ALLEGATO "1"

[K1.10] Cybersecurity Technician

Descrizione sintetica:
Il/La "Cybersecurity Technician" conosce i principali *framework* e le metodologie fondamentali nell'ambito della *cybersecurity governance.* Collabora alle attività di identificazione delle fonti di rischio per la sicurezza delle informazioni e di applicazione di soluzioni idonee al ripristino del corretto funzionamento dei sistemi e delle reti. Conosce le tecnologie "disruptive" abilitanti e di riconoscere le opportunità e i rischi ad esse correlati.

SISTEMI DI REFERENZIAZIONE	
Sistema di riferimento	**Denominazione**
Settore economico-professionale (S.E.P.)	Servizi digitali
Area/e di Attività (AdA) del Repertorio nazionale delle qualificazioni regionali a cui ilprofilo afferisce	[14.01.22] Gestione della Sicurezza dell'Informazione
Livello E.q.f.	5
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 – Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Supportare il team di lavoro nelle attività di analisi dei sistemi informativi, al fine di rilevare possibili minacce alla sicurezza delle informazioni ed eventuali disallineamenti rispetto alla normativa in vigore

LIVELLO E.q.f.: 5

CONOSCENZE

- Elementi di base di sicurezza informatica, ICT, cybersecurity ed Operational Technology
- I principi della sicurezza informatica (RID, minimo privilegio etc…)
- Framework normativo nazionale ed europeo in materia cybersecurity, information security e privacy
- Principali standard di riferimento per lo svolgimento di attività di auditing, assessment, risk assessment e risk management
- Metodologie di analisi delle vulnerabilità
- Strumenti per la verifica tecnica delle vulnerabilità e degli attacchi di rete
- Best practices, standards, frameworks e principi *dell'information security management*
- Standard e linee guida in materia di *Information Technology*, *Operation Tecnhnology* e protezione dei dati personali
- Fondamenti di processi ed organizzazione aziendale
- Il fattore umano nel contesto della cybersecurity

ABILITA'

- 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

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi informativi e del contesto organizzativo, riconoscere e segnalare l'insieme delle potenziali minacce applicabili ai sistemi informatici – per le componenti hardware e software – ai dati ed ai processi, individuando lo stato di conformità, con riferimento alle norme applicabili e gli elementi problematici

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE Per almeno una tipologia di sistema informatico e con riferimento all'insieme delle potenziali minacce e del contesto organizzativo, sulla base delle indicazioni date, individuazione delle norme applicabili, individuazione dei potenziali impatti delle minacce maggiormente rilevanti e definizione dei controlli essenziali per la protezione dei sistemi, dati e processi, inclusa la redazione di relativa reportistica
MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Supporto all'implementazione di soluzioni per la gestione di fattori di rischio all'interno dei sistemi e delle reti

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Supportare il team nell'implementazione, a seguito dell'analisi delle vulnerabilità, di soluzioni idonee ad arginare le minacce informatiche rilevate, tenendo conto del *framework* di riferimento

LIVELLO E.q.f.: 5

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*
- Principali ambienti cloud (MS Azure, AWS, Google Cloud)
- Elementi di infrastruttura IT (informatica, cloud, networking)

ABILITA'

- Riconoscere e 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 e divulgare le *best practices* per il miglioramento delle procedure di gestione della sicurezza
- Formalizzare gli standard e le linee guida in ambito cybersecurity

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi informativi e caratteristiche organizzative, impostare la definizione delle regole, dei ruoli e responsabilità, per garantire una corretta gestione della sicurezza del sistema, anche con riferimento alle norme applicabili

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema informatico e con riferimento ad un set di caratteristiche organizzative date, descrivere e motivare criticamente le scelte effettuate in merito alle regole per la protezione del sistema

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Utilizzare le tecnologie "disruptive" abilitanti nei diversi settori e aspetti in ambito security, riconoscendo ed informando rispetto ai rischi connessi al loro utilizzo

LIVELLO E.q.f.: 5

CONOSCENZE

- Rischi 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
- Inglese tecnico per l'informatica

ABILITA'

- 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"
- Comprendere, parlare, scrivere in inglese informatico

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di tecnologie "disruptive", descrivere le principali tipologie di minacce, le norme applicabili, e definire le contromisure ed operazioni tecniche da compiere, per garantire un adeguato livello di protezione dei sistemi

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema informatico e con riferimento ad un set di caratteristiche organizzative date, descrivere e motivare criticamente le scelte effettuate in merito alle regole per la protezione del sistema

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale