REPERTORIO DELLE QUALIFICAZIONI PROFESSIONALI DELLA REGIONE CAMPANIA

QUALIFICAZIONE PROFESSIONALE	
Denominazione qualificazione	**Tecnico esperto di sicurezza informatica**
Livello EQF	5
Settore Economico Professionale	SEP 16 - Servizi di informatica
Area di Attività	ADA.16.238.780 - Implementazione di misure di sicurezza dei sistemi informativi
Processo	Sviluppo e gestione di prodotti e servizi informatici
Sequenza di processo	Definizione e implementazione delle soluzioni di sviluppo in ambito ICT
Descrizione sintetica della qualificazione	Lo specialista in 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 o di consulenza o presso aziende di medio- grosse 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 suo lavoro opera con un ampio margine di autonomia e responsabilità operative, pur rispondendo del suo operato ad esperti che ricoprono ruoli di elevata responsabilità
Referenziazione ATECO 2007	J.62.01.00 - Produzione di software non connesso all'edizione J.62.02.00 - Consulenza nel settore delle tecnologie dell'informatica J.62.09.09 - Altre attività dei servizi connessi alle tecnologie dell'informatica nca J.63.11.20 - Gestione database (attività delle banche dati)
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	
Risultato atteso	Rischi per la sicurezza dei sistemi hardware e software individuati ed analizzati
Oggetto di osservazione	Le operazioni di analisi dei rischi per la sicurezza dei sistemi hardware e software.
Indicatori	Individuazione di vulnerabilità del sistema; progettazione di test di valutazione della vulnerabilità del sistema.
Abilità	1. predisporre report sull'attività svolta 2. predisporre report sui livelli di sicurezza dei sistemi 3. analizzare le minacce rilevate 4. progettare e applicare test di valutazione delle vulnerabilità mirato ai sistemi operativi e/o alle reti e/o ai data base 5. simulare le fasi di un attacco al sistema 6. individuare eventuali bug o imperfezioni nelle applicazioni 7. individuare eventuali vulnerabilità di sistemi hardware e software
Conoscenze	1. inglese tecnico per l'informatica 2. caratteristiche e funzionalità di software antivirus 3. tecniche e sistemi di crittografia e cifratura 4. tecniche e strumenti di rilevazione e prevenzione intrusioni 5. organizzazione e gestione della sicurezza informatica 6. principali tecniche di attacco alla sicurezza informatica 7. sicurezza dei sistemi e delle reti informatiche 8. normativa in materia di sicurezza informatica e relativa certificazione 9. normativa in materia di protezione dei dati trattati con sistemi informatici
Referenziazione ISTAT CP2011	

DETTAGLIO UNITA' DI COMPETENZA n.2	
Denominazione unità di competenza	**Monitoraggio della sicurezza di sistemi hardware e software**
Livello EQF	
Risultato atteso	Sistemi hardware e software sicuri ed in efficienza
Oggetto di osservazione	Le operazioni di monitoraggio della sicurezza di sistemi hardware e software.
Indicatori	Individuazione ed eliminazione corretta dei software malaware; corretta applicazione delle contromisure all'attacco subito al sistema.
Abilità	1. utilizzare sistemi identity management system (ims) 2. testare il funzionamento dei piani di business continuity e disaster recovery 3. controllare il rispetto delle misure di sicurezza progettate 4. ripristinare integrità, funzionamento e livello di sicurezza in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo 5. adottare le opportune contromisure in caso di attacco alla sicurezza del sistema informativo (hardware e software) 6. monitorare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo 7. riconoscere e bloccare attacchi denial of service 8. monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.) 9. gestire le regole di firewall 10. individuare ed eliminare malware (spyware, backdoor, trojans, ecc.) 11. utilizzare tecniche e sistemi di crittografia e cifratura
Conoscenze	1. inglese tecnico per l'informatica 2. tecniche e sistemi di crittografia e cifratura 3. tecniche e strumenti di rilevazione e prevenzione intrusioni 4. organizzazione e gestione della sicurezza informatica 5. principali tecniche di attacco alla sicurezza informatica 6. sicurezza dei sistemi e delle reti informatiche 7. normativa in materia di sicurezza informatica e relativa certificazione 8. normativa in materia di protezione dei dati trattati con sistemi informatici 9. categorie di malware 10. documenti di business continuity 11. sistemi identity management system (ims) 12. gestione degli accessi ai sistemi e alle reti 13. tecniche di disaster recovery 14. funzionamento dei firewall
Referenziazione ISTAT CP2011	

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	
Risultato atteso	Soluzioni per la sicurezza dei sistemi hardware e software adeguatamente progettate e implementate
Oggetto di osservazione	Le operazioni di progettazione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software.
Indicatori	Corretta installazione dei software antivirus, dei server proxy e dei firewall; corretta applicazione delle tecniche di back up, recupero dati e disater recovering.
Abilità	1. utilizzare programmi applicativi per effettuare l'intervento di back up individuato (back up completo, incrementale, differenziale, remoto, ecc.) 2. utilizzare tecniche e sistemi di crittografia e cifratura 3. istallare e configurare firewall 4. istallare e configurare software antivirus 5. installare le patch di aggiornamento dei vari software di protezione del sistema informativo 6. creare zone demilitarizzate (dmz) 7. implementare sistemi di honeypot 8. progettare e istallare sistemi di intrusion detection 9. applicare tecniche di recupero dati e disaster recovering 10. interagire con altre professionalità coinvolte nella realizzazione/gestione di sistema informatico 11. implementare e gestire sistemi di registrazione degli access log (log di accesso) 12. individuare e implementare modalità per il controllo degli accessi (logging, accountability, ecc.) 13. istallare e manutenere i server proxy 14. testare i back up 15. definire modalità e supporti da utilizzare per l?esecuzione del back up periodico e recupero dei dati
Conoscenze	1. inglese tecnico per l'informatica 2. tecniche di back up e recupero dati 3. caratteristiche e funzionalità di software antivirus 4. tecniche e sistemi di crittografia e cifratura 5. tecniche e strumenti di rilevazione e prevenzione intrusioni 6. organizzazione e gestione della sicurezza informatica 7. principali tecniche di attacco alla sicurezza informatica 8. sicurezza dei sistemi e delle reti informatiche 9. normativa in materia di sicurezza informatica e relativa certificazione 10. normativa in materia di protezione dei dati trattati con sistemi informatici 11. gestione degli accessi ai sistemi e alle reti 12. tecniche di disaster recovery 13. funzionamento dei firewall 14. policies per la creazione di dms 15. sistemi di honeypot 16. sistemi di intrusion detection 17. procedure di istallazione e manutenzione del server proxy 18. protocolli di trasmissione dati (tcp/ip)
Referenziazione ISTAT CP2011	