Università di Genova

MASTER UNIVERSITARIO DI II LIVELLO
IV EDIZIONE

CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

432 ORE DI DIDATTICA ONLINE

45 DOCENTI UNIGE E PROFESSIONISTI

420 ORE DI STAGE O PROJECT WORK

25 AZIENDE ED ENTI IN PARTNERSHIP

100% DI PLACEMENT NELLE ULTIME EDIZIONI

SPECIALIZZAZIONI in:

- Cyber Defence of IT/OT Systems
- GRC for Critical Infrastructure Protection and the Enterprise

Il Master forma un esperto nella progettazione e gestione dei sistemi ICT e della Cybersecurity Mobile, Web, Cloud, SCADA per la sicurezza e protezione di aziende, organizzazioni ed infrastrutture critiche.

master@formazione.unige.it

OBIETTIVI FORMATIVI

1. Fornire un insieme completo di nozioni fondamentali di **Cybersecurity** a laureati magistrali in materie legate aII'ICT.

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.

4. Fornire **capacità pratiche e padronanza operativa** di soluzioni e prodotti allo stato dell'arte della Cybersecurity. A tal fine, molti moduli del Master includono parti pratiche, mentre gli indirizzi di specializzazione contemplano hands-on mirati.

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 variato numero di scenari, in modo che sia flessibile e facilmente inseribile nella realtà aziendale in cui verrà coinvolto.

PIANO FORMATIVO

Il Master si basa su un approccio innovativo alla formazione che coniuga il rigore e la sistematicità della docenza accademica con l'esperienza sul campo ed il pragmatismo della docenza aziendale e professionale.

L'offerta formativa si compone di tre parti:

- **Formazione Culturale**, fornisce nozioni di base in diverse parti della cybersecurity ed un'introduzione agli aspetti legali alla cybersecurity.

- **Formazione Professionale**, approfondisce specifici aspetti di cybersecurity e di protezione delle infrastrutture critiche. Tale approfondimento permette di accompagnare lo studente alla scelta dell'indirizzo di specializzazione più consono alle proprie attitudini ed interessi.

- **Specializzazioni** è formata da due indirizzi

Cyber Defence of IT/OT Systems, più orientato alla cybersecurity.

GRC for Critical Infrastructure Protection and the Enterprise, focalizzato sulle tecniche e gli standard per la protezione di infrastrutture critiche.

DETTAGLIO PIANO FORMATIVO

PRIMA PARTE
Formazione culturale

- Introduction to Cybersecurity
- Computer Security
- Information Security Management and Legals
- Network Security
- Cryptography

TERZA PARTE
Specializzazioni

Indirizzo 1
Cyber Defence of IT/OT System

- Incident Response and Forensics Analysis
- Malware Analysis
- Mobile Security
- Cloud Security

Indirizzo 2
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

SECONDA PARTE
Formazione professionale

- Security and Threats to Critical Infrastructure
- Cryptographic Protocols & Blockchain Technologies
- Web Security
- Information Security & Risk Management
- Business Continuity and Crisis Management
- Informatica Legale, Privacy e Cyber Crime
- Fundamentals of Computer Forensics
- Cybersecurity in Financial and Credit Systems
- Cybersecurity in SCADA Systems, Industry Power and Energy
- IoT Security
- Defense-in-Depth Strategies for Critical Infrastructures
- Standards and Best Practices for Security and Safety
- Social Engineering and Intelligence for Cybersecurity

Su www.perform.unige.it tutti i profili dei docenti e i dettagli di ogni modulo

PROFILO IN USCITA

La figura professionale in uscita dal master è un **esperto ICT** con profonda ed eterogenea conoscenza nel campo della **sicurezza informatica**, degli **standard e metodologie** per la protezione delle attuali infrastrutture critiche. Per tale figura professionale si delineano alcuni sbocchi professionali di riferimento, seppur la rapidissima evoluzione dello scenario odierno offra prospettive e potenzialità ben ulteriori rispetto a quelle evidenziate:

- Information Security Officer in aziende o Corporate
- Operatore di Cybersecurity in Infrastrutture Critiche (comparto energia, banche e finanza, logistica, porto, etc...)
- Consulente di Cybersecurity per aziende
- Progettista per aziende legate ad automazione nei sistemi SCADA
- Analista e operatore di Intelligence preventiva
- Esperto e consulente di Incident Handling e Computer/Digital Forensics Responsabile/componente di CERT aziendale
- Auditor e esperto di Governance della Cybersecurity per analisi di conformità a standard ISO
- Sviluppatore di tool e metodi per aziende ad alto contenuto tecnologico

DATI OCCUPAZIONALI

Le figure inoccupate in uscita dalle precedenti edizioni sono state **tutte occupate in aziende del settore ICT entro un anno** dalla conclusione del master, sebbene la maggior parte di loro abbia trovato lavoro entro il primo mese o durante lo svolgimento dello Master.
Le figure già occupate in aziende in molti casi hanno cambiato mansione verso nuove attività legate alla cybersecurity ed alla protezione delle infrastrutture critiche, occupando posizioni fino ad allora scoperte.

SPONSORSHIP

Il Master, alla IV edizione, è da sempre progettato in s**inergia con le aziende e vanta prestigiose collaborazioni**. In aula sono numerosi gli interventi di esperti e i casi aziendali studiati. Negli ultimi anni ha ottenuto altissimi risultati di placement e di soddisfazione dei partner per l'alta qualità dei partecipanti.

Il Master è supportato dal laboratorio nazionale Cybersecurity National Lab

ed è svolto in collaborazione con il Centro di Competenza per la sicurezza e l'ottimizzazione delle infrastrutture strategiche START 4.0

START4.0

AGEVOLAZIONI E BORSE

Gli **inoccupati** hanno diritto ad uno sconto di 4.000 euro a copertura dell'iscrizione al Master.

I **dipendenti pubblici** hanno diritto a 4 borse di studio INPS e 1 borsa SNA di 6.500 euro a copertura dell'iscrizione al Master. Le borse saranno erogate a coloro in possesso dei requisiti, in ordine di graduatoria, secondo il bando pubblicato sul sito dell'INPS.

Per chi paga l'intera quota è prevista la possibilità di rateizzare il costo del Master in 3 rate.

PUNTI CHIAVE

Calendario

Lezioni frontali, case studies, visite aziendali, esami:
da Luglio 2021 a Giugno 2022
Giovedì 14-18, Venerdì 9-18, Sabato 9-13

Format

Lezioni a distanza su piattaforma Microsoft Teams con impegno partime.
Moduli didattici fruibili anche singolarmente.

Titolo rilasciato

Diploma di Master Universitario di II livello in Cybersecurity and Critical Infrastructure Protection.
60 CFU

Costo e Agevolazioni

Il Master ha un costo di 6.766 euro rateizzabili in 3 rate

- 5 borse di studio INPS per i dipendenti pubblici
- sconto di 4.000 euro per gli inoccupati.

Termine iscrizioni

Iscrizioni aperte fino all'11 giugno 2021
su piattaforma online

UniGe Master

MASTER UNIVERSITARIO DI II LIVELLO
IV EDIZIONE

CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

CONTATTI

Dott.ssa Alessia Popia

Coordinatrice del Master

email: alessia.popia@unige.it

www.perform.unige.it/master/master-cyber-security