Unione europea
Fondo sociale europeo

REGIONE LIGURIA

Alfa
Agenzia regionale per il lavoro
la formazione e l'accreditamento

Master Universitario di II Livello

Internet of Things & Big Data

PROGETTA E GESTISCE I SISTEMI DI IOT E BIG DATA ANALYTICS IN CONFORMITÀ CON IL BUSINNESS E LE ESIGENZE DELL'ORGANIZZAZIONE O DEL CLIENTE E NEL RISPETTO DI NORME E POLITICHE DI PRIVACY E SICUREZZA.
PER ULTERIORI APPROFONDIMENTI SUL MASTER È POSSIBILE SCARICARE LA SCHEDA INFORMATIVA DISPONIBILE SUL SITO.

DITEN - Università degli Studi di Genova

www.master-iot.it

Progetto cofinanziato Programma Operativo Regione Liguria Fondo Sociale Europeo 2014-2020 a valere sull'asse 3 "Istruzione e Formazione"

Master in “Internet of Things & Big Data”

Risponde alla richiesta, da parte di Aziende ed Enti, di personale specializzato nei settori **IoT&BD** (Internet of Things e Gestione di grandi moli di dati - Big Data). Forma personale specializzato in grado di cogliere, analizzare, valutare le opportunità che l’applicazione di una tecnologia innovativa porta a settori chiave per l’economia e la società quali: logistica, multimodalità, sicurezza, infomobilità, gestione delle infrastrutture critche, integrazione di sistemi complessi e robotici intelligenti, Industrie 4.0, smart city.

SEDE e CONTATTI

DITEN - Via Opera Pia 11a
16145 Genova
010 353 2733
diten@diten.unige.it

PROMOTORI & PARTNER

Fondazione Ansaldo · Forma Mentis S.r.l. · ABB · Gruppo SIGLA · Polo ADLTM · ABO DATA · netalia · cima Research Foundation · SECH · ilb software & consulting · Gruppo FOS soluzioni ad alta tecnologia · Soft Jam · Dibris · DITEN

Enabling Technologies for Internet of Things

Data Management & Analytics

Interconnected Devices
Wireless Sensors and Actuator Networks with Low Power Consumption

Distributed Systems
Cloud Computing
Fog Computing

Security and Data Protection

Semantic Web

Users Interface and Interaction

Social Internet of Things

Figura professionale di Internet of Things & Big Data Specialist conforme allo: European e-Competence Framework

Il Master si contraddistingue con un progetto formativo innovativo per contenuti e metodologie didattiche adottate e particolarmente adatto a soddisfare le esigenze delle imprese. Verrà dotato di un *Learning Content Management System* per poter integrare le attività d’aula e garantire una didattica più efficiente centrata su attività di gruppo guidate da facilitatori opportunamente formati. Particolare attenzione viene posta nel coniugare l’esperienza di realtà aziendali d’avanguardia e la capacità di modellizzazione e sistematizzazione dei problemi propria del mondo accademico con l’esperienza di gruppi di ricerca su formazione in rete.

Profilo Professionale - Missione

Contribuisce allo sviluppo del piano strategico aziendale su IoT&BD.
Assicura affidabilità, sicurezza, integrità dei sistemi IoT&DB.
Fornisce solide soluzioni per componenti e processi.
Conduce lo sviluppo e l’integrazione dei componenti.
Aumenta la consapevolezza delle innovazioni IoT&BD e del potenziale valore per il businness.
Contribuisce alla definizione degli standard di sicurezza per assicurre la sicurezza fisica e dei dati.
Organizza, coordina e conduce il team di progetto.
Pianifica la manutenzione ed il supporto all’utente.

www.master-iot.it

OBIETTIVI

Il Master forma esperti nella progettazione e nella gestione di sistemi ICT per la tutela della sicurezza e la protezione del patrimonio informativo e delle infrastrutture critiche di un'organizzazione.

PUNTI CHIAVE

Area: tecnico-scientifica
Sede: Genova
Inizio corso: maggio 2018
Durata: 460 ore aula e 450 ore stage
Format: part time, in aula
Iscrizioni: entro 30 marzo 2018

DESTINATARI

Sono ammessi giovani e adulti in cerca di occupazione e occupati 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 numero massimo di partecipanti è 20.

PROMOTORI E PARTNER

Il Master è promosso dal Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni DITEN in collaborazione con il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi DIBRIS dell'Università di Genova sulla base di un'Associazione Temporanea di Scopo con Fondazione Ansaldo.

Aderiscono al progetto le seguenti aziende:
ABB, AITEK, Aizoon, Ansaldo Energia, Ansaldo STS, Deloitte, Gruppo SIGLA, IREN, Kaspersky, Leonardo, RINA, UniCredit.

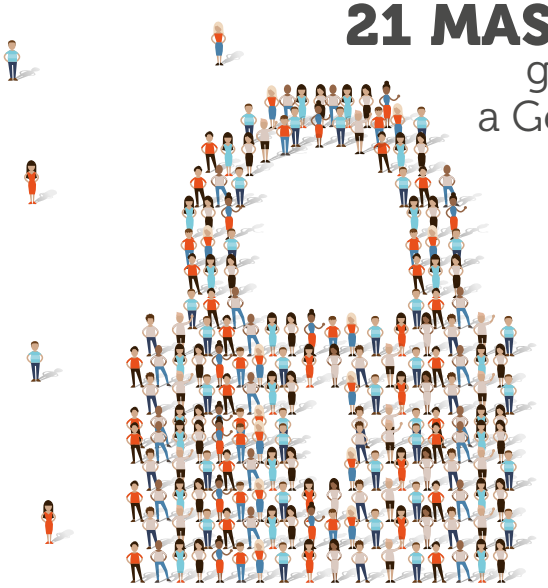
Contribuiscono al progetto:
Consiglio Nazionale delle Ricerche, ConsiQ, DASTech, ENEL, Fondazione Bruno Kessler, FortiNet, IBM, Minded Security, Piaggio AeroSpace, Protivity, RealityNet, TALOS, Vodafone.

Per ulteriori approfondimenti sul Master è possibile scaricare la scheda informativa disponibile sul sito

INFORMAZIONI
Prof. Rodolfo Zunino
Università degli Studi di Genova
Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni
Via all'Opera Pia 11 - 16145 Genova
email: rodolfo.zunino@unige.it
www.mastercybersecurity.it

www.masterfse.unige.it

Vuoi sapere di più su questo corso? Utilizza il QR code a lato



21 MASTER gratuiti a Genova

infinite opportunità

Master Universitario di II livello

Cybersecurity and Critical Infrastructure Protection

Progetto cofinanziato Programma Operativo Regione Liguria Fondo Sociale Europeo 2014-2020 a valere sull'asse 3 "Istruzione e Formazione"

PROFILO DEL CORSO

Il Master fornisce una preparazione specialistica sulle tecniche di Cybersecurity e dei suoi principali contesti applicativi, sulla governance della sicurezza digitale e delle procedure a livello aziendale, sulle relative nozioni in ambito legale, nonché 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, mentre gli indirizzi di specializzazione contemplano cyber-esercizi finalizzati ad incrementare le capacità pratiche dei partecipanti.

PROFILO PROFESSIONALE

Il Master forma professionisti nella progettazione e gestione dei sistemi basati sull'Information and Communications Technology (ICT) e di Cyber Security (Mobile, Web, Cloud, SCADA), preposti alla tutela della sicurezza e alla protezione del patrimonio informativo ed architetturale di un'organizzazione. La figura in uscita risponde all'attuale fabbisogno delle aziende di personale competente nella protezione delle proprie infrastrutture e nella gestione dei problemi di sicurezza trasversali a diverse tecnologie, dispositivi e contesti. La natura molteplice delle Aziende che aderiscono al Master evidenzia l'ampio spettro di ricadute occupazionali, confermate anche da recenti indagini a livello nazionale (Capital 4.0, Nro 447-448, sett/ott 2017) che evidenziano l'alto assorbimento di personale skilled in Cybersecurity da parte di tutto il comparto produttivo.

PARTE I Formazione Culturale
Introduction to Cybersecurity
Cryptographic Protocols
Information Security Management and Legals
Network Security
Computer Security

PARTE II Formazione Professionale
Information Security Management
Business Continuity and Crisis Management
Legal Informatics, Privacy and Cyber Crime
Fundamentals of Computer Forensics
Cryptography
Cybersecurity in Credit System, Management in Incident Response
Cybersecurity of SCADA Systems
Social Engineering and Intelligence for Cybersecurity
Mobile and Cloud Security
Security and Threats to Critical Infrastructures
Cybersecurity of Power and Energy Systems
Seminario Confindustria

PARTE III Specializzazioni
Vulnerability Assessment & Penetration Testing
Incident Response and Forensics Analysis
Malware Analysis
Web Security
Mobile Security
Cyber Exercise
Cybersecurity for Industrial Systems
ICT for Critical Infrastructure Protection
Cyber Defense and Cyber Intelligence
Standards and Best Practices in Security and Safety for Industry
SCADA and Industrial Systems Protection
Governance Finance
Security Assurance
Cyber Exercise
Security by Design for Critical Infrastructure Protection
ICT for Critical Infrastructure Protection
Cyber Defense and Cyber Intelligence
Standards and Best Practices in Security and Safety for Industry
Security-driven Design
Physical Security
Risk Propagation in Interconnected Infrastructures
Crisis Management for Critical Infrastructures

SELEZIONE e ISCRIZIONI

La partecipazione al Master è **gratuita**. Il Master è interamente finanziato da Regione Liguria con fondi comunitari. L'ammissione al Master avviene attraverso il superamento di una prova scritta e un colloquio orale. La domanda di ammissione al concorso deve essere presentata entro le ore 12.00 di **venerdì 30 marzo 2018**.

ORGANIZZAZIONE DIDATTICA

Il durata di 12 mesi, si svolge da **maggio 2018 a aprile 2019**. Il Master si articola in:

- attività formative d'aula e laboratorio
- studio individuale e verifiche di apprendimento
- stage/project work

La frequenza è a tempo parziale per un ammontare massimo di 32 ore settimanali. La fase d'aula è suddivisa in tre parti; le prime due, comuni a tutti gli studenti, tratteranno tematiche di Cybersecurity e infrastrutture critiche e i loro ambiti di applicazione. La terza parte offre tre indirizzi a scelta dello studente, ovvero: Vulnerability Assessment & Penetration Testing, Cybersecurity for Industrial Systems e Security by Design for Critical Master, della Infrastructure Protection.

STAGE

Al termine della fase didattica è previsto un periodo di stage presso aziende operanti nel settore.
Lo stage permetterà agli studenti un primo ingresso nel mondo del lavoro attraverso progetti formativi mirati e concordati con i soggetti ospitanti.

TITOLO RILASCIATO

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