STANDARD MINIMO DI PERCORSO FORMATIVO

QUALIFICAZIONE DI MANAGER DELLA SICUREZZA INFORMATICA

DETERMINAZIONE DIRIGENZIALE n. 1255/DPG025 (27-12-2023)

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
---	Principi, standard e framework in ambito cybersecurity
---	Inglese tecnico per l'informatica
---	Inglese tecnico per l'informatica
---	Sicurezza sui luoghi di lavoro
Svolgere analisi di vulnerabilità, rischi e conformità ai requisiti di sicurezza dei sistemi digitale, sulla base dei requisiti di business	Analizzare vulnerabilità, rischi e conformità ai requisiti di sicurezza dei sistemi digitale, sulla base dei requisiti di business
Definire ed implementare strategia, policy e misure per la sicurezza informatica	Definire strategia e policy per la sicurezza informatica
	Implementare le misure di sicurezza informatica
	Comunicare i rischi ed i comportamenti corretti
Monitorare i sistemi hardware e software e curare il loro ripristino, aggiornando le policy	Monitorare i sistemi hardware e software e supportare il loro ripristino in caso di problemi di integrità e sicurezza
	Gestire l’evoluzione delle policy di cybersecurity

2. LIVELLO EQF DELLA QUALIFICAZIONE IN USCITA: 6

3. REQUISITI OBBLIGATORI DI ACCESSO AL PERCORSO

- Laurea triennale o possesso di qualifica di Tecnico della sicurezza informatica di cui al Repertorio della Regione Abruzzo.
- 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 B2 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 • Aspetti contrattualistici, fiscali e previdenziali • Elementi di legislazione del lavoro • Aspetti etici dell'esercizio del ruolo	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. Credito di frequenza con valore a priori in caso di possesso di qualifica di Tecnico della sicurezza informatica ex DD n. 61/DPG025 (19-04-2023)

3	**Conoscenze** • Fondamenti teorici della sicurezza dei sistemi digitali • Evoluzione ed attuale scenario delle principali vulnerabilità note • Standard e framework nazionali ed internazionali in ambito cybersecurity (Security by design, Sistema di Gestione per la Sicurezza delle Informazioni – ISO 27001, Sistemi di gestione per la continuità operativa ISO 22301, NIST, Framework Nazionale per la Cyberse-curity e la data protection - FNCS, NIST SP800) • Quadro normativo nazionale: Perimetro di Sicurezza Nazionale Cibernetica • Quadro normativo nazionale e comunitario in materia di protezione dei dati personali	Principi, standard e framework in ambito cybersecurity	40	15	Ammesso il riconoscimento di credito formativo di frequenza esclusivamente sulla base della valutazione di apprendimenti formali
4	**Conoscenze** • Fondamenti di processi ed organizzazione aziendale. Potenziali impatti della vulnerabilità dei sistemi informativi sulla continuità del business • Metodologie e framework di riferimento per la misurazione vulnerabilità (es. CVSS, NVD) e conseguente strategie di mitigazione • Metodi e strumenti per attività di Penetration Testing • Application Security tools (Static and Dynamic Application Security Testing) • Metodi di valutazione dei rischi per la sicurezza legati alle componenti hardware e software del sistema digitale • Metodi di valutazione di rischi per la sicurezza legati alle componenti del sistema digitale dedicate al networking (protocolli, connessioni, apparecchiature di rete) • Standard e framework di riferimento per la definizione del processo di gestione della qualità dei dati (Data Quality Management) **Abilità** • Individuare, sulla base delle caratteristiche del business, il quadro normativo e gli standard e framework nazionali ed	Analizzare vulnerabilità, rischi e conformità ai requisiti di sicurezza dei sistemi digitale, sulla base dei requisiti di business	50	25	Ammesso il riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali

	internazionali in ambito cybersecurity applicabili • Eseguire un'analisi del rischio che evidenze le minacce e le vulnerabilità dell'Ecosistema legale, normativo e di business • Analizzare l'architettura del sistema digitale per individuare le possibili vulnerabilità per l’accesso al sistema o alle informazioni in esso contenute • Analizzare i requisiti richiesti al sistema digitale dalle previsioni normative vigenti in materia di privacy e sicurezza informatica • Individuare le vulnerabilità dell'architettura, delle apparecchiature hardware, del software e dei processi di gestione del sistema digitale • Elaborare documenti di valutazione dei rischi per la sicurezza del sistema digitale, contenenti l'analisi delle minacce e delle vulnerabilità individuate • Interagire con i responsabili dei vari livelli decisionali, supportando le scelte strategiche in materia di sicurezza dei sistemi digitale				
5	**Conoscenze** • Fondamenti di project management • Principi e metodi tecnico-economici di definizione di strategia di sicurezza informatica • Best practice in materia di sicurezza informatica (es. ITIL, COBIT, …) • Policy di sicurezza informatica: misure tecniche ed organizzative • Impatti organizzativi e professionali delle policy di sicurezza informatica e relativi piani di adeguamento e sviluppo **Abilità** • Definire strategia, policy ed approccio tecnico-organizzativo di implementazione, valutando la compatibilità economica delle scelte • Elaborare la documentazione relativa all’implementazione delle politiche di sicurezza	Definire strategia e policy per la sicurezza informatica	25	10	Ammesso il riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
6	**Conoscenze**	Implementare le misure di sicurezza informatica	65	30	Ammesso il riconoscimento di

	• Caratteristiche e funzionalità dei firewall • Principali caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection • Principali caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da client a server • Tipologie e logiche di funzionamento di virus, worm, trojan, malware, ransomware, … • Tipologie e caratteristiche degli attacchi al sistema digitale a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente • Algoritmi crittografici specifici (SHA, AES, RSA, ecc.) e loro applicazione alla trasmissione sicura dei dati e alla conservazione su file system • Principali metodi e tecniche di configurazione del sistema di protezione e del firewall • Autenticazione federata basata su Single Sign-On (SSO) e Identity Provider • Principali tipologie e funzionalità di un Security Operation Center • Sistemi di controllo degli accessi al sistema digitale ed alle reti: Architettura IAM (Identity Access Management), meccanismi di autenticazione distribuita, meccanismi di Strong Authentication **Abilità** • Installare e configurare sistemi di protezione della rete e software di protezione dai malware • Installare e configurare sistemi di controllo degli accessi (IAM), basati su identificazione, autenticazione e autorizzazione • Definire ed applicare le regole di configurazione dei firewall • Definire politiche di controllo degli accessi ed implementare i relativi profili di accesso selettivi • Definire le tecniche di autenticazione degli utenti (user-id, password, smart card, sistemi biometrici, etc.) • Definire politiche per la creazione e aggiornamento delle password				credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
7	**Conoscenze** • Comportamenti umani e cybersecurity	Comunicare i rischi ed i comportamenti corretti	15	10	Ammesso il riconoscimento di credito formativo di

	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				frequenza sulla base della valutazione di apprendimenti formali, non formali ed in-formali. Credito di frequenza con valore a priori in caso di possesso di qualifica di Tecnico della sicurezza informatica ex DD n. 61/DPG025 (19-04-2023)
8	**Conoscenze** • Sistemi di gestione dell'identità (IMS) ed autorizzazione degli 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 **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	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 frequenza sulla base della valutazione di apprendimenti formali, non formali ed in-formali. Credito di frequenza con valore a priori in caso di possesso di qualifica di Tecnico della sicurezza informatica ex DD n. 61/DPG025 (19-04-2023)

	sistema informativo • Individuare ed eliminare malware • Eseguire il piano di ripristino in caso di crisi • Svolgere il reporting delle operazioni compiute • Gestire le regole di firewall in funzione delle situazioni di minaccia e attacco				
9	**Conoscenze** • Metodi e tecniche di analisi dei dati di security analytics (es. threat detection, riconoscimento di cyber attacchi, ecc.) **Abilità** • Analizzare dati di security analytics (es. threat detection, riconoscimento di cyber attacchi, ecc.) modificando, in caso di risultati poco soddisfacenti, i tools utilizzati	Gestire l'evoluzione delle policy di cybersecurity	15	5	Ammesso il riconoscimento di credito formativo di frequenza sulla base della valutazione di apprendimenti formali, non formali ed informali
10		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 in-formali. Credito di frequenza con valore a priori in caso di possesso di qualifica di Tecnico della sicurezza informatica ex DD n. 61/DPG025 (19-04-2023)
11	**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 in-formali. Credito di frequenza con valore a priori in caso di possesso di qualifica di Tecnico della sicurezza informatica ex DD n. 61/DPG025 (19-04-2023)
12	**Conoscenze** • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza Fattori specifici di rischio professionale ed ambientale **Abilità** • Applicare procedure di sicurezza • Utilizzare dispositivi di sicurezza individuale • Agire nel rispetto della normativa sulla salute e la sicurezza nei luoghi di lavoro	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			**308**	**149**	

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 20% 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 6, 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; 50% 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