STANDARD MINIMO DI PERCORSO FORMATIVO

QUALIFICAZIONE DI TECNICO DELLA SICUREZZA INFORMATICA

DETERMINAZIONE DIRIGENZIALE n. 61/DPG025 (19-04-2023)

1. RAPPORTO FRA UNITÀ DI COMPETENZA E UNITÀ DI RISULTATI DI APPRENDIMENTO

Unità di Competenza	Unità di Risultati di Apprendimento
---	Inquadramento della professione
---	Basi di ICT
---	Fondamenti di information security e cybersecurity
---	Inglese tecnico per l'informatica
---	Sicurezza sui luoghi di lavoro
Supportare l’analisi di vulnerabilità, rischi e conformità ai requisiti di sicurezza dei sistemi digitale	Supportare l’analisi di vulnerabilità, rischi e conformità
	Comunicare i rischi ed i comportamenti corretti
Supportare l’implementazione di soluzioni per la sicurezza dei sistemi hardware e software	Supportare l’implementazione di soluzioni per la sicurezza dei sistemi hardware e software
Monitorare i sistemi hardware e software e supportare il loro ripristino in caso di problemi di integrità e sicurezza	Monitorare i sistemi hardware e software e supportare il loro ripristino in caso di problemi di integrità e sicurezza

2. LIVELLO EQF DELLA QUALIFICAZIONE IN USCITA: 5

3. REQUISITI OBBLIGATORI DI ACCESSO AL PERCORSO

- Diploma di scuola secondaria superiore di secondo grado

- Possesso di competenza digitale equivalente ad ECDL Full Standard, accertata tramite presentazione di idonea attestazione o dimostrata presenza dei contenuti nel programma scolastico o, in difetto, superamento di apposito test a cura del soggetto attuatore

- Per i cittadini stranieri conoscenza della lingua italiana almeno al livello B1 del Quadro Comune Europeo di Riferimento per le Lingue, restando obbligatorio lo svolgimento delle specifiche prove valutative in sede di selezione, ove il candidato già non disponga di attestazione di valore equivalente.

- I cittadini extracomunitari devono disporre di regolare permesso di soggiorno valido per l'intera durata del percorso o dimostrazione della attesa di rinnovo, documentata dall'avvenuta presentazione della domanda di rinnovo del titolo di soggiorno

4. ARTICOLAZIONE, PROPEDEUTICITÀ E DURATE MINIME

O.	Articolazione dell'Unità di competenza/Contenuti	Unità di Risultati di Apprendimento	Durata minima	di cui in FAD	Crediti Formativi
1	**Conoscenze** • Orientamento al ruolo • Elementi di legislazione del lavoro e dell'impresa • Aspetti contrattualistici, fiscali e previdenziali	Inquadramento della professione	5	0	Non ammesso il riconoscimento di credito formativo di frequenza
2	**Conoscenze** • Basi di ICT: architetture ed operatività dei sistemi informatici	Basi di ICT	15	10	Ammesso il riconoscimento di credito formativo di frequenza esclusivamente sulla base della valutazione di apprendimenti formali
3	**Conoscenze** • Principi di information security e cybersecurity • Framework normativo nazionale ed europeo in materia cybersecurity, information security e privacy • Standard e linee guida in materia di Information Technology, Operation Technology e protezione dei dati personali	Fondamenti di information security e cybersecurity	25	10	Ammesso il riconoscimento di credito formativo di frequenza esclusivamente sulla base della valutazione di apprendimenti formali
4	**Conoscenze**	Supportare l'analisi di vulnerabilità, rischi e	30	10	Ammesso il

	• Rischi relativi all'innovazione tecnologica delle ICT (intelligenza artificiale, Edge computing, applicazioni IoT, Blockchain, ...) • Standard di riferimento per auditing, assessment, risk assessment e risk management applicati a sistemi digitali • Metodi e strumenti di Vulnerability Assessment e Penetration Test • Fondamenti di processi ed organizzazione aziendale. Potenziali impatti della vulnerabilità dei sistemi informativi sulla continuità del business **Abilità** • Comprendere la natura dei rischi legata all'innovazione tecnologica delle ICT • Raccogliere e analizzare gli standard e le linee guida in materia di ITC • Verificare la conformità del sistema informativo alle normative vigenti in materia di privacy e sicurezza informatica • Supportare l'identificazione di minacce e vulnerabilità applicando metodi e strumenti di Vulnerability Assessment e Penetration Test • Supportare le attività di audit ed assessment • Applicare modelli coerenti di analisi del rischio • Supportare l'analisi di processi di business, contromisure tecniche ed organizzative di natura cybersecurity a supporto • Supportare le attività di risk reporting e definizione dei piani di trattamento del rischio	conformità			riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
5	**Conoscenze** • Comportamenti umani e cybersecurity **Abilità** • Comprendere, comunicare ed applicare requisiti legali e di business con impatto sulla cybersecurity • Comprendere e comunicare i rischi legati al fattore umano in ambito cybersecurity	Comunicare i rischi ed i comportamenti corretti	15	10	Ammesso il riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
6	**Conoscenze**	Supportare l'implementazione di soluzioni	60	20	Ammesso il

	• Tipologie e caratteristiche degli attacchi al sistema informativo a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente • Caratteristiche e funzionalità dei firewall • Caratteristiche e funzionalità dei programmi antivirus • Caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da client a server • Metodi e tecniche di configurazione del sistema di protezione e del firewall • Modalità di autorizzazione e controllo del traffico fra reti e tipologie di tentativi di violazione delle politiche di sicurezza • Sistemi di gestione dell'identità (IMS) ed autorizzazione degli accessi al sistema informativo ed alle reti • Tipologie di programmi di crittografia e cifratura **Abilità** • Supportare l'applicazione di modelli di gestione del rischio nei principali framework di riferimento • Utilizzare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema informativo e delle comunicazioni con l'esterno • Creare Zone Demilitarizzate (DMZ), per la protezione della rete informatica e del sistema informativo dai tentativi di attacco e violazione provenienti dall'esterno • Installare e configurare proxy e firewall, per garantire la sicurezza, la riservatezza e l'integrità delle connessioni tra client e server • Installare e configurare software antivirus • Installare e configurare sistemi di autenticazione, autorizzazione e controllo degli accessi • Definire profili di accesso selettivi, individuali o per gruppi omogenei, sulla base delle policies di sicurezza adottate • Definire le credenziali di autenticazione per l'identificazione degli utenti autorizzati ad accedere al sistema informativo • Svolgere il reporting delle attività compiute	per la sicurezza dei sistemi hardware e software			riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
7	**Conoscenze** • Sistemi di gestione dell'identità (IMS) ed autorizzazione degli	Monitorare i sistemi hardware e software e supportare il loro ripristino in caso di problemi di integrità e sicurezza	50	20	Ammesso il riconoscimento di credito formativo di

	accessi al sistema informativo ed alle reti • Sistemi di Security Information Event Management (SIEM) • Documenti di business continuity • Caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection • Tecniche di disaster recovery **Abilità** • Controllare il rispetto delle misure di sicurezza progettate • Testare il funzionamento dei piani di business continuity e disaster recovery • Monitorare ed interpretare log (server, dispositivi di rete, applicazioni, …) • Utilizzare sistemi di Security Information Event Management (SIEM) • Riconoscere e bloccare attacchi, adottando le opportune contromisure • Monitorare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo • Ripristinare integrità, funzionamento e livello di sicurezza in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo • Individuare ed eliminare malware • Gestire le regole di firewall in funzione della situazioni di minaccia e attacco • Eseguire il piano di ripristino in caso di crisi • Svolgere il reporting delle operazioni compiute				frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
8	**Conoscenze** • Inglese tecnico per l'informatica	Inglese tecnico per l'informatica	10	10	Ammesso il riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali

9	**Conoscenze** • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza Fattori specifici di rischio professionale ed ambientale **Abilità** • Agire nel rispetto della normativa sulla salute e la sicurezza nei luoghi di lavoro • Applicare procedure di sicurezza • Utilizzare dispositivi di sicurezza individuale	Sicurezza sui luoghi di lavoro	8	4	Ammesso credito di frequenza con valore a priori riconosciuto a chi ha già svolto con idonea attestazione (conformità settore di riferimento e validità temporale) il corso conforme all'Accordo Stato - Regioni 21/12/2011 - Formazione dei lavoratori ai sensi dell'art. 37 comma 2 del D.lgs. 8 1/2008
DURATA MINIMA TOTALE AL NETTO DEL TIROCINIO CURRICULARE			**218**	**94**	

Nota di propeduticità

Le unità di risultato di apprendimento n. 2, 3 e 4 vanno svolte antecedentemente alle successive

5. TIROCINIO CURRICULARE

Durata minima tirocinio, al netto dell'eventuale riconoscimento di crediti formativi di frequenza: 60 ore

Durata massima tirocinio: 100 ore

6. UNITÀ DI RISULTATI DI APPRENDIMENTO AGGIUNTIVE

A scopo di miglioramento/curvatura della progettazione didattica, nel limite massimo del 15% delle ore totali di formazione, al netto del tirocinio curriculare.

7. METODOLOGIA DIDATTICA

Le unità di risultato di apprendimento vanno realizzate attraverso attività di formazione d'aula specifica e metodologia attiva, utilizzando laboratori pratici con particolare riferimento alle unità di risultato di apprendimento n. 4, 6 e 7

8. VALUTAZIONE DIDATTICA DEGLI APPRENDIMENTI

Obbligo di tracciabile valutazione didattica degli apprendimenti per singola Unità di risultati di apprendimento.

9. GESTIONE DEI CREDITI FORMATIVI

- Crediti di ammissione: riconoscibile attraverso valutazione degli apprendimenti formali, non formali e informali dei richiedenti svolta da operatore abilitato, in applicazione della procedura regionale, con riferimento a risultati di apprendimento EQF 4, fermo restando il possesso di competenza digitale equivalente ad ECDL Full Standard

- Crediti formativi di frequenza: Percentuale massima riconoscibile 30% sulla durata di ore d'aula o laboratorio; 100% su tirocinio curriculare, al netto degli eventuali crediti con valore a priori.

10. REQUISITI PROFESSIONALI E STRUMENTALI

Qualificazione dei formatori, di cui almeno il 50% esperti provenienti dal mondo del lavoro, in possesso di una specifica e documentata esperienza professionale o di insegnamento, almeno triennale, nel settore di riferimento.

STANDARD MINIMO DI ATTREZZATURE: Laboratorio informatico (un pc per allievo), con connessione internet. Strumenti software antivirus e di sopporto all'esercizio delle attività di cui alle conoscenze ed abilità delle unità di risultato di apprendimento n.4, 6 e 7

11. ATTESTAZIONE IN ESITO RILASCIATA DAL SOGGETTO ATTUATORE

Documento di formalizzazione degli apprendimenti, con indicazione del numero di ore di effettiva frequenza. Condizioni di ammissione all'esame finale: frequenza di almeno il 70% delle ore complessive del percorso formativo

12. ATTESTAZIONE IN ESITO AD ESAME PUBBLICO

Certificato di qualificazione professionale rilasciato ai sensi del D.lgs 13/13