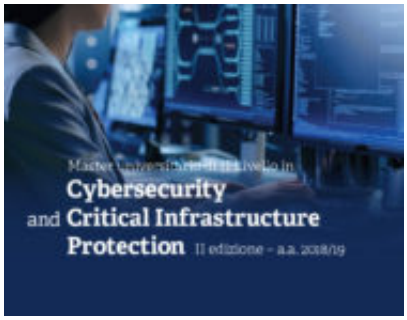
Master in Cybersecurity and Critical Infrastructure Protection

Author : Redazione

Date : 27 Febbraio 2019



Il Master forma 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.
Il master offre due specializzazioni: *Digital Forensics & Penetration Testing* e *Critical Infrastructure Protection & Security Assurance*.

1. Ai fini di potenziare la formazione pratica e professionale degli studenti per un inserimento aziendale, il Master si pone i seguenti obiettivi formativi:
2. Fornire un insieme completo di **nozioni fondamentali di Cybersecurity**
3. Fornire **competenze sulla governance della Cybersecurity** e delle relative procedure a livello aziendale o di Infrastruttura Critica
4. Fornire **nozioni in ambito legale sulla Cybersecurity**
5. Fornire **capacita? pratiche e padronanza operativa di soluzioni e tool** allo stato dell'arte nello scenario moderno di Cybersecurity.
6. Fornire **conoscenze e competenze sulla protezione delle Infrastrutture Critiche** in termini sia teorici sia pratici, includendo aspetti quali le tecnologie SCADA, Web Security, Mobile Security, Cloud Security, IoT Security

PROMOTORI & PARTNER

Il Master è promosso dal Dipartimento di Informatica, Biongegneria, Robotica e Ingegneria dei Sistemi (**DIBRIS**) e dal Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle telecomunicazioni (**DITEN**) in collaborazione con il **Servizio Apprendimento Permanente** dell'Università degli studi di Genova e in convenzione con **ISICT, Fondazione Ansaldo, Cyber Security National Lab (CINI), Consorzio Nazionale Interuniversitario per le telecomunicazioni (CNIT)**.

PROFILO PROFESSIONALE

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 possono delineare alcuni sbocchi professionali di riferimento, considerando la costante evoluzione dello scenario odierno:

- Information Security Officer in aziende o Corporate
- Operatore di Cybersecurity in Infrastrutture Critiche (comparto energia, banche e finanza)
- Consulente di Cybersecurity per aziende
- Sviluppatore e analista professionale per aziende legate ad automazione nei sistemi SCADA
- Analista e operatore di Intelligence preventiva
- Esperto e consulente legale di Incident Handling e Computer/Digital Forensics
- Responsabile/componente di CERT aziendale
- Auditor e esperto di Governance della (Cyber) Security per analisi di conformita? a standard ISO

- Sviluppatore di tool e metodi per aziende ad alto contenuto tecnologico

DESTINATARI DEL CORSO

Al Master sono ammessi 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.
Il dettaglio delle classi di laurea è indicato sul **bando**.
Il numero massimo di partecipanti è 20.

Per info e iscrizioni:
https://www.perform.unige.it/master/master-cybersecurity.html