# REPERTORIO DEI TITOLI E DELLE QUALIFICAZIONI DELLA REGIONE CAMPANIA

| QUALIFICAZIONE PROFESSIONALE | |
|---|---|
| **Denominazione qualificazione** | **Tecnico esperto di sicurezza informatica** |
| **Livello EQF** | 5 |
| **Settore Economico Professionale** | SEP 14 - Servizi digitali |
| **Area di Attività** | ADA.14.01.07 - Progettazione della User Experience |
| **Processo** | Sviluppo e gestione di prodotti e servizi digitali |
| **Sequenza di processo** | Progettazione di soluzioni ICT (Plan) |
| **Descrizione sintetica della qualificazione** | Il tecnico esperto di sicurezza informatica, nell'ambito di una organizzazione-cliente, identifica i rischi legati all'utilizzo di sistemi hardware e software e propone soluzioni volte a garantire un livello di sicurezza complessivo per il sistema informatico che risulti adeguato alle specifiche esigenze. Fornisce supporto al cliente per l'implementazione di tali soluzioni e la definizione di procedure organizzative che permettano la piena efficacia dei sistemi di sicurezza realizzati. Lavora generalmente presso aziende fornitrici di servizi informatici, di consulenza o presso aziende di medio-grandi dimensioni appartenenti a qualsiasi settore interessate ad assicurare un adeguato livello di sicurezza dei propri sistemi informatici. Può prestare la sua attività come dipendente o come lavoratore autonomo. Nello svolgimento del proprio lavoro opera con un ampio margine di autonomia e responsabilità operative, pur rispondendo del suo operato a soggetti che ricoprono ruoli di elevata responsabilità. |
| **Referenziazione ATECO 2007** | J.62.01.00 - Produzione di software non connesso all'edizione<br>J.62.02.00 - Consulenza nel settore delle tecnologie dell'informatica<br>J.62.03.00 - Gestione di strutture e apparecchiature informatiche hardware - housing (esclusa la riparazione)<br>J.62.09.09 - Altre attività dei servizi connessi alle tecnologie dell'informatica nca<br>J.63.11.30 - Hosting e fornitura di servizi applicativi (ASP) |
| **Referenziazione ISTAT CP2011** | 2.1.1.5.4 - Specialisti in sicurezza informatica |

**ELENCO DELLE UNITA' DI COMPETENZA**

1. Analisi dei rischi per la sicurezza dei sistemi hardware e software (2948)
2. Monitoraggio della sicurezza di sistemi hardware e software (2949)
3. Progettazione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software (2950)

| DETTAGLIO UNITA' DI COMPETENZA n.1 | |
|---|---|
| **Denominazione unità di competenza** | **Analisi dei rischi per la sicurezza dei sistemi hardware e software** |
| **Livello EQF** | 5 |
| **Descrizione della performance da osservare** | Rischi per la sicurezza dei sistemi hardware e software individuati ed analizzati |
| **Descrizione breve** | |
| **Abilità** | 1. Predisporre report sull'attività svolta<br>2. Predisporre report sui livelli di sicurezza dei sistemi<br>3. Analizzare le minacce rilevate<br>4. Progettare e applicare test di valutazione delle vulnerabilità mirato ai sistemi operativi e/o alle reti e/o ai data base<br>5. Simulare le fasi di un attacco al sistema<br>6. Individuare eventuali bug o imperfezioni nelle applicazioni<br>7. Individuare eventuali vulnerabilità di sistemi hardware e software |
| **Conoscenze** | 1. Inglese tecnico per l'informatica<br>2. Caratteristiche e funzionalità di software antivirus<br>3. Tecniche e sistemi di crittografia e cifratura<br>4. Tecniche e strumenti di rilevazione e prevenzione intrusioni<br>5. Organizzazione e gestione della sicurezza informatica<br>6. Principali tecniche di attacco alla sicurezza informatica<br>7. Sicurezza dei sistemi e delle reti informatiche<br>8. Normativa in materia di sicurezza informatica e relativa certificazione<br>9. Normativa in materia di protezione dei dati trattati con sistemi informatici |
| **Referenziazione ISTAT CP2011** | 2.1.1.5.1 - Specialisti in reti e comunicazioni informatiche<br>2.1.1.5.3 - Amministratori di sistemi<br>2.1.1.5.4 - Specialisti in sicurezza informatica |
| **Risultati attesi** | |
| **Attività** | |

| DETTAGLIO UNITA' DI COMPETENZA n.2 | |
|---|---|
| **Denominazione unità di competenza** | **Monitoraggio della sicurezza di sistemi hardware e software** |
| **Livello EQF** | 5 |
| **Descrizione della performance da osservare** | Sistemi hardware e software sicuri e funzionanti |
| **Descrizione breve** | |
| **Abilità** | 1. Utilizzare sistemi identity management system (ims)<br>2. Testare il funzionamento dei piani di business continuity e disaster recovery<br>3. Controllare il rispetto delle misure di sicurezza progettate<br>4. Ripristinare integrità, funzionamento e livello di sicurezza in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo<br>5. Adottare le opportune contromisure in caso di attacco alla sicurezza del sistema informativo (hardware e software)<br>6. Monitorare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo<br>7. Riconoscere e bloccare attacchi denial of service<br>8. Monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.)<br>9. Gestire le regole di firewall<br>10. Individuare ed eliminare malware (spyware, backdoor, trojans, ecc.)<br>11. Utilizzare tecniche e sistemi di crittografia e cifratura |
| **Conoscenze** | 1. Inglese tecnico per l'informatica<br>2. Tecniche e sistemi di crittografia e cifratura<br>3. Tecniche e strumenti di rilevazione e prevenzione intrusioni<br>4. Organizzazione e gestione della sicurezza informatica<br>5. Principali tecniche di attacco alla sicurezza informatica<br>6. Sicurezza dei sistemi e delle reti informatiche<br>7. Normativa in materia di sicurezza informatica e relativa certificazione<br>8. Normativa in materia di protezione dei dati trattati con sistemi informatici<br>9. Categorie di malware<br>10. Documenti di business continuity<br>11. Sistemi identity management system (ims)<br>12. Gestione degli accessi ai sistemi e alle reti<br>13. Tecniche di disaster recovery<br>14. Funzionamento dei firewall |
| **Referenziazione ISTAT CP2011** | 2.1.1.5.4 - Specialisti in sicurezza informatica<br>3.1.2.5.0 - Tecnici gestori di reti e di sistemi telematici |
| **Risultati attesi** | |
| **Attività** | |

| DETTAGLIO UNITA' DI COMPETENZA n.3 | |
|---|---|
| **Denominazione unità di competenza** | **Progettazione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software** |
| **Livello EQF** | 5 |
| **Descrizione della performance da osservare** | Soluzioni per la sicurezza dei sistemi hardware e software adeguatamente progettate e implementate |
| **Descrizione breve** | |
| **Abilità** | 1. Utilizzare programmi applicativi per effettuare l'intervento di back up individuato (back up completo, incrementale, differenziale, remoto, ecc.)<br>2. Utilizzare tecniche e sistemi di crittografia e cifratura<br>3. Installare le patch di aggiornamento dei vari software di protezione del sistema informativo<br>4. Creare zone demilitarizzate (dmz)<br>5. Implementare sistemi di honeypot<br>6. Progettare e istallare sistemi di intrusion detection<br>7. Applicare tecniche di recupero dati e disaster recovering<br>8. Interagire con altre professionalità coinvolte nella realizzazione/gestione di sistema informatico<br>9. Implementare e gestire sistemi di registrazione degli access log (log di accesso)<br>10. Individuare e implementare modalità per il controllo degli accessi (logging, accountability, ecc.)<br>11. Istallare e manutenere i server proxy<br>12. Testare i back up<br>13. Definire modalità e supporti da utilizzare per l'esecuzione del back up periodico e recupero dei dati<br>14. Installare e configurare software antivirus<br>15. Installare e configurare firewall |
| **Conoscenze** | 1. Inglese tecnico per l'informatica<br>2. Tecniche di back up e recupero dati<br>3. Caratteristiche e funzionalità di software antivirus<br>4. Tecniche e sistemi di crittografia e cifratura<br>5. Tecniche e strumenti di rilevazione e prevenzione intrusioni<br>6. Organizzazione e gestione della sicurezza informatica<br>7. Principali tecniche di attacco alla sicurezza informatica<br>8. Sicurezza dei sistemi e delle reti informatiche<br>9. Normativa in materia di sicurezza informatica e relativa certificazione<br>10. Normativa in materia di protezione dei dati trattati con sistemi informatici<br>11. Gestione degli accessi ai sistemi e alle reti<br>12. Tecniche di disaster recovery<br>13. Funzionamento dei firewall<br>14. Policies per la creazione di dms<br>15. Sistemi di honeypot<br>16. Sistemi di intrusion detection<br>17. Procedure di istallazione e manutenzione del server proxy<br>18. Protocolli di trasmissione dati (tcp/ip) |
| **Referenziazione ISTAT CP2011** | 2.1.1.5.4 - Specialisti in sicurezza informatica<br>3.1.2.5.0 - Tecnici gestori di reti e di sistemi telematici |
| **Risultati attesi** | |
| **Attività** | |