ALLEGATO "2"

STANDARD MINIMO DI PERCORSO FORMATIVO
QUALIFICAZIONE DI ESPERTO IN SICUREZZA INFORMATICA

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

Unità di Competenza	**Unità di Risultati di Apprendimento**
--	Inquadramento della professione
--	Architetture di sistemi digitali
--	Fondamenti di organizzazione e project management
--	Quadro normativo, standard e framework in ambito cybersecurity e data quality management
Analisi delle vulnerabilità software e hardware e della conformità alla normativa vigente	Analizzare le vulnerabilità software e hardware e la conformità alla normativa vigente
Individuazione di soluzioni per la sicurezza dei sistemi hardware e software	Individuare processi e soluzioni a protezione del sistema digitale
Monitoraggio e supporto al ripristino della sicurezza dei sistemi hardware e software	Monitorare lo stato di sicurezza dei sistemi digitali
--	Inglese tecnico
--	Operare in sicurezza nel luogo di lavoro

2. ***LIVELLO EQF DELLA QUALIFICAZIONE IN USCITA:*** 6

3. ***REQUISITI OBBLIGATORI DI ACCESSO AL PERCORSO:***

- Qualificazione regionale di livello EQF 5 in ambito STEM, Diploma ITS Academy in ambito STEM, Laurea triennale o titolo superiore in ambito STEM.
- 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 di dimostrazione dell'attesa di rinnovo, documentata dall'avvenuta presentazione della domanda di rinnovo del titolo di soggiorno.
- Conoscenza della lingua inglese almeno al livello B1 del Quadro Comune Europeo di Riferimento per le Lingue, dimostrabile tramite certificazioni linguistiche o titoli equipollenti o prove valutative in sede di selezione.

- Conoscenze e competenze avanzate in ambito IT e conoscenze e competenze di base in ambito cybersecurity, dimostrabile tramite prove valutative in sede di selezione.

4. *ARTICOLAZIONE, PROPEDEUTICITÀ E DURATE MINIME:*

N.	Articolazione dell'Unità di competenza	Unità di Risultati di apprendimento	Durata minima	di cui in FaD	Crediti formativi
1.	***Conoscenze*** - Orientamento al ruolo - Elementi di diritto del lavoro, contrattualistica, regimi fiscali e responsabilità civile	*Inquadramento della professione*	8	0	Non ammesso il riconoscimento di credito formativo di frequenza
2.	***Conoscenze*** - Architettura hardware e software dei sistemi digitali - Sistemi digitali ed ingegneria del software	*Architetture di sistemi digitali*	20	*Max* 10, di cui almeno 8 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
3.	***Conoscenze*** - Fondamenti di organizzazione aziendale - Fondamenti di project management	*Fondamenti di organizzazione e project management*	10	*Max* 5, di cui almeno 4 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
4.	***Conoscenze*** - Quadro normativo nazionale e comunitario in materia di sicurezza informatica, cybersecurity - Quadro normativo nazionale: Perimetro di Sicurezza Nazionale Cibernetica - Quadro normativo nazionale e comunitario in materia di protezione dei dati personali - 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 Cybersecurity e la data protection – FNCS, NIST SP800-9 - Standard e framework di riferimento per la definizione del processo di gestione della qualità dei dati (Data Quality Management)	*Quadro normativo, standard e framework in ambito cybersecurity e data quality management*	30	*Max* 15, di cui almeno 12 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, esclusivamente da apprendimenti formali

N.	Articolazione dell'Unità di competenza	Unità di Risultati di apprendimento	Durata minima	di cui in FaD	Crediti formativi
5.	***Conoscenze*** - Fondamenti teorici della sicurezza dei sistemi digitali - Evoluzione ed attuale scenario delle principali vulnerabilità note - Metodologie e framework di riferimento per la misurazione vulnerabilità (es. CVSS, NVD) e conseguenti strategie di mitigazione - Metodi e strumenti per attività di Penetration Testing - Application Security tools (Static and Dynamic Application Security Testing) - Awareness, Red Teaming e Lesson Learned Techniques - 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) ***Abilità*** - Analizzare l'architettura del sistema digitale, per individuare i possibili punti di 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 digitali	*Analizzare le vulnerabilità software e hardware e la conformità alla normativa vigente*	80	*Max* 40, di cui almeno 32 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali

N.	Articolazione dell'Unità di competenza	Unità di Risultati di apprendimento	Durata minima	di cui in FaD	Crediti formativi
6.	***Conoscenze*** - 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 dei programmi informatici creati per diffondersi e sottrarre informazioni o danneggiare sistemi digitali (virus, worm, Trojan, malware, ransomware, ecc…) - Tipologie e caratteristiche degli attacchi al sistema digitale a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente - Caratteristiche e funzionalità dei *firewall* - 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* - Elementi di metodologie, tecniche e strumenti in ambito *asset management* - Autenticazione federata basata su Single Sign-On (SSO) e Identity Provider - Sistemi per la creazione e gestione di password complesse - 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*** - Contribuire alle procedure per allestire e mantenere un *asset inventory* - Utilizzare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema digitale e per la loro comunicazione - Installare e configurare sistemi di protezione della rete, per garantire la sicurezza, la riservatezza e l'integrità delle connessioni tra client e server - Installare e configurare un efficace ed efficiente software di protezione dai malware sui dispositivi digitali, per l'individuazione e la rimozione dei programmi informatici finalizzati all'attacco dei sistemi digitali - Installare e configurare sistemi di controllo degli accessi (IAM), basati su identificazione, autenticazione e autorizzazione, che garantiscano, in modo sostenibile per gli utenti, un uso più sicuro dei sistemi digitali - Configurare e aggiornare le regole di firewall - Definire profili di accesso selettivi, individuali o per ruoli (configurazione dello IAM), basati su effettive necessità operative o su una politica di controllo degli accessi preventivamente approvata - Definire le credenziali di autenticazione per l'identificazione degli utenti autorizzati ad accedere al sistema digitale, prevedendo l'utilizzo delle tecniche più appropriate	*Individuare processi e soluzioni a protezione del sistema digitale*	64	*Max* 16, di cui almeno 13 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali

N.	Articolazione dell'Unità di competenza	Unità di Risultati di apprendimento	Durata minima	di cui in FaD	Crediti formativi
	(user-id, password, smart card, sistemi biometrici, etc.) - Definire politiche per la creazione e aggiornamento delle password - Contribuire all'elaborazione di documentazione relativa all'implementazione delle politiche di sicurezza				
7.	***Conoscenze*** - Principali strumenti e tecniche per l'analisi e gestione degli incidenti informatici: monitoraggio, analisi valutazione e gestione degli eventi informatici (SIEM), individuazione di anomalie - Principali metodi e tecniche per la classificazione degli eventi ed incidenti informatici (es. tassonomie nazionali/comunitarie, il framework MITRE ATT&CK™) - Principali metodi, per infrastrutture con soluzioni in locale o su cloud, e strumenti per implementare una politica di backup e restore dei sistemi digitali - Cenni sulle metodologie e strumenti per la protezione fisica dei sistemi e delle reti - Fondamenti di *crisis management* - Elementi sulle tecniche e infrastrutture di *disaster recovery* - Elementi di sistemi di gestione per la continuità aziendale (ISO 22301) - Cenni sulle metodologie e tecniche di simulazione e role playing per lo svolgimento di test e simulazioni del sistema di gestione della continuità operativa (test di DR e BC) - Cenni su metodi e tecniche per lo svolgimento di *Business Impact Analysis* - Principali standard e framework di riferimento in ambito gestione degli incidenti informatici - Cenni sul funzionamento e organizzazione del CERT e dei SOC e sul sistema di alert dello CSIRT nazionale - Fondamenti di organizzazione aziendale - Fondamenti di project management ***Abilità*** - Collaborare per il ripristino dell'integrità e del funzionamento delle strutture informatiche di riferimento, danneggiate a seguito di una violazione tentata o riuscita - Controllare il rispetto delle misure di sicurezza progettate - Supportare le procedure per il test dei piani di *business continuity* e *disaster recovery* - Configurare strumenti per riconoscere e mitigare attacchi denial of service - Monitorare il traffico interno ed esterno, riconoscendo potenziali minacce alla sicurezza del sistema digitale - Monitorare e valutare gli eventi informatici e dei log dei sistemi digitali - Supportare l'implementazione delle politiche di backup e restore - Collaborare alla definizione ed esecuzione dei piani di ripristino - Supportare nell'elaborazione dei piani di *Disaster Recovery* e *Business Continuity* che, in caso di incidente grave o interruzione per cause non controllabili, consentano il mantenimento o il ripristino, nel più breve tempo possibile, della corretta funzionalità	*Monitorare lo stato di sicurezza dei sistemi digitali*	48	*Max* 16, di cui almeno 13 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali

N.	Articolazione dell'Unità di competenza	Unità di Risultati di apprendimento	Durata minima	di cui in FaD	Crediti formativi
	del sistema digitale - Monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.) - Configurare strumenti per l'individuazione e la segnalazione di malware (spyware, backdoor, trojans, ecc.) nei sistemi digitali - Supportare il design e lo sviluppo di un incident response playbook				
8.	***Conoscenze*** - Inglese tecnico per l'informatica	*Inglese tecnico*	32	*Max* 16, di cui almeno 13 in modalità sincrona	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
9.	***Conoscenze*** - Legislazione sulla salute e sicurezza sui luoghi di lavoro e applicazione delle norme di sicurezza - Gli obblighi del datore di lavoro e del lavoratore - Dispositivi di protezione individuali ***Abilità*** - Applicare i protocolli di prevenzione e riduzione del rischio professionale	*Operare in sicurezza nel luogo di lavoro*	8	*Max* 4, anche in modalità totalmente asincrona	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 del 21/12/2011 – Formazione dei lavoratori, ai sensi dell'art. 37, comma 2 del D.lgs. 81/2008
DURATA MINIMA TOTALE, AL NETTO DEL TIROCINIO CURRICULARE			**300**	***Max* 122**	

5. *TIROCINIO CURRICULARE:*

Durata minima: 120 ore; durata massima: 150 ore.

6. *UNITA' 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 risultati di apprendimento vanno realizzate attraverso attività di formazione d'aula specifica e metodologia attiva, utilizzando attrezzature professionali e idonei spazi attrezzati.

8. *VALUTAZIONE DIDATTICA DEGLI APPRENDIMENTI:*
Obbligo di tracciabile valutazione didattica degli apprendimenti, per singola Unità di risultati di apprendimento.

9. *GESTIONE DEI CREDITI FORMATIVI:*
- Credito di ammissione: riconoscibile sulla base della valutazione degli apprendimenti formali, non formali e informali.
- Crediti di frequenza: la percentuale massima riconoscibile è il 30% sulla durata di ore d'aula e laboratorio; il 50% sul 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.

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 l'80% delle ore complessive del percorso formativo. È consentita l'ammissione all'esame finale anche a fronte della frequenza di almeno il 70% delle ore complessive del percorso formativo, previo parere favorevole - documentato – del collegio dei docenti/formatori.

12. *ATTESTAZIONE IN ESITO AD ESAME PUBBLICO:*
Certificato di qualificazione professionale, rilasciato ai sensi del D.lgs. 13/2013.