ALLEGATO "2"

STANDARD MINIMO DI PERCORSO FORMATIVO
QUALIFICAZIONE DI CYBERSECURITY TECHNICIAN

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

Unità di Competenza	**Unità di Risultati di Apprendimento**
	Inquadramento della professione
	Elementi di base di cyber security, IT e sicurezza informatica
Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni	Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni
Supporto all'implementazione di soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti	Supporto all'implementazione di soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti
Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie	Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie
	Inglese tecnico
	Operare in sicurezza nel luogo di lavoro

2. ***LIVELLO EQF DELLA QUALIFICAZIONE IN USCITA:*** 5

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

- Diploma di scuola secondaria di secondo grado o qualifica di livello EQF 4;
- Possesso di competenze di base in ambito IT (Elementi minimi di architetture di sistemi informativi e di elaborazione dati; conoscenza di strumenti digitali e tecnologie di lavoro da remoto; modalità e soluzioni di archiviazione dei dati; elementi teorici minimi di Information Security), dimostrabili tramite prove valutative in sede di selezione.
- 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.

4. *ARTICOLAZIONE, PROPEDEUTICITÀ E DURATE MINIME:*[1]

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*	5	0	Non ammesso il riconoscimento di credito formativo di frequenza
2.	***Conoscenze*** - Elementi di base di sicurezza informatica, ICT, cybersecurity ed Operational Technology - Fondamenti di processi ed organizzazione aziendale - Elementi di infrastruttura IT (informatica, cloud, networking) - Principali ambienti cloud (MS Azure, AWS, Google Cloud)	*Elementi di base di cyber security, IT e sicurezza informatica*	55	*Max* 30	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali. Credito formativo con valore a priori, per i laureati nelle classi "L-08", "L-30", "L-31", "LM-18", "LM32".

[1] La colonna "Durata minima", indica il numero di ore complessive obbligatorie di attività didattica in aula/laboratorio, al netto dell'eventuale tirocinio curriculare.
La colonna "di cui in FaD", indica il numero massimo di ore realizzabili con tale modalità, con il vincolo della tracciabilità individuale delle attività svolte e nell'ambito del monte ore complessivo di cui alla colonna "Durata minima". Infine nella colonna "Crediti formativi", sono indicate le condizioni ed i limiti di riconoscibilità del credito di frequenza della corrispondente Unità di risultati di apprendimento.

3.	***Conoscenze*** - Principi di sicurezza informatica (RID, minimo privilegio etc…) - Standard e linee guida in materia di Information Technology e Operation Technology e protezione dei dati personali - Framework normativo nazionale ed europeo in materia cybersecurity, information security e privacy - Il fattore umano nel contesto della cybersecurity - Principali standard di riferimento per lo svolgimento di attività di auditing, assessment, risk assessment e risk management - Metodologie di analisi delle vulnerabilità - Best practices, standards, frameworks e principi dell'information security management - Strumenti per la verifica tecnica delle vulnerabilità e degli attacchi di rete ***Abilità*** - Applicare i principi information security e cybersecurity ai processi aziendali ed alle tecnologie - Supportare il team nelle attività di audit ed assessment utilizzando strumenti e metodologie idonee alla verifica degli aspetti cybersecurity ed information security - Applicare attività di controllo ai sistemi informativi - Svolgere attività di supporto per l'identificazione di minacce e vulnerabilità - Verificare l'aderenza del sistema informativo alle normative vigenti in materia di privacy e sicurezza informatica - Applicare modelli di gestione del rischio nei principali framework di riferimento - Applicare modelli coerenti di analisi del rischio - Effettuare attività di risk reporting e definizione dei piani di trattamento del rischio - Raccogliere e analizzare le evidenze a supporto delle attività di audit, assessment ed analisi del rischio - Formalizzare gli standard e le linee guida in materia di ITC - Analizzare processi di business e processi di supporto, contromisure tecniche ed organizzative di natura cybersecurity a supporto - Comprendere, comunicare ed applicare requisiti legali con impatto sulla cybersecurity - Comprendere, comunicare ed applicare i requisiti di business con impatto sul governo cybersecurity - Comprendere e comunicare i rischi legati al fattore umano in ambito cybersecurity - Eseguire il piano di ripristino in caso di crisi	*Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni*	70	*Max 20*	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali

4.	***Conoscenze*** - *Framework* di riferimento in ambito IT ed OT: contromisure preventive e reattive - Tassonomie, fonti in merito a minacce e vulnerabilità - Principali metodologie di *Vulnerability Assessment* e *Penetration Test* - Framework di riferimento, pratiche, metodologie e sistemi per la gestione degli asset informatici - Framework di riferimento, pratiche, metodologie e sistemi per la gestione della sicurezza nell'ambito della supply chain - Framework di riferimento, pratiche, metodologie e sistemi per la gestione della continuità operativa ed applicazione di modelli di disaster recovery - Elementi di *network security* - Elementi di *web security* - Elementi di *mobile security* - Modelli per la reazione e gestione degli *Incident management* - Pratiche di sicurezza all'interno della tecnologia cloud ***Abilità*** - Riconoscere ed applicare pratiche per la sicurezza dei sistemi e delle reti - Supportare il team nell'applicazione di tecniche di gestione del rischio in ambito network, web e mobile - Applicare modelli di gestione degli incidenti - Applicare modelli per la continuità operativa ed in ambito disaster recovery - Individuare edivulgare le best practices per il miglioramento delle procedure di gestione della sicurezza - Formalizzare gli standard e le linee guida in ambito cybersecurity	*Supporto all'implementazione di soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti*	70	*Max 20*	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
5.	***Conoscenze*** - Rischi ed opportunità relativi alle tecnologie "Disruptive" abilitanti - Principali applicazioni dell'intelligenza artificiale - Principali rischi dell'intelligenza artificiale in ambito cyber - Modelli e rischi dell'Edge computing - Principali applicazioni dell'IoT e rischi correlati - Principali applicazioni delle tecnologie Blockchain ai diversi settori in ambito security ***Abilità*** - Comprendere e comunicare rispetto ad opportunità e rischi delle tecnologie "disruptive" abilitanti - Applicare al contesto delle tecnologie "disruptive" i principi ed i principali framework di riferimento in ambito ICT, cybersecurity e protezione dei dati - Comprendere e comunicare rispetto alle principali applicazioni delle tecnologie "disruptive"	*Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie*	70	*Max 20*	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali

6.	***Conoscenze*** - Inglese tecnico per l'informatica ***Abilità*** - Comprendere, parlare, scrivere in inglese informatico	*Inglese tecnico*	22	*Max 14*	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
7.	***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*	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 108***	

NOTA:
L'Unità di risultati di apprendimento n. 2, va realizzata antecedentemente alle Unità n. 3, 4 e 5.

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 ed 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 ed informali.
- Crediti di frequenza: la percentuale massima riconoscibile è il 30% sulla durata di ore d'aula o 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. Presenza di aule/laboratori adeguadatamente attrezzati.

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.