Università di Genova

Master universitario di II livello
VII edizione

CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

PRESENTAZIONE ALLE AZIENDE

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.

cybersecurity.master.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 numeri 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 una 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
- 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 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

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

DESTINATARI

Laureati magistrali in Informatica, Fisica, Matematica ed Ingegneria. Possono essere ammessi laureati in discipline diverse, purché in possesso di un curriculum formativo-professionale ritenuto idoneo dal Comitato di Gestione del Master.
I diplomati con un background informatico che intendono approfondire la preparazione su tematiche verticali nell'ambito della cybersecurity e della protezione delle infrastrutture critiche possono partecipare al Corso di perfezionamento.

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 del 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.

PARTNERSHIP

Il Master, alla VI 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 patrocinato dal Cybersecurity National Lab del CINI

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

DIVENTA PARTNER

Le aziende possono contribuire al Master e diventare Partner, inviando la propria manifestazione di interesse utilizzando il fac-simile disponibile sul sito del master.

I PARTNER

Le aziende che decidono di collaborare con il master, accedono ad una rete di eccellenze e possono partecipare attivamente alla formazione dei futuri professionisti, contribuendo alla definizione delle tematiche dei project work e interagendo con i migliori talenti.

- La visibilità nell'elenco delle aziende partner in un articolo “ad hoc” su sito UniGe
- La massima visibilità nella brochure istituzionale del Master
- La visibilità in tutte le comunicazioni, le news, gli articoli
- La menzione dell'azienda sul canale LinkedIn di UniGe
- La presenza aziendale ad eventi pubblici legati al Master
- La selezione dei candidati per project work: possibilità di interviste ai potenziali candidati e proporre gli argomenti dei project work
- La pubblicazione annunci di lavoro e stage sui gruppi linkedIn UniGe
- La pubblicazione annunci di lavoro e stage su gruppo Alumni
- l’accesso ai CV dei candidati
- la partecipazione al Comitato di Gestione
- la possibilità di iscrivere i propri dipendenti a singoli parti del corso di interesse per l’azienda

PARTNERSHIP

Le **aziende partner** contribuiscono al master offrendo docenze gratuite e/o ospitando gli studenti per i project work.
Ad ogni partner il comitato direttivo garantisce:

- Riconoscimento dello stato di partner sulla pagina Partner del sito del master.
- Presenza della miniatura del logo aziendale in brochure e volantini pubblicitari master nella parte bassa.

È possibile garantire forme di sovvenzione miste (denaro e prestazione) per la partnership. Per discutere questo tipo di sovvenzionamento si richiede di contattare il direttore del Master.

L'elenco delle aziende partner che hanno anche collaborato nelle scorse edizioni è in costante aggiornamento sul sito.

PUNTI CHIAVE

Calendario

Lezioni on line in streaming, cases studies, visite aziendali, esami da ottobre 2024 a ottobre 2025

Format

Lezioni a distanza su piattaforma Microsoft Teams con impegno part-time.
Moduli didattici fruibili anche singolarmente.

Titolo rilasciato

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

Scadenza manifestazioni di interesse delle aziende

Le manifestazioni di interesse dovranno pervenire entro il **26 agosto 2024**

Master universitario di II livello
VII edizione

CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

CONTATTI

Prof. Luca Verderame

Direttore del Master

master.cybersecurity@unige.it

cybersecurity.master.unige.it