CAMERA DI COMMERCIO
SASSARI

Avviso pubblico per la partecipazione al corso di specializzazione in materia di "Sicurezza informatica" (60 Ore) erogato dall'Accademia Digitale - CUP: C84E20010170002

Premessa

L'Ente Camerale è firmatario dell'Accordo di Programma Quadro relativo al Progetto di Sviluppo Territoriale (PST) - PT-CRP 32 "Rete Metropolitana del Nord Sardegna, un territorio di città" (di seguito "Progetto Rete Metropolitana") - tra la Regione Autonoma della Sardegna, la Rete Metropolitana del Nord Sardegna, il Parco di Porto Conte, la Camera di Commercio di Sassari - reso esecutivo con decreto del Presidente della Regione Autonoma della Sardegna n. 124 del 21.12.2018.

La Camera di Commercio di Sassari nell'ambito dell'accordo in discorso ha realizzato specifici interventi ricompresi nell'Azione 32.06 "Competitività delle imprese" tra cui la sub-azione 32.06.1 denominata "Realizzazione del Centro di competenza digitale".

Tale sub-azione ha previsto la creazione dell'SSI-Lab, un centro di competenza nella formula di Innovation Lab, specializzato su tematiche digitali che possa lavorare in rete con centri di rango superiore (hub) e con gli altri attori del territorio regionale nell'ambito di una più ampia rete di I-LAB realizzata ad opera dell'Agenzia Sardegna Ricerche.

Gli I-LAB sono "contesti aperti di progettazione, sperimentazione e validazione di nuovi prodotti e servizi", in cui tutti i soggetti interessati (utenti, possibili fruitori o erogatori) possono interagire e sperimentare tali prodotti e servizi.

Presso l'SSI-Lab è attiva l'Accademia Digitale che attraverso formazione e orientamento intende accompagnare studenti, NEET, imprenditori e liberi professionisti nella crescita e consolidamento di competenze specifiche e professionalizzanti sempre più richieste.
Il progetto nasce dall'esperienza dell'I-Lab che, tramite le attività di orientamento e informazione – con percorsi seminariali e laboratoriali – ha consentito ai partecipanti di avvicinarsi al digitale e sperimentare con mano le tecnologie che sono alla base della transizione digitale ed ecologica.

In questo quadro si inserisce il corso di specializzazione in materia di "*Sicurezza Informatica*" che consentirà ai partecipanti di avere una preparazione tecnica e pratica per lavorare nell'ambito della cyber security.

Il percorso, in quanto sperimentale, prevede un'attività di monitoraggio da parte della Camera di commercio di Sassari mediante verifiche sul gradimento e valutazione della qualità ed efficacia del corso e delle attività svolte. Azioni necessarie al fine di ricevere una restituzione dai partecipanti per valutare l'impatto dell'iniziativa e l'eventuale prosecuzione dei servizi dell'Accademia Digitale.

Il presente avviso regola le modalità di selezione dei candidati che avranno l'opportunità di frequentare gratuitamente il corso.

Art. 1 - Obiettivo del corso

L'obiettivo del corso di 60 ore è far acquisire ai partecipanti nuove competenze spendibili nel mondo del lavoro nell'ambito della Sicurezza Informatica.

Il corso, di taglio tecnico, offre ai partecipanti un'esperienza formativa teorica e pratica sulle tematiche della sicurezza informatica.

Dopo una panoramica sui principali ruoli del responsabile della sicurezza informatica si approfondiranno i temi della Business continuity e disaster recovery insieme alla legislazione e alla normativa in materia di cybersecurity e privacy.

I partecipanti verranno coinvolti in esercitazioni pratiche per la costruzione di una strategia di difesa cyber, sulle metodologie e strumenti per la gestione degli incidenti informatici (incident response planning).

Si approfondiranno inoltre le metodologie e gli strumenti per il monitoraggio, la rilevazione e la risposta agli attacchi informatici insieme ai relativi framework di riferimento.

I partecipanti acquisiranno competenze sulle tecniche di analisi forense e completeranno il corso con 20 ore dedicate ad esercitazioni hands-on su ambienti di penetration testing e allo sviluppo di un project work finale sulla valutazione della sicurezza di un sistema.

Il corso è stato progettato in collaborazione con Pluribus One Srl.

Art. 2 - Destinatari del corso e requisiti minimi per la candidatura

Il corso tecnico è rivolto ad un numero di 15 persone fisiche ed è pensato per soddisfare l'esigenza formativa di coloro che abbiano maturato esperienza nel settore ICT sui temi della sicurezza informatica.

Coloro che intendono candidarsi alla selezione devono essere in possesso dei seguenti requisiti minimi:

A. Residenza/domicilio in Sardegna;
B. avere cittadinanza italiana o di altro Stato membro dell'Unione Europea con un'adeguata conoscenza della lingua italiana. (Possono accedere alla selezione, secondo quanto disposto dall'art. 38 del D. Lgs. n. 165/2001 come modificato ed integrato dall'art. 7 della Legge n. 97/2013, i cittadini di uno degli Stati membri dell'Unione europea o loro familiari non aventi la cittadinanza di uno Stato membro che siano titolari del diritto di soggiorno o del diritto di soggiorno permanente, nonché i cittadini di Paesi terzi che siano titolari del permesso di soggiorno UE per soggiornanti di lungo periodo o che siano titolari dello status di rifugiato ovvero dello status di protezione sussidiaria);
C. aver conseguito Diploma di Maturità o Diploma di Laurea presso le Università italiane o titolo di studio all'estero riconosciuto equipollente in base ad accordi internazionali o norme di legge;
D. godere dei diritti civili e politici; anche negli Stati di appartenenza o provenienza, secondo le vigenti disposizioni di legge;
E. non aver riportato condanne penali e non avere procedimenti penali in corso.

Considerate le tematiche trattate, al fine di partecipare attivamente al corso, sono necessarie le seguenti competenze tecniche propedeutiche:

- Avere una conoscenza degli elementi di base della sicurezza informatica;
- Avere una conoscenza base della lingua inglese al fine di comprendere e apprendere correttamente la terminologia tecnica.

Costituirà titolo preferenziale l'aver conseguito il diploma di Liceo Scientifico o Istituto Tecnico Informatico, Laurea Triennale e/o Laurea Magistrale in materie scientifiche.

Gli eventuali ulteriori titoli post Diploma e Laurea saranno valutati in sede di selezione tramite il CV presentato.

Art. 3 - Articolazione del corso (60 ore)

Lo svolgimento del programma del corso prevede un approccio teorico-pratico che si articola in lezioni frontali svolte sia in presenza che online.
Le lezioni saranno registrate e messe a disposizione dei partecipanti attraverso la piattaforma e-learning camerale.
Il corso si sviluppa in 60 ore, di cui 40 ore di lezioni frontali e 20 ore dedicate ad esercitazioni e sviluppo di un projectwork finale, finalizzati alla sperimentazione pratica delle nozioni apprese con trainer esperti e aziende, secondo la seguente programmazione di massima:

- **Modulo 1:** Introduzione alla cybersecurity e alle figure professionali nel settore (13 ore)
- **Modulo 2:** Fondamenti di sicurezza informatica e metodologie di penetration testing (11 ore)
- **Modulo 3**: Attacchi social engineering e phishing: (6 ore)
- **Modulo 4**: Analisi e risposta agli incidenti di sicurezza (10 ore)
- **Modulo 5:** Laboratori pratici e project work (20 ore)

Articolazione di massima del corso per moduli didattici:

Modulo	Titolo	Argomenti trattati	Metodologia	Modalità	Ore
1	**Introduzione alla Cybersecurity e alle figure professionali nel settore**	• Panoramica sui principali ruoli di un responsabile della sicurezza informatica; • Business Continuity & Disaster Recovery – Come rendere le organizzazioni resilienti con ISO 31000 (Risk Management), 22301 (Business Continuity) e 27001 (Cyber Security); • Cos'è il Crisis Management e a cosa serve(Processo di crisis management e tipologie di rischi aziendali - ISO 22361 (Crisis Management Guidelines); • Legislazione in materia di cybersecurity e privacy (es. GDPR, NIS2, DORA, CYBER RESILIENCE ACT),profili di responsabilita, implicazioni connesse all'uso dell'AI; • Costruzione di una strategia di Difesa Cyber;	Teorico/ Pratico	In presenza /Online	13

		• Normative e standard di sicurezza informatica (es. NIST); Framework pratici per la gestione del rischio (e.g. CIS RAM).			
2	**Fondamenti di sicurezza informatica e metodologie di penetration testing**	• MITRE ATT&CK MATRIX for ENTERPRISE - Descrizione di una attack kill-chain; • Panoramica delle soluzioni per il monitoraggio e la protezione di una infrastruttura IT (FW, VPN, IDS/IPS, WAF, SOAR, SIEM, NDR, EDR, VULNERABILITY SCANNERS) • Metodologia di pentesting: Reconnaissance, scanning, gaining access, maintaining access, reporting; • Tecniche di enumerazione e mappatura di sistemi e reti; • Vulnerability Management (Vulnerability Identification, Scoring, CVE, Prioritization); • Vulnerabilità e tecniche di attacco a applicazioni web (es. OWASP Top 10 Applications, OWASP Top 10 API, OWASP Top 10 LLM); • Strumenti e framework per il pentesting (es. Kali Linux, Metasploit, Burp Suite); • Exploitation di vulnerabilità note.	Teorico/ Pratico	In presenza /Online	11
3	**Attacchi social engineering e phishing**	• Valori mancanti, valori anomali, variabili categoriche; • Ricerca a griglia e convalida incrociata; • Riduzione dimensionale; • Un esercizio avanzato completo (con XGBoost o simile); • Machine Learning Explainability; • Costruire un'app web per utilizzare il modello addestrato con Streamlit o Gradio.	Teorico/ Pratico	In presenza /Online	6
4	**Analisi e risposta agli incidenti di sicurezza**	• Incident response planning e procedure di gestione degli incidenti; • Strumenti per il monitoraggio, la rilevazione e la risposta agli attacchi; • Tecniche di analisi forense digitale (analisi forense di un attacco malware).	Teorico/ Pratico	In presenza /Online	10
5	**Laboratori pratici e project work**	• Esercitazioni hands-on su ambienti di penetration testing (e.g. Juice shop); • Sviluppo di un project work finale sulla valutazione della sicurezza di un sistema.	Pratico	In presenza /Online	20

La Camera di commercio si riserva, in caso di necessità e accordi con Pluribus One Srl, il fornitore individuato per la realizzazione del corso, di aggiornare il programma, la suddivisione dei moduli e delle ore e relativa modalità di erogazione.

Art. 4 - Calendario del corso e patto formativo

Il corso si svolgerà indicativamente nel periodo tra ottobre e novembre 2024. Il calendario definitivo sarà comunicato successivamente ai soli candidati ammessi.

I partecipanti dovranno garantire la frequenza ad almeno il **75%** del monte ore complessivo di 60 ore (pari a 45 ore) e la puntualità, limitando assenze e i ritardi solo alle situazioni di effettiva necessità.
In caso di collegamenti online, la telecamera dovrà essere accesa. L'accesso alla piattaforma e-learning e alle registrazioni sarà consentito esclusivamente ai partecipanti che hanno seguito le lezioni secondo le modalità e indicazioni previste dagli organizzatori.
Le presenze saranno rilevate dalla segreteria organizzativa, al fine di monitorare la partecipazione attiva degli ammessi al corso.

Durante il percorso sono previste delle verifiche intermedie e/o finali per la valutazione delle competenze acquisite.

Al fine di monitorare la qualità e l'efficacia dell'iniziativa e dei servizi erogati dall'Accademia Digitale, ai partecipanti saranno somministrati durante il percorso appositi questionari.

Art. 5 - Modalità di candidatura

Gli interessati dovranno inviare la domanda di partecipazione, debitamente compilata e sottoscritta in originale (con copia del documento d'identità) o provvista di firma digitale.

La domanda di partecipazione dovrà pervenire via PEC al seguente indirizzo: cciaa@ss.legalmail.camcom.it **entro il 16 settembre 2024.** Nell'oggetto della comunicazione dovrà essere riportata la dicitura:

Candidatura corso "Sicurezza Informatica" 60 ore – "proprio nome e cognome".

Al modulo di domanda di partecipazione, pena l'esclusione, dovranno essere allegati i seguenti documenti:

- **CV (massimo quattro pagine)**
- **Lettera motivazionale**
- **In caso di firma autografa, copia di un documento di identità in corso di validità**

Non saranno prese in considerazione le candidature pervenute oltre il termine di scadenza indicato, non sottoscritte, non conformi o prive del modulo di domanda allegato al presente avviso e/o degli allegati richiesti.

La lettera motivazionale dovrà essere redatta in lingua italiana, in formato .pdf di lunghezza massima di non più di due pagine e secondo la seguente traccia:

- **Introduzione:** breve descrizione di se stessi, dei propri interessi e aspirazioni;
- **Esperienze di studio e lavoro:** sintesi del proprio background formativo e delle eventuali principali esperienze lavorative, dando evidenza delle competenze tecniche propedeutiche necessarie per la frequentazione delle lezioni del corso;

- **Obiettivi e risultati attesi:** descrizione degli obiettivi personali e professionali che si intende raggiungere con la frequentazione del corso e dei risultati attesi.

Art. 6 - Criteri di selezione

La selezione dei partecipanti al corso teorico-pratico sarà effettuata da esperti del gruppo di lavoro del fornitore Pluribus One Srl ed eventualmente integrata da personale interno o collaboratori della Camera di Commercio di Sassari.

La selezione dei candidati si baserà sulla valutazione del CV e della lettera motivazionale. A ciascuna prova sarà attribuito un punteggio, per un totale massimo di **30 punti.**

La Camera di Commercio di Sassari in accordo con il fornitore, ove ritenuto necessario, si riserva di svolgere anche un colloquio con i candidati.

CRITERIO	DESCRIZIONE	PUNTI
CV	• coerenza del percorso formativo e/o lavorativo rispetto ai contenuti e l'obiettivo del corso; • valutazione del profilo ed eventuali titoli preferenziali previsti dall'avviso (Art.2 Destinatari del corso);	20
Lettera motivazionale	• coerenza delle competenze tecniche propedeutiche necessarie per partecipare al corso; • capacità espressive e argomentative, originalità e congruenza dei contenuti; • ragioni e aspettative sulla partecipazione al corso.	10

A tutte le dichiarazioni rese nella domanda di partecipazione, nonché negli eventuali allegati alla stessa, si riconosce valore di autocertificazione ai sensi e per gli effetti del DPR n. 445/2000 s.m.i..

La Camera di Commercio di Sassari si riserva, in ogni caso, di verificare - anche a campione e in ogni fase della procedura - la veridicità delle dichiarazioni rese e attestate dai candidati al momento della presentazione della domanda nonché di tutte le dichiarazioni presenti negli eventuali allegati.

Art. 7 - Graduatoria e ammissione

Al termine della selezione si procederà alla definizione di una graduatoria finale stilata sulla base dei criteri di selezione e punteggi di cui alla tabella precedente.
A parità di punteggio, precedono in graduatoria i candidati più giovani di età. Nel caso di rinuncia di un candidato si scorrerà la graduatoria finale.

Ai soli primi 15 candidati col maggior punteggio di cui alla graduatoria finale verrà notificata l'ammissione alla frequenza del corso mediante PEC.

La graduatoria finale sarà pubblicata anche sul sito ufficiale della Camera di commercio di Sassari https://www.ss.camcom.it/.
La graduatoria pubblicata sul sito ha valore di notifica per i candidati idonei (ammessi e non ammessi). Sarà, quindi, responsabilità dei richiedenti prendere visione dei risultati della selezione e verificarne l'esito.
La Camera di commercio di Sassari si riserva di posticipare l'avvio del corso nel caso in cui non si raggiunga il numero minimo di 10 candidati ammessi.

Art. 8 - Trattamento dei dati

I dati personali di cui L'Ente promotore o loro incaricati entrano in possesso a seguito dell'applicazione e gestione del presente avviso verranno trattati nel rispetto della vigente normativa, secondo le disposizioni specifiche approvate dalla Camera di commercio di Sassari. A seguito di espresso consenso da parte del beneficiario, tali dati potranno essere inseriti nei sistemi di comunicazione dell'Ente.

I dati personali trattati potranno essere comunicati:
a) al competente personale della Camera di Commercio di Sassari;
b) ai soggetti autorizzati al trattamento ex art. 28 del GDPR;
c) alle aziende fornitrici di servizi relativi ai siti web istituzionali del Titolare e di casella di posta elettronica ordinaria e certificata, di assistenza tecnica e manutenzione hardware e/o software;
d) agli organi di controllo comunitari e nazionali in relazione al finanziamento ricevuto;
e) all'Autorità Giudiziaria, amministrativa o ad altro soggetto pubblico legittimato a richiederli nei casi previsti dalla legge.
f) al fornitore Pluribus One Srl, incaricato dell'erogazione del corso, per le attività di sua competenza.

Art. 9 - Struttura responsabile

Ai sensi della legge 241/90 e ss.mm. la struttura amministrativa responsabile dell'esecuzione del presente avviso è il Servizio Promozione Economica e Statistica della Camera di commercio di Sassari.
Il presente avviso è disponibile sul sito camerale (https://ss.camcom.it/) nella sezione "Accademia Digitale – Bandi"

Art. 10 - Informazioni aggiuntive

Per ulteriori informazioni in merito alla selezione e al corso, è possibile inviare un'e-mail all'indirizzo di posta elettronica ilab@ss.camcom.it specificando nell'oggetto: **Richiesta informazioni corso di specializzazione in materia di "Sicurezza Informatica".**

Art. 11 – Allegati

- Allegato 1 – Modulo di Domanda di partecipazione
- Informativa Privacy sul trattamento dei dati personali