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
SCUOLA POLITECNICA
DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI (DIBRIS)

Decreto rep. n. 402

IL DIRETTORE

- Visto il Decreto del Ministro dell'Università e della Ricerca Scientifica e Tecnologica del 22 ottobre 2004 n. 270 "Modifiche al regolamento recante norme concernenti l'autonomia didattica degli atenei, approvato con decreto del Ministro dell'Università e della Ricerca Scientifica e Tecnologica 3 novembre 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 del 19/02/2018 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. 2018/2019;
- Visto il Regolamento per la disciplina dei contratti di ricerca, di consulenza e di formazione per conto terzi (in vigore dal 20/05/2017) (D.R. n. 5321 del 31/10/2018);
- Vista la Delibera del 16/01/2019 del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) con la quale è stata approvata l'attivazione del Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - I edizione.

D E C R E T A

Art. 1
Norme Generali

È attivato per l'anno accademico 2018/19 il **Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - I edizione** presso il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS).

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:

1. Fornire un insieme completo di nozioni fondamentali di Cybersecurity, al fine di incrementare la preparazione dei laureati e diplomati su tali tematiche emergenti.
2. 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.
3. 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.
4. Fornire capacità pratiche e padronanza operativa di soluzioni e prodotti allo stato dell'arte nello scenario moderno di Cybersecurity. A tal fine, molti moduli del Corso includono parti pratiche, mentre gli indirizzi di specializzazione contemplano cyber-esercizi finalizzati 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.

5. 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, Cloud Security ecc. Lo scopo è rendere lo studente operativo in un elevato e variato numeri di scenari, 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 Fisica, Ingegneria, Informatica e Matematica conseguita secondo l'ordinamento previgente o titoli equipollenti.
- 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

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.

Art. 3
Organizzazione didattica e contenuti

Il Corso prevede 1350 ore di formazione, articolate come segue:
- 432 ore di lezioni frontali
- 918 ore di studio individuale

Al Corso sono attribuiti 54 CFU.

Programma didattico:

Modulo	SSD	CFU	h Univ	h Esterni	Docenti	h studio individuale	h verifica di apprendimento
Parte I: Formazione Culturale							
Introduction to Cyber Security	ING-INF/01	1,5	4	8	Zunino, Meda	25,5	2
Cryptographic Protocols	ING-INF/05	2	8	8	Armando, Carbone R.	34	2
Information Security Management and Legals	ING-INF/01	3	0	24	Meda, Bassoli	51	4
Network Security	ING-INF/03	4	16	16	Chiola, Picasso, Arrigoni, Marchese	68	4
Computer Security	INF/01	4	24	8	Chiola, Lagorio, Ranise	68	4

Parte II: Formazione Professionale							
Information Security Management	ING-INF/01	3,5	0	28	Meda, Ferretti, De Bertol	59,5	4
Legal Informatics, Privacy and Cyber Crime	IUS/01	4	8	24	Bassoli, Losengo, Surlinelli, Zunino	68	4
Fundamentals of Computer Forensics	ING-INF/05	1	0	8	Massa, Epifani	17	2
Cryptography & Blockchain Technologies	INF/01	4	32	0	Chiola, Lagorio, Zunino, Ribaudo	68	4
Cyber Security in Financial and Credit Systems	ING-INF/05	1	0	8	Carbone P.	17	2
Security and Threats to Critical Infrastructure	ING-IND/31	1,5	8	4	Girdinio, Perna, Marchese	25,5	2
Business Continuity and Crisis Management	ING-INF/05	3	0	24	Buson, Cerasoli, Marson	51	4
Cybersecurity of SCADA Systems	ING-INF/01	2	0	16	Rebora	34	2
Social Engineering and Intelligence for Cyber Security	ING-INF/01	2	16	0	Zunino	34	2
IoT Applications Security	ING-INF/05	3	12	12	Merlo, Zunino, Verderame	51	4

Indirizzo 1: Digital Forensics & Penetration Testing							
Incident Response and Forensics Analysis	ING-INF/05	4	0	32	Massa, Epifani, Picasso	68	4
Malware Analysis	INF/01	4	16	16	Massa, Lagorio	68	4
Web Security	ING-INF/05	2,5	12	8	Merlo, Armando, Braccio	42,5	4
Mobile Security	ING-INF/05	3	24	0	Merlo	51	4
Cyber Exercise	ING-INF/05	1	8	0	Armando, Merlo, Leonardo	17	0

Indirizzo 2: Critical Infrastructure Protection and Security Assurance							
Cyber Defense and Cyber Intelligence	ING-INF/01	2	8	8	Zunino, Martinazzo	34	2
Standards and Best Practices in Security and Safety	ING-IND/31	2,5	0	20	Rassega, Pugni, Marmo, Ramacciotti	42,5	2
SCADA and Industrial System Protection	ING-INF/01	2,5	0	20	Nani, Caserza, Rebora	42,5	2
Defense-in-Depth Strategies for critical Infrastructures	ING-INF/05	1	0	8	Verderame	17	2
ISO/IEC 27001 & 27002 Standards and Security Assurance	ING-INF/05	2	0	16	Cerasoli, Lorenzi, Leonardo	34	2
Physical Security	ING-INF/01	1,5	0	12	Rebora	25,5	2
Risk Propagation in Interconnected Infrastructures	ING-IND/31	2	8	8	Girdinio, Detoni	34	2
Cybersecurity for power and energy systems	ING-INF/03	1	0	8	Marchese	17	2

Il Corso si svolgerà da maggio 2019 ad aprile 2020 con un impegno indicativo 16 ore alla settimana divise tra il giovedì pomeriggio (4h), il venerdì (8h) ed il sabato mattina (4h).
La frequenza al Corso è obbligatoria; per ricevere l'attestato di partecipazione è richiesta la frequenza di almeno il 30% del monte ore.

Sede del Corso: Università degli Studi di Genova.
Lingua nella quale si svolgerà il Corso: italiano.

Art.4
Valutazione

Alla fine di ogni modulo 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 al concorso 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 04/04/2019.**
La data di presentazione della domanda di partecipazione al concorso 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 all'eventuali prove di selezione e per la frequenza del Corso ai cittadini stranieri è disciplinato dalla nota del Ministero dell'Università e della Ricerca del 19/02/2018 (Norme per l'accesso degli studenti stranieri ai corsi per l'a.a. 2018/2019).

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 e studiorum.

Il Comitato di Gestione provvederà alla valutazione adottando i seguenti criteri di valutazione:
Valutazione esperienze formative (max 15 punti)

- Valutazione della laurea (massimo 8 punti):
  - 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 3 punti per la pertinenza della laurea
- Massimo 4 punti per altre esperienze formative pertinenti
- Massimo 3 punti per il possesso di ulteriori certificazioni (es. conoscenza dell'inglese e competenze informatiche di base)

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. Gli eventuali candidati idonei oltre il ventesimo in graduatoria costituiranno le riserve da cui attingere, secondo l'ordine della graduatoria stessa, in caso si verifichino rinunce da parte dei candidati ammessi.
In caso di parità di punteggio verrà data preferenza al candidato con minore età anagrafica.

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 al Corso, redatta a seguito degli esiti della selezione, sarà pubblicata a cura della Segreteria organizzativa del Corso sul sito internet www.perform.unige.it entro il 15/04/2019.

L'Università può adottare, anche successivamente alla pubblicazione della graduatoria di ammissione, provvedimenti di esclusione nei confronti dei candidati privi dei requisiti richiesti.

Borse di studio:
Potranno essere messe a disposizione degli ammessi borse di studio a copertura parziale o totale della quota di iscrizione.
L'entità dei contributi e le modalità di assegnazione degli eventuali contributi verranno comunicate e pubblicate sul sito internet **www.perform.unige.it** entro la scadenza del presente bando.

Art. 6
Modalità e quota d'iscrizione

I candidati ammessi all'intero Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" od a uno o più singoli insegnamenti 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 24/04/2019 alle ore 12:00.**

Il pagamento della quota d'iscrizione pari a:

- **€ 6.516,00 per occupati per l'intero Corso (compresi di bollo)**
- **€ 2.516,00 per inoccupati per l'intero Corso (compresi di bollo)**
- **€ 166 moltiplicato per il numero di CFU corrispondente al singolo insegnamento (compresi di bollo)**

dovrà essere effettuato entro la scadenza sopraindicata mediante (https://www.studenti.unige.it/tasse/pagamento_online**/)**:

- Servio pago PA
- Pagamento online con Carta di Credito/Debito
- Servizi di Banca Popolare di Sondrio

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

Direttore: Alessio Merlo
Comitato di Gestione:
Docenti interni: Alessandro Armando (DIBRIS), Rodolfo Zunino (DITEN), Giovanni Chiola (DIBRIS), Paola Girdinio (DITEN), Giovanni Lagorio (DIBRIS), Mario Marchese (DITEN), Paolo Pinceti (DITEN), Sebastiano B. Serpico (DITEN)
Docenti esterni: Maurizio Aiello (CNR), Cocurullo Fabio (Leonardo), Mattia Epifani (RealityNet), Ermete Meda (Ansaldo STS), Massa Danilo (Aizoon), Silvio Ranise (FBK), Antonio Rebora (Ansaldo Energia), Gen. B. A. Francesco Vestito (CIOC - Ministero della Difesa)
Delegato della struttura cui è affidata la gestione amministrativa, organizzativa e finanziaria: Elena Tortora

La struttura a cui sarà affidata la segreteria organizzativa e amministrativo-contabile e la funzione di sportello informativo del Corso è: Area Apprendimento permanente e orientamento - Servizio Apprendimento Permanente - Settore Gestione Progetti (Piazza della Nunziata 2 Genova, tel +39 010 209 9466, **www.perform.unige.it**, **perform@unige.it**.

Art. 9
Trattamento dei dati personali

I dati personali forniti dai candidati saranno raccolti dall'Università degli Studi di Genova (Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) e Area Apprendimento permanente e orientamento - Servizio Apprendimento Permanente - Settore Gestione Progetti) 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.

Genova, 30/01/2019

IL DIRETTORE DEL DIPARTIMENTO
F.to Prof. Enrico Puppo

Responsabile del procedimento: Sig.ra Lorella Vongher