

# Borse di studio

## CyberX – Mind4Future

### Premessa

Il Centro di Competenza Cyber 4.0 in collaborazione con Leonardo S.p.A. e le seguenti Università ("Università Partecipanti"):

- Università Campus Bio-Medico di Roma
- Università degli Studi dell'Aquila
- Università degli Studi della Tuscia
- Università degli Studi di Cassino e del Lazio Meridionale
- Università degli Studi di Roma "La Sapienza"
- Università degli Studi di Roma "Tor Vergata"
- Università degli Studi Roma Tre
- Università Luiss Guido Carli

intende bandire n. **10 Borse di studio** nell'ambito del Progetto CyberX – Mind4Future.

Cyber 4.0 è il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, uno degli 8 centri di competenza ad alta specializzazione finanziati dal Ministero delle Imprese e del Made in Italy (già Ministero dello Sviluppo Economico). Cyber 4.0 è un partenariato pubblico-privato che include 45 soci, provenienti dal mondo dell'Università e della ricerca, da istituzioni pubbliche, dal mondo privato – grandi aziende e PMI specializzate, associazioni e fondazioni. Cyber 4.0 svolge attività di rafforzamento delle competenze di imprese e PA, sviluppando iniziative di formazione, programmi di advisory e orientamento, e promuovendo progetti di ricerca e innovazione.

Leonardo sviluppa capacità operative multidominio nel settore dell'Aerospazio, Difesa e Sicurezza. L'azienda è protagonista dei principali programmi strategici internazionali e partner tecnologico di Governi, Amministrazioni della Difesa, Istituzioni e imprese. Innovazione, ricerca continua, industria digitale e sostenibilità sono i pilastri del suo business nel mondo.

Il progetto CyberX – Mind4Future offre opportunità di formazione addizionale e sperimentale finalizzate allo sviluppo pratico di competenze per la difesa delle moderne infrastrutture ICT. Alle attività formative tradizionali (focalizzate al trasferimento di conoscenza) si affiancano formule innovative e coinvolgenti ispirate alla simulazione e al gaming (mirate all'acquisizione di abilità e competenze, ovvero alla risoluzione dei problemi).

Le borse di studio sono finalizzate allo svolgimento di attività in collaborazione con la Divisione Cyber & Security Solutions di Leonardo S.p.A. e sotto la supervisione del personale

docente delle *“Università partecipanti”* e saranno assegnate a seguito di un percorso che prevede attività di formazione ed esercitazioni sperimentali, come meglio definito nella sezione *“Descrizione dell’iniziativa”*.

L’importo delle borse di studio, istituite su fondi erogati da Leonardo S.p.A., è il seguente:

- 5.000 EUR lordi per il primo classificato
- 3.000 EUR lordi per il secondo classificato
- 2.500 EUR lordi per il terzo classificato
- 2.000 EUR lordi per il quarto classificato
- 1.500 EUR lordi per il quinto classificato
- 1.000 EUR lordi ciascuno per i classificati dalla sesta alla decima posizione

## **Il contesto di riferimento**

Il progetto CyberX – Mind4Future nasce dalla necessità di rimediare allo skill-gap in ambito cybersecurity. Nel 2022 infatti a livello mondiale, il Cyber skill-gap è di oltre 3,43 milioni di posizioni, destinato ad aumentare del 26,2% annualmente, e di oltre 317 mila posizioni nella regione EMEA, con un aumento atteso del 59,3% annuo.

Al contempo, a livello mondiale, l'80% delle organizzazioni ha subito uno o più attacchi informatici attribuibili a una mancanza di competenze e/o consapevolezza in materia di cybersecurity.

L’iniziativa ha il triplice obiettivo di:

- Fornire un modello didattico innovativo, che coniuga momenti formativi tradizionali con attività laboratoriali e di gaming, per creare un percorso altamente esperienziale ed immersivo.
- Promuovere lo sviluppo delle soft skills attraverso un approccio human-tech che coniuga le competenze tecniche con la valorizzazione del *“capitale umano”*, aiutando ad accrescere la capacità di comunicare, lavorare in gruppo risolvere conflitti e prendere decisioni
- Contribuire a diffondere la cultura della sicurezza nazionale e formare le competenze necessarie al Paese per riconoscere, comprendere e affrontare le minacce cibernetiche per un futuro sicuro.

Partecipando a questa iniziativa, gli studenti potranno sviluppare di mindset, competenze, conoscenze *“del futuro”* nell’ambito di un ecosistema sinergico di università, centri di competenza e aziende. I partecipanti potranno acquisire comprensione e capacità di cogliere le opportunità che la cyber security offre in uno scenario dinamico e in continua evoluzione per il proprio futuro professionale e accademico.

## **Descrizione dell’iniziativa**

Il progetto consiste in un programma di formazione evoluta ed esperienziale sui temi della cyber security, aperto a tutti gli studenti delle Università facenti parti di Cyber 4.0 (triennale e magistrale) delle **lauree del settore dell'informazione, dell'ingegneria industriale e dell'informazione**, e delle **lauree in Matematica, Fisica, Data science, Management and Computer Science**. Il programma ha i seguenti obiettivi:

- valorizzare e favorire lo sviluppo delle conoscenze nella sicurezza cyber ritenute indispensabili per la difesa delle moderne infrastrutture ICT;
- promuovere lo sviluppo di competenze trasversali (soft-skill) attraverso esercitazioni coinvolgenti ed immersive con piattaforme ispirate a tecniche di gaming;
- Contribuire ad aumentare la cultura della sicurezza sul territorio nel centro Italia in particolare in relazione alla popolazione universitaria.

Il progetto si sviluppa nelle seguenti quattro fasi principali:

- Publicazione del bando di iscrizione sul sito web del Centro di Competenza Cyber 4.0. Sarà possibile compilare il bando di iscrizione entro il 25.01.2023, termine di chiusura del bando.
- Febbraio 2023: **sessioni di formazione avanzata**, aggiuntiva rispetto al corso e/o addestramento pratico su una selezione di temi, quali: crittografia, sicurezza delle reti di calcolatori, analisi del codice binario, sicurezza sistemi e reti. Le sessioni di formazione sono svolte presso le Università o in modalità ibrida con docenti universitari e/o esperti aziendali.
- Marzo 2023: questa fase prevede lo svolgimento di attività laboratoriale e di gaming in realtà virtualizzate ed immersive, in particolare:
  - **Capture The Flag**, una gara in cui gli studenti sono chiamati a risolvere un percorso di sfide di cybersecurity a complessità crescente e grazie alla quale, a partire dai candidati iniziali, si seleziona un numero ridotto di finalisti.
  - **Esercitazione CyberRange**: una sfida in cui difendere un'infrastruttura cyber-fisica da attacchi lanciati da un gruppo di specialisti, ethicalhacker in un ambiente virtualizzato realistico
- Aprile 2023: finalizzazione progetto con **assegnazione delle borse di studio ai miglior studenti classificati** anche nell'ambito di un evento di premiazione

## Requisiti per i candidati

L'iniziativa è gratuita e riservata a candidati/e in possesso dei seguenti requisiti:

- essere residenti o domiciliati in Italia. Nel caso di cittadini/e extracomunitari/e, essere in regola con le norme vigenti in materia di soggiorno in Italia;
- essere studenti regolarmente iscritti nell'a.a. 2022/23 a un Corso di Laurea Triennale, di Laurea Magistrale delle lauree del settore dell'informazione, dell'ingegneria

industriale e dell'informazione, o delle lauree in Matematica, Fisica, Data science, Management and Computer Science delle università partecipanti elencate in "Premessa"

- essere in possesso delle seguenti competenze di base necessarie
  - Conoscenza di almeno un linguaggio di programmazione
  - Conoscenza dei principi di funzionamento e dell'architettura di un calcolatore
- essere di madrelingua italiana ovvero in possesso di un livello di conoscenza della lingua italiana B2 del Quadro Comune Europeo di Riferimento per le Lingue, dimostrabile tramite certificazioni linguistiche o titoli equipollenti o autodichiarazione.

I citati requisiti devono essere posseduti al momento della presentazione della domanda di ammissione al programma.

Gli aspiranti partecipanti non comunitari dovranno allegare alla domanda anche copia del permesso di soggiorno.

## **Modalità di invio delle candidature**

La domanda di partecipazione alla selezione CyberX – Mind4Future dovrà essere effettuata online, tramite la compilazione dell'apposito modulo di iscrizione presente all'indirizzo <https://bit.ly/3iWQyzy> **entro le ore 23.59 del giorno 25/01/2023**. Le domande successive a tale data e ora non saranno prese in considerazione.

I chiarimenti o altre richieste di informazioni, potranno essere richiesti entro 48 ore prima della data di scadenza del bando, scrivendo all'indirizzo e-mail: **cyber@cyber40.it**.

## **Ammissione dei candidati**

La selezione sarà curata da una commissione che valuterà le candidature e le successive prove pratiche. Le decisioni della commissione saranno prese a maggioranza e sono definitive e inappellabili.

La commissione sarà composta da un rappresentante per ciascuna delle organizzazioni che collaborano alla realizzazione dell'iniziativa.

La commissione si riserva di effettuare controlli a campione per confermare l'attendibilità delle autodichiarazioni presentate tramite il modulo di iscrizione.

La commissione definirà e validerà le prove a cui i candidati saranno sottoposti consistenti:

- a. Nella fase di candidatura in relazione all'inserimento di informazioni pertinenti alla candidatura stessa e la preparazione;
- b. Nelle esercitazioni pratiche consistenti in una "Capture the Flag" (CTF), e nella difesa di uno scenario di attacco cyber emulato "Cyber Range".

È facoltà della commissione definire modalità e tempistiche per un eventuale test di selezione integrativo alla procedura di cui al presente bando, nel caso in cui il numero di domande di ammissione dovesse eccedere il massimo numero di partecipanti previsto per questa iniziativa (200).

La commissione potrà inoltre integrare le prove soprastanti con colloqui di presentazione da parte dei candidati per valutarne attitudini e motivazione e per possibile discussione congiunta sulle prove stesse. Qualora si optasse per queste prove le stesse saranno svolte per tutti i candidati ancora in concorso (ad esempio dopo la conclusione della CTF o dopo la conclusione dell'attacco emulato).

## **Tutela della Privacy**

I dati personali dei candidati al bando e dei candidati all'iniziativa saranno trattati da Cyber 4.0 nel rispetto della normativa europea e nazionale in materia di protezione dei dati personali di cui al Regolamento UE 679/2016 e al D.Lgs. n° 196/2003, come modificato dal D.Lgs. n° 101/2018 (c.d. Codice della privacy). Con la partecipazione alla presente procedura, i candidati accettano i termini e condizioni per il trattamento dei dati personali effettuato da Cyber 4.0 ed acconsentono, previa apposita autorizzazione prevista dal format di iscrizione, alla condivisione dei dati a Leonardo S.p.A. ed alle Università partecipanti all'iniziativa al fine dell'esecuzione del presente progetto.

Per eventuali approfondimenti in materia di protezione dei dati personali nonché per avere informazioni in merito agli obblighi di pubblicazione, alle modalità e finalità dei trattamenti effettuati sui dati personali dei candidati/partecipanti al presente Bando, si rinvia all'informativa predisposta in osservanza dell'art. 13 Regolamento UE 679/2016 pubblicata e consultabile tramite il form di iscrizione <https://bit.ly/3iWQyzy>.

Il presidente Cyber 4.0

Prof. Leonardo Quarzoni

