Repertorio Regionale delle Qualificazioni e delle Competenze

Scheda di Figura Professionale

Denominazione Figura	TECNICO DELLA SICUREZZA INFORMATICA
Esempi di possibili denominazioni ricorrenti nel mondo del lavoro	
Settori di riferimento	SETTORE 14. Servizi digitali
Ambito di attività	Produzione di beni e servizi
Livello di complessità	Gruppo – Livello B
Livello EQF	4
Descrizione	Il Tecnico della sicurezza informatica è in grado di proporre e implementare soluzioni volte a garantire la protezione dei sistemi da possibili minacce e criticità di funzionamento, adeguate alle specifiche esigenze e conformi alle previsioni normative vigenti, gestendo le situazioni di crisi conseguenti a una violazione e fornendo supporto al committente per la definizione di procedure organizzative che permettano la piena efficacia e il mantenimento dei sistemi di sicurezza realizzati.

Contesto di esercizio

Tipologia rapporti di lavoro	La tipologia contrattuale più frequente è il rapporto di lavoro dipendente, a tempo indeterminato o determinato, non è escluso quello autonomo
Collocazione contrattuale	Nel caso di rapporto di lavoro dipendente, trova collocazione come impiegato di livello medio o medio-alto
Collocazione organizzativa	Può operare all'interno di aziende di medio-grandi dimensioni appartenenti a qualsiasi settore interessate ad assicurare un adeguato e semplice livello di interazione con i clienti, con i fornitori, con le community interessate all'attività dell'azienda. Può operare anche in proprio o all'interno di aziende fornitrici di servizi informatici o di consulenza in progetti presso aziende clienti.
Opportunità sul mercato del lavoro	In un mercato del lavoro in profonda trasformazione come quello odierno, le aziende avranno sempre più bisogno di professionisti in grado di comprendere le logiche degli ambienti e delle comunità digitali, appositamente formati per farlo e con skill tecniche piuttosto avanzate.
Percorsi formativi	Titolo di istruzione secondaria di secondo grado preferibilmente di indirizzo tecnico-informatico, oppure almeno 3 anni di esperienza lavorativa nell'attività professionale di riferimento
Fonti documentarie	

Indici di conversione

Sistemi di classificazione a fini statistici

ISCO - 08	
ISTAT Professioni (CP 2011)	2.1.1.5.4 Specialisti in sicurezza informatica
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

Repertori di descrizione

Repertorio nazionale delle figure per i percorsi IFTS	
Repertorio nazionale delle figure per i percorsi IeFP	

Elenco Aree di Attività

Denominazione AdA	ADA.14.01.18 – Sviluppo della Strategia per la Sicurezza Informatica (D1) ADA.14.01.22 - Gestione della Sicurezza dell'Informazione
Descrizione della performance	Definire e rimodulare le strategie e le politiche aziendali di Information Security, a partire dalla individuazione di standard e requisiti legali di riferimento, curando anche gli aspetti organizzativi relativi alla sua implementazione
UC	Rappresentazione del contesto informatico di intervento
Capacità-abilità	• Definire l'asset inventory allo scopo di mantenere in ordine e aggiornato l'elenco delle strumentazioni informatiche in dotazione hardware e software • Individuare gli elementi costitutivi dell'architettura del sistema informativo, tenuto conto della confidenzialità, disponibilità e integrità dei dati, al fine di identificare vulnerabilità e possibili punti di attacco al sistema o alle informazioni in es • Riconoscere i requisiti richiesti al sistema informativo dalle normative vigenti in materia di tutela dei dati e sicurezza informatica • Tradurre l'analisi delle minacce, delle vulnerabilità individuate e delle possibili contromisure in report di valutazione dei rischi per la sicurezza del sistema informativo
Conoscenze	• Architettura hardware e software dei sistemi digitali • Fondamenti teorici della sicurezza dei sistemi informativi • Metodologie di analisi dei rischi per la sicurezza di un sistema informativo • Protocolli, connessioni e apparecchiature di rete • Tipologia delle potenziali minacce all'integrità, riservatezza e disponibilità delle informazioni e delle risorse di un sistema informativo o di una rete • Principali riferimenti normativi in materia di tutela dei dati personali e sicurezza informatica • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza • La sicurezza sul lavoro: regole e modalità di comportamento (generali e specifiche)
Denominazione AdA	ADA.14.01.22 - Gestione della Sicurezza dell'Informazione
Descrizione della performance	Sviluppare le soluzioni tecniche di protezione dei sistemi informativi progettate e implementate
UC	Sviluppo di soluzioni tecniche di sicurezza informatica
Capacità-abilità	• Adottare procedure per l'installazione e configurazione di sistemi di sicurezza diversificati per garantire la protezione delle funzionalità e dei dati dei sistemi informativi (software antivirus o edr-endpoint detection and response, proxy e firewall, si • Definire azioni di rafforzamento dell'architettura della rete prevedendo zone demilitarizzate (dmz), per la protezione della rete informatica e del sistema informativo dai tentativi di attacco e violazione provenienti dall'esterno • Definire le credenziali di autenticazione per l'identificazione degli utenti autorizzati ad accedere al sistema informativo mediante le tecniche più appropriate (user-id, password, smart card, sistemi biometrici, ecc.) sulla base dei profili di accesso st • Individuare e utilizzare programmi per effettuare gli interventi di backup stabiliti (backup completo, incrementale, differenziale, remoto, ecc.) allo scopo di preservare i dati

Conoscenze	• Caratteristiche e funzionalità dei programmi informatici di network scanning ed intrusion detection • Tipologie e caratteristiche degli attacchi al sistema informativo a livello di ip, tcp/udp, protocollo applicativo, applicazione, utente • Tipologie e logiche di funzionamento dei programmi informatici creati per la violazione o il danneggiamento dei sistemi informativi (virus, worm, trojan, malware, ecc.) • Tecniche di backup e di ripristino dei sistemi informativi • Modelli di identity and access management system (iam) • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza • La sicurezza sul lavoro: regole e modalità di comportamento (generali e specifiche)
Denominazione AdA	ADA.14.01.22 – Gestione della Sicurezza dell'Informazione
Descrizione della performance	Applicare protocolli di controllo e affrontamento di criticità relative alla sicurezza del sistema informativo, dando corso all'esecuzione di piani di ripristino in caso di crisi. Implementare politiche di sicurezza informatica e tendere al loro miglioramento nel tempo anche effettuando analisi comparative e realizzando audit, test e simulazioni
UC	Gestione sicurezza informatica
Capacità-abilità	• Adottare procedure per il monitoraggio dei sistemi di sicurezza aziendale utilizzando sistemi di security information event management (siem) • Applicare i protocolli previsti per ristabilire integrità, funzionamento e livello di sicurezza del sistema informativo in seguito ad una violazione tentata o riuscita, adottando le opportune contromisure • Definire le procedure per bloccare le diverse possibili tipologie di attacco (attacchi denial of service, malware – spyware, backdoor, trojans, ecc.) adottando le tecniche più adeguate all'intervento da realizzare • Definire metodi e strumenti utili a valutare l'efficacia e l'efficienza dei piani di ripristino attraverso test periodici e simulazioni di incidenti e attacchi al sistema informativo
Conoscenze	• Fondamenti teorici della sicurezza dei sistemi informativi • Tipologia delle potenziali minacce all'integrità, riservatezza e disponibilità delle informazioni e delle risorse di un sistema informativo o di una rete • Principi di organizzazione e gestione della sicurezza informatica • Metodologie e strumenti per l'effettuazione di penetration test • Lingua inglese di settore • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza • La sicurezza sul lavoro: regole e modalità di comportamento (generali e specifiche)
Denominazione AdA	ADA.14.01.18 – Sviluppo della Strategia per la Sicurezza Informatica (D1) ADA.14.01.22 - Gestione della Sicurezza dell'Informazione
Descrizione della performance	Configurare policies organizzative di sicurezza definite e implementate
UC	Configurazione delle misure organizzative e di sicurezza informatica
Capacità-abilità	• Definire 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 inform • Definire ruoli, procedure e funzioni nel contesto di riferimento, al fine di organizzare una gestione efficace delle emergenze in caso di incidente o attacco informatico • Prefigurare modalità e tempi per la programmazione di un piano di audit e controlli sulla sicurezza, per verificare il livello di protezione del sistema informativo e ridurre i rischi di distruzione o perdita anche accidentale dei dati, accesso non autori • Stabilire le procedure per il controllo dei log, degli accessi e del traffico verso l'esterno, del sistema informativo
Conoscenze	• Principi di organizzazione e gestione della sicurezza informatica • Strumenti e tecnologie per la protezione fisica delle strutture e dei locali da possibili rischi ambientali • Principali riferimenti normativi in materia di tutela dei dati personali e

	sicurezza informatica • Principali modelli di business continuity plan • Principali modelli di disaster recovery plan • Principi comuni e aspetti applicativi della legislazione vigente in materia di sicurezza • La sicurezza sul lavoro: regole e modalità di comportamento (generali e specifiche)