REGIONE LAZIO

REGIONE LAZIO

Direzione: ISTRUZIONE, FORMAZIONE E POLITICHE PER L'OCCUPAZIONE

Area: PROGRAMMAZIONE DELL'OFFERTA FORMATIVA E DI ORIENTAMENTO

DETERMINAZIONE *(con firma digitale)*

N. G04291 **del** 30/03/2023 **Proposta n.** 12974 **del** 29/03/2023

Oggetto:

Repertorio regionale delle competenze e dei profili formativi. Approvazione delle modifiche allo standard professionale ed allo standard minimo di percorso formativo del profilo di "Esperto in sicurezza informatica".

Proponente:

Estensore	CASCINO STEFANO	_____*firma elettronica*_____
Responsabile del procedimento	TOMAI ALESSANDRA	_____*firma elettronica*_____
Responsabile dell' Area	A. TOMAI	_____*firma digitale*_____
Direttore Regionale	E. LONGO	_____*firma digitale*_____

Firma di Concerto

Richiesta di pubblicazione sul BUR: SI

Oggetto: Repertorio regionale delle competenze e dei profili formativi. Approvazione delle modifiche allo standard professionale ed allo standard minimo di percorso formativo del profilo di "Esperto in sicurezza informatica".

LA DIRETTRICE DELLA DIREZIONE REGIONALE ISTRUZIONE, FORMAZIONE E POLITICHE PER L'OCCUPAZIONE

su proposta del Dirigente dell'Area Programmazione dell'offerta formativa e di orientamento

VISTI:

- la Legge n. 845 del 21 dicembre 1978: "Legge-quadro in materia di formazione professionale.";
- la Legge n. 241 del 7 agosto 1990, recante: "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.";
- il Decreto legislativo n. 13 del 16 gennaio 2013, avente ad oggetto: "Definizione delle norme generali e dei livelli essenziali delle prestazioni per l'individuazione e validazione degli apprendimenti non formali e informali e degli standard minimi di servizio del sistema nazionale di certificazione delle competenze, a norma dell'articolo 4, commi 58 e 68, della legge 28 giugno 2012 n. 92.";
- il Decreto del 30 giugno 2015 del Ministro del Lavoro e delle Politiche sociali e del Ministro dell'istruzione, dell'università e della ricerca che ha recepito l'Intesa in sede di Conferenza Stato-Regioni e PP.AA del 22 gennaio 2015, riguardante la definizione di un quadro operativo per il riconoscimento a livello nazionale delle qualificazioni regionali e delle relative competenze, nell'ambito del Repertorio nazionale dei titoli istruzione e formazione e delle qualificazioni professionali di cui all'articolo 8 del decreto legislativo 16 gennaio 2013, n. 13;
- la Legge statutaria n. 1 dell'11 novembre 2004: "Nuovo Statuto della Regione Lazio.";
- la Legge regionale n. 23 del 25 febbraio 1992, di: "Ordinamento della formazione professionale.";
- la Legge regionale n. 6 del 18 febbraio 2002, avente ad oggetto: "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale.";
- la Legge regionale n. 17 del 31 dicembre 2015, la "Legge di stabilità regionale 2016" e, in particolare, l'art.7 contenente "Disposizioni attuative della legge 7 aprile 2014, n. 56 "Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni" e successivo riordino delle funzioni e dei compiti di Roma Capitale, della Città metropolitana di Roma Capitale e dei comuni. Disposizioni in materia di personale.";
- il Regolamento regionale n. 1 del 6 settembre 2002, "Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale.";
- la Deliberazione di Giunta regionale n. 452 dell'11 settembre 2012, avente ad oggetto: "Istituzione di un Repertorio Regionale delle competenze e dei profili formativi. Approvazione Linee di indirizzo e Procedura di aggiornamento – Approvazione di n. 108 profili formativi caratterizzanti settori economici del territorio regionale e inserimento nel Repertorio. Revoca della deliberazione di Giunta regionale 22 marzo 2006, n. 128";
- la Deliberazione di Giunta regionale n. 56 del 23 febbraio 2016, recante: "Legge Regionale 31 dicembre 2015, n.17 "Legge di stabilità regionale 2016" - attuazione disposizioni di cui all'art.7, comma 8.";
- la Deliberazione di Giunta regionale n. 122 del 22 marzo 2016, di "Attuazione delle disposizioni dell'Intesa 22 gennaio 2015, recepite con decreto interministeriale 30 giugno 2015 – Direttiva istitutiva del Sistema regionale di certificazione delle competenze acquisite in contesti di apprendimento formale, non formale e informale. Primi indirizzi operativi.";

- la Deliberazione di Giunta regionale n. 273 del 24 maggio 2016, concernente: “Approvazione dei principi generali e delle procedure di revisione ed aggiornamento del Repertorio regionale delle competenze e dei profili professionali, approvato con DGR 452/2012. Revoca e sostituzione dell’allegato A della Deliberazione di Giunta regionale n. 452 dell’11 settembre 2012.”;
- la Deliberazione di Giunta regionale n. 254 del 5 giugno 2018, di “Istituzione del Repertorio regionale degli standard di percorso formativo e approvazione disposizioni in materia di riconoscimento di crediti formativi.”;
- la Deliberazione di Giunta regionale n. 816 del 14 dicembre 2018, di “Attuazione dell’art. 13, comma 4, della D.G.R. 122/2016 – approvazione della “Direttiva per l’accreditamento dei soggetti titolati per l’erogazione dei servizi di individuazione e validazione e/o del servizio di certificazione delle competenze nella Regione Lazio.”;
- la Deliberazione di Giunta regionale n. 15 del 22 gennaio 2019, avente ad oggetto l’“Attuazione art.12 della D.G.R. 122/2016: approvazione delle disposizioni relative agli standard minimi di processo per l'erogazione dei servizi di individuazione e validazione e del servizio di certificazione delle competenze. Modifica delle D.G.R. 452/2012 e 122/2016.”;
- la Deliberazione di Giunta regionale n. 682 del 1° ottobre 2019, di “Revoca della D.G.R. 29 novembre 2007, n.968 e s.m.i.. Approvazione nuova Direttiva concernente l’accreditamento dei soggetti che erogano attività di formazione e di orientamento nella Regione Lazio.”;
- la Deliberazione di Giunta regionale n. 16 del 25 gennaio 2022, recante “Disposizioni sulle modalità di erogazione della formazione teorica, a distanza e in presenza, per le attività di formazione professionale, autofinanziate e/o finanziate con il Fondo sociale europeo e per lo svolgimento degli esami finali. Recepimento dell’Accordo sottoscritto dalla Conferenza delle Regioni e delle Province Autonome n. 21/181/CR5a/C17 nella seduta del 3 novembre 2021 e approvazione delle Linee guida”;
- la Deliberazione di Giunta regionale n. 81 del 1° marzo 2022, di “Approvazione dello schema di Accordo interistituzionale ai sensi dell’art. 15, L. 241/90 tra la Regione Lazio e l’Agenzia per la Cybersicurezza Nazionale finalizzato alla diffusione e al rafforzamento della cybersicurezza”;
- la Deliberazione di Giunta regionale n. 339 del 26 maggio 2022, avente ad oggetto: “Modifiche al regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni”;
- la Determinazione dirigenziale n. G01803 del 20 febbraio 2019, di “Attuazione art.15 della DGR 15 del 22 gennaio 2019. Approvazione format tipo del patto di servizio, degli standard informativi, documentali ed attestatori e degli standard di costo relativi al servizio di individuazione e validazione delle competenze. Revoca della D.D. G 12038 del 18 ottobre 2016.”;
- la Determinazione dirigenziale n. G16339 del 28 dicembre 2020, con la quale sono stati approvati – tra gli altri – gli standard professionale e minimo di percorso formativo del profilo di “Esperto in sicurezza informatica”;
- la Determinazione dirigenziale n. G07786 del 15 giugno 2022, con cui è stato costituito il gruppo di lavoro previsto dall'art. 4 dell'Accordo interistituzionale ai sensi dell'art. 15, L. 241/90 tra la Regione Lazio e l'Agenzia per la Cybersicurezza Nazionale, con il compito di supervisionare e coordinare le attività finalizzate alla diffusione e al rafforzamento della cybersicurezza;
- la Determinazione dirigenziale n. G07939 del 17 giugno 2022, avente ad oggetto: “Riorganizzazione delle strutture organizzative della Direzione regionale “Istruzione, Formazione e Politiche per l’Occupazione”. Attuazione direttiva del Direttore generale prot. n. n. 583446 del 14 giugno 2022”;
- la circolare protocollo 267914 del 20 maggio 2016 della Direzione regionale Formazione, Ricerca e Innovazione, Scuola e Università, Diritto allo Studio, avente ad oggetto: “Autorizzazione corsi di formazione privati non finanziati – Circolare operativa.”;

TENUTO CONTO CHE

- con l'Accordo interistituzionale di cui alla richiamata Deliberazione 81 del 2022, la Regione Lazio e l'Agenzia per la Cybersicurezza Nazionale, hanno convenuto di collaborare – tra l'altro – per la promozione della formazione, della crescita tecnico-professionale e della qualificazione delle risorse umane, in particolare nell'ambito dell'Accademia di Cybersicurezza della medesima Regione Lazio;
- al fine di aggiornare e migliorare i contenuti dello standard professionale del profilo di "Esperto in sicurezza informatica", approvato con la Determinazione dirigenziale G16339/2020 citata in premessa e di ampliare l'offerta formativa dell'Accademia di cui appena sopra, è stata predisposta, da parte del gruppo di lavoro costituito con la Determinazione dirigenziale G07786/2022, la scheda relativa allo standard rivisto del profilo in oggetto, che è stata poi trasmessa al Comitato tecnico di cui alla richiamata Deliberazione 273/2016, per ottenerne il prescritto parere di merito;

PRESO ATTO CHE

- il Comitato di cui sopra, nella seduta in videoconferenza, convocata tramite la comunicazione protocollo 141878 del 07/02/2023 e svoltasi il 27 febbraio 2023, ha approvato le proposte di modifica al profilo in questione ed il nuovo standard professionale correlato;

CONSIDERATO CHE

- con la suindicata Deliberazione di Giunta regionale 254/2018, è stato istituito il "Repertorio degli standard di percorso formativo" e sono state approvate la struttura e la disciplina concernente tali standard ed anche la disciplina per il riconoscimento di crediti formativi, applicabile ai profili del Repertorio regionale, per i quali sia stato approvato il relativo standard minimo di percorso formativo;

RILEVATO CHE

- è stata predisposta, da parte del medesimo gruppo di lavoro istituito con la Determinazione dirigenziale G07786/2022, la scheda relativa allo standard minimo di percorso formativo del profilo sopra indicato, elaborata in conformità del corrispondente standard professionale;

RITENUTO pertanto **NECESSARIO**:

- approvare lo standard professionale del profilo di "Esperto in sicurezza informatica", come descritto nell'allegato "1" della presente Determinazione, che sostituisce lo standard approvato con la Determinazione n. G16339 del 28 dicembre 2020;
- approvare lo standard minimo di percorso formativo del profilo di "Esperto in sicurezza informatica", come descritto nell'allegato "2" della presente Determinazione, che sostituisce lo standard approvato con la Determinazione n. G16339 del 28 dicembre 2020;

FATTI SALVI gli effetti derivanti da corsi realizzati o in corso di svolgimento alla data della notifica della presente Determinazione, autorizzati e/o approvati con riferimento all'originaria definizione del profilo succitato;

DETERMINA

Per le motivazioni sopra esposte, che formano parte integrante e sostanziale della presente determinazione,

1) di approvare lo standard professionale del profilo di “Esperto in sicurezza informatica”, come descritto nell’allegato “1” della presente Determinazione, che sostituisce lo standard approvato con la Determinazione n. G16339 del 28 dicembre 2020;

2) di approvare lo standard minimo di percorso formativo del profilo di “Esperto in sicurezza informatica”, come descritto nell’allegato “2” della presente Determinazione, che sostituisce lo standard approvato con la Determinazione n. G16339 del 28 dicembre 2020;

3) di fare salvi gli effetti derivanti da corsi realizzati o in corso di svolgimento, alla data della notifica della presente Determinazione, autorizzati e/o approvati, con riferimento all’originaria definizione del profilo di cui ai punti 1) e 2);

4) di pubblicare il presente provvedimento sul Bollettino Ufficiale della Regione Lazio e nella sezione “Documentazione” della pagina “Formazione” del sito regionale, al fine di darne la più ampia diffusione.

La pubblicazione sul Bollettino Ufficiale della Regione Lazio ha valore di notifica per gli interessati, a tutti gli effetti di legge.

Avverso la presente determinazione è ammesso ricorso giurisdizionale innanzi al T.A.R. del Lazio, nel termine di giorni 60 (sessanta) dalla notifica ovvero ricorso straordinario al Capo dello Stato, entro il termine di giorni 120 (centoventi).

La Direttrice
Avv. Elisabetta Longo

ALLEGATO "1"

[K1.8] ESPERTO IN SICUREZZA INFORMATICA

Descrizione sintetica:
L'Esperto/a in sicurezza informatica opera in autonomia nell'analisi dei sistemi digitali hardware e software e nella valutazione di possibili vulnerabilità e rischi alla sicurezza dei sistemi. In tale ambito, l'Esperto/a in sicurezza informatica agisce, secondo i principi di security by design per un'efficace ed efficiente gestione della sicurezza informatica. Inoltre, testa la sicurezza dei sistemi contro intrusioni, virus e minacce - intenzionali o accidentali - la recuperabilità di dati e operazioni, a seguito di incidenti o malfunzionamenti e la corretta funzione di protezione delle informazioni, mediante opportune tecniche di crittografia. Individua soluzioni per la mitigazione dei possibili rischi, tramite opportune misure di sicurezza dei sistemi e supporta nelle attività di ripristino delle corrette funzionalità dei sistemi.

SISTEMI DI REFERENZIAZIONE	
Sistema di riferimento	**Denominazione**
Settore economico-professionale (S.E.P.)	14. Servizi digitali
Area/e di Attività (AdA) del Repertorio nazionale delle qualificazioni regionali a cui il profilo afferisce	AdA.14.01.22 - Gestione della Sicurezza dell'Informazione
Livello E.q.f.	6
Posizione classificatoria ISTAT CP 2011	2.1.1.5.4 - Specialisti in sicurezza informatica
Posizione/i classificatoria/e ISTAT ATECO 2007	62.01.00 - Produzione di software non connesso all'edizione 62.02.00 - Consulenza nel settore delle tecnologie dell'informatica 62.03.00 – Gestione di strutture e apparecchiature informatiche hardware – housing (esclusa la riparazione) 62.09.09 - Altre attività dei servizi connessi alle tecnologie dell'informatica nca 63.11.20 - Gestione database (attività delle banche dati) 63.11.30 – Hosting e fornitura di servizi applicativi (ASP) 63.12.00 – Portali web

UNITÀ DI COMPETENZA – Analisi delle vulnerabilità software e hardware e della conformità alla normativa vigente
RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA Analizzare sistemi digitali, per le componenti hardware e software, dati ed operazioni, al fine di rilevarne rischi di sicurezza e vulnerabilità rispetto alle possibili minacce ed alla continuità di funzionamento ed integrità, individuando ed applicando metodi e norme di riferimento e supportando i relativi processi decisionali di adeguamento
LIVELLO E.q.f.: 6

CONOSCENZE

- Architettura hardware e software dei sistemi digitali
- Sistemi digitali ed ingegneria del software
- 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)
- 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)
- Fondamenti di organizzazione aziendale
- Fondamenti di project management
- Inglese tecnico per l'informatica

ABILITA'

- 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

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi digitali, all'insieme delle tipologie di potenziali minacce, considerando la criticità dei dati e delle operazioni processate da un determinato sistema, analizzarne i livelli di sicurezza– per le componenti hardware e software –,e identificare il livello di analisi del rischio informatico potenziale

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema digitale e con riferimento all'insieme delle potenziali minacce, sulla base delle indicazioni date, identificazione del livello di rischio potenziale e predisposizione e condivisione della reportistica associata

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Individuazione di soluzioni per la sicurezza dei sistemi hardware e software

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Individuare, considerando l'esito delle analisi dei rischi e delle vulnerabilità tecniche, processi e soluzioni a protezione del sistema digitale, agendo sulle diverse componenti e funzioni, mediante tecniche di configurazione degli specifici applicativi

LIVELLO E.q.f.: 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
- Elementi di architettura Zero Trust e cenni sull'autenticazione in ambito IoT
- Inglese tecnico per l'informatica

ABILITA'

- 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 (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

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA
Sulla base di indicazioni relative a tipologie di sistemi digitali ed all'insieme delle minacce applicabili, in coerenza con il piano di trattamento del rischio, in conformità con le normative cogenti ed i regolamenti interni, identificare le soluzioni ed i meccanismi per la protezione della rete
PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE
Per almeno una tipologia di sistema digitale e con riferimento all'insieme delle potenziali minacce, sulla base delle regole e dei processi interni, identificare, implementare, configurare e mantenere aggiornato un sistema per il controllo degli accessi e/o un sistema di protezione dei sistemi digitali o delle reti
MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA
Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Monitoraggio e supporto al ripristino della sicurezza dei sistemi hardware e software

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Monitorare lo stato di sicurezza dei sistemi digitali, verificando l'efficacia delle soluzioni di protezione adottate e intervenendo in caso di attacchi o malfunzionamenti, supportando il team nella fase di ripristino

LIVELLO E.q.f.: 6

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
- Inglese tecnico per l'informatica

ABILITA'

- 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 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

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi digitali e all'insieme delle minacce applicabili, in coerenza con il piano di gestione del rischio, individuare una procedura di esecuzione, mantenimento e restore dei backup in conformità con i piani di BC e/o DR qualora previsto e in particolare considerando l'esito della B.I.A.

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE
Per almeno una tipologia di sistema digitale, considerando il contesto ed il processo di riferimento anche in coerenza con quanto previsto dalla B.I.A., eseguire un test dei piani di Business Continuity o Disaster Recovery, precedentemente forniti, nonché le operazioni e le tecniche per il ripristino dei dati, tenendo in considerazione la normativa di riferimento, valutandone l'esito e identificando eventuali piani di rimedio
MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA
Audizione, colloquio tecnico e/o prova prestazionale

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.