la cui iscrizione deve essere confermata) una volta ricevute indicazioni dalla segreteria del corso.

Il pagamento della quota d'iscrizione pari a:

- € 5.016,00 per occupati per l'intero Corso (compresi di bollo)
- € 2.516,00 per inoccupati per l'intero Corso (compresi di bollo)
- € 180,00 moltiplicato il numero di CFU corrispondente al singolo insegnamento. A tale valore va sommato il costo di 16 euro di imposta (una sola volta per iscrizione a più insegnamenti)

Eventuali agevolazioni economiche e/o borse
Sono previste le seguenti agevolazioni economiche:
- € 2.516,00 per inoccupati per l'intero Corso (compresi di bollo)

- Sconto del 50% per singoli insegnamenti e parti (I, II, IIIa oppure IIIb) per dottorandi UNIGE, e inoccupati o occupati con forme di lavoro flessibile (vedi tabella sottostante)

Il pagamento è da effettuarsi online tramite il servizio bancario disponibile nell'Area dei Servizi online agli Studenti (https://servizionline.unige.it/studenti/unigepay20/), utilizzando una delle carte di credito appartenenti ai circuiti Visa, Visa Electron, CartaSì, MasterCard, Maestro o tramite "avviso di pagamento" cartaceo (pago PA).
Si invita a leggere attentamente la pagina web https://www.studenti.unige.it/tasse/pagamento_online/ (modalità di pagamento).

	SSD	**CFU**	**ore di didattica**	**costo in € per insegnamento incluso 16 € marca da bollo per iscrizione**	**costo in € per singola parte**
PARTE I - FORMAZIONE CULTURALE					
Introduction to Cybersecurity	ING-INF/01	0,8	8	160	
Computer Security	INF/01	2,4	24	448	
Information Security Management and Legals	ING-INF/01	2,4	24	448	
Network Security	ING-INF/03	2,8	28	520	
Cryptography	INF/01	2,4	24	448	
Totale		**11,6**	**116**		**2024**
PARTE II - FORMAZIONE PROFESSIONALE					
Security and Threats to Critical Infrastructure	ING-IND/31	1,2	12	232	
Cryptographic Protocols	ING-INF/05	1,6	16	304	
Blockchain Technologies	ING-INF/05	1,6	16	304	
Web Security	ING-INF/05	2	20	376	
Information Security & Risk Management	ING-INF/01	2,8	28	520	
Business Continuity and Crisis Management	ING-INF/05	1,6	16	304	
Informatica Legale, Privacy and Cyber Crime	IUS/01	3,6	36	664	
Fundamentals of Computer Forensics	ING-INF/05	0,8	8	160	
Cyber Security in Financial and Credit Systems	ING-INF/05	0,4	4	88	
Cybersecurity in SCADA Systems, Industry, Power, and Energy	ING-INF/01, ING-INF/03	3,2	32	592	
IoT Applications Security	ING-INF/05	2	20	376	
Defense-in-Depth Strategies for Critical Infrastructures	ING-INF/05	1,2	12	232	

Standards and Best Practices for Security and Safety	ING-IND/31	1,6	16	304	
Social Engineering and Intelligence for Cyber Security	ING-INF/01	1,6	16	304	
Totale:		**24,4**	**244**		**4760**
PARTE III - SPECIALIZZAZIONI - INDIRIZZO I: Cyber Defence of IT/OT Systems					
Incident Response and Forensics Analysis	ING-INF/05	2,4	24	448	
Malware Analysis	INF/01	2,4	24	448	
Mobile Security	ING-INF/05	1,2	12	232	
Cloud Security	ING-INF/05	1,2	12	232	
Totale:		**7,2**	**72**		**1360**
PARTE III - SPECIALIZZAZIONI - INDIRIZZO II: GRC for Critical Infrastructure Protection and the Enterprise					
Cyber Defense and Cyber Intelligence	ING-INF/01	2,4	24	448	
Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301	ING-INF/05, ING-IND/31	2,4	24	448	
Physical Security	ING-INF/01	1,2	12	232	
Risk Propagation in Interconnected Infrastructures	ING-IND/31	1,2	12	232	
Totale:		**7,2**	**72**		**1360**

Le scadenze per iscriversi ai singoli insegnamenti saranno indicate alla pagina del corso **sul sito internet** https://www.perform.unige.it/corsi/corso-cybersecurity-iv-edition.html

Non è possibile effettuare alcun pagamento mediante bonifico bancario.

Ai sensi dell'art. 8 comma 3 del Regolamento per gli Studenti emanato con D.R. n. 1218 del 16.09.2014, lo studente iscritto ad un Percorso Formativo universitario non ha diritto alla restituzione delle tasse e dei contributi versati, anche se interrompe gli studi o si trasferisce ad altra Università.
In caso di mancato avvio del Corso, potrà essere restituito solo il contributo (bolli esclusi ai sensi dell'art. 37 DPR 26 ottobre 1972 n. 642).
I candidati che non avranno provveduto ad iscriversi entro il termine sopraindicato di fatto sono considerati rinunciatari.

Art. 7
Rilascio dell'attestato di frequenza

A conclusione del Corso agli iscritti che, a giudizio del Comitato di Gestione, abbiano svolto le attività ed ottemperato agli obblighi previsti, verrà rilasciato dal Direttore del Corso stesso un attestato di partecipazione, che non costituisce titolo accademico, ai sensi dell'art. 8 del Regolamento dei corsi di perfezionamento, di aggiornamento professionale e di formazione permanente e dei corsi per master universitari di primo e secondo livello.

Art. 8
Comitato di Gestione e Direttore

Presidente: Rodolfo Zunino
Vice Presidente: Alessio Merlo

Componenti Unige del Comitato di Gestione: Alessandro Armando (DIBRIS), Giovanni Chiola (DIBRIS), Paola Girdinio (DITEN), Lorenzo Ivaldi (DITEN), Giovanni Lagorio (DIBRIS), Mario Marchese (DITEN), Enrico Russo (DIBRIS).
Componenti esterni del Comitato di Gestione: Fabio Cocurullo (Leonardo), Mattia Epifani (RealityNet), Ermete Meda (Cyber Security Information Expert), Danilo Massa (RCS), Silvio Ranise (FBK), Antonio Rebora (Leonardo), Gabriele Nani (ABB), Gaetano Sanacore (A2A).
Partecipano alle riunioni di CG: un rappresentante del Centro di competenza per la sicurezza e l'ottimizzazione delle infrastrutture strategiche - Start 4.0 e un delegato della struttura cui è affidata la gestione amministrativa, organizzativa e finanziaria.
Struttura Unige cui è affidata la gestione amministrativa, organizzativa e finanziaria del Corso:
Servizio Rapporti con imprese e territorio: Alessia Popia (Settore Gestione Progetti)

Art. 9
Trattamento dei dati personali

I dati personali forniti dai candidati saranno raccolti dall'Università degli Studi di Genova e trattati per le finalità di gestione della selezione e delle attività procedurali correlate, secondo le disposizioni del REGOLAMENTO (UE) 2016/679 del PARLAMENTO EUROPEO e del CONSIGLIO del 27 aprile 2016, articolo 13 in materia di protezione di dati personali, reperibile al link https://unige.it/regolamenti/org/privacy.html.

IL RETTORE
F.to digitalmente
Prof. Federico Delfino

Responsabile del procedimento Dott.ssa Ilaria Burlando
Per informazioni: mail: Dott.ssa Alessia Popia popia@perform.unige.it