D.D. n. 199 del 27/11/2024

Università degli Studi di Napoli "*Federico II*"

Ce.S.M.A. – Centro Servizi Metrologici e Tecnologici Avanzati

Il Direttore

Visto *il contratto di cooperazione tra il Centro Servizi Metrologici e Tecnologici Avanzati (CeSMA) dell'Università degli Studi di Napoli Federico II e Accenture sottoscritto in data 22.11.2024;*

Considerato *che l'Università degli Studi di Napoli, in collaborazione Accenture intende attuare un'iniziativa di formazione avanzata denominata "Accenture Cyber HackAdemy" per l'anno accademico 2024/2025;*

Visto *che il percorso formativo è a numero chiuso (fino a 30 studenti suddivisi in 2 gruppi distinti) e avrà come obiettivo la progettazione ed erogazione di attività formative avanzate nel campo della sicurezza informatica, con particolare riferimento alle tecniche ed ai protocolli per la sicurezza di rete, delle infrastrutture cloud, degli ecosistemi IoT (Internet of Things), alle metodologie cosiddette di "Offensive Defense", all'impiego delle moderne tecniche di Machine Learning per l'analisi di grosse moli di dati ai fini di sicurezza, all'uso dell'Intelligenza Artificiale Generativa per l'automatizzazione delle tecniche di attacco e di difesa in ambito informatico;*

Vista *la necessità di reclutare fino ad un massimo di 30 studenti per il percorso formativo;*

Ce S M A
CENTRO SERVIZI METROLOGICI E TECNOLOGICI AVANZATI
COMPLESSO UNIVERSITARIO SAN GIOVANNI
CORSO NICOLANGELO PROTOPISANI 80146 NAPOLI
TEL 0812530001 MAIL CESMA@UNINA.IT

D e c r e t a

È autorizzata l'emanazione di 1 bando per l'ammissione di un numero massimo di 30 studenti alla "Cyber HackAcademy" edizione 2024/2025, che avrà come obiettivo la formazione di esperti di cybersecurity. L'iniziativa consisterà nella progettazione ed erogazione di attività formative avanzate nel campo della sicurezza informatica, con particolare riferimento alle tecniche ed ai protocolli per la sicurezza di rete, delle infrastrutture cloud, degli ecosistemi IoT (Internet of Things), alle metodologie cosiddette di "Offensive Defense", all'impiego delle moderne tecniche di Machine Learning per l'analisi di grosse moli di dati ai fini di sicurezza, all'uso dell'Intelligenza Artificiale Generativa per l'automatizzazione delle tecniche di attacco e di difesa in ambito informatico.

Il presente decreto sarà sottoposto a ratifica nella prossima adunanza del Comitato Direttivo.

Il Direttore
prof. Domenico Accardo

Ce S M A
CENTRO SERVIZI METROLOGICI E TECNOLOGICI AVANZATI
COMPLESSO UNIVERSITARIO SAN GIOVANNI
CORSO NICOLANGELO PROTOPISANI 80146 NAPOLI
TEL 0812530001 MAIL CESMA@UNINA.IT

Università degli Studi di Napoli Federico II -
Centro Servizi Metrologici e Tecnologici Avanzati (CeSMA)

Bando di selezione per l'ammissione alla

"Accenture Cyber HackAdemy 2024/2025"

Articolo 1

Disposizioni Generali

Nell'ambito del contratto di cooperazione tra il Centro Servizi Metrologici e Tecnologici Avanzati (CeSMA) dell'Università degli Studi di Napoli Federico II e l'azienda Accenture, si intende attuare un'iniziativa di formazione avanzata denominata *"**Accenture Cyber HackAdemy**" 2024-2025* (nel seguito *HackAdemy*), che avrà come obiettivo la formazione di esperti di cybersecurity. L'iniziativa consisterà nella progettazione ed erogazione di attività formative avanzate nel campo della sicurezza informatica, con particolare riferimento alle tecniche e ai protocolli per la sicurezza di rete, delle infrastrutture cloud, degli ecosistemi IoT (Internet of Things), alle metodologie cosiddette di "Offensive Defense", all'impiego delle moderne tecniche di Machine Learning per l'analisi di grosse moli di dati ai fini di sicurezza, all'uso dell'Intelligenza Artificiale Generativa per l'automatizzazione delle tecniche di attacco e di difesa in ambito informatico. Al fine di determinare i partecipanti alla *HackAdemy*, è indetta una selezione pubblica per l'ammissione di **un numero massimo di 30 studenti, suddivisi in due gruppi distinti,** aventi le seguenti caratteristiche:

- profilo "Junior Cybersecurity Specialist" (max 15 partecipanti);
- profilo "Senior Cybersecurity Specialist" (max 15 partecipanti).

Per entrambi i profili, il progetto didattico sarà articolato su circa **6 mesi, suddivisi in tre periodi consecutivi,** come descritto nel successivo articolo 3 di questo bando, e prevederà un impegno, in presenza, di 4 ore giornaliere, dal lunedì al venerdì, per un totale di 20 ore settimanali (salvo eccezioni dovute a speciali iniziative che saranno programmate durante il corso). Le attività si svolgeranno presso il polo tecnologico di San Giovanni a Teduccio dell'Università degli Studi di Napoli Federico II. Non si esclude la possibilità di svolgere parte delle attività anche presso le sedi di aziende partner. La partecipazione ai momenti formativi in laboratorio dovrà essere affiancata da uno studio autonomo dei partecipanti.

Ce S M A
CENTRO SERVIZI METROLOGICI E TECNOLOGICI AVANZATI
COMPLESSO UNIVERSITARIO SAN GIOVANNI
CORSO NICOLANGELO PROTOPISANI 80146 NAPOLI
TEL 0812530001 MAIL CESMA@UNINA.IT

Agli studenti che avranno completato con successo il percorso didattico della HackAdemy, Accenture avrà la facoltà di offrire l'inserimento in stage per un periodo di 6 mesi presso una delle sue sedi.

Articolo 2

Obiettivi formativi e Profili Professionali

Il percorso formativo oggetto del bando si propone di formare esperti su tematiche di sicurezza informatica in presenza di architetture di rete avanzate. In tali contesti, la cybersecurity va affrontata con un approccio olistico, prevedendo la presenza di elementi di sicurezza fin dalle primissime fasi di progetto e tenendo conto della eterogeneità delle piattaforme di rete coinvolte, nonché dei servizi end-to-end da esse supportati. L'approccio formativo della HackAdemy è di tipo hands-on e sarà inquadrato nel contesto più ampio dell'apprendimento basato su sfide (Challenge Based Learning – CBL). Il percorso formativo sarà dunque sviluppato con una metodologia basata sull'integrazione tra formazione in presenza, apprendimento autonomo e didattica esperienziale basata sul lavoro di gruppo per la soluzione di sfide pratiche a difficoltà crescente.

Articolo 3

Sede, durata, articolazione e svolgimento delle attività

Il progetto didattico della HackAdemy si svilupperà da gennaio 2025 a luglio 2025 e comprenderà lezioni frontali, esercitazioni, studio autonomo, sviluppo di lavori di gruppo e "project-work/stage".

Agli studenti che frequenteranno la HackAdemy è richiesto un impegno in presenza di 20 ore alla settimana (salvo eccezioni dovute a speciali iniziative che saranno programmate durante il corso) per la partecipazione alle attività didattiche che si svolgeranno presso il polo tecnologico di San Giovanni a Teduccio dell'Università degli Studi di Napoli Federico II, nonché presso le sedi di aziende partner. La partecipazione ai momenti formativi on-line ed in laboratorio dovrà, comunque, essere affiancata da uno studio autonomo da parte dei partecipanti.

Per il profilo "Junior Cybersecurity Specialist", il percorso didattico completo si articolerà in tre fasi come di seguito specificato:

- Fase 1 - La prima fase ha come obiettivo l'acquisizione delle competenze di base necessarie a sviluppare soluzioni efficaci nell'ambito della sicurezza informatica. Tali competenze vanno dall'ambito delle reti di calcolatori, a quello dei sistemi operativi, delle architetture di elaborazione, della programmazione.

- Fase 2 - La seconda fase si specializza nel contesto della sicurezza informatica, declinata nelle sue accezioni di *software security, computer security* e *network security.* In questa fase si darà particolare risalto alle tecniche cosiddette di "ethical hacking" e ci si concentrerà sulle architetture di rete in cloud e sugli ecosistemi del tipo IoT (Internet of Things).
- Fase 3 - La terza fase ha come obiettivo quello di sviluppare la capacità di applicazione delle competenze acquisite nei primi due periodi di formazione, concentrandosi su di un "project-work" di gruppo relativo a temi di interesse aziendale.

Per il profilo "Senior Cybersecurity Specialist", il percorso didattico completo si articolerà in tre fasi, come di seguito specificato:

- Fase 1 - La prima fase ha come obiettivo l'acquisizione di competenze avanzate nell'ambito della sicurezza informatica, con particolare riferimento alle tecniche di attacco e di difesa, nonché allo studio delle metodologie formali per lo studio della *safety* e della *security* di architetture complesse basate sul cloud.
- Fase 2 - La seconda fase si specializza nello studio dell'impiego di grosse moli di dati nell'ambito della cybersecurity, sia ai fini del miglioramento delle capacità di rilevazione di minacce, sia con lo scopo di fornire informazioni utili al miglioramento della postura di sicurezza delle moderne architetture di rete.
- Fase 3 - La terza fase ha come obiettivo quello di sviluppare la capacità di applicazione delle competenze acquisite nei primi due periodi di formazione, concentrandosi su di un "project-work" di gruppo relativo a temi di interesse aziendale.

Per entrambi i profili, l'ammissione alla terza fase della HackAdemy sarà subordinata al superamento di una valutazione intermedia.

La frequenza alle attività del corso è obbligatoria almeno per il 75% del totale dell'impegno orario previsto per ciascuno dei tre periodi. La mancata frequenza per un numero di ore superiore al 25% del monte ore complessivo dedicato agli interventi formativi per i quali sarà prevista la presenza, determinerà l'esclusione automatica dal corso. In caso di mancata frequenza, di scarso profitto o di comportamenti comunque censurabili, il partecipante potrà essere escluso dal proseguimento delle attività della HackAdemy.

La partecipazione alla HackAdemy è gratuita in quanto, per l'anno accademico 2024/2025, i costi per la sua realizzazione sono completamente a carico degli enti organizzatori. Inoltre, ai primi due

classificati in ciascuna delle graduatorie di ammissione (profilo "Junior" e profilo "Senior"), sarà corrisposta una borsa di studio dell'importo mensile lordo pari a 500,00 (cinquecento) euro per tutta la durata del percorso. In caso di recesso, e quindi termine anticipato del corso, lo studente beneficiario sarà tenuto a restituire l'intero importo percepito.

Articolo 4

Requisiti di ammissione

Possono partecipare alla selezione, secondo le modalità indicate al successivo articolo 5, i cittadini italiani, i cittadini dell'Unione Europea ovunque soggiornanti, e i cittadini non dell'Unione Europea in possesso di regolare permesso di soggiorno, che alla data di scadenza del presente bando siano in possesso:

- per il Profilo "Junior Cybersecurity Specialist" del seguente requisito:
    - **Diploma di scuola secondaria superiore** o titolo equipollente conseguito in Italia o all'estero. Ai soli fini della procedura in oggetto, la commissione si riserverà di valutare l'equipollenza del titolo.
- per il Profilo "Senior Cybersecurity Specialist" di uno dei seguenti requisiti:
    - **Laurea Triennale** in una disciplina STEM (Science, Technology, Engineering, Mathematics), conseguita ai sensi del D.M. 270/04, ovvero qualora non conseguito in Italia, titolo universitario equipollente o conseguito presso Istituti di formazione riconosciuti a livello europeo. Ai soli fini della procedura in oggetto, la commissione di selezione si riserverà di valutare l'equipollenza del titolo.
    - **Laurea Magistrale** in una disciplina STEM (Science, Technology, Engineering, Mathematics), conseguita ai sensi del D.M. 270/04, ovvero qualora non conseguito in Italia, titolo universitario equipollente o conseguito presso Istituti di formazione riconosciuti a livello europeo. Ai soli fini della procedura in oggetto, la commissione di selezione si riserverà di valutare l'equipollenza del titolo.
    - **Laurea Specialistica** in una disciplina STEM (Science, Technology, Engineering, Mathematics), conseguita ai sensi del D.M. 509/99, ovvero qualora non conseguito in Italia, titolo universitario equipollente o conseguito presso Istituti di formazione riconosciuti a livello europeo. Ai soli fini della procedura in oggetto, la commissione di selezione si riserverà di valutare l'equipollenza del titolo.

- **Laurea Vecchio Ordinamento** (ante D.M. 509/99) in una disciplina STEM (Science, Technology, Engineering, Mathematics), ovvero qualora non conseguito in Italia, titolo universitario equipollente o conseguito presso Istituti di formazione riconosciuti a livello europeo. Ai soli fini della procedura in oggetto, la commissione di selezione si riserverà di valutare l'equipollenza del titolo.

Nella fase di selezione sarà garantito il principio della pari opportunità.

I requisiti prescritti devono essere posseduti entro il termine stabilito nel presente avviso. I candidati sono ammessi alla selezione con riserva e l'Università può disporre, con provvedimento motivato, in qualunque fase della procedura selettiva, nonché alla conclusione della stessa, l'esclusione di un candidato per difetto dei requisiti prescritti.

Articolo 5

Modalità di presentazione della domanda di ammissione

La domanda di ammissione al presente avviso di selezione dovrà essere presentata **esclusivamente in modalità on-line attraverso il portale web https://www.cyberhackademy.unina.it, a partire dalla data di pubblicazione del presente avviso ed irrevocabilmente, pena esclusione dalla procedura di selezione, entro e non oltre le ore 14:00 (GMT+1) del giorno 23/12/2024.**

Per potersi iscrivere alla selezione ogni candidato dovrà necessariamente essere dotato di un indirizzo di posta elettronica e collegarsi al sito web **https://www.cyberhackademy.unina.it.**

L'inosservanza di una delle prescrizioni sopra indicate comporterà la non ammissione alla prova di selezione e, comunque, l'esclusione dalla procedura stessa.

I candidati diversamente abili che hanno necessità di ausilio per lo svolgimento delle prove dovranno selezionare la voce "*si*" nel campo "Richiedi l'uso di strumenti compensativi per DSA?" e dovranno inoltrare, ***per posta elettronica all'indirizzo cyberhackademy@unina.it*** – pena la mancata applicazione del beneficio richiesto - **entro e non oltre le ore 14:00 *(GMT+1)* del giorno 16/12/2024**, apposita istanza nella quale siano indicati gli ausili necessari in relazione alla propria disabilità.

Ai candidati affetti da disturbi specifici dell'apprendimento (DSA – dislessia, discalculia, disgrafia e disortografia), la cui diagnosi sia certificata (il relativo certificato dovrà essere inviato all'indirizzo mail ***cyberhackademy@unina.it*** entro il termine sopra indicato) è concesso l'eventuale uso di strumenti

compensativi. Tali candidati dovranno, pertanto, inoltrare (con le modalità ed entro i termini sopra indicati) un'istanza nella quale verranno indicati con chiarezza gli strumenti compensativi richiesti, così come risultanti dal profilo funzionale contenuto nella diagnosi. Non saranno ritenute idonee ai fini dell'autorizzazione all'uso degli strumenti compensativi, le diagnosi prive del profilo funzionale. All'istanza, pertanto, deve essere allegato il certificato contenente la diagnosi clinica di DSA.

L'Amministrazione valuterà le istanze di ausilio presentate dai candidati disabili o con diagnosi di DSA, con la collaborazione della competente Struttura di Ateneo, il Centro Servizi di Ateneo per l'Inclusione Attiva e Partecipata degli Studenti (S.IN.A.P.S.I.).

L'esito delle valutazioni stesse verrà comunicato agli interessati tramite mail.

Articolo 6

Commissione Giudicatrice per Selezione

La Commissione preposta alla selezione sarà nominata con Decreto del Direttore del CeSMA successivamente al termine di scadenza per la presentazione delle domande di partecipazione. La composizione della citata commissione sarà resa nota mediante Decreto, **pubblicato esclusivamente nell'Albo Ufficiale di Ateneo (presente sul sito www.unina.it) e sul sito web https://www.cyberhackademy.unina.it.**

Articolo 7

Criteri e modalità di svolgimento delle selezioni

La procedura selettiva per l'ammissione al corso *"**Cyber HackAdemy 2024/2025**"* verrà svolta sulla base di una valutazione dei titoli presentati dal candidato nel proprio CV, di una prova scritta (diversa a seconda del profilo per il quale si concorre) e di una successiva prova orale, che si terranno entrambe in presenza.

Il punteggio massimo complessivo, per entrambi i profili, è di **100 punti**, di cui:

- **30** riservati alla valutazione dei titoli,
- **30** riservati alla prova scritta,
- **40** alla prova orale.

La data, il luogo, l'orario e le modalità di svolgimento della prova scritta e del colloquio orale saranno resi noti esclusivamente mediante pubblicazione sul sito web **https://www.cyberhackademy.unina.it**.

Per entrambi i profili, ai fini della valutazione dei titoli posseduti dai candidati, saranno considerati come titoli:

- **Laurea di primo livello (triennale)** o titolo universitario equipollente, conseguito in Italia o all'estero, valutato fino a 5 punti, secondo la attinenza del corso di laurea al tema della HackAdemy;
- **Laurea magistrale** o titolo universitario di secondo livello equipollente, conseguito in Italia o all'estero, valutato fino a 5 punti, secondo la attinenza del corso di laurea al tema della HackAdemy;
- **Dottorato di ricerca** conseguito presso Università italiana o estera, valutato fino a 5 punti, secondo la attinenza del dottorato al tema della HackAdemy;
- **Master di primo o secondo livello**, conseguito presso Università italiana o estera, fino a 5 punti;
- **Pubblicazioni scientifiche** su argomenti attinenti ai temi della HackAdemy, fino a 5 punti;
- **Certificazioni** industriali rilevanti in ambito ICT, fino a 5 punti.

Ai soli fini della procedura in oggetto, la commissione incaricata della selezione si riserverà di valutare l'equipollenza dei titoli di studio posseduti.

Alla prova orale saranno ammessi, per ciascuna graduatoria ("Junior" e "Senior"), esclusivamente i candidati che risulteranno nei primi 30 posti della graduatoria risultante dalla somma dei punteggi conseguiti da ciascun candidato nella valutazione dei titoli e della prova scritta.

I candidati che abbiano presentato regolare domanda di partecipazione, nel termine e con le modalità di cui al precedente articolo 5, devono presentarsi alla prova orale, che si svolgerà in presenza, nel giorno, luogo ed orario resi noti mediante la suddetta pubblicazione, muniti di **valido documento di riconoscimento** (carta d'identità, passaporto).

La prova scritta si terrà in presenza, fatti salvi eventuali rinvii, il giorno **8 gennaio 2025,** secondo un calendario che sarà pubblicato sul sito web **https://www.cyberhackademy.unina.it.**

La prova orale, fatti salvi eventuali rinvii, si svolgerà nei giorni **14 e 15 gennaio 2025**, secondo un calendario che sarà pubblicato sul sito web **https://www.cyberhackademy.unina.it.**

L'inizio delle attività didattiche della HackAdemy è previsto, salvo eventuali rinvii, per il giorno **27 gennaio 2025.**

La prova scritta consisterà in un test a risposta multipla volto a verificare la preparazione dei candidati sui seguenti argomenti:

- Profilo “Junior”:
  - Computer Networks;
  - Computer Programming;
  - Principi fondamentali della sicurezza informatica.
- Profilo “Senior”:
  - Tecniche di hacking in reti IP;
  - Ciclo di sviluppo sicuro del codice;
  - Analisi di grosse moli di dati.

La prova orale sarà volta a valutare la conoscenza della lingua inglese, la motivazione alla partecipazione al corso di formazione, l’attitudine del candidato alle tematiche del progetto formativo, il lavoro di gruppo, il problem setting, il problem solving e le relazioni interpersonali.

Ai sensi dell’art. 3, comma 7, della L. 15 maggio 1997, n. 127, come modificato dall’art. 2 della L. 16 giugno 1998, n.191, se due o più candidati ottengono, a conclusione della procedura di valutazione, pari punteggio, è preferito il candidato più giovane d’età.

Le graduatorie dei vincitori (profilo “Junior” e profilo “Senior”) saranno stilate sommando il punteggio relativo alla valutazione dei titoli, il punteggio relativo alla prova scritta ed il punteggio risultante dalla valutazione della prova orale.

Gli avvisi pubblicati sul sito https://www.cyberhackademy.unina.it avranno valore di notifica ufficiale e non saranno inoltrate comunicazioni personali agli interessati.

I candidati che, per qualsiasi motivo, risultino assenti alla prova scritta o alla prova orale, saranno considerati automaticamente rinunciatari alla procedura di selezione.

Articolo 8

Modalità di accettazione degli ammessi

I candidati dichiarati ammessi nella suddetta graduatoria dovranno formalizzare, ***a pena di decadenza***, la volontà di partecipare all’attività formativa prevista, mediante sottoscrizione di un contratto, entro **tre** (3) giorni dalla pubblicazione della graduatoria, con il quale il candidato ammesso si impegna a rispettare le prescrizioni previste dal presente bando di selezione.

Decorso il termine per l'accettazione, qualora residuassero posti per mancanza di accettazioni o di successive rinunce, si procederà allo scorrimento della graduatoria, secondo l'ordine della stessa. Gli eventuali scorrimenti ed i relativi termini per effettuare le accettazioni saranno resi noti **esclusivamente mediante pubblicazione** sul sito **https://www.cyberhackademy.unina.it.**

Articolo 9

Attestato del percorso formativo

Al termine della HackAdemy, ciascun allievo che abbia frequentato con profitto il corso riceverà un **attestato di partecipazione** rilasciato dall'Università degli Studi di Napoli Federico II e da Accenture.

L'Università degli Studi di Napoli Federico II determinerà, secondo le procedure di Ateneo, il riconoscimento di eventuali crediti agli studenti iscritti ad un Corso di Studi dell'Ateneo e che siano in possesso dell'attestato di partecipazione alla HackAdemy.

Articolo 10

Pubblicità degli atti della selezione

Il presente bando di selezione è reso pubblico mediante pubblicazione sul sito web **https://www.cyberhackademy.unina.it**, nonché sui siti istituzionali degli enti promotori dell'iniziativa.

Tutti gli atti collegati al bando saranno resi pubblici esclusivamente mediante pubblicazione sul sito web **https://www.cyberhackademy.unina.it**.

La pubblicazione sul sito **https://www.cyberhackademy.unina.it** ha valore di notifica ufficiale a tutti gli effetti e non saranno inoltrate comunicazioni personali agli interessati.

Articolo 11

Accesso agli atti, Informativa in materia di dati personali

Ai candidati è garantito l'accesso alla documentazione inerente al procedimento concorsuale, ai sensi della vigente normativa. Tale diritto si eserciterà secondo le modalità stabilite con Regolamento di Ateneo recante norme in materia di procedimento amministrativo e di diritto di accesso ai documenti, emanato con Decreto del Decano n. 2294 del 02/07/2010 e s.m.i.

I dati personali saranno trattati dall'Amministrazione ai sensi del Regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio del 27/04/2016 (RGPD), del Codice in materia di protezione dei dati

personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 (Decreto Legislativo 30/06/2003 n. 196), nonché del Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei Dati Personali emanato con decreto rettorale n. 2088 del 29/05/2019. I dati sopra riportati sono raccolti e trattati ai fini del procedimento per il quale vengono rilasciati e verranno utilizzati esclusivamente per tale scopo e, comunque, nell'ambito delle attività istituzionali dell'Ateneo Federico II. All'interessato competono i diritti di cui agli articoli 15 – 22 del Regolamento UE.

Articolo 12

Disposizioni finali

L'Università degli Studi di Napoli Federico II si riserva di escludere in qualsiasi momento i candidati che partecipano alla prova indetta con il presente avviso per mancata osservanza delle disposizioni ivi impartite o nei termini indicati ovvero per difetto dei requisiti richiesti ai candidati.

Delle esclusioni si darà notizia esclusivamente mediante pubblicazione sull'Albo Ufficiale dell'Università degli Studi di Napoli Federico II (presente sul sito web di Ateneo all'indirizzo https://**www.unina.it**), **nonché tramite pubblicazione sul sito web https://www.cyberhackademy.unina.it.**

L'amministrazione si riserva, a suo insindacabile giudizio, secondo le esigenze di progetto, la facoltà di prorogare, sospendere, modificare, revocare o annullare il presente avviso senza che ciò comporti diritti o pretese di sorta a favore dei candidati.

Il sito web https://www.cyberhackademy.unina.it sarà costantemente aggiornato con l'inserimento di ogni altra informazione che sarà ritenuta utile per gli interessati. Si raccomanda, pertanto, la consultazione del predetto sito.

Per informazioni, scrivere a cyberhackademy@unina.it.

Napoli, 27/11/2024

F.to Il Direttore del CeSMA

prof. ing. Domenico Accardo