Avviso per l'assegnazione di n. 35 borse di studio a copertura totale del costo di iscrizione

Executive Program in Cyber Security Management (EXECSM)

Una nuova generazione di Information Security Manager

II[a] edizione
Anno 2024 / 2025

Con il sostegno del Ministero dell'Università e della Ricerca a valere sui fondi di cui all'art. 14-bis del decreto-legge 6 novembre 2021, n. 152, convertito con modificazioni dalla legge 29 dicembre 2021, n. 233.

Art. 1 - Premesse

L'Università LUM *Giuseppe Degennaro*, in virtù della sua adesione ai "Patti Territoriali per l'Alta Formazione delle Imprese", ai sensi dell'Avviso MUR n. 1290 del 8 agosto 2022, mette a disposizione n. 35 borse di studio a copertura totale della quota di partecipazione all'Executive Program in "Cyber Security Management (EXECSM)", A.A. 2024/2025, con l'obiettivo di sviluppare profili professionali innovativi e altamente specializzati in grado di soddisfare i fabbisogni espressi dal mondo del lavoro regionale pugliese relativamente alla filiera delle Tecnologie ICT (Trasformazione Digitale delle imprese).

Art. 2 - Premesse e obiettivi

La costante evoluzione del panorama delle minacce legate allo sviluppo delle tecnologie digitali, ha evidenziato la necessità di formare nuove figure professionali sempre più specializzate nella gestione della sicurezza delle informazioni.

Ad oggi, se presente, il ruolo di Responsabile della Sicurezza delle Informazioni *(Chief Information Security Officer – CISO – oppure Information Security Manager*) coincide, in oltre metà delle realtà aziendali italiane, con quello di *Chief Information Officer (CIO)* o di IT Manager.

Queste due figure, che dovrebbero lavorare in stretta sinergia, hanno però obiettivi completamente diversi:

- compito del CIO/IT Manager è focalizzarsi su come la tecnologia possa migliorare i modelli di business;
- compito del CISO/Information Security Manager è individuare le strategie di sicurezza adeguate a favorire e aumentare la fiducia dei clienti nei confronti dell'azienda.

La figura dell'Information Security Manager non deve, infatti, essere necessariamente una figura operativa; è anzi estremamente esplicativo, a tal proposito, citare quanto indicato da ENISA, l'Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'Informazione, nel proprio report del 2018: "l'orientamento tecnico della maggior parte degli addetti o esperti di Cyber Security è considerato un ostacolo alla sensibilizzazione del Management".

L'*Information Security Manager* deve quindi coincidere con una risorsa di profilo consulenziale/ manageriale capace di impostare le linee guida delle policy di sicurezza e controllare che queste siano rispettate.

In particolare, il programma executive in Cyber Security Management ha l'obiettivo di fornire ai partecipanti le basi di conoscenza e competenze formative per ruoli professionali quali:

- Information Security Manager
- Consulenti in Information Security
- Auditor e architetti di sicurezza
- Chief Information Security Officer (CISO)
- Chief Compliance/Privacy/Risk Officer

Questi profili professionali specializzati offrono l'opportunità di numerosi sbocchi lavorativi presso, ad esempio, imprese, pubbliche amministrazioni, studi di consulenza e legali, start-up.

I temi affrontati permetteranno ai partecipanti comprendere e gestire le minacce informatiche, in continua evoluzione sia in termini di complessità che di numerosità e di pianificare sistemi di prevenzione dei relativi attacchi.

Art. 3 - Destinatari

I destinatari dell'Executive Program in Cyber Security Management sono:

- candidati interessati a costruire una professionalità spendibile sul mercato del lavoro in ambito cyber security;
- candidati con una breve esperienza nel ruolo che intendano acquisire una specializzazione ulteriore in vista di opportunità di crescita professionale;
- professionisti con background umanistico che vogliano acquisire conoscenze in ambito cyber security;
- dipendenti di aziende e consulenti operanti nello specifico settore ICT, Network etc.

Art. 4 - Durata e modalità di erogazione del percorso formativo

Il percorso formativo, articolato in 5 moduli didattici, sarà erogato in modalità mista (in presenza, presso la sede di Casamassima - Bari dell'Università LUM e on line in modalità sincrona) e avrà la durata di 120 ore, per un totale di 4 mesi.

Le lezioni avranno inizio ad ottobre 2024 e si svolgeranno in formula week end, venerdì (dalle ore 14:00 alle ore 19:00) e sabato (dalle ore 9:00 alle ore 14:00).

La Direzione del percorso formativo si riserva la facoltà di variare la calendarizzazione del programma. Ogni variazione sarà tempestivamente segnalata ai candidati.

La programmazione delle lezioni, sia in presenza che a distanza, è di esclusiva competenza della Direzione e non è lasciata alla discrezione degli studenti che non possono scegliere liberamente tra la partecipazione in presenza o a distanza. La Direzione stabilisce il calendario, gli orari e la modalità di erogazione delle lezioni in base a criteri didattici e organizzativi.

La frequenza è obbligatoria e non potrà essere inferiore all'80% delle ore complessive. Il superamento del numero di assenze consentito comporterà l'esclusione dal percorso formativo e il mancato rilascio dell'attestazione finale prevista.

Art. 5 - Contenuto dell'Executive Program

L'Executive Program in "Cyber Security Management" è articolato nei seguenti moduli formativi:

Modulo 1: Cyber Security e Digital Transformation (15 ore - in presenza)

- Trasformazione Digitale: impatto sulle imprese e PA
- Tecnologie digitali dell'industria 4.0: introduzione e vantaggi
- Ruolo delle tecnologie digitali sui processi di business
- Cybersecurity: una visione generale
- Lo spazio: Surface Web, Deep & Dark web
- Cosa c'è nel Dark web
- Sicurezza fisica e logica
- Cos'è la cybersecurity
- Cosa sono le reti digitali
- IT/OT Security
- Social Engineering, Pishing, DDOS, APT, Brute Force Attacks

Modulo 2: Information Security Management: Governance, Risk e Compliance (30 ore - on line in modalità sincrona)

- Governance e Gestione del Rischio.
- Rischio: analisi, controllo delle minacce, valutazione e gestione.
- Controlli, Conformità e Gestione degli accessi.
- Gestione del ciclo di vita dei controlli di sicurezza, monitoraggio e mantenimento.
- Conformità: GDPR, NIST e gli standard della famiglia ISO27000. Linee guida e Best Practice: CIS e OWASP.
- Tipologie di Audit e gestione delle remediation.
- Introduzione ai concetti di gestione e risposta agli incidenti.
- Gestione della Business Continuity e Piano di Disaster Recovery.
- Security Operation: SIEM, Vulnerability Management, Vulnerability Assessment, Penetration Test e Threat Hunting. Condivisione degli scenari nei diversi ambiti.
- Controllo degli accessi, sicurezza fisica, sicurezza delle reti.
- Protezione degli endpoint e sicurezza delle applicazioni.
- Tecnologie di criptazione, sicurezza degli ambienti virtualizzati e sicurezza del cloud computing.

- Nuove tecnologie: intelligenza artificiale, realtà aumentata, ecc.

Modulo 3: Security Program Management & Operations (30 ore - on line in modalità sincrona)

- Pianificazione strategica. Organizzazione, struttura, obiettivi, stakeholder, aspetti finanziari e piano strategico.
- Progettazione, sviluppo e manutenzione di un programma di sicurezza delle informazioni per la propria organizzazione.
- Gestione degli aspetti finanziari legati alla sicurezza: risorse, definizione delle metriche finanziarie, rinnovo delle tecnologie, ottenimento e gestione del budget.
- Concetti base per la gestione di gare e appalti e servizi gestiti da terzi (TCO, RFI, RFP, SLA, ec…).
- Gestione dei vendor e delle terze parti.

Modulo 4: Tutela delle informazioni strategiche (15 ore - on line in modalità sincrona)

- Principi di sicurezza delle informazioni strategiche.
- Organizzazione (Autorità, organi e uffici, ocs, sps, organi periferici, operatori economici) classifiche e qualifiche.
- Autorizzazioni alla trattazione di informazioni strategiche.
- Principi di sicurezza delle infrastrutture informatiche strategiche.
- Definizioni e contesto normativo.
- Minaccia e rischio informatico.
- Modelli di protezione delle infrastrutture informatiche strategiche.
- La legislazione nazionale in materia di tutela delle informazioni classificate.
- Funzione del security manager.
- Definizioni e principi della sicurezza delle comunicazioni.
- Metodologie di risk analysis dei sistemi di protezione delle comunicazioni e sicurezza crittografica.
- Misure di sicurezza fisica.
- Procedure di sicurezza.
- Applicazioni alle reti di comunicazioni sicure.
- Certificazione di prodotti per la sicurezza (apparati tempest, camere tempest/anecoiche).
- Sicurezza delle comunicazioni (materiali e documenti, autorizzazioni e organizzazione, protezione conservazione e trasporto).

Modulo 5: Prevenzione e Gestione degli Incidenti (30 ore - on line in modalità sincrona)

- Gestione e Risposta agli incidenti.
- Strumenti a supporto.
- Gestione delle comunicazioni.
- Analisi Post-Incident.
- Verifica dei piani di risposta.
- Procedure e gestione della crisi.
- Analisi forense e catena di custodia.
- Affrontare diverse tipologie di incidenti: Malware Incident, Email Security Incident, Network Security Incident, Web Application Security Incident, Cloud Security Incident, Minacce interne.

- Cyber Threat Intelligence.

Per i moduli 2, 3 e 4 i partecipanti saranno ripartiti in gruppi di lavoro per lo svolgimento di attività e Project Work.

Art. 6 - Costi e borse di studio

La quota di iscrizione all'Executive Program in "Cyber Security Management" è di 3.500.00 €.

Sono disponibili nr. 35 borse di studio a copertura totale del costo di iscrizione.

La borsa di studio consiste nella esenzione dal pagamento della quota complessiva di iscrizione al percorso formativo e non copre eventuali spese di viaggio, vitto e alloggio che restano a totale carico del beneficiario.

Art. 7 - Requisiti di ammissione

Possono candidarsi all'assegnazione delle all'assegnazione delle borse di studio di cui al presente Avviso i soggetti in possesso di laurea (almeno triennale) in qualsiasi disciplina.

Art. 8 - Modalità di candidatura

Per partecipare alle procedure di assegnazione delle borse di studio è necessario presentare la candidatura **entro il 20 settembre 2024** compilando il form disponibile al seguente ***LINK***.

Nella domanda on line il candidato dovrà dichiarare, sotto la propria personale responsabilità, ai sensi degli articoli 46 e 47 del D.P.R. n. 445 del 28 dicembre 2000 e consapevole delle sanzioni penali previste dagli artt. 75 e 76 del citato decreto per le ipotesi di falsità in atti e dichiarazioni mendaci:

- le proprie generalità, la data e il luogo di nascita, la cittadinanza, la residenza e il recapito digitale eletto agli effetti della selezione;
- di essere in possesso dei titoli richiesti dall'Avviso di selezione e indicati al precedente articolo;
- la propria situazione lavorativa;
- breve descrizione del proprio profilo con cenno ai propri obiettivi futuri e alle motivazioni a supporto della propria candidatura (max 1.300 battue spazi inclusi).

Ai sensi dell'art. 71 del D.P.R. n. 445 del 28 dicembre 2000, l'Amministrazione universitaria si riserva di verificare la veridicità delle dichiarazioni rilasciate dai partecipanti alla procedura, i quali si intendono consapevoli delle conseguenze sotto il profilo penale, civile e amministrativo delle dichiarazioni false o mendaci, ai sensi degli articoli 75 e 76 del predetto D.P.R., ivi compresa la perdita degli eventuali benefici conseguiti sulla base di dichiarazioni non veritiere.

L'Università può adottare, anche successivamente all'espletamento delle procedure di selezione, provvedimenti di esclusione nei confronti dei candidati che a seguito delle verifiche di cui al precedente punto dovessero risultare privi dei requisiti richiesti.

Art. 9 - Graduatorie

Le candidature, previa verifica dei requisiti, saranno ammesse secondo l'ordine cronologico di presentazione fino ad esaurimento delle borse di studio a disposizione. Per la formazione della graduatoria, verranno applicati i seguenti criteri di priorità riferiti alla residenza:

1. residenza in Puglia; *a seguire (in ordine di precedenza)*
2. residenza nelle altre regioni del Mezzogiorno; (*e, successivamente)*
3. residenza nelle altre regioni italiane;

Art. 10 - Iscrizione all'Executive Program

Successivamente alla pubblicazione delle graduatorie, i candidati, risultati in posizione utile ai fini dell'assegnazione della borsa di studio, riceveranno una comunicazione dall'Università mediante avviso trasmesso all'indirizzo di posta elettronica ordinaria indicato nella domanda di candidatura.

I predetti candidati, entro i termini indicati nella comunicazione di cui al capoverso precedente, dovranno formalizzare l'accettazione della borsa di studio secondo le modalità indicate nell'anzidetta comunicazione alla quale dovrà essere allegata la seguente documentazione:

- copia di un documento di identità
- certificato di laurea

La mancata accettazione nei termini indicati equivale ad espressa rinuncia. A seguito di eventuali rinunce si procederà con lo scorrimento della graduatoria.

I candidati che avranno formalizzato l'accettazione della borsa di studio, saranno iscritti al percorso formativo senza dover effettuare il pagamento della quota di iscrizione di iscrizione.

Art. 11 - Ritiro e mancato conseguimento dell'attestato

Salvo che per documentati motivi di salute del beneficiario della borsa di studio, ostativi alla prosecuzione dell'Executive Program e certificati da una struttura sanitaria pubblica, nel caso di ritiro dalla frequenza del percorso formativo intervenuto successivamente all'inizio delle lezioni o superamento del monte ore previsto per il conseguimento dell'attestato, verrà disposta la revoca della borsa di studio, e conseguentemente, il beneficiario sarà tenuto a pagare l'intero importo della quota di partecipazione all'Executive Program.

Art. 12 - Comunicazioni

Tutte le comunicazioni inerenti il presente Avviso verranno effettuate all'indirizzo di posta elettronica indicato nella richiesta di partecipazione.

L'amministrazione universitaria non assume alcuna responsabilità in caso di dispersione di comunicazioni, dipendente da inesatte indicazioni dei recapiti indicati nella domanda da parte del candidato oppure da mancata o tardiva comunicazione del cambiamento degli stessi, nonché da eventuali disguidi imputabili a fatto di terzo, a caso fortuito o forza maggiore.

Art. 13 - Note e avvertenze

Eventuali variazioni e integrazioni del contenuto del presente Avviso di selezione saranno rese note mediante pubblicazione sul sito web della School of Management dell'Università LUM nella pagina dedicata al percorso formativo.

È, pertanto, onere del candidato verificare tutte comunicazioni riguardanti il presente Avviso pubblicati con le modalità indicate al precedente comma.

La partecipazione al percorso formativo non comporta in alcun modo l'ottenimento delle certificazioni in ambito Cyber Security e non dà diritto a condizioni economiche o procedurali agevolate per il conseguimento delle stesse presso gli Enti certificatori. I requisiti per poter sostenere l'esame di certificazione, le modalità di esame e i costi sono stabiliti dagli Enti certificatori e sono a carico del singolo studente che rimane, pertanto, libero di decidere tempi e modalità di conseguimento della certificazione.

Art. 14 - Privacy

I dati personali forniti dai candidati saranno utilizzati per le finalità connesse e strumentali alle procedure di selezione ivi comprese l'eventuale successivo espletamento delle procedure di immatricolazione e carriera come specificatamente indicate nell'informativa accessibile al seguente ***LINK***.

I dati saranno trattati dall'Università LUM Giuseppe Degennaro - S.S. 100 km 18, 70100 Casamassima (Ba) - in qualità di titolare del trattamento, in conformità al Regolamento (UE) n. 2016/679 e al D.Lgs 101/2018.

Art. 15 - Informazioni

La presentazione della candidatura ai sensi del presente Avviso comporta l'accettazione incondizionata delle norme contenute nello stesso.

Per eventuali informazioni gli aspiranti potranno rivolgersi ai seguenti recapiti: tel. 080 6978224 – schoolofmanagement@lum.it

Casamassima (Ba), 18 luglio 2024