UNIVERSITÀ DEGLI STUDI DI GENOVA
SCUOLA POLITECNICA
DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA,
ROBOTICA E INGEGNERIA DEI SISTEMI - DIBRIS

Decreto Rep. n. 3468 Genova, 16 settembre 2020

**IL DIRETTORE**

- 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.2019-2020 (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);
- Visto il Decreto d'urgenza n. 1842 del 13 maggio 2020 del Direttore del Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni – DITEN con il quale è stata approvata l'attivazione del Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - II edizione.
- Vista la Delibera del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi – DIBRIS del 10/07/2020 con la quale è stata preso in carico la realizzazione nell'a.a. 2019/2020 del Master universitario di II livello in "Cybersecurity and Critical Infrastructure Protection" III edizione e l'analogo corso di Perfezionamento;
- Vista la Delibera del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi – DIBRIS del 10/09/2020 con la quale si approva la riapertura del suddetto bando relativamente agli insegnamenti ancora da svolgersi

**D E C R E T A**

**Art. 1**
**Norme Generali**

L'attivazione per l'anno accademico 2019/2020 nell'ambito del **Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - II edizione** dei seguenti insegnamenti:

*PARTE II - FORMAZIONE PROFESSIONALE*
- Web Security
- Information Security & Risk Management
- Business Continuity and Crisis Management
- Informatica Legale, Privacy and Cyber Crime
- Fundamentals of Computer Forensics
- Cyber Security in Financial and Credit Systems
- Cybersecurity in SCADA Systems, Industry, Power, and Energy
- IoT Applications Security
- Defense-in-Depth Strategies for Critical Infrastructures
- Standards and Best Practices for Security and Safety
- Social Engineering and Intelligence for Cyber Security

*PARTE III - SPECIALIZZAZIONI - INDIRIZZO I: Cyber Defence of IT/OT Systems*
- Incident Response and Forensics Analysis
- Malware Analysis

- Mobile Security and IoT
- Cyber Exercise

*PARTE III - SPECIALIZZAZIONI - INDIRIZZO II: GRC for Critical Infrastructure Protection and the Enterprise*
- Cyber Defense and Cyber Intelligence
- Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301
- Physical Security
- Risk Propagation in Interconnected Infrastructures

**E' possibile iscriversi a uno o più insegnamenti presenti in elenco.**

I suddetti insegnamenti nell'ambito del Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - II edizione sono realizzati dal Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi – DIBRIS. Il corso è realizzato in collaborazione con Area Internazionalizzazione, Ricerca e Terza missione, Servizio Rapporti con imprese e territorio - Settore apprendimento permanente.

## Art. 2
## Finalità del Corso e destinatari

Finalità dell'attività formativa:
Gli insegnamenti nell'ambito del Corso di Perfezionamento in "Cybersecurity and Critical Infrastructure Protection" - II edizione si propongono di fornire conoscenze utili a chi intende formarsi quale 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:
1. 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.
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 Master 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.
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, 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.

Gli insegnamenti sono rivolti 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:
- 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,**
**Modalità e quota di iscrizione**

La lingua di insegnamento e di verifica del profitto: ITALIANO. È richiesto livello di certificazione B2 della lingua Italiana per gli studenti stranieri.

**Gli insegnamenti sono erogati in modalità telematica, attraverso la piattaforma Microsoft Teams**

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.

Nella tabella sottostante sono indicati i periodi di erogazione di ciascun insegnamento e la relativa scadenza per iscriversi.

Ad avvenuta iscrizione sarà comunicato il calendario del/degli insegnamenti prescelti.

Gli insegnamenti si svolgono nelle seguenti giornate della settimana: giovedì pomeriggio (4h), venerdì (8h) e sabato mattina (4h).

| **PARTE II - FORMAZIONE PROFESSIONALE** | | | | | | |
|---|---|---|---|---|---|---|
| **TITOLO SINGOLO INSEGNAMENTO** | | **CFU** | **ORE** | **QUOTA ISCRIZIONE + €16,00 DI BOLLO** | **PERIODO** | **SCADENZA PRESENTAZ. DOMANDA** |
| Web Security | ING-INF/05 | 2 | 20 | 360 | 16/10/2020 - 23/10/2020<br>Esame 29/10/2020 | 09/10/2020 |
| Information Security & Risk Management | ING-INF/01 | 2,8 | 28 | 504 | 23/10/2020 - 06/11/2020<br>Esame 12/11/2020 | 16/10/2020 |
| Business Continuity and Crisis Management | ING-INF/05 | 1,6 | 16 | 288 | 06/11/2020 - 19/11/2020<br>Esame 03/12/2020 | 30/10/2020 |
| Informatica Legale, Privacy and Cyber Crime | IUS/01 | 3,6 | 36 | 648 | 13/11/2020 - 28/11/2020<br>Esame 03/12/2020 | 06/11/2020 |
| Fundamentals of Computer Forensics | ING-INF/05 | 0,8 | 8 | 144 | 04/12/2020<br>Esame 10/12/2020 | 27/11/2020 |
| Cyber Security in Financial and Credit Systems | ING-INF/05 | 0,4 | 4 | 72 | 5/12/2020<br>Esame 10/12/2020 | 27/11/2020 |
| Cybersecurity in SCADA Systems, Industry, Power, and Energy | ING-INF/01, ING-INF/03 | 3 | 30 | 540 | 11/12/2020 -19/12/2020<br>Esame 14/01/2021 | 04/12/2020 |
| IoT Applications Security | ING-INF/05 | 2 | 20 | 360 | 08/01/2021 - 15/01/2021<br>Esame 21/01/2021 | 30/12/2020 |
| Defense-in-Depth Strategies for Critical Infrastructures | ING-INF/05 | 1,2 | 12 | 216 | 16/01/2021 – 22/01/2021<br>Esame 28/01/2021 | 08/01/2021 |
| Standards and Best Practices for Security and Safety | ING-IND/31 | 1,8 | 18 | 340 | 23/01/2021 – 04/02/2021<br>Esame 11/02/2021 | 15/01/2021 |
| Social Engineering and Intelligence for Cyber Security | ING-INF/01 | 1,6 | 16 | 288 | 05/02/2021 –12/02/2021<br>Esame 13/02/2021 | 29/01/2021 |
| **PARTE III - SPECIALIZZAZIONI - INDIRIZZO I: Cyber Defence of IT/OT Systems** | | | | | | |
| Incident Response and Forensics Analysis | ING-INF/05 | 2,4 | 24 | 432 | 18/02/2021 – 26/02/2021<br>Esame 04/03/2021 | 11/02/2021 |
| Malware Analysis | INF/01 | 2,4 | 24 | 432 | 26/02/2021 – 11/03/2021<br>Esame 18/03/2021 | 19/02/2021 |
| Mobile Security and IoT | ING-INF/05 | 2 | 20 | 360 | 12/03/2021 – 19/03/2021<br>Esame 25/03/2021 | 05/03/2021 |
| Cyber Exercise | ING-INF/05 | 0,4 | 4 | 72 | 20/03/2021 | 12/03/2021 |
| **Totale:** | | **7,2** | **72** | | | |
| **PARTE III - SPECIALIZZAZIONI - INDIRIZZO II: GRC for Critical Infrastructure Protection and the Enterprise** | | | | | | |
| Cyber Defense and Cyber Intelligence | ING-INF/01 | 2,4 | 24 | 432 | 18/02/2021 – 26/02/2021<br>Esame 04/03/2021 | 11/02/2021 |
| Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301 | ING-INF/05, ING-IND/31 | 2,4 | 24 | 432 | 26/02/2021 – 11/03/2021<br>Esame 18/03/2021 | 19/02/2021 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Physical Security | ING-INF/01 | 1,2 | 12 | 216 | 12/03/2021 – 13/03/2021 Esame 25/03/2021 | 05/032021 |
| Risk Propagation in Interconnected Infrastructures | ING-IND/31 | 1,2 | 12 | 216 | 19/03/2021 – 20/03/2021 Esame 25/03/2021 | 12/03/2021 |
| **Totale:** | | **7,2** | **72** | | | |

La domanda di ammissione 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 facendo riferimento alle scadenze indicate nella tabella sopra riportata.**

Nella stessa tabella sono indicati i costi previsti per ciascun insegnamento, al quale va aggiunta l'imposta di bollo di € 16.

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.

Il pagamento della quota d'iscrizione **dovrà essere effettuato, collegandosi alla pagina https://servizionline.unige.it/studenti/unigepay20/, mediante**:

- Carta di credito (anche prepagata)
- Servizi di Banca Popolare di Sondrio
- Presso lo sportello di qualsiasi banca con bollettino bancario (bollettino Freccia)
- Tramite il proprio sistema di homebanking qualora lo stesso consenta il pagamento utilizzando il "bollettino freccia" di cui sopra.

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. 228 del 25/09/2001 e successive modifiche, 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, sarà restituito il contributo versato (bolli esclusi ai sensi dell'art. 37 DPR 26 ottobre 1972 n. 642).

**La domanda di iscrizione decade automaticamente qualora il pagamento non venga effettuato entro 48 ore lavorative.**

Gli ammessi dovranno inoltre 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) a seguito di comunicazione che verrà inviata via email. In questa fase dovrà essere sottoscritto digitalmente il contratto formativo (consultabile sul sito www.perform.unige.it).
Indicazioni su come procedere saranno fornite agli allievi ammessi al corso successivamente alla chiusura del bando.
Non sono previste esenzioni del pagamento della quota di iscrizione.

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 frequenza del corso ai cittadini stranieri è disciplinato dalle disposizioni 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. 2019/2020, disponibile all'indirizzo http://www.studiare-in- italia.it/studentistranieri/5.html. I cittadini stranieri non ancora in possesso del codice fiscale, lo potranno ottenere rivolgendosi all'Area didattica e internazionalizzazione-Servizio internazionalizzazione-Settore accoglienza studenti stranieri (SASS): Telefono: (+39) 010 209 51525, E-mail: sass@unige.it

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.

**Art. 4**
**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 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. 5**
**Comitato di Gestione e Direttore**

**Presidente:** Alessio Merlo
**Componenti Unige del Comitato di Gestione**: Alessandro Armando (DIBRIS), Rodolfo Zunino (DITEN), Giovanni Chiola (DIBRIS), Paola Girdinio (DITEN), Giovanni Lagorio (DIBRIS), Mario Marchese (DITEN), Sebastiano B. Serpico (DITEN).
**Componenti esterni del Comitato di Gestione:** Cocurullo Fabio (Leonardo), Mattia Epifani (RealityNet), Ermete Meda (Hitachi Rail STS), Massa Danilo (Aizoon), Silvio Ranise (FBK), Antonio Rebora (Ansaldo Energia), Danilo Moresco (ABB).
Delegato della struttura cui è affidata la gestione amministrativa, organizzativa e finanziaria: Alessia Popia (Settore apprendimento permanente).
**Struttura Unige cui è affidata la gestione amministrativa, organizzativa e finanziaria del Corso: Servizio Rapporti con imprese e territorio, Settore apprendimento permanente**

**Art. 6**
**Trattamento dei dati personali**

I dati personali forniti dai candidati saranno raccolti dall'Università degli Studi di Genova, Dipartimento di Ingegneria Civile, Chimica e Ambientale, e trattati per le finalità di gestione della selezione e delle attività procedurali correlate, secondo le modalità stabilite dal Regolamento (UE) 679/2016 "Regolamento Generale sulla protezione dei dati" e dal D.Lgs. n. 196/2003come modificato dal D.Lgs. 10/08/2018, n. 101, ove compatibili nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.

Il Direttore del DIBRIS

Responsabile del procedimento
Dr.ssa Lorella Vongher