PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296

APPENDICE 3B - PROFILI PROFESSIONALI LOTTO 2

Indice

PREMESSA

Il presente documento è redatto sulla base del framework E-CF (European Competence Framework)[1] del Comitato Europeo di Normazione (CEN) e del documento "Competenze Digitali"[2] emesso da AgID nel dicembre 2019 e disponibile anche in Docs Italia.

I profili inseriti, come indicato, fanno riferimento, per le competenze, ai profili di seconda generazione (dei lavori del CEN) e ai profili professionali dedicati alla sicurezza informatica

Per tutti i profili, conoscenze ed abilità sono stati predisposti con l'obiettivo di integrare le professionalità "standard" al contesto della Cyber security come previsto dal Piano Triennale e dalla normativa di settore.
Trattasi di requisiti minimi che dovranno evolversi nel contesto delle migliori professionalità presenti nel settore della Cyber security per sostenere la protezione dei perimetri di sicurezza delle PA, a tutela della protezione del Paese.

Le figure professionali necessarie per lo svolgimento dei servizi di Compliance e controllo dovranno aderire ai profili di seguito descritti.

Il presente documento considera le esigenze di servizi in ambito Cyber security espresse sulla base del Codice dell'Amministrazione Digitale, del Piano Triennale per l'informatica nella Pubblica Amministrazione che sulla normativa relativa al perimetro di sicurezza nazionale cibernetica; pertanto ciascun profilo professionale si riferisce a risorse professionali con ampia esperienza, competenza funzionale e tecnica per l'ambito del lotto e non ad una singola persona. Tali competenze dovranno essere costantemente aggiornate all'evoluzione della tecnologia, normativa e organizzativa della Cyber security nonchè degli standard, delle linee guida e best practices applicabili.

I curriculum vitae delle figure professionali da impiegare nei vari servizi dovranno essere resi disponibili alla Amministrazione secondo quanto previsto dalle Condizioni di fornitura, rispettando lo schema di CV Europeo o diversi template indicati dall'Amministrazione. In ogni caso, dovranno essere particolarmente dettagliate le competenze/conoscenze/esperienze tecniche al fine di verificare la corrispondenza con i requisiti minimi, gli eventuali requisiti migliorativi offerti e il contesto dell'Amministrazione.
Nel presente documento, e laddove citati nelle Condizioni di fornitura e nell'Appendice 3, ogni riferimento ad attività o metodologie basate sull'adozione di prodotti e ogni riferimento a prodotti vanno intesi in relazione ai prodotti e/o ai componenti di tali prodotti che sono effettivamente adottati per i sistemi informatici gestiti dalla singola Amministrazione.
Le competenze e conoscenze tecniche delle figure che seguono non sono esaustive delle esigenze future. Infatti le competenze iniziali potranno variare in funzione dell'evoluzione tecnologica e in relazione a ulteriori tematiche, prodotti, sistemi e metodologie che emergeranno durante la validità dell'AQ e dei contratti attuativi. A tal fine, la presente appendice potrà essere aggiornata nel corso della vigenza dell'AQ e dei contratti esecutivi, in accordo tra le parti, su richiesta degli Organismi di coordinamento e controllo, anche eventualmente sentita/e una o più amministrazioni contraenti, e/o dei Fornitori.
Si precisa che:

[1] http://www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_IT.pdf
[2] https://www.agid.gov.it/it/agenzia/competenze-digitali

- fatto salvo il possesso del diploma di scuola media superiore, i requisiti accademici richiesti per ogni figura (titoli di studio) possono essere utilmente soddisfatti attraverso il possesso di una cultura equivalente, maturata attraverso lo svolgimento di esperienze lavorativo-professionali, pari a:
  - **5 (cinque) anni aggiuntivi nel settore ICT nel caso di laurea magistrale specialistica;**
  - **3 (tre) anni aggiuntivi nel settore ICT nel caso di laurea triennale;**
- le certificazioni possedute dalle risorse per ciascun ruolo dovranno essere mantenute aggiornate e in corso di validità per tutta la durata contrattuale e seguendo l'evoluzione del prodotto/tecnologia a cui si riferiscono;
- una certificazione può, nei casi espressamente autorizzati dall'Amministrazione, essere sostituita da comprovate esperienze di almeno 4 anni sul prodotto/tecnologia oggetto della certificazione (resta fermo in ogni caso il possesso delle certificazioni espressamente offerte in AQ dal fornitore).

Il piano dei Fabbisogni dell'Amministrazione sarà corredato dalla descrizione del contesto IT tecnologico e applicativo attuale e futuro di riferimento. Nell'ambito del Piano Operativo predisposto dal fornitore, saranno declinati i profili professionali in coerenza con l'ambiente di riferimento.

1. SECURITY PRINCIPAL

Titolo del profilo	SECURITY PRINCIPAL		
Descrizione sintetica	Figura professionale dedicata alla gestione di progetti per raggiungere la performance ottimale conforme alle specifiche originali.		
Missione	Definisce, implementa e gestisce progetti dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.		
Principali Task	• Valutazione (stima di tempi / costi / rischi / risorse), pianificazione, realizzazione e monitoraggio dei progetti IT nel dominio della Cyber security. • Organizzazione, coordinamento e conduzione di team di progetto per l'erogazione dei servizi. • Supervisione delle milestone di progetto e del suo andamento complessivo. • Coordinamento, registrazione e monitoraggio della conformità alla qualità. • Diffusione e distribuzione delle informazioni di progetto e relazione con il committente. • Pianificazione e coordinamento delle attività relative ai servizi di Compliance e controllo. • Assicurazione della conformità dei deliverable di progetto alle specifiche tecniche. • Aggiornamento del piano di progetto secondo i cambiamenti del contesto ed i mutevoli accadimenti. • Coordinamento del team di lavoro applicando metodologia e strumenti di lavoro per raggiungere un flusso di lavoro ottimale attraverso il continuo miglioramento delle attività. • Governo dei progetti di analisi della postura del sistema di sicurezza con gruppi di progetto di medie e grandi dimensioni. • Stima di risorse ed effort per la gestione dei progetti utilizzando metodologia e tecniche di project management.		
Competenze	A.2.	Gestione dei Livelli di Servizio	Livello 3
	A.3.	Sviluppo del Business Plan	Livello 3
	D.8.	Gestione del Contratto	Livello 4
	E.2.	Project and Portfolio Management	Livello 4
	E.3.	Gestione del Rischio	Livello 4
	E.4.	Gestione delle Relazioni	Livello 4
	E.7.	Business Change Management	Livello 4
Conoscenze	• Conoscenza della normativa di riferimento in ambito di appalti pubblici. • Conoscenza della normativa di riferimento in materia di CAD, Crescita Digitale e di Piano Triennale con focus sull'ambito Cyber Security. • Conoscenza della normativa e Linee Guida AgiD di settore in materia di Sicurezza Informatica. • Conoscenza della normativa in materia di privacy.		

	• Conoscenza approfondita delle metodologie e processi di Security Governance e Security Management. • Conoscenza approfondita delle tecniche di problem solving e di risk management • Conoscenza approfondita delle metodologie di vulnerability assessment, penetration test, compliance management e Security Audit. • Disegno e nella valutazione dei sistemi per la gestione della sicurezza delle informazioni. • Conoscenza delle metodologie e degli strumenti operativi richiesti in progetti di IT Security. • Conoscenza dei processi e delle procedure operative IT. • Conoscenza delle tecnologie principali per la sicurezza IT. • Conoscenza dei modelli di servizio del Cloud computing (IaaS, PaaS, SaaS) e le principali architetture cloud-native. • ISO/IEC 27018:2014 – Gestione della privacy nel cloud. • Conoscenza approfondita dei principali framework di service management quali ITIL, COBIT, CMMI.
Abilità	• Capacità nel tradurre i principali elementi di un piano strategico di sicurezza in requisiti funzionali per lo sviluppo dei servizi ICT. • Capacità nella identificazione dei requisiti per i processi collegati ai servizi ICT e formalizza i requisiti dell'utente. • Capacità di gestione dell'ambiente dei dati comuni, processi e procedure, convalidando le conformità e le non conformità. • Capacità di gestire progetti su piattaforme di erogazione servizi da remoto con elevato grado di integrazione tra sistemi informativi (modelli ibridi). • Capacità di mantenere il modello informativo per soddisfare gli standard di integrità e sicurezza in conformità ai requisiti degli utenti. • Capacità di governare l'interazione e di gestire il rapporto con le Amministrazioni.
Certificazioni	Possesso della **certificazione CISM (Certified Information Security Manager)**.
Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente.
Anzianità lavorativa	Minimo 10 anni da computarsi successivamente alla data di conseguimento della laurea, di cui almeno 5 nella funzione.

2. SENIOR INFORMATION SECURITY CONSULTANT

Titolo del profilo	SENIOR INFORMATION SECURITY CONSULTANT
Descrizione sintetica	Figura professionale di riferimento per insiemi definiti di attività e progetti collegate alla gestione della sicurezza delle informazioni.

<table>
<tr><td>Missione</td><td colspan="3">Presidia l’attuazione della strategia definita all’interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo.
Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni.
Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.</td></tr>
<tr><td>Principali Task</td><td colspan="3">• Coordinamento di figure professionali Junior.
• Controllo delle reti dell’organizzazione per rilevare violazioni della sicurezza e indagare quando si verifica.
• Esperienza nell’utilizzo di software, quali firewalls e programmi di data encryption per proteggere informazioni sensibili.
• Elaborazione di documentazione e reportistica relativa a violazioni di sicurezza e la valutazione del danno da questa causato.
• Esperienza in Penetration Test, ovvero quando gli analisti simulano gli attacchi per cercare le vulnerabilità nei loro sistemi prima che possano essere sfruttate.
• Ricerche sugli ultimi trend in materia di Sicurezza ICT.
• Pianificazione e realizzazione di un modello con cui un'organizzazione gestisce la sicurezza informatica.
• Adozione e sviluppo di standard di Sicurezza e di best practices per l’organizzazione.
• Identificazione delle raccomandazioni di sicurezza al management o al personale IT.
• Supporta gli utenti quando devono installare o conoscere nuovi prodotti e procedure di sicurezza.</td></tr>
<tr><td rowspan="7">Competenze e-CF assegnate</td><td>A.7.</td><td>Monitoraggio dei trend tecnologici</td><td>Livello 4</td></tr>
<tr><td>B.2.</td><td>Integrazione dei componenti</td><td>Livello 4</td></tr>
<tr><td>B.3.</td><td>Testing</td><td>Livello 4</td></tr>
<tr><td>C.4.</td><td>Gestione del problema</td><td>Livello 4</td></tr>
<tr><td>D.1.</td><td>Sviluppo della strategia per la Sicurezza informatica</td><td>Livello 4</td></tr>
<tr><td>E.8.</td><td>Gestione della sicurezza dell’informazione</td><td>Livello 4</td></tr>
<tr><td>E.9.</td><td>Governance dei sistemi informativi</td><td>Livello 4</td></tr>
<tr><td>Conoscenze</td><td colspan="3">• Conoscenza approfondita delle metodologie di vulnerability assessment, penetration test, compliance management e Security Audit.
• Conoscenza approfondita delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente.
• Conoscenza approfondita di network security (firewall, web application firewall, IPS, Network access control).
• Conoscenza approfondita delle metodologie e degli strumenti operativi richiesti in progetti di IT Security.
• Conoscenza approfondita di security events (SIEM, IDS, End Point).
• Conoscenza dei processi e delle procedure operative IT.</td></tr>
</table>

	• Conoscenza delle tecnologie principali per la sicurezza IT. • Conoscenza approfondita delle metodologie e linee guida ISO in materia di Risk Assessment e Risk Treatment e degli strumenti a supporto delle fasi di gestione del rischio. • Conoscenza dei sistemi SGSI in accordo con la norma ISO 27001. • Conoscenza dei modelli per l'analisi del rischio. • Conoscenza della normativa e linee Guida AgiD di settore in materia di Sicurezza Informatica. • Conoscenza della normativa in materia di privacy. • Conoscenza delle policy e linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. gestione del rischio, classificazione delle informazioni, gestione degli incidenti, utilizzo sicure dei servizi informatici).
Abilità	• Capacità di coordinamento di figure professionali Junior. • Capacità di redazione di documentazione a supporto dei processi di compliance rispetto alle normative applicabili (es. Documento programmatico della sicurezza, Studio di fattibilità per la continuità operativa...). • Capacità di redazione di documentazione tecnica e di progetto. • Capacità di studio dei sistemi e delle reti di computer e di valutare i rischi per determinare come migliorare le politiche e i protocolli di sicurezza. • Capacità di correlare i cambiamenti dei sistemi informatici con gli attacchi informatici possono essere difficili da rilevare. • Capacità di anticipare i rischi per la sicurezza delle informazioni e implementare nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni. • Capacità di rispondere agli avvisi di sicurezza, scoprire e correggere i difetti nei sistemi e nelle reti di computer.
Certificazioni	Possesso della qualifica di **Lead Auditor ISO 27001** aggiornata all'ultima release, per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.
Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente.
Anzianità lavorativa	Minimo 8 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 4 nella funzione.

3. JUNIOR INFORMATION SECURITY CONSULTANT

Titolo del profilo	JUNIOR INFORMATION SECURITY CONSULTANT
Descrizione sintetica	Figura professionale di riferimento per insiemi definiti di attività e progetti collegate alla gestione della sicurezza delle informazioni.
Missione	Contribuisce nell'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) partecipando al ruolo di raccordo tra la struttura di governance della Cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Attua misure di sicurezza per proteggere le reti e i sistemi informatici di una

<table>
<tr><td></td><td colspan="3">organizzazione.</td></tr>
<tr><td>Principali Task</td><td colspan="3">Partecipazione al controllo delle reti dell’organizzazione per rilevare violazioni della sicurezza e indagare quando si verifica.
Utilizzo del software, quali firewalls, web application firewalls e programmi di data encryption per proteggere informazioni sensibili.
Collaborazione nella stesura documentazione e reportistica relativa a violazioni di sicurezza e la valutazione del danno da questa causato.
Partecipazione alla effettuazione dei test di penetrazione, ovvero quando gli analisti simulano gli attacchi per cercare le vulnerabilità nei loro sistemi prima che possano essere sfruttate.
Aiuto nella pianificazione e realizzare un modello con cui un'organizzazione gestisce la sicurezza informatica.
Partecipazione nell’adozione di standard di Sicurezza e di best practices per l’organizzazione.
Attuazione delle raccomandazioni di sicurezza al management o al personale IT
Supporto agli utenti quando devono installare o conoscere nuovi prodotti e procedure di sicurezza.</td></tr>
<tr><td></td><td>B.2.</td><td>Integrazione dei componenti</td><td>Livello 3</td></tr>
<tr><td></td><td>B.3.</td><td>Testing</td><td>Livello 3</td></tr>
<tr><td></td><td>C.4.</td><td>Gestione del problema</td><td>Livello 3</td></tr>
<tr><td></td><td>D.1.</td><td>Sviluppo della strategia per la Sicurezza informatica</td><td>Livello 2</td></tr>
<tr><td></td><td>E.8.</td><td>Gestione della sicurezza dell’informazione</td><td>Livello 3</td></tr>
<tr><td></td><td>E.9.</td><td>Governance dei sistemi informativi</td><td>Livello 2</td></tr>
<tr><td>Conoscenze</td><td colspan="3">Conoscenza delle metodologie di vulnerability assessment, penetration test, compliance management e Security Audit.
Conoscenza delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente.
Conoscenza di network security (firewall, web application firewall, IPS, Network access control, pila TCP/IP).
Conoscenza delle metodologie e linee guida ISO in materia di Risk Assessment e Risk Treatment e degli strumenti a supporto delle fasi di gestione del rischio.
Conoscenza acquisita dalla partecipazione a progetti di Risk Assessment.
Conoscenza acquisita dalla partecipazione alla definizione di modelli per l’analisi del rischio.
Conoscenza della normativa e linee Guida AgiD di settore in materia di Sicurezza Informatica.
Conoscenza della normativa in materia di privacy.
Conoscenza delle policy e linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. gestione del rischio, classificazione delle informazioni, gestione degli incidenti, utilizzo sicure dei servizi informatici).</td></tr>
<tr><td>Abilità</td><td colspan="3">Capacità di contribuire alla redazione di documentazione a supporto dei</td></tr>
</table>

	processi di compliance rispetto alle normative applicabili (es. Documento programmatico della sicurezza, Studio di fattibilità per la continuità operativa...). • Capacità di contribuire alla redazione di documentazione tecnica e di progetto. • Capacità di partecipare allo studio dei sistemi e delle reti di computer per la valutazione dei rischi per determinare come migliorare le politiche e i protocolli di sicurezza. • Capacità di contribuire alla correlazione dei cambiamenti dei sistemi informatici con gli attacchi informatici possono essere difficili da rilevare. • Capacità di supporto nell'anticipare i rischi per la sicurezza delle informazioni e nell'implementare nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni. • Capacità di collaborare nella risposta agli avvisi di sicurezza, nella correzione dei difetti nei sistemi e nelle reti di computer.
Certificazioni	N/A
Titolo di studio	Laurea triennale in materie scientifiche o cultura equivalente.
Anzianità lavorativa	Minimo 4 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 2 nella funzione

4. SECURITY SOLUTION ARCHITECT

Titolo del profilo	SECURITY SOLUTION ARCHITECT
Descrizione sintetica	Figura professionale dedicata al mantenimento della sicurezza del sistema informatico di un organizzazione.
Missione	Progetta, costruisce, esegue test e implementa i sistemi di sicurezza all'interno della rete IT di un'organizzazione. Ha l'obiettivo di anticipare tutte le potenziali mosse e tattiche che eventuali criminali possono utilizzare per cercare di ottenere l'accesso non autorizzato al sistema informatico tramite la progettazione di un'architettura di rete sicura.

<table>
<tr><td>Principali Task</td><td colspan="3">Analisi dell'infrastruttura IT e delle relazioni tra i differenti sistemi e componenti infrastrutturali volta all’individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza.
Analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l’infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza).
Verifica dell’efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un’infrastruttura IT complessa.
Analisi dell’efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT mediante uso di metodologie e strumenti operativi.
Identificazione di soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per traguardare la piena adozione delle contromisure previste.
Adozione delle tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento.
Adozione di sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione.
Adozione di sistemi di autenticazione, sistemi di Identity & Access Management con esperienza di integrazione.</td></tr>
<tr><td rowspan="6">Competenze e-CF assegnate</td><td>B.2.</td><td>Integrazione dei componenti</td><td>Livello 4</td></tr>
<tr><td>B.3.</td><td>Testing</td><td>Livello 4</td></tr>
<tr><td>B.6.</td><td>Ingegneria dei sistemi</td><td>Livello 4</td></tr>
<tr><td>C.2.</td><td>Supporto alle modifiche/evoluzioni del sistema</td><td>Livello 4</td></tr>
<tr><td>D.1.</td><td>Sviluppo della strategia per la Sicurezza informatica</td><td>Livello 3</td></tr>
<tr><td>E.8.</td><td>Gestione della sicurezza dell’informazione</td><td>Livello 4</td></tr>
<tr><td></td><td>E.9.</td><td>Governance dei sistemi informativi</td><td>Livello 4</td></tr>
<tr><td>Conoscenze</td><td colspan="3">Conoscenza approfondita delle infrastrutture IT, delle relazioni tra i differenti sistemi e componenti infrastrutturali volta all’individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza.
Conoscenza approfondita delle configurazioni, delle regole tecniche e delle principali soluzioni di sicurezza utilizzate per proteggere l’infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza).
Conoscenza approfondita delle problematiche di sicurezza delle infrastrutture IT.
Conoscenza delle metodologie e degli strumenti operativi richiesti per verificare l’efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT.
Conoscenza approfondita delle tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento.</td></tr>
</table>

	• Conoscenza approfondita dei sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione. • Conoscenza approfondita dei sistemi di autenticazione, sistemi di Identity & Access Management con esperienza di integrazione.
Abilità	• Capacità di comprendere l'infrastruttura IT, le relazioni tra i differenti sistemi e componenti infrastrutturali volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza • Capacità di analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza); • Capacità di verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT mediante uso di metodologie e strumenti operativi. • Capacità di utilizzo delle tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento. • Capacità di utilizzo di sistemi di correlazione eventi, di progettazione regole di correlazione e di tuning di sistemi di analisi eventi con esperienza di integrazione. • Capacità di utilizzo di sistemi di autenticazione, sistemi di Identity & Access Management con esperienza di integrazione.
Certificazioni	N/A
Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 4 nella funzione

5. SENIOR SECURITY AUDITOR

Titolo del profilo	SENIOR SECURITY AUDITOR
Descrizione sintetica	Figura professionale dedicata allo svolgimento delle operazioni di security auditing all'interno delle organizzazioni.
Missione	Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Completa i giornali di audit documentando test e risultati dell'audit. Individua i possibili punti vulnerabili di un sistema informativo.
Principali Task	• Pianificazione ed esecuzione del monitoraggio della sicurezza di reti, applicazioni ed utenti che compongono il sistema in esame. • Rilevazione di eventuali abusi e violazioni sia accidentali che dolosi. • Simulazione del comportamento degli hacker, cercando di "compromettere" il sistema stesso attraverso attacchi mirati e sistematici che ne rivelino gli

<table>
<tr><td></td><td colspan="3">eventuali punti deboli.
• Produzione di resoconti finale che sintetizzano i risultati raggiunti.
• Conduzione di IT Audit.
• Valutazione dei sistemi SGSI in accordo con la norma ISO:27001.
• Utilizzo di metodologie e delle linee guida ISO in materia di IT audit e nell'applicazione delle stesse in funzione deli criteri di audit identificati.
• Utilizzo delle linee guida ISO sui controlli di sicurezza in ambito Enterprise e cloud ed esperienza nella contestualizzazione nel processo di mitigazione del rischio.
• Valutazione di analisi di compliance in materia Privacy e direttive AgID e nella definizione e governo dei piani di rientro.
• Valutazione della documentazione a supporto per i processi di compliance al cogente (es. Documento Programmatico della Sicurezza, Studio di fattibilità per la continuità operativa del CAD) o certificazione CISA (Certified Information System Auditor).</td></tr>
<tr><td rowspan="6">Competenze e-CF assegnate</td><td>B.3.</td><td>Testing</td><td>Livello 3</td></tr>
<tr><td>B.5.</td><td>Produzione della documentazione</td><td>Livello 4</td></tr>
<tr><td>D.1.</td><td>Sviluppo della strategia per la sicurezza informatica</td><td>Livello 4</td></tr>
<tr><td>C.2.</td><td>Supporto alle modifiche/evoluzioni del sistema</td><td>Livello 4</td></tr>
<tr><td>E.8.</td><td>Gestione della sicurezza dell'informazione</td><td>Livello 4</td></tr>
<tr><td>E.9.</td><td>Governance dei sistemi informativi</td><td>Livello 4</td></tr>
<tr><td>Conoscenze</td><td colspan="3">• Conoscenza dei processi e delle procedure operative IT.
• Conoscenza approfondita della conduzione di IT Audit.
• Conoscenza approfondita delle metodologie e delle linee guida ISO in materia di IT audit e nell'applicazione delle stesse in funzione deli criteri di audit identificati.
• Conoscenza approfondita delle linee guida ISO sui controlli di sicurezza in ambito Enterprise e Cloud e nella contestualizzazione nel processo di mitigazione del rischio.
• Conoscenza nella valutazione di sistemi SGSI in accordo con la norma ISO:27001.
• Conoscenza approfondita della normativa sulla Privacy e dei Provvedimenti del Garante sia in ambito Italiano che Europeo.
• Conoscenza approfondita delle direttive dell'AgID in materia di sicurezza delle informazioni e continuità operativa dei servizi.
• Conoscenza nella valutazione di analisi di compliance in materia Privacy e direttive AgID e nella definizione e governo dei piani di rientro.
• Conoscenza approfondita nella valutazione della documentazione a supporto per i processi di compliance al cogente (es. Documento Programmatico della Sicurezza, Studio di fattibilità per la continuità operativa del CAD).
• Conoscenze tecniche di Information Security (crittografia, firma digitale, protocolli di comunicazione, sistemi di autenticazione e controllo, tecniche di Hacking e di Intrusion Detection).</td></tr>
<tr><td>Abilità</td><td colspan="3">• Capacità di adozione di processi e delle procedure operative IT.</td></tr>
</table>

	• Capacità di condurre IT Audit. • Capacità di applicazione delle metodologie e delle linee guida ISO in materia di IT audit, e di applicazione delle stesse in funzione deli criteri di audit identificati; • Capacità di applicazione delle linee guida ISO sui controlli di sicurezza in ambito Enterprise e Cloud ed esperienza nella contestualizzazione nel processo di mitigazione del rischio. • Capacità di valutazione dei sistemi SGSI in accordo con la norma ISO:27001. • Capacità di valutazione di analisi di compliance in materia Privacy e direttive AgID su contesti analoghi. • Capacità di definire e governare piani di rientro. • Capacità di valutare la documentazione a supporto per i processi di compliance al cogente (es. Documento Programmatico della Sicurezza, Studio di fattibilità per la continuità operativa del CAD) o certificazione CISA (Certified Information System Auditor).
Certificazioni	Possesso della **certificazione CISA (Certified Information System Auditor)** per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo**.**
Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 6 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 3 nella funzione

6. SENIOR SECURITY ANALYST

Titolo del profilo	SENIOR SECURITY ANALIST
Descrizione sintetica	Figura operativa dedicata alla verifica tecnica della sicurezza delle informazioni dei sistemi, delle reti e delle applicazioni.
Missione	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.
Principali Task	• Coordinamento di figure professionali Junior. • Adozione dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica. • Adozione dei processi di analisi forense e acquisizione degli elementi probatori e conservazione degli stessi. • Utilizzo di sistemi di rilevazione e di analisi degli allarmi. • Svolgimento di analisi tecniche di incidenti all'interno di strutture SOC o CERT nell'ambito della Pubblica Amministrazione. • Gestione delle attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici. • Definizione proattiva di configurazioni e analisi di sicurezza. • Definizione di regole di correlazione e tuning delle stesse. • Conduzione di analisi forense di malware mediante strumenti di analisi e attività di reverse. • Analisi forense del traffico di rete e nell'identificazione di anomalie o elementi a

<table>
<tr><td></td><td colspan="3">supporto per la corretta gestione degli incidenti di sicurezza.</td></tr>
<tr><td rowspan="6">Competenze e-CF assegnate</td><td>B.3.</td><td>Testing</td><td>Livello 4</td></tr>
<tr><td>B.6.</td><td>Ingegneria dei sistemi</td><td>Livello 4</td></tr>
<tr><td>C.2.</td><td>Supporto alle modifiche/evoluzioni del sistema</td><td>Livello 4</td></tr>
<tr><td>D.1.</td><td>Sviluppo della strategia per la sicurezza informatica</td><td>Livello 4</td></tr>
<tr><td>E.8.</td><td>Gestione della sicurezza dell’informazione</td><td>Livello 4</td></tr>
<tr><td>E.9.</td><td>Governance dei sistemi informativi</td><td>Livello 3</td></tr>
<tr><td>Conoscenze</td><td colspan="3">• Conoscenza approfondita dei processi e delle procedure operative IT.
• Conoscenza approfondita dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica.
• Conoscenza approfondita dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi.
• Conoscenza approfondita dei sistemi di rilevazione e analisi degli allarmi.
• Conoscenza approfondita di metodologie o esperienza comprovata nell’analisi tecnica di incidenti all’interno di strutture SOC o CERT nell’ambito della Pubblica Amministrazione.
• Conoscenza approfondita o esperienza comprovata nella gestione delle attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici.
• Conoscenza approfondita o esperienza comprovata nella definizione proattiva di configurazioni e analisi di sicurezza.
• Conoscenza approfondita o esperienza nella definizione di regole di correlazione e nel tuning delle stesse.
• Conoscenza dei processi di reverse engineering dei malware ed esperienza comprovata nella analisi forense di malware mediante strumenti di analisi e attività di reverse.
• Conoscenza approfondita dei protocolli di rete e della tipologia di traffico all’interno di un contesto complesso con esperienza comprovata nell’analisi forense del traffico di rete e nell’identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.</td></tr>
<tr><td>Abilità</td><td colspan="3">• Capacità di coordinamento di figure professionali Junior.
• Capacità di comprendere i processi e le procedure operative IT.
• Capacità di comprendere e attuare i processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica.
• Capacità di comprendere e attuare i processi di analisi forense, di acquisizione degli elementi probatori e di conservazione degli stessi.
• Capacità di utilizzo dei sistemi di rilevazione e analisi degli allarmi.
• Capacità di esecuzione dell’analisi tecnica di incidenti all’interno di strutture SOC o CERT nell’ambito della Pubblica Amministrazione.
• Capacità di gestire le attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici.
• Capacità di definire proattivamente le configurazioni e analisi di sicurezza e la definizione di regole di correlazione e tuning delle stesse.
• Capacità di comprendere e attuare i processi di reverse engineering dei malware.
• Capacità di analisi forense di malware mediante strumenti di analisi e attività di reverse.</td></tr>
</table>

	• Capacità di analisi forense del traffico di rete e identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.
Certificazioni	Possesso di almeno una delle seguenti certificazioni: • EC-Council CSA (Certified SOC Analyst); • e/o CompTIA CySA+ (Cyber Security Analyst); • e/o GIAC Certified Intrusion Analyst; per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.
Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente.
Anzianità lavorativa	Minimo 8 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 4 nella funzione.

7. JUNIOR SECURITY ANALYST

Titolo del profilo	JUNIOR SECURITY ANALIST		
Descrizione sintetica	Figura operativa dedicata alla verifica tecnica della sicurezza delle informazioni dei sistemi, delle reti e delle applicazioni.		
Missione	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.		
Principali Task	• Partecipazione nell'adozione dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica. • Utilizzo di sistemi di rilevazione e di analisi degli allarmi. • Collaborazione nella gestione delle attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici. • Supporto nella definizione di configurazioni e analisi di sicurezza. • Supporto nella definizione di regole di correlazione e tuning delle stesse. • Collaborazione nella conduzione di analisi forense di malware mediante strumenti di analisi e attività di reverse. • Collaborazione nell'identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.		
Competenze e-CF assegnate	B.3.	Testing	Livello 3
	B.6.	Ingegneria dei sistemi	Livello 3
	C.2.	Supporto alle modifiche/evoluzioni del sistema	Livello 2
	E.8.	Gestione della sicurezza dell'informazione	Livello 3
Conoscenze	• Conoscenza dei processi e delle procedure operative IT. • Conoscenza dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica. • Conoscenza dei sistemi di rilevazione e analisi degli allarmi. • Conoscenza nella definizione proattiva di configurazioni e analisi di sicurezza. • Conoscenza nella definizione di regole di correlazione e nel tuning delle stesse. • Conoscenza dei processi di reverse engineering dei malware. • Conoscenza dei protocolli di rete e della tipologia di traffico nell'identificazione		

	di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.
Abilità	• Capacità di comprendere i processi e le procedure operative IT. • Capacità di comprendere e attuare i processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica. • Capacità di utilizzo dei sistemi di rilevazione e analisi degli allarmi. • Capacità di partecipare alla definizione delle configurazioni, all'analisi di sicurezza e alla definizione di regole di correlazione e tuning delle stesse. • Capacità di comprendere i processi di reverse engineering dei malware. • Capacità di collaborare all'analisi forense di malware mediante strumenti di analisi e attività di reverse. • Capacità di collaborare all'analisi forense del traffico di rete e identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.
Certificazioni	N/A
Titolo di studio	Laurea triennale in materie scientifiche.
Anzianità lavorativa	Minimo 4 anni da computarsi successivamente al conseguimento della diploma, di cui almeno 2 nella funzione.

8. SENIOR PENETRATION TESTER

Titolo del profilo	SENIOR PENETRATION TESTER
Descrizione sintetica	Figura operativa dedicata alla verifica dell'efficacia della sicurezza dei sistemi, delle reti e delle applicazioni.
Missione	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.
Principali Task	• Coordinamento di figure professionali Junior. • Analisi dinamica delle vulnerabilità e penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Analisi statica del codice sorgente o delle configurazioni di sistema. • Analisi statica/dinamica del codice sorgente o delle configurazioni di sistema in ambito mobile. • Verifiche fisiche su sistemi e dispositivi di rete. • Disegno e valutazione dei sistemi di gestione per la sicurezza. • Gestione processo di hardening di sistemi e di piattaforme middleware; • Validazione pattern di sviluppo sicuro del codice. • Utilizzo delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente. • Analisi delle vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi. • Documentazione completa, precisa e semplice gli attacchi condotti, affinché siano ripetibili. • Verifica dell'efficacia delle misure applicate come remediation alla fine

	dell'engagement.		
Competenze e-CF assegnate	B.3.	Testing	Livello 4
	B.6.	Ingegneria dei sistemi	Livello 4
	C.2.	Supporto alle modifiche/evoluzioni del sistema	Livello 4
	D.1.	Sviluppo della strategia per la sicurezza informatica	Livello 4
	E.8.	Gestione della sicurezza dell'informazione	Livello 4
Conoscenze	• Conoscenza della metodologia OSSTMM. • Conoscenza approfondita delle vulnerabilità e delle modalità, tecniche e strumenti penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Conoscenza approfondita delle metodologie, tecniche e strumenti di analisi statiche e dinamiche del codice sorgente o delle configurazioni di sistema. • Conoscenza approfondita sulle modalità di disegno e di valutazione dei sistemi di gestione per la sicurezza. • Conoscenza approfondita del processo di hardening di sistemi e piattaforme middleware. • Conoscenza approfondita dei pattern di sviluppo sicuro del codice. • Conoscenza approfondita delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente. • Conoscenza approfondita o esperienza comprovata nell'analisi delle vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi. • Conoscenza complessiva delle problematiche di sicurezza dei dati e delle informazioni.		
Abilità	• Capacità di coordinamento di figure professionali Junior. • Capacità di operare simulando i comportanti sia del ruolo di attaccante, contestualmente rispettando le regole di ingaggio, che del ruolo utente target. • Capacità di comprendere e di considerare l'importanza per il management delle informazioni recuperate, individuando velocemente potenziali punti utili a condurre ulteriori attacchi. • Capacità di adozione delle modalità, tecniche e strumenti penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Conoscenza di adozione delle metodologie, tecniche e strumenti di analisi statiche e dinamiche del codice sorgente o delle configurazioni di sistema. • Capacità di attuazione delle modalità di disegno e di valutazione dei sistemi di gestione per la sicurezza. • Capacità di adozione del processo di hardening di sistemi e piattaforme middleware. • Capacità di adozione dei pattern di sviluppo sicuro del codice. • Capacità di esecuzione di diverse tipologie di attacco informatico, attraverso le tecniche di penetration test più diffusamente conosciute, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente. • Capacità di documentare in maniera completa, precisa e semplice gli attacchi condotti, affinché siano ripetibili; • Capacità di verificare l'efficacia delle misure applicate come remediation alla		

	fine dell'engagement.
Certificazioni	Possesso della **certificazione OSSTMM Professional Security Tester (OPST)** o della **certificazione Certified Etical Hacher (CEH)**, per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.
Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente.
Anzianità lavorativa	Minimo 6 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 3 nella funzione.

9. JUNIOR PENETRATION TESTER

Titolo del profilo	JUNIOR PENETRATION TESTER		
Descrizione sintetica	Figura operativa dedicata alla verifica dell'efficacia della sicurezza dei sistemi, delle reti e delle applicazioni.		
Missione	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio.		
Principali Task	• Partecipazione all'analisi dinamica delle vulnerabilità e penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Partecipazione all'analisi statica del codice sorgente o delle configurazioni di sistema. • Partecipazione all'analisi statica/dinamica del codice sorgente o delle configurazioni di sistema in ambito mobile. • Partecipazione alle verifiche fisiche su sistemi e dispositivi di rete. • Partecipazione alla gestione processo di hardening di sistemi e di piattaforme middleware; • Partecipazione ai penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente. • Collaborazione nella stesura della documentazione degli attacchi condotti, affinché siano ripetibili.		
Competenze e-CF assegnate	B.3.	Testing	Livello 3
	B.6.	Ingegneria dei sistemi	Livello 3
	C.2.	Supporto alle modifiche/evoluzioni del sistema	Livello 3
	D.1.	Sviluppo della strategia per la sicurezza informatica	Livello 2
	E.8.	Gestione della sicurezza dell'informazione	Livello 2
Conoscenze	• Conoscenza della metodologia OSSTMM. • Conoscenza delle vulnerabilità e degli strumenti penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Conoscenza delle tecniche e strumenti di analisi statiche e dinamiche del codice sorgente o delle configurazioni di sistema. • Conoscenza del processo di hardening di sistemi e piattaforme middleware. • Conoscenza dei pattern di sviluppo sicuro del codice. • Conoscenza delle diverse tipologie di attacco informatico, delle tecniche di		

	penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente. • Conoscenza delle problematiche di sicurezza dei dati e delle informazioni.
Abilità	• Capacità di collaborazione nell'attuazione delle tecniche e nell'uso di strumenti penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Capacità di collaborazione nell'adozione delle tecniche e degli strumenti di analisi statiche e dinamiche del codice sorgente o delle configurazioni di sistema. • Capacità di collaborazione nell'adozione del processo di hardening di sistemi e piattaforme middleware. • Capacità di utilizzo dei pattern di sviluppo sicuro del codice. • Capacità di collaborazione nell'esecuzione degli attacchi informatici, attraverso l'uso di strumenti software, tool ed exploit disponibili pubblicamente. • Capacità di collaborazione nella stesura di documentazione degli attacchi condotti, affinché siano ripetibili; • Capacità di partecipare alla verifica dell'efficacia delle misure applicate come remediation alla fine dell'engagement.
Certificazioni	N/A
Titolo di studio	Diploma in materie scientifiche.
Anzianità lavorativa	Minimo 4 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 2 nella funzione.

10. FORENSIC EXPERT

Titolo del profilo	FORENSIC EXPERT
Descrizione sintetica	Figura operativa dedicata all'analisi tecnica della sicurezza delle informazioni dei sistemi, delle reti e delle applicazioni al fine di ricostruirne l'utilizzo nel tempo.
Missione	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.
Principali Task	• Guida nelle indagini sulle violazioni dei dati e sugli incidenti di sicurezza in cui sono già stati generati allarmi. • Collaborazione nello smantellamento e nella ricostruzione dei sistemi interessati e nel successivo recupero di dati incriminanti. • Analisi dei computer e altri dispositivi digitali, garantendo la conservazione delle prove digitali, il recupero, l'analisi, l'esame della posta elettronica e del database. • Analisi ed acquisizione di informazioni su ambienti di tipo Public Cloud. • Mantenimento, custodia adeguata e conduzione dei metodi di recupero e di raccolta, gestione e archiviazione delle prove in modo coerente per mantenere la conservazione e la protezione dei dati e delle prove nella loro forma originale; • Identificazione, acquisizione, recupero, pulizia, estrazione e messa in sicurezza di grandi quantità di informazioni archiviate elettronicamente.

	• Gestione e analisi tecniche complete anche mediante l'utilizzo di software forensi. • Scrittura di IOC (Indicator of Compromise). • Gestione degli incidenti e avvio delle indagini quando ritenuto necessario. • Raccolta, analisi e presentazione in tribunale di prove elettroniche. • Consegna dei dati e dei rapporti dettagliati, per consentirne poi l'utilizzo da esperti legali terzi. • Testimonianza da esperto in tribunale per supportare l'accusa di coloro che sono responsabili del cyber crime o tentativi di hacking non autorizzato.		
Competenze e-CF assegnate	B.3.	Testing	Livello 3
	B.6.	Ingegneria dei sistemi	Livello 3
	C.2.	Supporto alle modifiche/evoluzioni del sistema	Livello 4
	D.1.	Sviluppo della strategia per la sicurezza informatica	Livello 4
	E.8.	Gestione della sicurezza dell'informazione	Livello 4
Conoscenze	• Conoscenza approfondita dei più diffusi sistemi operativi, delle architetture, dei protocolli di rete, delle strutture dei database e tecniche di criptazione dei dati. • Conoscenza approfondita dei metodi utilizzati dagli hacker per aggirare le difese poste a salvaguardia della sicurezza informatica. • Conoscenze nell'ambito IT delle pratiche di installazione, configurazione ed aggiornamento hardware e software. • Conoscenza dei processi di analisi e gestione dei rischi aziendali e delle modalità di elaborazione ed attuazione del piano di security aziendale. • Conoscenza delle soluzioni tecniche adottate per garantire la sicurezza di un sistema informativo e della loro efficacia. • Conoscenza delle tecniche e delle metodologie per la raccolta dei dati. • Conoscenza approfondita delle procedure forensi e delle norme che tutelano i dati personali e i patrimoni informativi. • Conoscenza approfondita delle attività informatiche tecnico-pratiche applicate al diritto (informatica giuridica). • Conoscenza approfondita e comprensione di tutte le nozioni riguardanti il crimine informatico. • Conoscenza della disciplina giuridica in materia di crimine informatico (Legge 547/93) e di protezione dei dati personali, con particolare riferimento al quadro normativo delineato dalla legge n. 675/96 sulla privacy e successive modifiche ed integrazioni. • Conoscenza di almeno uno dei tool di analisi tra X-Ways, Magnet Axiom, FTK Forensics Toolkit. • Conoscenza di almeno un tool di analisi di mobile forensics. • Conoscenza delle principali metodologie di analisi proattiva delle minacce ATP quali ad esempio Tattiche Tecniche e Procedure (TTP).		
Abilità	• Capacità di analizzare nel dettaglio i dati raccolti e di effettuarne una catalogazione. • Capacità di esprimersi con un linguaggio rigoroso sul piano giuridico ma al tempo stesso comprensibile sul piano tecnico, anche per chi non possieda conoscenze informatiche. • Capacità di mantenersi sempre aggiornati sulle tematiche normative e tecniche		

	legate alla continua rilevazione di nuove tecniche di cyber-crime. • Capacità analitiche e investigative. • Capacità di lavorare sia autonomamente che in team, in modalità multitasking anche in situazione di forte stress. • Capacità di problem solving.
Certificazioni	Possesso di almeno una tra le seguenti certificazioni: • GIAC – Certification Forensic Analyst; • GIAC – Certification Forensic Esaminer; • GIAC – Advanced Digital Forensics Investigation Professional (DFIP); • GIAC – Certified Incident Handler (CIH); • EnCASE Certified Examiner (ENCE); • AccessData Certified Examiner; per almeno il 50% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.
Titolo di studio	Laurea magistrale specialistica in materie scientifiche e/o giuridiche o cultura equivalente.
Anzianità lavorativa	Minimo 4 anni da computarsi successivamente al conseguimento della diploma di laurea, di cui almeno 2 nella funzione.

11. DATA PROTECTION SPECIALIST

Titolo del profilo	DATA PROTECTION SPECIALIST
Descrizione sintetica	Figura professionale dedicata ad affiancare il titolare, gli addetti ed i responsabili del trattamento dei dati affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo.
Missione	Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche, verifica il rispetto di quanto previsto nelle normative italiane ed europee in termini di protezione dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali.
Principali Task	• Controlla la corretta applicazione del GDPR e verifica che ogni trattamento di dati personali avvenga nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679. • Sviluppa e mantiene aggiornato un programma di gestione della protezione dei dati (DPMP) che copra le politiche, i processi e le persone per la gestione dei dati personali in ogni fase del ciclo di vita dei dati. • individua le tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto (DPIA) per identificare, valutare e affrontare i rischi aziendali, in base alle funzioni, alle esigenze e ai processi dell'organizzazione • sensibilizza il personale che tratta dati personali sviluppando un programma di formazione sulle politiche e sui processi di protezione dei dati personali. • Supervisiona le attività per favorire la consapevolezza della protezione dei dati personali all'interno dell'organizzazione.

<table>
<tr><td></td><td colspan="3">Migliora i processi di conformità sulla base di una verifica delle operazioni aziendali nelle varie fasi del ciclo di vita dei dati o delle informazioni.
informa e fornisce supporto al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento.
indica al Titolare e/o al Responsabile le aree funzionali alle quali riservare un audit interno o esterno in tema di protezione dei dati.
Coopera nei rapporti con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità.
Testimonia da esperto in tribunale per supportare l’accusa di coloro che sono responsabili del cyber crime o tentativi di hacking non autorizzato.</td></tr>
<tr><td></td><td>D.1.</td><td>Sviluppo della strategia per la sicurezza informatica</td><td>Livello 4</td></tr>
<tr><td></td><td>D.3.</td><td>Fornitura dei servizi di Formazione</td><td>Livello 4</td></tr>
<tr><td></td><td>E.3.</td><td>Gestione del rischio</td><td>Livello 3</td></tr>
<tr><td></td><td>E.4.</td><td>Miglioramento dei processi</td><td>Livello 3</td></tr>
<tr><td></td><td>E.8.</td><td>Gestione della sicurezza dell’informazione</td><td>Livello 4</td></tr>
<tr><td>Conoscenze</td><td colspan="3">Conoscenza approfondita della normativa e delle prassi in materia di protezione dei dati, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.
Conoscenze di risk management e di analisi dei processi.
Conoscenza delle procedure tecnico-informatiche più diffuse.
Conoscenza di base delle funzioni di gestione della Sicurezza (cyber-crime, eventi data-breach).
Conoscenza delle procedure forensi e delle norme che tutelano i dati personali e i patrimoni informativi.
Conoscenza delle attività informatiche tecnico-pratiche applicate al diritto (informatica giuridica).
Conoscenza della disciplina giuridica in materia di crimine informatico (Legge 547/93) e di protezione dei dati personali, con particolare riferimento al quadro normativo delineato dalla legge n. 675/96 sulla privacy e successive modifiche ed integrazioni.</td></tr>
<tr><td>Abilità</td><td colspan="3">Capacità di identificare i processi rilevanti ai fini della protezione dei dati.
Capacità di svolgere accuratamente le attività di verifica dell’attribuzione delle responsabilità e di formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.
Capacità di catalogazione e raccolta di tutte le informazioni rilevanti anche ai fini della supervisione alla tenuta del registro dei trattamenti.
Capacità di gestire, nelle modalità più idonee, lo svolgimento delle diverse incombenze quali ad esempio la procedura di Data Protection Impact Assessment (DPIA).
Capacità di valutare l'impatto delle tendenze e delle tecnologie emergenti (ad es. Tecnologie per il miglioramento della privacy, cloud computing, blockchain, cybersecurity) e sviluppi normativi a livello mondiale che comportano rischi significativi associati alla protezione dei dati.
Capacità di individuare quali siano le priorità in funzione del livello di rischio nella protezione dei dati di ciascun singolo trattamento.
Capacità di progettare, verificare e mantenere un sistema organizzato di</td></tr>
</table>

	gestione dei dati personali. • Capacità comunicative e di collaborare in team multidisciplinari costituiti anche da informatici.
Certificazioni	N/A
Titolo di studio	Laurea magistrale specialistica in materie scientifiche e/o giuridiche o cultura equivalente.
Anzianità lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del diploma di laurea, di cui almeno 2 nella funzione.