Denominazione Figura / Profilo / Obiettivo	Tecnico per la sicurezza delle reti
Professioni NUP/ISTAT correlate	• 2.1.1.5.4 - Specialisti in sicurezza informatica
Attività economiche di riferimento: ATECO 2007/ISTAT	• 62.01.00 - Produzione di software non connesso all'edizione (a cura della Regione) • 62.02.00 - Consulenza nel settore delle tecnologie dell'informatica • 62.09.09 - Altre attività dei servizi connessi alle tecnologie dell'informatica nca • 63.11.20 - Gestione database (attività delle banche dati) (a cura della Regione)
Area professionale	CULTURA INFORMAZIONE E TECNOLOGIE INFORMATICHE
Sottoarea professionale	Servizi di Informatica
Descrizione	Il Tecnico per la sicurezza delle reti opera per garantire che il sistema che permette lo scambio o condivisione di dati e risorse (sia hardware sia software) tra diversi calcolatori sia adeguatamente protetto rispetto ad usi inappropriati e minacce/intrusioni, garantendo al contempo una appropriata funzionalità della rete, archiviazione dei dati e preservando efficacemente la loro riservatezza. A partire da analisi sullo stato dell'architettura delle reti attuali e future e considerando anche le normative vigenti in materia di privacy e sicurezza informatica, identifica le necessità di protezione, concorre all'elaborazione di piani per la sicurezza ed alla progettazione dei meccanismi che assicurano la protezione delle reti, sia di natura tecnica sia di natura organizzativa. La figura in oggetto assicura la gestione operativa della sicurezza, monitorando e verificando il buon funzionamento delle reti, e concorre all' identificazione delle azioni, di natura formativa e informativa, necessarie perché il personale s i muova nel rispetto delle procedure per la sicurezza. Il Tecnico per la sicurezza delle reti possiede competenze tecnico - professionali collegate ai processi di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati di cui al Regolamento UE 2016/679 e delle Linee guida elaborate dal Gruppo di lavoro ex articolo 29 della direttiva 95/46 per la protezione dei dati (WP 29).

Livello EQF	5
Certificazione rilasciata	Specializzazione
Processo di lavoro caratterizzante la figura	Implementazione di misure di sicurezza dei sistemi informativi • A - Pianificazione/progettazione della sicurezza delle reti • B - Gestione operativa della sicurezza delle reti

PROCESSO DI LAVORO - ATTIVITÀ	COMPETENZE
A - Pianificazione/progettazione della sicurezza delle reti **ATTIVITÀ** • Analisi dell'architettura della rete per individuare i possibili punti di attacco a livello di hardware, software, processi di gestione ed informazioni • Valutazione di rischi e minacce alla sicurezza • Definizione degli standard e dei requisiti di sicurezza delle reti in base alle normative vigenti in materia di privacy e sicurezza informatica • Adeguamento dei sistemi alla normativa vigente • Elaborazione del documento di valutazione dei rischi per la sicurezza del sistema informativo • Identificazione dei security test da implementare per valutare l'efficacia della soluzioni tecniche adottate • Definizione dei piani di formazione/informazione al personale e a soggetti esterni sui sistemi di sicurezza	• 1 - Analizzare i rischi del sistema • 2 - Progettare le misure tecniche per la sicurezza del sistema informativo • 3 - Progettare le misure organizzative per la sicurezza del sistema informativo • 4 - Progettare le misure atte a soddisfare aspetti legali ed amministrativi legati alla sicurezza dei sistemi informativi

PROCESSO DI LAVORO - ATTIVITÀ	COMPETENZE
B - Gestione operativa della sicurezza delle reti **ATTIVITÀ** • Analisi degli accessi ai sistemi e gestione dei profili • Effettuazione di controlli sulla vulnerabilità e l'efficienza dei sistemi informativi • Gestione dei rischi operative • Implementazione di metriche sulla sicurezza informatica	• 5 - Gestire la sicurezza e manutenzione del sistema

COMPETENZE TECNICO PROFESSIONALI
• 1 - Analizzare i rischi del sistema • 2 - Progettare le misure tecniche per la sicurezza del sistema informativo • 3 - Progettare le misure organizzative per la sicurezza del sistema informativo • 4 - Progettare le misure atte a soddisfare aspetti legali ed amministrativi legati alla sicurezza dei sistemi informativi • 5 - Gestire la sicurezza e manutenzione del sistema

COMPETENZA N. 1
Analizzare i rischi del sistema

ABILITA' MINIME	COMPETENZA N. 1 CONOSCENZE ESSENZIALI
• Interagire in maniera efficace con i responsabili dei vari livelli decisionali, comunicando in maniera rapida e chiara gli elementi decisivi per le scelte strategiche in materia di sicurezza dei sistemi informativi • Analizzare i requisiti richiesti al sistema informativo dalle previsioni normative vigenti in materia di privacy e sicurezza informatica B6 • Analizzare l'architettura del sistema informativo per individuare i possibili attacchi • Individuare le vulnerabilità dell'architettura del sistema informativo • Elaborare un documento con la valutazione dei rischi per la sicurezza del sistema informativo, contenente l'analisi delle minacce e delle vulnerabilità individuate e delle possibili contromisure	• Architettura hardware e software dei sistemi di elaborazione elettronica, con particolare riferimento ai punti di forza e di debolezza in relazione alle esigenze di sicurezza e protezione dei dati • Fondamenti teorici della sicurezza dei sistemi informativi, per operare una corretta valutazione dei rischi legati alle componenti hardware e software del sistema • Protocolli, connessioni e apparecchiature di rete, per analizzare i rischi per la sicurezza legati alle componenti del sistema informativo dedicate al networking • Tipologia delle potenziali minacce all'integrità, riservatezza e disponibilità delle informazioni e delle risorse di una rete • Tecniche di monitoring & analysis dei rischi per la sicurezza di una rete • Inglese tecnico • Sicurezza sul lavoro: regole e modalità di comportamento generali e specifiche

COMPETENZA N. 2

Progettare le misure tecniche per la sicurezza del sistema informativo

ABILITA' MINIME	COMPETENZA N. 2 CONOSCENZE ESSENZIALI
• Identificare standard e requisiti per la sicurezza fisica delle reti e dei dati • Definire profili di accesso selettivi, individuali o per gruppi omogenei, 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, ecc.) • Definire i proxy, per garantire la sicurezza, la riservatezza e l'integrità delle connessioni tra client e server • Selezionare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema informativo e delle comunicazioni con l'esterno • Scegliere il software antivirus adeguato alle caratteristiche della rete e alle sue funzionalità • 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	• Network di connessione di IT devices (computers, mobile phones, periferiche) e punti di accesso (router, switch, ecc.) • Caratteristiche e funzionalità dei proxy, per controllare le connessioni e il traffico TCP (Transmission Control Protocol)/IP (Internet Protocol address), da client a server • Sistemi di autorizzazione degli accessi • Tipologie e logiche di funzionamento dei programmi creati per la violazione o il danneggiamento dei sistemi informativi (virus, worm, Trojan, malware, ecc.) • Caratteristiche e funzionalità dei programmi informatici di network scanning ed intrusion detection • Caratteristiche e funzionalità dei firewall • Tipologie e caratteristiche degli attacchi al sistema informativo a livello di IP (Internet Protocol address), TCP (Transmission Control Protocol)/UDP (User Datagram Protocol), protocollo applicativo, applicazione, utente • Inglese tecnico • Tecniche crittografiche e di cifratura • Sicurezza sul lavoro: regole e modalità di comportamento generali e specifiche • Normativa e principali aspetti legali di riferimento in ambito informatico

COMPETENZA N. 3

Progettare le misure organizzative per la sicurezza del sistema informativo

ABILITA' MINIME

- Definire gli strumenti, l'organizzazione, i ruoli e le responsabilità per la gestione della sicurezza del sistema informativo
- 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
- Pianificare attività di internal auditing per la verifica dell'adeguatezza delle misure di sicurezza adottate
- Individuazione delle necessità formative e informative del personale sulla sicurezza delle reti e la protezione dei dati

CONOSCENZE ESSENZIALI

- Tipologie dei possibili attacchi al sistema informativo
- Tecniche di backup e di restore dei sistemi informativi
- 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
- Metodologie per l'organizzazione per di un sistema di internal auditing
- Strumenti e tecnologie per la protezione fisica delle strutture
- Inglese tecnico
- Sicurezza sul lavoro: regole e modalità di comportamento generali e specifiche
- Normativa e principali aspetti legali di riferimento in ambito informatico

COMPETENZA N. 4

Progettare le misure atte a soddisfare aspetti legali ed amministrativi legati alla sicurezza dei sistemi informativi

ABILITA' MINIME

- Applicare procedure tecniche conformi alle normative vigenti per consentire l'accesso ai dati da parte del titolare o del responsabile del trattamento anche in assenza degli incaricati e di distruzione o perdita dei dati
- Elaborare e tenere aggiornato il Documento programmatico sulla Sicurezza (DPS) secondo le scadenze previste dal D.Lgs. 196/2003 (Codice sulla Privacy)
- Verificare in caso di outsourcing di parti del sistema informativo il rispetto delle norme vigenti in relazione al trattamento dei dati personali da parte dell'outsourcer
- Pianificare attività di internal auditing per la verifica dell'adeguatezza delle misure di sicurezza adottate
- Individuazione delle necessità formative e informative del personale sulla sicurezza delle reti e la protezione dei dati

CONOSCENZE ESSENZIALI

- Normativa in materia di privacy e sicurezza dei dati personali a livello nazionale (D. Lgs 196/2003 e successive modificazioni), ed europeo (Regolamento UE 2016/679, Linee guida WP29 e successive modificazioni)
- Responsabilità civili e penali connesse alla violazione della sicurezza informatica
- Normative in materia di copyright, diritto d'autore e tutela del software
- Tipologie di dati personali comuni e sensibili
- Inglese tecnico
- Sicurezza sul lavoro: regole e modalità di comportamento generali e specifiche

COMPETENZA N. 5

Gestire la sicurezza e manutenzione del sistema

ABILITA' MINIME	COMPETENZA N. 5	CONOSCENZE ESSENZIALI

- Installare e gestire apparecchiature di rete con specifico riguardo alla sicurezza
- Svolgere attività di internal auditing e verifica dell'adeguatezza delle misure di sicurezza adottate
- Testare periodicamente il funzionamento dei piani di Business Continuity e Disaster Recovery anche attraverso simulazioni di incidenti ed attacchi al sistema informativo
- Installare e gestire sistemi operativi (ad esempio: di tipo Linux, Microsoft) con particolare riguardo a networking e sicurezza
- Verificare l'aggiornamento, l'efficacia e l'efficienza del software antivirus installato per la protezione del sistema informativo
- Installare le patch di aggiornamento del sistema operativo e dei vari software di protezione del sistema informativo, dopo averne verificato l'autenticità e l'integrità
- Verificare l 'effettivo rispetto di tutte le misure di sicurezza tecniche ed organizzative definite da parte di tutte le funzioni aziendali interessate
- Ripristinare l'integrità, il corretto funzionamento ed il necessario livello di sicurezza in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo
- Controllare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo
- Gestire efficacemente le situazioni di crisi e di violazione del sistema informativo, riportando il sistema ad un corretto funzionamento, individuando i dati violati ed identificando se possibile gli autori della violazione

- Tecniche di attacco e metodologie di difesa dei sistemi informativi
- Sviluppo dei sistemi e delle nuove tecnologie per la sicurezza dei sistemi informativi
- Tecniche di risk management, per una corretta gestione dei rischi legati alla sicurezza del sistema informativo
- Strumenti di rafforzamento (hardening) dei servizi e dei protocolli di rete
- Metodologie e strumenti per l'effettuazione di penetration test
- Tecniche di social engineering,per individuare le vulnerabilità del sistema informativo ad attacchi che si basino sulle debolezze del fattore umano
- Inglese tecnico
- Sicurezza sul lavoro: regole e modalità di comportamento generali e specifiche
- Normativa e principali aspetti legali di riferimento in ambito informatico