REPERTORIO
DELLE QUALIFICAZIONI PROFESSIONALI DELLA REGIONE CAMPANIA

SETTORE ECONOMICO PROFESSIONALE[1] ***Servizi di informatica***	
Processo	Sviluppo e gestione di prodotti e servizi informatici
Sequenza di processo	Definizione e implementazione delle soluzioni di sviluppo in ambito ICT
Area di Attività	ADA.16.238.780 Implementazione di misure di sicurezza dei sistemi informativi
Qualificazione regionale	Tecnico esperto di sicurezza informatica
Referenziazioni	Nomenclatura delle unità Professionali (NUP/CP ISTAT 2006): 2.1.1.4.4 Specialisti in sicurezza informatica Nomenclatura delle unità Professionali (NUP/CP ISTAT 2011): 2.1.1.5.4 Specialisti in sicurezza informatica
	Classificazione delle attività economiche (ATECO 2007/ISTAT): 62.02.00 Consulenza nel settore delle tecnologie dell'informatica 62.09.09 Altre attività dei servizi connessi alle tecnologie dell'informatica nca 62.01.00 Produzione di software non connesso all'edizione 63.11.20 Gestione database (attività delle banche dati)
Livello EQF	5
Descrizione sintetica della qualificazione e delle attività	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

[1] *Rif. Accordo Stato-Regioni del 27 luglio 2011*

STANDARD DELLE COMPETENZE TECNICO-PROFESSIONALI CARATTERIZZANTI LA QUALIFICAZIONE

COMPETENZA N. 1 - Titolo Analisi dei rischi per la sicurezza dei sistemi hardware e software	
Risultato atteso Rischi per la sicurezza dei sistemi hardware e software individuati ed analizzati	
Abilità	**Conoscenze**
• predisporre report sull'attività svolta • predisporre report sui livelli di sicurezza dei sistemi • analizzare le minacce rilevate • progettare e applicare test di valutazione delle vulnerabilità mirato ai sistemi operativi e/o alle reti e/o ai data base • simulare le fasi di un attacco al sistema • individuare eventuali bug o imperfezioni nelle applicazioni • individuare eventuali vulnerabilità di sistemi hardware e software	• caratteristiche e funzionalità di software antivirus • tecniche e sistemi di crittografia e cifratura • tecniche e strumenti di rilevazione e prevenzione intrusioni • organizzazione e gestione della sicurezza informatica • principali tecniche di attacco alla sicurezza informatica • sicurezza dei sistemi e delle reti informatiche • normativa in materia di sicurezza informatica e relativa certificazione • normativa in materia di protezione dei dati trattati con sistemi informatici • inglese tecnico per l'informatica

Indicazioni per la valutazione delle competenze

Titolo competenza e Risultato atteso	Oggetto di osservazione	Indicatori
Analisi dei rischi per la sicurezza dei sistemi hardware e software. Rischi per la sicurezza dei sistemi hardware e software individuati ed analizzati.	Le operazioni di analisi dei rischi per la sicurezza dei sistemi hardware e software.	Individuazione di vulnerabilità del sistema; progettazione di test di valutazione della vulnerabilità del sistema.

STANDARD DELLE COMPETENZE TECNICO-PROFESSIONALI CARATTERIZZANTI LA QUALIFICAZIONE

COMPETENZA N. 2 - Titolo Monitoraggio della sicurezza di sistemi hardware e software	
Risultato atteso Sistemi hardware e software sicuri ed in efficienza	
Abilità	**Conoscenze**
• utilizzare sistemi identity management system (ims) • testare il funzionamento dei piani di business continuity e disaster recovery • controllare il rispetto delle misure di sicurezza progettate • ripristinare integrità, funzionamento e livello di sicurezza in seguito ad una violazione tentata o riuscita della sicurezza del sistema informativo • adottare le opportune contromisure in caso di attacco alla sicurezza del sistema informativo (hardware e software) • monitorare e bloccare il traffico interno ed esterno che costituisca una potenziale minaccia alla sicurezza del sistema informativo • riconoscere e bloccare attacchi denial of service • monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.) • gestire le regole di firewall • individuare ed eliminare malware (spyware, backdoor, trojans, ecc.) • utilizzare tecniche e sistemi di crittografia e cifratura	• categorie di malware • documenti di business continuity • sistemi identity management system (ims) • gestione degli accessi ai sistemi e alle reti • tecniche e sistemi di crittografia e cifratura • tecniche e strumenti di rilevazione e prevenzione intrusioni • organizzazione e gestione della sicurezza informatica • principali tecniche di attacco alla sicurezza informatica • sicurezza dei sistemi e delle reti informatiche • normativa in materia di sicurezza informatica e relativa certificazione • tecniche di disaster recovery • normativa in materia di protezione dei dati trattati con sistemi informatici • funzionamento dei firewall • inglese tecnico per l'informatica

Indicazioni per la valutazione delle competenze

Titolo competenza e Risultato atteso	Oggetto di osservazione	Indicatori
Monitoraggio della sicurezza di sistemi hardware e software. Sistemi hardware e software sicuri ed in efficienza.	Le operazioni di monitoraggio della sicurezza di sistemi hardware e software.	Individuazione ed eliminazione corretta dei software malaware; corretta applicazione delle contromisure all'attacco subito al sistema.

STANDARD DELLE COMPETENZE TECNICO-PROFESSIONALI CARATTERIZZANTI LA QUALIFICAZIONE

COMPETENZA N. 3 - Titolo Progettazione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software	
Risultato atteso Soluzioni per la sicurezza dei sistemi hardware e software adeguatamente progettate e implementate	
Abilità	**Conoscenze**
• istallare e configurare firewall • istallare e configurare software antivirus • installare le patch di aggiornamento dei vari software di protezione del sistema informativo • utilizzare tecniche e sistemi di crittografia e cifratura • creare zone demilitarizzate (dmz) • implementare sistemi di honeypot • progettare e istallare sistemi di intrusion detection • applicare tecniche di recupero dati e disaster recovering • interagire con altre professionalità coinvolte nella realizzazione/gestione di sistema informatico • implementare e gestire sistemi di registrazione degli access log (log di accesso) • individuare e implementare modalità per il controllo degli accessi (logging, accountability, ecc.) • istallare e manutenere i server proxy • utilizzare programmi applicativi per effettuare l'intervento di back up individuato (back up completo, incrementale, differenziale, remoto, ecc.) • testare i back up • definire modalità e supporti da utilizzare per l?esecuzione del back up periodico e recupero dei dati	• policies per la creazione di dms • sistemi di honeypot • sistemi di intrusion detection • gestione degli accessi ai sistemi e alle reti • caratteristiche e funzionalità di software antivirus • tecniche e sistemi di crittografia e cifratura • tecniche e strumenti di rilevazione e prevenzione intrusioni • organizzazione e gestione della sicurezza informatica • principali tecniche di attacco alla sicurezza informatica • sicurezza dei sistemi e delle reti informatiche • normativa in materia di sicurezza informatica e relativa certificazione • tecniche di disaster recovery • procedure di istallazione e manutenzione del server proxy • normativa in materia di protezione dei dati trattati con sistemi informatici • protocolli di trasmissione dati (tcp/ip) • funzionamento dei firewall • tecniche di back up e recupero dati • inglese tecnico per l'informatica

Indicazioni per la valutazione delle competenze

Titolo competenza e Risultato atteso	Oggetto di osservazione	Indicatori
Progettazione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software. Soluzioni per la sicurezza dei sistemi hardware e software adeguatamente progettate e implementate.	Le operazioni di progettazione e implementazione di soluzioni per la sicurezza dei sistemi hardware e software.	Corretta installazione dei software antivirus, dei server proxy e dei firewall; corretta applicazione delle tecniche di back up, recupero dati e disater recovering.