

MASTER UNIVERSITARIO DI 1° LIVELLO IN  
**CYBERSECURITY  
& DEFENCE**





## Informazioni generali



### LUOGO

Free Mind Foundry Academy  
Via Sclafani 40, Acireale (CT)



### LINGUA

Italiano



### CFU

60 in totale



### QUOTA DI ISCRIZIONE

€ 4.356



### DATA DI AVVIO

Gennaio 2021



### ORE DI FORMAZIONE

318 ore + Stage in azienda



### TIPOLOGIA

Professionalizzante



### MODALITÀ DI EROGAZIONE

In presenza



### PARTECIPANTI

Min 15 / Max 35



### DURATA

Annuale

#aunpassodalfuturo

# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## Consiglio scientifico del corso

**Prof. Giampaolo Bella** (Direttore del Master)

**Prof. Dario Catalano**

**Prof. Salvatore Riccobene**

**Prof. Emiliano Tramontana**

**Prof. Sebastiano Battiato**

**Prof. Alessandro Ortis**

**Ing. Simone Massaro**

**Prof. Andrea Viridi**

Struttura a cui fa capo la gestione amministrativa e finanziaria  
Dipartimento di Matematica e informatica dell'Università degli Studi di Catania

## A chi è rivolto

Il Master è rivolto prioritariamente a chi è interessato ad apprendere i fondamenti della sicurezza delle infrastrutture informatiche, dei dati e della loro trasmissione. Consente la formazione di figure professionali preposte alla tutela della sicurezza e alla protezione del patrimonio informativo di un'azienda, di un'infrastruttura critica o di un'organizzazione.

## Contributi esterni

Il Master si avvarrà della collaborazione della Free Mind Foundry in termini di know-how su soluzioni e servizi tecnologici di ultimissima generazione, e di partnership di valore con Istituti di certificazione riconosciuti internazionalmente quali Cisco e Fortinet. In particolare, i corsisti, qualora fosse di loro interesse, avranno l'opportunità di intraprendere un percorso di intership presso le aziende digitali del Campus operanti nei settori dell'energia, delle telecomunicazioni, dei trasporti, dell'IoT e dell'intelligenza artificiale.

#aunpassodalfuturo

# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## Obiettivi formativi

Il Master Universitario di Primo Livello in “Cybersecurity & Defence” risponde alla pressante necessità, tipica della nostra epoca, di figure professionali di alto livello che siano adeguatamente formate sui temi legati alla sicurezza informatica, alla prevenzione e costante difesa da attività offensive delle risorse e dei servizi che un’istituzione o azienda eroga con strumenti digitali, nonché alla protezione dei dati personali di tutte le persone fisiche, ad inclusione, quindi, di dipendenti, fornitori, clienti, ed altri attori. Pertanto, il Master si caratterizza come strumento abilitante relativamente ai temi succitati, diventando attraente per una qualunque funzione istituzionale, a partire dal Chief Technical Officer o dal Sys Admin che intendano espandere le proprie competenze sui rischi di attacco e sugli strumenti di difesa, fino a tutte le funzioni che, trattando dati personali, sono soggette a sessioni periodiche di formazione sulla sicurezza dei trattamenti, come richiesto dal Regolamento Europeo 2016/679, o General Data Protection Regulation.

## Sbocchi occupazionali

- CHIEF INFORMATION SECURITY OFFICER
- DATA PROTECTION OFFICER
- INTERNAL SECURITY AUDITOR
- CHIEF TECHNICAL OFFICER PREPOSTO ALLA CYBERSECURITY AZIENDALE
- SYS ADMIN CON FUNZIONI DI CONFIGURAZIONE DELLE DIFESE AZIENDALI (E.G. FIREWALL)
- ESPERTO SISTEMI DI PROTEZIONE CISCO
- ESPERTO SISTEMI DI PROTEZIONE FORTINET

# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## Note integrative

La richiesta di esperti di sicurezza informatica è cresciuta tre volte più velocemente di qualsiasi altro ruolo nel settore ICT, e la disponibilità sul mercato di figure preparate e specializzate è molto bassa. Il Master in Cybersecurity & Defence, unico nel panorama formativo degli Atenei siciliani, risponde all'esigenza di formare esperti con le competenze specialistiche necessarie per affrontare una carriera nel settore della Sicurezza Informatica o di rafforzare le conoscenze già possedute consentendo di operare rapidamente, con cognizione, nel rispetto degli ultimi standard.

## Criteri di valutazione

Requisiti indispensabili per l'ammissione alla selezione sono il possesso di una delle Lauree specificate al punto 3 del presente bando. Nel caso in cui il numero degli aspiranti allievi fosse superiore al numero massimo dei posti previsti, verrà effettuata una selezione sulla base dei titoli presentati nella domanda di ammissione e sulla base di un colloquio. L'eventuale colloquio integrativo, si terrà presso il Dipartimento di Matematica e Informatica dell'Università degli Studi di Catania, V.le Andrea Doria, 6. La data del colloquio sarà comunicata preventivamente con avviso pubblicato sul sito web dell'Ateneo ([www.unict.it](http://www.unict.it) seguendo il percorso [didattica/post laurea/master universitario](#)).

Ai titoli presentati nella domanda di ammissione verranno assegnati i seguenti punteggi:

- per la laurea fino a un massimo di punti 5 in base alla votazione: punti 1 da 103 a 104; 2 da 105 a 106; 3 da 107 a 108; 4 da 109 a 110; 5 per 110 con lode;
- per la tesi di laurea su temi attinenti gli insegnamenti del Master fino a punti 6;
- per ulteriori titoli di studio (seconda laurea, laurea magistrale, specializzazione, dottorato di ricerca) fino a punti 5; documentata esperienza in attività (stage, tirocini, progetti formativi,) attinenti gli insegnamenti del Master: punti 1 per ciascun periodo non inferiore a mesi sei con un massimo di punti 5;
- pubblicazioni scientifiche pertinenti le tematiche oggetto del Master: fino ad un massimo di punti 4.

Per un massimo complessivo di punti 25.

La Commissione esaminatrice si riserva di accertare il possesso dei requisiti attraverso una prova attitudinale e/o un colloquio motivazionale, che sarà svolto anche in lingua inglese, disponendo di ulteriori punti fino ad un massimo di 10.

A parità di punteggio complessivo, la graduatoria verrà determinata sulla base dell'età dei candidati, dal più giovane al più anziano (art. 2, comma 9, L. 16/06/1998 n. 191).

# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## Destinatari

Gli aspiranti corsisti dovranno essere in possesso di uno dei seguenti titoli di Laurea: Tecnologie informatiche (L/31); Ingegneria dell'informazione (L/08); Ingegneria Elettronica (LM/29); Ingegneria delle telecomunicazioni (LM/27); Ingegneria Informatica (LM/32). In subordine a coloro in possesso di una delle lauree fra quelle citate, il Comitato Scientifico del Master si riserva di decidere sull'eventuale ammissione anche di coloro che posseggano una laurea diversa ma dimostrino un curriculum formativo e professionale valutabile come appropriato ai contenuti del Master.

Possono essere ammessi "con riserva" anche studenti laureandi, purché conseguano il titolo entro la data di avvio delle attività didattiche e, comunque, non oltre il 30 Aprile del 2021. In tal caso, il candidato sarà tenuto a produrre, a pena di decadenza, entro il 30 Maggio 2021, relativa autocertificazione di avvenuto conseguimento del titolo.

Il numero di studenti ammessi a frequentare il corso è fissato in un massimo di 35 e in un minimo di 15. Al di sotto di tale soglia il Master non sarà attivato.

### Eventuali altri requisiti e titoli preferenziali

Conoscenza di una seconda lingua straniera; livello B/2;

Documentata esperienza nel settore della Cybersecurity.

## Moduli didattici

### 1- Misure tecnico organizzative di difesa

Principali misure, sia tecniche che organizzative, per la prevenzione di attacchi informatici a scopi malevoli, principali vettori di attacco, insider versus outsider, bug versus ingegneria sociale, misure preventive e di contenimento dell'appropriamento indebito di risorse e del furto di dati.

### 2- Strumenti di protezione

Principali strumenti tecnologici di protezione, in termini di rilevamento, valutazione e contenimento; intrusion, detection e prevention, firewall software e firewall commerciali embedded, security information and event management.

### 3- Attività offensive a scopi etici

Principali metodologie ed attività finalizzate alla violazione, a scopi etici e di testing preventivo, di un sistema o servizio informatico, Vulnerability, Assessment e Penetration Testing, linee guida dell'Open Web Application Security Project (OWASP).

### 4- Continuità operativa e protezione dei dati personali

Continuità operativa e protezione dei dati personali.

Principi fondamentali e standard di riferimento per la continuità dei sistemi e dei servizi informatici, concetti di backup e restore fino alla definizione di un disaster recovery plan, Regolamento UE General Data Protection Regulation (GDPR).

## Piano didattico

N*	Denominazione	SSD	CFU
1	Misure tecnico organizzative di difesa	INF/01	12
2	Strumenti di protezione	INF/01	12
3	Attività offensive a scopi etici	INF/01	12
4	Continuità operativa a protezione dei dati personali	INF/01	9
pf	Prova finale		3
T	Tirocinio		12
			<b>TOT. 60</b>

## Dettaglio dei contenuti

### 1- Reti informatiche:

- TCP/IP e Internet
- Overlay network
- Protocolli principali (Web, DNS, E-Mail, Share di rete, Accesso Remoto)
- Reti avanzate (edge, fog, ad-hoc)

### 2- Schemi e vettori d'attacco:

- Schemi di attacco (MITM, WiFi, BGP Hijacking, DoS, DDoS, DrDoS)
- Vettori di attacco (fisico, insider, web e ingegneria sociale)
- Vulnerabilità di rete (DNS, IP Spoofing, NTP)

### 3- Attacchi notevoli:

- Attacchi al perimetro (Web Application, Brute Force, Exploit)
- Attacchi ai dipendenti (Malware, Trojan, Phishing e Ransomware)
- Attacchi SCADA e IoT
- APT (Stuxnet, APT1, APT28), RCE, XSS, XSRF, SQLInj, IDOR, etc.

### 4- Vulnerability Assessment & Penetration Testing

- Entità offensive  
(Script Kiddie, ECrime e Malware Writer, Hacktivist LulzSec, Anonymous)
- Cyberwarfare
- Metodologie di VAPT (OWASP, PTES, etc)
- Reportistica
- Misure rimediali

# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## 5- Monetizzazione dei crimini informatici:

- a. Blackmarket e Intelligence
- b. TOR, reti anonime e criptovalute
- c. Security economics

## 6- Misure tecnico-organizzative di difesa e protezione:

- a. Le tecnologie (Firewall, AV, EDR, Sandbox, SIEM)
- b. Le attività (Security Monitoring, Malware Analysis, Incident Response, Threat Hunting, Intelligence)
- c. Security infrastructure assessment
- d. Domain and Brand Reputation

## 7- Misure per la continuità dei sistemi e dei servizi:

- a. Gli uffici (SOC, CERT, CSIRT)
- b. Sicurezza dei backup e degli strumenti di ripristino
- c. Business continuity & disaster recovery

## 8- Applied Cryptology:

- a. Protezione dei dati a riposo (basic crypto, Bitlocker, LUKS)
- b. Protezione dei dati in transito (TLS3.0, SSH)
- c. Cloud security

## 9- Ambiente Active Directory:

- a. Configurazioni sicure
- b. Identity e Access Management
- c. Scripting powershell

## 10- Linux e soluzioni opensource

- a. Community e gestione dei fix
- b. Scripting Bash
- c. Configurazioni sicure

## 11- Standard e certificazioni

- a. Cyber Kill Chain Lockheed Martin
- b. MITRE ATT&CK®
- c. ISO27001

## 12- Cybersecurity risk management

- a. Metodologie (ISO27005, Mehari, Stride)
- b. Figure professionali nel settore Cybersecurity
- c. GDPR
- d. NIST
- e. NIS

## 13- Multimedia Security

- a. Integrità e autenticità di contenuti multimediali
- b. Steganografia/Watermarking
- c. Deep Fake

## 14- Machine Learning in Cybersecurity.

- a. Adversarial Learning and Trusted data
- b. Generative Adversarial Networks (GAN)
- c. Applicazioni: Intrusion Detection, Biometry, etc.



# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## Modalità di svolgimento

### Sede delle attività didattiche

Free Mind Foundry Academy - Via Scalfani 40 Acireale (CT)

### Calendario

Data di inizio: Gennaio 2021

Data esame finale: TBD

11 Settimane, 5 giorni a settimana, 6 ore al giorno.

Frequenza obbligatoria - Percentuale minima richiesta dell'80%

Tirocinio in qualificate aziende nel settore di riferimento, ad esempio:

N*	Azienda o ente	Attività prevista
1	Free Mind Foundry Srl ambito ICT/IT	STAGE
2	BE-ON Srl ambito Open Fiber	STAGE
3	BaxEnergy Srl	STAGE
4	Cloud IntelliSyc Srl	STAGE

### Prova finale

Al termine del Corso i partecipanti dovranno presentare un elaborato scritto, in cui approfondire un particolare tema affrontato durante le lezioni o durante il tirocinio/stage. L'elaborato sarà discusso in una sessione orale pubblica di esame finale.

# Master Universitario di I Livello in CYBERSECURITY & DEFENCE



## Modalità di iscrizione e pagamento

### MODALITÀ CLASSICA

La quota di partecipazione al Master è stabilita in **€ 4.356** (quattromilatrecentocinquantasei/00) così rateizzata:

> 1° rata

All'atto dell'iscrizione **€ 356.00** (contributo annuale d'Ateneo) e prima rata di **€ 600.00**;

> 2° rata

**€ 850.00** entro il 28 Febbraio 2021;

> 3° rata

**€ 850.00** entro il 15 Aprile 2021;

> 4° rata

**€ 850.00** entro il 30 Giugno 2021

> 5° rata

**€ 850.00** entro il 30 Settembre 2021

### MODALITÀ DI PAGAMENTO

Bonifico bancario da effettuare a c.c. intestato a **Free Mind Foundry srl**,

**IBAN IT61G030 6916901100000007114**

(nella causale indicare il titolo del master, nome, cognome, codice fiscale del corsista e n° rata di iscrizione).

### MODALITÀ FINANZIAMENTO:

Pagamento a rate fino a 36 mesi

(Per info sui requisiti necessari per poter chiedere una rateizzazione con Soisy e tasso di interesse agevolato, mail a [academy@freemindfoundry.com](mailto:academy@freemindfoundry.com))

## Come iscriversi

In FMF Academy puoi prenotare una consulenza individuale gratuita (via call e/o in presenza) per ottenere informazioni dettagliate sui programmi di studio, approfondire meglio i tuoi obiettivi di crescita professionale e definire il percorso di studi più adatto a te.

Prenota il tuo colloquio di orientamento:

### FMF

#### E-mail

[academy@freemindfoundry.com](mailto:academy@freemindfoundry.com)

#### WhatsApp:

+39 3427688003

#### Segreteria

09516957606

#### Indirizzo

Via Sclafani 40 - Acireale (CT)

### UNICT

#### Website

[unict.it/didattica/master-universitari](http://unict.it/didattica/master-universitari)

#### Segreteria

095/7383072 - 0957307998/953

#### Indirizzo

P.zza Università 16 - Catania (CT)

#aunpassodalfuturo



UNIVERSITÀ  
degli STUDI  
di CATANIA