ALLEGATO "4"

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
--	Fondamenti di sicurezza informatica
Analisi delle vulnerabilità software e hardware e della conformità alla normativa vigente	Analizzare le vulnerabilità software e hardware e della conformità alla normativa vigente
Definizione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software	Definire e implementare soluzioni per la sicurezza dei sistemi hardware e software
Monitoraggio e ripristino della sicurezza di sistemi hardware e software	Monitorare e ripristinare la sicurezza di sistemi hardware e software
Definizione ed adozione delle misure organizzative per la sicurezza del sistema informativo	Definire ed adottare misure organizzative per la sicurezza del sistema informativo
--	Inglese tecnico
--	Operare in sicurezza nel luogo di lavoro

2. LIVELLO EQF DELLA QUALIFICAZIONE IN USCITA: 6

3. REQUISITI OBBLIGATORI DI ACCESSO AL PERCORSO:

- Diploma ITS, Laurea triennale o titolo superiore.
- 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 di dimostrazione dell'attesa di rinnovo, documentata dall'avvenuta presentazione della domanda di rinnovo del titolo di soggiorno.

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*** - Fondamenti teorici della sicurezza dei sistemi informativi - Architettura hardware e software dei sistemi digitali - Tipologia delle potenziali minacce all'integrità, riservatezza e disponibilità delle informazioni e delle risorse di un sistema informativo o di una rete - Principali tecniche di attacco alla sicurezza informatica - Normativa in materia di sicurezza informatica e relativa certificazione - Normativa in materia di protezione dei dati trattati con sistemi informatici	*Fondamenti di sicurezza informatica*	50	*Max* 20	Ammesso il riconoscimento di credito formativo di frequenza, solo in presenza di evidenze relative a coerenti apprendimenti formali o a percorsi teorico-pratici, conclusi da valutazione degli apprendimenti di parte seconda
3.	***Conoscenze*** - Metodi di analisi dei rischi di sicurezza e di individuazione delle vulnerabilità per la sicurezza di sistemi informatici - Metodi di analisi dei punti di forza e di debolezza in relazione alle esigenze di sicurezza e protezione dei dati - Metodi di valutazione dei rischi per la sicurezza legati alle componenti hardware e software del sistema - Metodi di valutazione di rischi per la sicurezza legati alle componenti del sistema informativo dedicate al networking (protocolli, connessioni, apparecchiature di rete) ***Abilità*** - Allestire e manutenere asset inventory - Analizzare l'architettura del sistema informativo per individuare i possibili punti di attacco al sistema o alle informazioni in esso contenute - Analizzare i requisiti richiesti al sistema informativo dalle previsioni normative	*Analizzare le vulnerabilità software e hardware e della conformità alla normativa vigente*	50	*Max* 20	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali

[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.

N.	Articolazione dell'Unità di competenza	Unità di Risultati di apprendimento	Durata minima	di cui in FaD	Crediti formativi
	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 informativo - Elaborare documenti di valutazione dei rischi per la sicurezza del sistema informativo, contenenti l'analisi delle minacce e delle vulnerabilità individuate e delle possibili contromisure - Interagire con i responsabili dei vari livelli decisionali, orientando e supportando le scelte strategiche in materia di sicurezza dei sistemi informativi				
4.	***Conoscenze*** - Tipologie e logiche di funzionamento dei programmi informatici creati per la violazione o il danneggiamento dei sistemi informativi (virus, worm, Trojan, malware, ecc…) - Tipologie e caratteristiche degli attacchi al sistema informativo a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente - Caratteristiche e funzionalità dei firewall - 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 - Caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection - Caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da client a server - Sistemi di autorizzazione degli accessi al sistema informativo ed alle reti ***Abilità*** - Utilizzare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema informativo e delle comunicazioni con l'esterno - Rafforzare l'architettura della rete con la creazione di 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 un efficace ed efficiente software antivirus o EDR, per	*Definire e implementare soluzioni per la sicurezza dei sistemi hardware e software*	70	*Max* 30	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
	l'individuazione e la rimozione dei programmi informatici finalizzati alla violazione o al danneggiamento del sistema informativo - Installare e configurare sistemi di autenticazione, autorizzazione e controllo degli accessi (IAM), che garantiscano la sicurezza del sistema informativo senza creare difficoltà agli utenti autorizzati - Definire profili di accesso selettivi, individuali o per gruppi omogenei (configurazione dello IAM), basati su effettive necessità operative o su autorizzazioni preventivamente approvate - Definire le credenziali di autenticazione per l'identificazione degli utenti autorizzati ad accedere al sistema informativo, prevedendo l'utilizzo delle tecniche più appropriate (user-id, password, smart card, sistemi biometrici, etc.) - Progettare un Security Operation Center (SOC)				
5.	***Conoscenze*** - Strumenti e tecnologie per la protezione fisica delle strutture, per assicurare la sicurezza dei locali e delle componenti del sistema informativo, dai rischi ambientali connessi: ad interruzioni dell'alimentazione, incidenti, danneggiamenti, calamità naturali - Tecniche di backup e di restore dei sistemi informativi - Metodologie per l'organizzazione di un sistema di internal auditing, per verificare l'effettivo livello di sicurezza dei sistemi informativi ***Abilità*** - Programmare un piano di audit e controlli sulla sicurezza, per verificare l'effettivo livello di protezione del sistema informativo	*Monitorare e ripristinare la sicurezza di sistemi hardware e software*	35	*Max* 10	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
6.	***Conoscenze*** - Tecniche di analisi dei costi e dei benefici dell'adozione di modelli organizzativi finalizzati all'incremento del livello di sicurezza dei sistemi informativi - Tecniche di progettazione dell'organizzazione per la sicurezza: divisione delle responsabilità e definizione delle funzioni - Tecniche di formazione degli utenti finali e delle professionalità interessate dal mantenimento della sicurezza del sistema informativo ***Abilità***	*Definire ed adottare misure organizzative per la sicurezza del sistema informativo*	30	*Max* 20	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
	- Organizzare una gestione efficace delle emergenze, con una chiara definizione dei ruoli e delle procedure ed una corretta attribuzione delle responsabilità, in caso di incidente o attacco informatico - Organizzare le procedure per il controllo dei log, degli accessi e del traffico verso l'esterno, del sistema informativo - Elaborare i 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 del sistema informativo - Definire gli strumenti, l'organizzazione, i ruoli e le responsabilità, per garantire una corretta gestione della sicurezza del sistema informativo - Orientare e supportare il processo di adeguamento delle competenze e dei comportamenti di sicurezza informatica, di tutti i membri dell'organizzazione				
7.	***Conoscenze*** - Inglese tecnico per l'informatica	*Inglese tecnico*	12	*Max* 8	Ammesso il riconoscimento di credito formativo di frequenza, da apprendimenti formali, non formali ed informali
8.	***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			**260**	***Max 112***	

NOTA:
L'Unità di risultati di apprendimento n. 2, va realizzata antecedentemente alle Unità n. 3, 4, 5 e 6.

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.

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.