



**GARA A PROCEDURA APERTA AI SENSI DEL
D.LGS. 36/2023 E S.M.I., PER LA CONCLUSIONE DI
UN ACCORDO QUADRO PER OGNI LOTTO AVENTE
AD OGGETTO L’AFFIDAMENTO DI SERVIZI
MANAGED SECURITY SERVICES DA REMOTO, DI
GOVERNANCE, ANALISI DEL RISCHIO E
CONTROLLO PER LE PUBBLICHE
AMMINISTRAZIONI (ID 2737)**

LOTTI 3 e 4

**APPENDICE 2 AL CAPITOLATO TECNICO
SPECIALE - PROFILI PROFESSIONALI**

Classificazione Consip: Ambito pubblico

Indice

1.	SCOPO DEL DOCUMENTO	3
2.	SECURITY PRINCIPAL	7
3.	INFORMATION SECURITY CONSULTANT SENIOR	10
4.	INFORMATION SECURITY CONSULTANT JUNIOR	13
5.	SECURITY SOLUTION ARCHITECT	16
6.	SECURITY SOLUTION ARCHITECT SENIOR	19
7.	CLOUD SECURITY EXPERT	23
8.	OT/IOT SECURITY EXPERT	26
9.	DATA PROTECTION SPECIALIST	29
10.	DATA PRIVACY & PROTECTION SPECIALIST	31
11.	FORENSIC EXPERT	34
12.	RISK MANAGER	36
13.	SECURITY AUDITOR SENIOR	38
14.	SECURITY MANAGER	40
15.	PENETRATION TESTER SENIOR	42
16.	PENETRATION TESTER JUNIOR	45
17.	SCHEMA PER LA PRESENTAZIONE DEI CURRICULA	47

1. SCOPO DEL DOCUMENTO

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.

Per i profili inseriti dedicati alla sicurezza informatica si fa riferimento, ove applicabile, allo European Cybersecurity Skills Framework Role Profiles (ECSF) di ENISA.

Trattasi di requisiti minimi che dovranno evolversi nel contesto delle migliori professionalità presenti nel settore della cybersicurezza 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 supporto specialistico** dovranno aderire ai profili di seguito descritti.

Il presente documento considera le esigenze di servizi in ambito cybersicurezza espresse sulla base del Piano Triennale per l’informatica nella Pubblica Amministrazione che sulla normativa relativa al perimetro di sicurezza nazionale cibernetica. Ciascun profilo professionale si riferisce a risorse professionali con ampia esperienza, competenza funzionale e tecnica per l’ambito del lotto. Tali competenze dovranno essere costantemente aggiornate all’evoluzione della tecnologia, normativa e organizzativa della cybersicurezza nonché degli standard, delle linee guida e best practices applicabili.

Nel presente documento, e laddove citati nel Capitolato Tecnico Generale e Speciale, 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 Esecutivi, nonché nei casi di cui al paragrafo 10.1 del Capitolato Tecnico Generale. A tal fine, la presente appendice potrà essere aggiornata nel corso della vigenza dell’AQ e dei Contratti Esecutivi, in accordo tra le parti e comunque previa approvazione del Comitato Tecnico.

Per ogni profilo è richiesto il possesso di una esperienza lavorativa minima, che deve essere stata maturata in ambito ICT. Per ogni profilo è richiesto inoltre il possesso di uno specifico titolo di studio oppure di una “cultura equivalente”; la cultura equivalente corrisponde ad una esperienza lavorativa maturata in ambito ICT aggiuntiva rispetto a quella minima indicata nel profilo stesso; l’entità dell’esperienza aggiuntiva necessaria dipende dal titolo di studio posseduto dalla risorsa rispetto a quello richiesto, come sintetizzato nella seguente tabella. In ogni caso, il titolo di studio posseduto

¹ <https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf>

² <https://www.agid.gov.it/it/agenzia/competenze-digitali>

deve essere almeno un diploma di scuola secondaria di secondo grado.

Titolo di studio posseduto	Laurea magistrale in discipline tecnico scientifiche e/o giuridiche	Laurea triennale in discipline tecnico scientifiche oppure corso Istituto Tecnico Superiore (ITS Academy)	Laurea magistrale (altre discipline)	Laurea triennale (altre discipline)	Diploma di Perito industriale in informatica oppure Diploma Istruzione Tecnica Indirizzo INFORMATICA E TELECOMUNICAZIONI Articolazione "INFORMATICA"	Diploma di scuola secondaria di secondo grado (diverso da perito industriale in informatica)
Titolo di studio richiesto						
Laurea magistrale in discipline tecnico scientifiche e/o giuridiche	-	+ 2 anni	+ 2 anni (o master 2° livello in cybersicurezza)	+ 3 anni (o + 2 anni e master 1° livello in cybersicurezza)	+ 5 anni	+ 7 anni
Laurea triennale in discipline tecnico scientifiche	-	-	+ 1 anno (o master 1° livello in cybersicurezza)	+ 2 anni (o + 1 anno e master 1° livello in cybersicurezza)	+ 4 anni	+ 5 anni

Tabella 1 - Esperienza aggiuntiva da considerare come "cultura equivalente"

Ad esempio, nel caso in cui fosse richiesta una laurea magistrale in discipline tecnico-scientifiche con esperienza minima maturata in ambito ICT di 10 anni, il possesso di laurea triennale in discipline tecnico-scientifiche richiederebbe esperienza minima di 12 anni (10 + 2).

Si precisa che per lauree in discipline tecnico-scientifiche si intendono le lauree che possono essere ricondotte alle classi di laurea che prevedono, nelle proprie attività formative di base e/o caratterizzanti, uno o più dei settori scientifico disciplinari inclusi nelle aree "scienze matematiche e informatiche" o "ingegneria industriale e dell'informazione".

Le classi di laurea e i settori scientifico-disciplinari suddetti fanno riferimento alla classificazione fornita dal Ministero dell'Istruzione, Università e Ricerca nell'ambito dei D.M. 16 marzo 2007 e s.m.i. e 4 ottobre 2000 e s.m.i., nonché secondo quanto previsto dai DM. 1648 e 1649 del 19 dicembre 2023 emanati dal Ministero dell'Università e Ricerca.

L'eventuale equiparazione dei diplomi di laurea conseguiti in base ad ordinamenti previgenti è regolata da quanto previsto nel Decreto Interministeriale 9 luglio 2009 (G.U. 7 ottobre 2009 n. 233) e s.m.i..

Per ciascun profilo professionale le competenze, le conoscenze e le abilità indicate nel presente documento devono essere presenti nel complesso delle risorse professionali che il Fornitore può mettere a disposizione dell'Amministrazione per l'erogazione dei servizi e non devono essere interamente possedute da un'unica risorsa. Resta inteso che, al contrario, i titoli di studio (o la cultura equivalente) e l'esperienza lavorativa pregressa dovranno essere posseduti da ciascuna risorsa. Per le certificazioni valgono le regole indicate in corrispondenza di ciascun profilo professionale.

È facoltà dell'Amministrazione dettagliare le proprie esigenze dettagliando le competenze/conoscenze/abilità relativamente a quelle indicate per ciascun profilo nell'ambito del presente documento.

Le certificazioni possedute dalle risorse per ciascun ruolo dovranno essere mantenute aggiornate e in corso di validità per tutta la durata contrattuale e dovranno essere allineate all'evoluzione del prodotto/tecnologia a cui si riferiscono.

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.

Permane in ogni caso l'obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del contesto tecnologico, adeguando le conoscenze del personale impiegato nell'erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguato, fermo restando quanto previsto nel presente documento.

I curriculum vitae delle figure professionali da impiegare nei vari servizi dovranno essere resi disponibili alla Amministrazione secondo quanto previsto dal presente documento, rispettando lo schema di CV Europeo riportato in calce al presente documento 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.

2. SECURITY PRINCIPAL

Titolo del profilo	SECURITY PRINCIPAL		
Riferimento profilo ECSF	N/A		
Descrizione sintetica	Figura professionale dedicata alla gestione di progetti per raggiungere la performance ottimale conforme alle specifiche originali.		
Missione	<ul style="list-style-type: none"> 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 in ambito cybersicurezza. 		
Principali Task	<ul style="list-style-type: none"> Valutare (stima di tempi / costi / rischi / risorse), pianificare, realizzare e monitorare i progetti IT nel dominio della Cyber security. Organizzare, coordinare e condurre team di progetto per l'erogazione dei servizi. Supervisionare le milestone di progetto e del suo andamento complessivo. Coordinare, registrare e monitorare la conformità alla qualità. Diffondere e distribuire le informazioni di progetto e la relazione con il committente. Pianificare e coordinare le attività relative ai servizi di Compliance e controllo. Assicurare la conformità dei deliverable di progetto alle specifiche tecniche. Aggiornare il piano di progetto secondo i cambiamenti del contesto ed i mutevoli accadimenti. Coordinare il team applicando metodologie e strumenti per raggiungere un flusso di lavoro ottimale attraverso il continuo miglioramento delle attività. Governare i progetti di analisi della postura del sistema di sicurezza. Stimare risorse ed effort per la gestione dei progetti utilizzando metodologie e tecniche di project management. 		
Competenze	A.2.	Gestione dei Livelli di Servizio	Livello e-3
	A.3.	Sviluppo del Business Plan	Livello e-3
	D.8.	Gestione del Contratto	Livello e-4

	E.2.	Project and Portfolio Management	Livello e-4
	E.3.	Gestione del Rischio	Livello e-4
	E.4.	Gestione delle Relazioni	Livello e-4
	E.7.	Business Change Management	Livello e-4
	E.8.	Gestione della sicurezza dell'informazione	Livello e-3
Conoscenze	<ul style="list-style-type: none"> • Normativa di riferimento in ambito di appalti pubblici e della normativa PNRR. • Normativa di riferimento nazionale ed europea di riferimento in materia cyber, del CAD, della Crescita Digitale e del Piano Triennale AgID con focus sull'ambito Cyber Security. • Normativa e Linee Guida AgID di settore in materia di Sicurezza Informatica. • Normativa in materia di privacy. • Metodologie e processi di Security Governance e Security Management. • Tecniche di problem solving, incident response e risk management. • Metodologie di vulnerability assessment, penetration test, compliance management e Security Audit. • Sistemi per la gestione della sicurezza delle informazioni. • Metodologie e strumenti operativi richiesti in progetti di IT Security. • Metodologie e processi in ambito continuità operativa. • Processi e procedure operative IT. • Principali tecnologie per la sicurezza IT. • Modelli di servizio del Cloud computing (IaaS, PaaS, SaaS) e le principali architetture cloud-native. • ISO/IEC 27018:2014 – Gestione della privacy nel cloud. • Principali framework di service management quali ITIL, COBIT, CMMI. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di tradurre i principali elementi di un piano strategico di sicurezza in requisiti funzionali per lo sviluppo dei servizi ICT. • Essere in grado di identificare i requisiti per i processi collegati ai servizi ICT e formalizzare i requisiti dell'utente. • Essere in grado di gestire l'ambiente dei dati comuni, processi e procedure, convalidando le conformità e le non conformità. • Essere in grado di gestire progetti su piattaforme di erogazione di servizi da remoto con elevato grado di integrazione tra sistemi informativi (modelli ibridi). 		

	<ul style="list-style-type: none"> • Essere in grado di mantenere il modello informativo per soddisfare gli standard di integrità e sicurezza in conformità ai requisiti degli utenti. • Essere in grado di gestire la relazione con le Pubbliche Amministrazioni.
Certificazioni	Possesso di almeno una delle seguenti certificazioni: <ul style="list-style-type: none"> • Certified Information Security Manager (CISM). • Certified in Risk and Information Systems Control (CRISC). • CompTIA Security+. • CompTIA CASP.
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 6 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.

3. INFORMATION SECURITY CONSULTANT SENIOR

Titolo del profilo	INFORMATION SECURITY CONSULTANT SENIOR
Riferimento profilo ECSF	Chief Information Security Officer
Descrizione sintetica	Figura professionale di riferimento per attività e progetti relativi all'attuazione della strategia di cybersicurezza dell'organizzazione per garantire la sicurezza e la protezione dei sistemi, servizi e asset digitali.
Missione	<ul style="list-style-type: none"> • Attuare la 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 cybersicurezza e il resto del personale operativo. • Controllare il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. • Attuare misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione. • Identificare e risolvere i problemi di cybersicurezza e anticipare le possibili minacce, esigenze e le sfide future.
Principali Task	<ul style="list-style-type: none"> • Valutare e migliorare la postura di sicurezza dell'organizzazione. • Analizzare e implementare politiche di sicurezza informatica certificazioni, standard, metodologie e framework di cybersicurezza. • Analizzare leggi, regolamenti e normative in materia di sicurezza informatica, comprendere gli obblighi e le misure che impongono e realizzare le azioni che consentano di rispettarli. • Implementare una strategia di cybersicurezza. • Progettare, applicare, monitorare e revisionare periodicamente il sistema di gestione della sicurezza delle informazioni (ISMS) direttamente o guidando risorse in outsourcing. • Attuare un piano di cybersicurezza. • Comunicare, coordinare e cooperare con gli stakeholder interni ed esterni all'organizzazione. • Controllare le reti dell'organizzazione per rilevare violazioni della sicurezza e indagare quando si verifica. • Elaborare documentazione e reportistica relativa a violazioni di sicurezza. • Realizzare progetti in ambito continuità operativa. • Adottare standard di sicurezza e best practices per l'organizzazione.

Competenze e-CF assegnate	A.7.	Competenze e-CF assegnate	A.7.
	B.3.	Testing	B.3.
	B.5.	Produzione di documentazione	B.5.
	C.4.	Gestione del problema	C.4.
	D.1.	Sviluppo della strategia per la Sicurezza informatica	D.1.
	E.3.	Gestione del rischio	E.3.
	E.8.	Gestione della sicurezza dell'informazione	E.8.
	E.9.	Governance dei sistemi informativi	E.9.
Conoscenze	<ul style="list-style-type: none"> • Policy e procedure di cybersicurezza. • Standard, metodologie e framework di cybersicurezza. • Raccomandazioni e buone pratiche di cybersicurezza. • Leggi, regolamenti e normative della cybersicurezza. • Framework delle certificazioni relative alla cybersicurezza. • Pratiche di Ethical hacking. • Modelli di misurazione della maturità relativi alla cybersicurezza. • Standard, metodologie, processi e framework relativi al Risk management. • Pratiche e principi di mitigazione del rischio cyber. • Standard in materia di sicurezza dei sistemi informativi (ad esempio ISO 27001, ISO 27002, ISO 15408, ISO 22399, ISO 22301, OWASP, OSSTMM) e principali standard di sicurezza (ITSEC, ISO27001). • Metodologie e processi in ambito continuità operativa. • Network security (firewall, web application firewall, IPS, Network access control). • Security events (SIEM, SOAR, IDS, End Point). • Sistemi ISMS in accordo con la norma ISO 27001. • Normativa in materia di privacy. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di coordinare figure professionali Junior. • Essere in grado di redigere documentazione a supporto dei processi di compliance rispetto alle normative applicabili (ad esempio Studio di fattibilità per la continuità operativa, documentazione relative alla gestione degli incidenti informatici, analisi post-mortem). • Essere in grado di eseguire assessment tecnologici per l'identificazione degli strumenti e degli asset atti a garantire la Cyber Resilience. • Essere in grado di definire piani di Disaster Recovery. 		

	<ul style="list-style-type: none"> • Essere in grado di governare/gestire attività di patching (no implementazione) • Essere in grado di redigere documentazione tecnica e di progetto. • Essere in grado di gestire i rischi per la sicurezza delle informazioni e implementazione di nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni. • Essere in grado di gestire gli avvisi di sicurezza. • Essere in grado di individuare e correggere i difetti nei sistemi e nelle reti di computer.
<p>Certificazioni</p>	<p>Possesso di almeno una delle seguenti certificazioni aggiornate all'ultima release disponibile:</p> <ul style="list-style-type: none"> • Certified Information Security Manager (CISM). • Certified information systems security professional (CISSP). • Certified Ethical Hacker (CEH). • Certified Information Systems Auditor (CISA). • Certified Information Privacy Professional (CIPP). • CompTIA Security+. • Lead Auditor ISO 27001. <p>per almeno il 60% delle risorse (arrotondato all'unità superiore) previste per il singolo Contratto esecutivo.</p>
<p>Titolo di studio</p>	<p>Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.</p>
<p>Esperienza lavorativa</p>	<p>Minimo 10 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 5 nella funzione.</p>

4. INFORMATION SECURITY CONSULTANT JUNIOR

Titolo del profilo	INFORMATION SECURITY CONSULTANT JUNIOR		
Riferimento profilo ECSF	Chief Information Security Officer		
Descrizione sintetica	Figura professionale di riferimento per attività e progetti correlati alla strategia di cybersicurezza dell'organizzazione alla sua implementazione per garantire la sicurezza e la protezione dei sistemi, servizi e asset digitali.		
Missione	<ul style="list-style-type: none"> • Contribuire all'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location). • Controllare il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. • Attuare misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione. 		
Principali Task	<ul style="list-style-type: none"> • Collaborare nella valutazione della postura di sicurezza dell'organizzazione. • Implementare politiche di sicurezza informatica, certificazioni, standard, metodologie e framework di cybersicurezza. • Analizzare leggi, regolamenti e normative in materia di sicurezza informatica, comprendere gli obblighi e le misure che impongono e collaborare alle azioni che consentano di rispettarli. • Collaborare nello sviluppo e implementazione di una strategia di cybersicurezza. • Monitorare periodicamente il sistema di gestione della sicurezza delle informazioni (ISMS). • Supportare la risoluzione dei problemi di cybersicurezza. • Collaborare alla definizione di un piano di cybersicurezza. • Comunicare e cooperare con gli stakeholder interni ed esterni all'organizzazione. • Controllare le reti dell'organizzazione per rilevare violazioni della sicurezza. • Collaborare alla elaborazione di documentazione e reportistica relativa a violazioni di sicurezza. • Collaborare a progetti in ambito continuità operativa. 		
Competenze e-CF assegnate	A.7.	Competenze e-CF assegnate	A.7.
	B.3.	Testing	B.3.

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)

Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

	B.5.	Produzione di documentazione	B.5.
	C.4.	Gestione del problema	C.4.
	D.1.	Sviluppo della strategia per la Sicurezza informatica	D.1.
	E.3.	Gestione del rischio	E.3.
	E.8.	Gestione della sicurezza dell'informazione	E.8.
	E.9.	Governance dei sistemi informativi	E.9.
Conoscenze	<ul style="list-style-type: none"> • Policy e procedure di cybersicurezza. • Standard, metodologie e framework di cybersicurezza. • Raccomandazioni e buone pratiche di cybersicurezza. • Leggi, regolamenti e normative relative alla cybersicurezza. • Framework delle certificazioni relative alla cybersicurezza. • Pratiche di Ethical hacking. • Modelli di misurazione della maturità relativi alla cybersicurezza. • Standard, metodologie, processi e framework relativi al Risk management. • Pratiche e principi di mitigazione del rischio. • Standard in materia di sicurezza dei sistemi informativi (ad esempio ISO 27001, ISO 27002, ISO 15408, ISO 22399, ISO 22301, OWASP, OSSTMM) e principali standard di sicurezza (ITSEC, ISO27001). • Metodologia e processi in ambito continuità operativa. • Network security (firewall, web application firewall, IPS, Network access control). • Security events (SIEM, SOAR, IDS, End Point). • Sistemi ISMS in accordo con la norma ISO 27001. • Normativa in materia di privacy. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di redigere documentazione a supporto dei processi di compliance rispetto alle normative applicabili (ad esempio Studio di fattibilità per la continuità operativa, documentazione relative alla gestione degli incidenti informatici, analisi post-mortem). • Essere in grado di redigere documentazione tecnica e di progetto. • Essere in grado di gestire attività di patching (no implementazione). • Essere in grado di elaborare studi di sistemi e delle reti di computer per la valutazione dei rischi per determinare come migliorare le politiche e i protocolli di sicurezza. • Essere in grado di elaborare studi di sistemi e delle reti informatiche, incluso il processo di valutazione dei rischi di sicurezza. 		

	<ul style="list-style-type: none">• Essere in grado di correlare tra i cambiamenti dei sistemi informatici e gli attacchi informatici.• Essere in grado di gestire i rischi per la sicurezza delle informazioni e implementazione di nuovi modi per proteggere i sistemi informatici e le reti delle organizzazioni.
Certificazioni	N/A
Titolo di studio	Laurea triennale in materie tecnico-scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 3 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 2 nella funzione.

5. SECURITY SOLUTION ARCHITECT

Titolo del profilo	SECURITY SOLUTION ARCHITECT
Riferimento profilo ECSF	Cybersecurity Architect
Descrizione sintetica	Figura professionale che si occupa della progettazione di soluzioni sicure, sviluppa la documentazione relativa all'architettura delle soluzioni e delle infrastrutture.
Missione	<ul style="list-style-type: none"> • Progettare, costruire, eseguire test e implementare i sistemi di sicurezza all'interno della rete IT di un'organizzazione. • Progettare un'architettura di rete sicura al fine anticipare tutte le potenziali mosse e tattiche che eventuali attaccanti possono utilizzare per ottenere l'accesso non autorizzato al sistema informatico.
Principali Task	<ul style="list-style-type: none"> • Condurre l'analisi dei requisiti di cybersicurezza. • Definire le specifiche architeturali e funzionali delle soluzioni di cybersicurezza. • Rendere resiliente l'architettura per evitare "Single Point Of Failure" (SPOF). • Analizzare i sistemi in essere per identificare soluzioni di cybersicurezza efficaci. • Progettare nuovi sistemi e architetture tenendo conto dei requisiti imposti dalle norme relative alla cybersicurezza e dalla privacy rispettando il principio della Security and Privacy by Design. • Guidare e collaborare con chi si occupa operativamente dell'implementazione e con il personale Information Technology (IT) e Operational Technology (OT). • Proporre architetture di cybersicurezza. • Selezionare specifiche, procedure e controlli appropriati nel contesto dell'organizzazione. • Coordinare l'integrazione delle soluzioni di cybersicurezza. • Analizzare le configurazioni e le regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, SOAR, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi Cloud oriented per la sicurezza). • Identificare soluzioni tecnologiche e organizzative da porre in essere per ottimizzare e migliorare le configurazioni di infrastrutture ICT.

	<ul style="list-style-type: none"> • Adottare tecnologie per la sicurezza IT, soprattutto in ambito sicurezza cloud. • Adottare tecniche di correlazione eventi, progettazione di regole di correlazione e tuning sistemi. 	
Competenze e-CF assegnate	A.5. Competenze e-CF assegnate	A.5.
	A.6. Disegno delle applicazioni	A.6.
	B.1. Sviluppo delle applicazioni	B.1.
	B.3. Testing	B.3.
	B.6. Ingegneria dei sistemi	B.6.
	C.2. Supporto alle modifiche/evoluzioni del sistema	C.2.
	D.1. Sviluppo della strategia per la Sicurezza informatica	D.1.
	E.8. Gestione della sicurezza dell'informazione	E.8.
	E.9. Governance dei sistemi informativi	E.9.
Conoscenze	<ul style="list-style-type: none"> • Raccomandazioni e buone pratiche relative alla cybersicurezza. • Standard, metodologie e framework relative alla cybersicurezza • Requisiti di analisi relativi alla cybersicurezza. • Ciclo di vita dello sviluppo software sicuro. • Modelli di riferimento e di integrazione per le architetture di sicurezza. • Tecnologie, soluzioni e controlli relativi alla cybersicurezza. • Rischi, minacce, vulnerabilità e tendenze relative alla cybersicurezza. • Requisiti di compliance a regolamenti, normative e buone pratiche. • Procedure legacy di cybersicurezza. • Privacy-Enhancing Technology (PET). • Standard, metodologie e framework relativi alla Privacy by Design; • Algoritmi di cifratura. • Pratiche e principi relativi ai controlli degli accessi. • Framework delle certificazioni relative alla cybersicurezza. • 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). 	
Abilità	<ul style="list-style-type: none"> • Essere in grado di comprendere l'infrastruttura IT, le relazioni tra i differenti sistemi e componenti infrastrutturali al fine di individuare 	

	<p>problematiche architetturali che ne potrebbero compromettere la sicurezza.</p> <ul style="list-style-type: none"> • Essere in grado di analizzare le configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, SOAR, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza). • Essere in grado di verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT. • Essere in grado di utilizzare sistemi di correlazione eventi, di progettazione regole di correlazione e di tuning di sistemi di analisi eventi. • Essere in grado di utilizzare sistemi di autenticazione, sistemi di Identity & Access Management con esperienza di integrazione.
Certificazioni	<p>possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • Certified information systems security professional (CISSP). • Certified Information Systems Security Architecture Professional (CISSP-ISSAP). • Certified Information Systems Security Engineering Professional (CISSP-ISSEP). • CompTIA CySA+. <p>per almeno il 60% delle risorse (arrotondato all'unità superiore) previste per il singolo Contratto esecutivo.</p>
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 6 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione

6. SECURITY SOLUTION ARCHITECT SENIOR

Titolo del profilo	SECURITY SOLUTION ARCHITECT SENIOR
Riferimento profilo ECSF	Cybersecurity Architect
Descrizione sintetica	Figura professionale che si occupa della progettazione di soluzioni sicure, e sviluppa la documentazione relativa all'architettura delle soluzioni e delle infrastrutture.
Missione	<ul style="list-style-type: none"> • Progettare, costruire, eseguire test e implementare i sistemi di sicurezza all'interno della rete IT di un'organizzazione. • 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.
Principali Task	<ul style="list-style-type: none"> • Condurre l'analisi dei requisiti di cybersicurezza. • Definire le specifiche architeturali e funzionali delle soluzioni di cybersicurezza. • Rendere resiliente l'architettura per evitare "Single Point Of Failure" (SPOF). • Analizzare i sistemi in essere per identificare soluzioni di cybersicurezza efficaci. • Progettare nuovi sistemi e architetture tenendo conto dei requisiti imposti dalla cybersicurezza e dalla privacy rispettando il principio della Security and Privacy by Design. • Guidare e collaborare con chi si occupa operativamente dell'implementazione e con il personale Information Technology (IT) e Operational Technology (OT). • Proporre architetture di cybersicurezza che si basino sulle esigenze e sul budget degli stakeholder. • Selezionare specifiche, procedure e controlli appropriati nel contesto dell'organizzazione. • Coordinare l'integrazione delle soluzioni di cybersicurezza. • Analizzare delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, SOAR, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi Cloud oriented per la sicurezza).

	<ul style="list-style-type: none"> • Identificare soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per trarre la piena adozione delle contromisure previste. • Adottare tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento. • Adottare tecnologie di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione. • Coordinare figure professionali Junior. 		
Competenze e-CF assegnate	A.5	Progettazione di architetture	Livello e-5
	A.6.	Disegno delle applicazioni	Livello e-4
	B.1.	Sviluppo delle applicazioni	Livello e-4
	B.3.	Testing	Livello e-4
	B.6.	Ingegneria dei sistemi	Livello e-5
	C.2.	Supporto alle modifiche/evoluzioni del sistema	Livello e-5
	D.1.	Sviluppo della strategia per la Sicurezza informatica	Livello e-4
	E.8.	Gestione della sicurezza dell'informazione	Livello e-5
	E.9.	Governance dei sistemi informativi	Livello e-4
Conoscenze	<ul style="list-style-type: none"> • Raccomandazione e buone pratiche relative alla cybersicurezza. • Standard, metodologie e framework relative alla cybersicurezza • Requisiti di analisi relativi alla cybersicurezza. • Ciclo di vita dello sviluppo di software sicuro. • Modelli di riferimento e di integrazione per le architetture di sicurezza. • Tecnologie, soluzioni e controlli relativi alla cybersicurezza. • Rischi, minacce, vulnerabilità e tendenze relative alla cybersicurezza. • Requisiti di compliance a regolamenti, normative e buone pratiche. • Procedure legacy di cybersicurezza. • Privacy-Enhancing Technology (PET). • Standard, metodologie e framework relativi alla Privacy by Design. • Algoritmi di cifratura. • Pratiche e principi relativi ai controlli degli accessi. • Framework delle certificazioni relative alla cybersicurezza. • 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).
Abilità	<ul style="list-style-type: none"> • Essere in grado di comprendere l'infrastruttura IT, le relazioni tra i differenti sistemi e componenti infrastrutturali volta all'individuazione di problematiche architettoniche che ne potrebbero compromettere la sicurezza. • Essere in grado di analizzare le configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, SOAR, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza). • Essere in grado di verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT mediante uso di metodologie e strumenti operativi. • Essere in grado di utilizzare tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento. • Essere in grado di utilizzare sistemi di correlazione eventi, di progettazione regole di correlazione e di tuning di sistemi di analisi eventi con esperienza di integrazione. • Essere in grado di utilizzare sistemi di autenticazione, sistemi di Identity & Access Management con esperienza di integrazione.
Certificazioni	<p>possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • Certified information systems security professional (CISSP). • Certified Information Systems Security Architecture Professional (CISSP-ISSAP). • Certified Information Systems Security Engineering Professional (CISSP-ISSEP). • CompTIA CySA+ <p>per almeno il 60% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente
Esperienza lavorativa	Minimo 10 anni da computarsi successivamente al conseguimento al conseguimento del titolo di studio requisito del profilo, di cui almeno 5 nella funzione



Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

Classificazione Consip: Ambito pubblico

7. CLOUD SECURITY EXPERT

Titolo del profilo	CLOUD SECURITY EXPERT		
Riferimento profilo ECSF	Cybersecurity Implementer		
Descrizione sintetica	Figura professionale responsabile di sviluppare, rilasciare e rendere operative soluzioni di cybersicurezza relative alle infrastrutture Cloud e impostare le configurazioni sicure sui sistemi.		
Missione	<ul style="list-style-type: none"> • Creare la strategia di sicurezza delle risorse e dei dati durante il processo di migrazione in ambito Cloud. • Progettare, implementare e gestire soluzioni cloud sicure, efficienti e scalabili, identificando i servizi e le tecnologie cloud più adatti per scenari multi-cloud (Azure, AWS, GCP). 		
Principali Task	<ul style="list-style-type: none"> • Integrare le soluzioni di cybersicurezza nell'infrastruttura dell'organizzazione. • Configurare le soluzioni in base ai criteri di cybersicurezza dell'organizzazione. • Valutare la sicurezza e le prestazioni delle soluzioni di cybersicurezza. • Sviluppare codice, script e programmi. • Identificare e risolvere i problemi di cybersicurezza. • Implementare e gestire soluzioni di sicurezza per proteggere i dati e le applicazioni nel cloud. • Monitorare l'infrastruttura cloud, identificando e rispondendo rapidamente ad eventuali minacce. • Implementare soluzioni di gestione degli accessi (IAM) ai dati e alle risorse cloud al fine assicurare accessi autorizzati. Garantire che le soluzioni cloud siano conformi alle normative e agli standard di sicurezza applicabili, come GDPR, HIPAA e ISO 27001. • Condurre regolari valutazioni delle vulnerabilità e test di penetrazione per identificare e mitigare i rischi di sicurezza. • Implementare piani di risposta agli incidenti per affrontare eventuali violazioni della sicurezza. 		
Competenze assegnate e-CF	A.5.	Disegno architetture	Livello e-3
	A.6.	Disegno applicazioni	Livello e-3
	A.7.	Monitoraggio dei trend tecnologici	Livello e-3
	B.3.	Testing	Livello e-3
	B.4.	Deploy delle soluzioni	Livello e-4

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)

Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

	B.6. Ingegneria dei sistemi	Livello e-3
Conoscenze	<ul style="list-style-type: none"> • Ciclo di vita dello sviluppo di software sicuro. • Sicurezza dei sistemi informativi e delle reti. • Soluzioni e controlli relativi alla cybersicurezza. • Pratiche di sicurezza difensive e offensive. • Raccomandazioni e buone pratiche relativi alla cybersicurezza. • Raccomandazioni e buone pratiche relative allo sviluppo sicuro del software. • Standard, metodologie e framework relative al testing del software. • Algoritmi di cifratura. • Tecniche di autorizzazione. • Cloud Services Provider quali AWS, Google Cloud, e Microsoft Azure. • Soluzioni IAM. • Strumenti di vulnerability assessment e penetration testing. 	
Abilità	<ul style="list-style-type: none"> • Essere in grado di valutare situazioni complesse e prendere decisioni basate sui dati. • Essere in grado di identificare rapidamente i problemi di sicurezza e sviluppare soluzioni efficaci. • Essere in grado di monitorare e valutare le minacce di sicurezza. • Essere in grado di gestire progetti e priorità in modo efficiente, rispettando le scadenze. • Essere in grado di gestire le autorizzazioni di accesso ai dati e alle risorse cloud. • Essere in grado di rispondere in modo flessibile a nuove sfide e minacce di sicurezza in continua evoluzione. 	
Certificazioni	<p>possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • CompTIA Security+. • Certified Ethical Hacker (CEH). • Certified Cloud Security Professional (CCSP). • AWS Certified Security – Specialty. • Microsoft Certified: Azure Security Engineer Associate <p>per almeno il 60% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>	
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.	

Esperienza lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.
-----------------------	--

8. OT/IOT SECURITY EXPERT

Titolo del profilo	OT/IOT SECURITY EXPERT		
Riferimento profilo ECSF	Cybersecurity Implementer		
Descrizione sintetica	Figura professionale responsabile di sviluppare, rilasciare e rendere operative soluzioni di cybersicurezza relative di servizi e sistemi OT/IoT e impostare le configurazioni sicure sui sistemi		
Missione	<ul style="list-style-type: none"> • Creare la strategia di sicurezza delle risorse e dei dati nell'ambito dei sistemi IT/IoT. • Implementare gli aspetti di security a partire dalla fase di progettazione fino alla fase di esercizio, verifica e testing in campo delle performance di servizi e sistemi OT/IoT. 		
Principali Task	<ul style="list-style-type: none"> • Integrare le soluzioni di cybersicurezza nell'infrastruttura dell'organizzazione. • Configurare le soluzioni in base ai criteri di cybersicurezza dell'organizzazione. • Valutare la sicurezza e le prestazioni delle soluzioni. • Sviluppare codice, script e programmi. • Identificare e risolvere i problemi di cybersicurezza. • Valutare controlli di sicurezza messi in atto per proteggere i sistemi OT/IoT, mediante l'utilizzo di metodologie e framework adatte per il mondo industriale. • Gestire le vulnerabilità, reverse engineering, penetration testing di hardware e software. • Conoscenza degli strumenti e delle normative di sicurezza OT/IoT. • Revisionare architetture di rete OT/IoT per renderla più sicura e resiliente contro gli attacchi cyber. • Garantire la conformità agli standard e alle normative del settore (ad esempio, NERC CIP, IEC 62443, NIST SP 800-82). • Monitorare reti e sistemi OT al fine di rilevare violazioni della sicurezza, attività insolite e potenziali minacce. 		
Competenze assegnate e-CF	A.5.	Disegno architetture	Livello e-3
	A.6.	Disegno applicazioni	Livello e-3
	A.7.	Monitoraggio dei trend tecnologici	Livello e-3
	B.3.	Testing	Livello e-3
	B.4.	Deploy delle soluzioni	Livello e-4
	B.6.	Ingegneria dei sistemi	Livello e-3

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)

Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

<p>Conoscenze</p>	<ul style="list-style-type: none"> • Ciclo di vita dello sviluppo di software sicuro. • Sicurezza dei sistemi informativi e delle reti. • Soluzioni e controlli relativi alla cybersicurezza. • Pratiche di sicurezza difensive e offensive. • Raccomandazioni e buone pratiche relativi alla cybersicurezza. • Raccomandazioni e buone pratiche relative allo sviluppo sicuro del software. • Standard, metodologie e framework relative al testing di cybersicurezza. • Algoritmi di cifratura. • Tecniche di autorizzazione. • Risk & Maturity Assessment sui sistemi OT/IoT. • Tecniche di Incident Response. • Network Security Monitoring e Secure Network Architecture. • Web Application Security, Penetration Testing, Reverse Engineering. • Tecnologie operative come controllori logici programmabili (PLC), software SCADA (Supervisory Control and Data Acquisition), RTU, HMI e sistemi di controllo distribuito (DCS). • Standard e framework di sicurezza, tra cui: IEC62443, NIST CSF. • Protocolli di comunicazione di rete IT e OT (ad esempio: TCP/IP, UDP, DNP3, Modbus, IEC 61850, OPC, OPC UA, PROFINET, ecc.).
<p>Abilità</p>	<ul style="list-style-type: none"> • Essere in grado di applicare politiche e procedure di sicurezza dei sistemi IoT/OT coerenti con le politiche delle organizzazioni e gli standard di settore (ad esempio, ISO/IEC 27001, ISA/IEC 62443). • Essere in grado di lavorare a stretto contatto con i team di sicurezza IT per garantire il rilevamento e la risposta completi alle minacce negli ambienti IoT e OT. • Essere in grado di supportare le risposte agli incidenti specifici per gli incidenti di sicurezza OT, inclusa l'analisi e la risoluzione delle cause principali. • Essere in grado di sviluppare e mantenere piani di risposta agli incidenti per gli ambienti OT.
<p>Certificazioni</p>	<p>Possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • CompTIA Security+. • Certified Ethical Hacker (CEH). • Global Industrial Cyber Security Professional (GICSP). • Certified Information Security Manager (CISM). • Certified SCADA Security Architect (CSSA).

	<ul style="list-style-type: none">• SC-200: Microsoft Security Operations Analyst.• Certified Information Systems Security Professional (CISSP) per almeno il 60% 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 tecnico-scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.

9. DATA PROTECTION SPECIALIST

Titolo del profilo	DATA PROTECTION SPECIALIST		
Riferimento profilo ECSF	Cyber legal, policy & compliance officer		
Descrizione sintetica	Figura professionale che garantisce la conformità rispetto alle normative (interne ed esterne), ai framework/standard internazionali e alle politiche organizzative.		
Missione	<ul style="list-style-type: none"> Fornire consulenza legale e organizzativa per lo sviluppo dei processi di Cybersecurity Governance e raccomanda strategie e soluzioni per garantire il rispetto di requisiti normativi. 		
Principali Task	<ul style="list-style-type: none"> Sviluppare la strategia dell'organizzazione alla luce di requisiti normativi o imposti da standard. Gestire le problematiche che possono sorgere in materia di rischio cyber conseguentemente all'attuazione dei processi organizzativi o della strategia organizzativa. Guidare lo sviluppo, la diffusione, la comprensione e l'attuazione di adeguate politiche di cybersicurezza e di procedure che integrino i requisiti organizzativi e quelli legali. Condurre, monitorare e revisionare le valutazioni di impatto normativo sull'organizzazione utilizzando standard, framework, metodologie e strumenti opportuni. Conoscere, recepire i requisiti e gli standard etici nella gestione dei dati personali. Analizzare le conseguenze che potrebbero derivare da modifiche del quadro giuridico. Verificare l'allineamento della strategia cyber dell'Amministrazione con le linee guida, le direttive e normative a livello nazionale ed europeo. Valutare gli impatti ed i rischi in ambito cybersicurezza inerente i contratti di servizio in essere dell'Amministrazione. Verificare la conformità a normative nell'utilizzo di framework e linee guida per la gestione del rischio di cybersicurezza. 		
Competenze e-CF assegnate	A.1.	Allineamento dei Sistemi informativi alla strategia di business	Livello e-4
	D.1.	Sviluppo della strategia per la sicurezza informatica	Livello e-4
	E.3.	Gestione del rischio	Livello e-3

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)

Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

	E.4.	Miglioramento dei processi	Livello e-3
	E.8.	Gestione della sicurezza dell'informazione	Livello e-3
Conoscenze	<ul style="list-style-type: none"> • Leggi, regolamenti e norme relative alla cybersicurezza. • Standard, metodologie e framework relative alla cybersicurezza. • Policy e procedure di cybersicurezza. • Requisiti di conformità legale e regolatori, raccomandazioni e buone pratiche relative alla cybersicurezza. • Requisiti, framework e modelli relativi al Risk Management. • Analisi dei processi. • Misure di sicurezza tecniche ed organizzative necessarie per proteggere i dati personali da accessi non autorizzati, perdite o distruzioni. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di analizzare i rischi per la protezione dei dati personali nei processi dell'organizzazione, identificando le vulnerabilità e le potenziali violazioni. • Essere in grado di utilizzare strumenti e le tecnologie per la gestione, la protezione e la sicurezza dei dati personali. • Essere in grado di promuovere una cultura della privacy all'interno dell'organizzazione. • Essere in grado di diffondere, spiegare e adattare i requisiti legali e normativi alle necessità dell'organizzazione. • Essere in grado di valutare l'impatto delle tendenze e delle tecnologie emergenti e sviluppi normativi a livello mondiale che comportano rischi significativi associati alla cybersecurity. • Essere in grado di comunicare e collaborare in team multidisciplinari. 		
Certificazioni	<p>possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • Certified Information Privacy Professional/Europe (CIPP/E). • Certified Information Systems Security Professional (CISSP) <p>per almeno il 60% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>		
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche e/o giuridiche o cultura equivalente.		
Esperienza lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.		

10. DATA PRIVACY & PROTECTION SPECIALIST

Titolo del profilo	DATA PRIVACY & PROTECTION SPECIALIST
Riferimento profilo ECSF	Cyber legal, policy & compliance officer
Descrizione sintetica	Figura professionale che garantisce la conformità rispetto alle normative (interne ed esterne), ai framework/standard internazionali e alle politiche organizzative. Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche.
Missione	<ul style="list-style-type: none"> • Verificare 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	<ul style="list-style-type: none"> • Gestire i problemi che possono sorgere in materia di protezione dei dati e della privacy conseguentemente all'attuazione dei processi organizzativi o della strategia organizzativa; • Guidare lo sviluppo, la diffusione, la comprensione e l'attuazione di adeguate politiche di protezione della privacy e di procedure che integrino i requisiti organizzativi e quelli legali; • Condurre, monitorare e revisionare le valutazioni di impatto sulla privacy utilizzando standard, framework, metodologie e strumenti opportuni; • Produrre informative e comunicazioni in ambito di protezione dei dati e privacy da diffondere agli stakeholder e agli utenti dell'organizzazione; • Conoscere e recepire i requisiti e gli standard etici nella gestione dei dati personali. • Controllare la corretta applicazione del GDPR. • Sviluppare e mantenere aggiornato un programma di gestione della protezione dei dati (DPMP) che copra le politiche, i processi e le persone in ogni fase del ciclo di vita dei dati. • Individuare le tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione d'impatto (DPIA) per identificare, valutare i rischi nell'utilizzo dei dati li, in base alle funzioni, alle esigenze e ai processi dell'organizzazione. • Sensibilizzare il personale che tratta dati personali sviluppando un programma di formazione sulle politiche e sui processi di protezione dei dati personali.

	<ul style="list-style-type: none"> • Favorire la consapevolezza della protezione dei dati personali all'interno dell'organizzazione. • Migliorare i processi di conformità nelle varie fasi del ciclo di vita dei dati o delle informazioni. • Informare e fornire supporto al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento. • Individuare il Titolare e/o al Responsabile le aree funzionali alle quali riservare un audit interno o esterno in tema di protezione dei dati. • Cooperare nei rapporti con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità. 		
Competenze e-CF assegnate	A.1.	Allineamento dei Sistemi informativi alla strategia di business	Livello e-4
	D.1.	Sviluppo della strategia per la sicurezza informatica	Livello e-4
	E.3.	Gestione del rischio	Livello e-3
	E.4.	Miglioramento dei processi	Livello e-3
	E.8.	Gestione della sicurezza dell'informazione	Livello e-3
Conoscenze	<ul style="list-style-type: none"> • Leggi, regolamenti e norme relative alla privacy. • Standard, metodologie e framework relative alla privacy. • Policy e procedure di privacy • Requisiti di conformità legale e regolatoria, raccomandazioni e buone pratiche relative alla privacy. • Analisi dei processi. • Misure di sicurezza tecniche ed organizzative necessarie per proteggere i dati personali da accessi non autorizzati, perdite o distruzioni. • Procedure forensi e norme che tutelano i dati personali e i patrimoni informativi. • Informatica giuridica. 		
Abilità	<ul style="list-style-type: none"> • Essere in grado di identificare i processi rilevanti ai fini della protezione dei dati. • Essere in grado di svolgere le attività di verifica dell'attribuzione delle responsabilità e di formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. • Essere in grado di raccogliere e catalogare le informazioni rilevanti ai fini della supervisione alla tenuta del registro dei trattamenti. 		

	<ul style="list-style-type: none"> • Essere in grado di gestire la procedura di Data Protection Impact Assessment (DPIA). • Essere in grado di valutare l'impatto delle tendenze e delle tecnologie emergenti e sviluppi normativi a livello mondiale che comportano rischi significativi associati alla protezione dei dati. • Essere in grado di individuare le priorità in funzione del livello di rischio nella protezione dei dati di ciascun singolo trattamento. • Essere in grado di progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali. • Essere in grado di comunicare e collaborare in team multidisciplinari.
Certificazioni	<p>possesso di almeno una delle seguenti certificazioni:</p> <ul style="list-style-type: none"> • Certified Information Privacy Professional/Europe (CIPP/E). • Certified Information Privacy Manager (CIPM). • Certified Information Privacy Technologist (CIPT) <p>per almeno il 60% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche e/o giuridiche o cultura equivalente.
Esperienza lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.

11. FORENSIC EXPERT

Titolo del profilo	FORENSIC EXPERT		
Riferimento profilo ECSF	Digital Forensics Investigator		
Descrizione sintetica	Figura operativa che si occupa del recupero e dell'analisi di prove digitali nell'ambito di investigazioni forensi. La figura deve essere costantemente aggiornata sulle normative e sulle tecniche di cyber-crime.		
Missione	<ul style="list-style-type: none"> Gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente di cybersicurezza documentando il tutto in modo che sia correttamente presentabile in sede processuale. 		
Principali Task	<ul style="list-style-type: none"> Identificare, analizzare e correlare gli eventi di cybersicurezza. Spiegare e presentare prove digitali in modo semplice e facilmente comprensibile. Elaborare ed esporre rapporti di indagine dettagliati e motivati. Guidare le indagini sulle violazioni dei dati e sugli incidenti di sicurezza in cui sono già stati generati allarmi. Collaborare nello smantellamento e nella ricostruzione dei sistemi interessati e nel successivo recupero di dati incriminanti. Analizzare i computer e altri dispositivi digitali, garantendo la conservazione delle prove digitali, il recupero, l'analisi, l'analisi dei dati. Analizzare ed acquisire informazioni su ambienti di tipo Public Cloud. Gestire analisi tecniche anche mediante l'utilizzo di software forensi. Redigere IOC (Indicatori di Compromissione). Avviare indagini relative ad incidenti informatici. Raccogliere, analizzare e presentare in tribunale prove digitali. Consegnare dati e rapporti dettagliati, per consentirne poi l'utilizzo da esperti legali dell'Amministrazione. Supportare l'Amministrazione nei rapporti con l'Autorità Giudiziaria. 		
Competenze e-CF assegnate	A.7.	Monitoraggio dei trend tecnologici	Livello e-3
	B.3.	Testing	Livello e-4
	B.5.	Produzione di documentazione	Livello e-3
	E.3.	Gestione del Rischio	Livello e-3
	E.8.	Gestione della sicurezza dell'informazione	Livello e-4
Conoscenze	<ul style="list-style-type: none"> Raccomandazioni, Standard, metodologie e framework relative alla Digital Forensic. 		

	<ul style="list-style-type: none"> • Principi, pratiche e procedure di analisi della Digital Forensic analysis e di testing. • Algoritmi, tecniche e strumenti di cifratura e decifratura. • Standard, procedure, metodologie e framework relativi alla Criminal Investigation. • Leggi, regolamenti e norme relative alla cybersecurity. • Strumenti di analisi dei malware. • Minacce cyber e vulnerabilità dei sistemi informatici. • Procedure relative agli attacchi informatici. • Sicurezza dei sistemi operativi e delle reti. • Framework delle certificazioni relative alla cybersecurity. • Metodi utilizzati dagli hacker per aggirare le difese poste a salvaguardia della sicurezza informatica. • Tecniche e metodologie per la raccolta dei dati. • Procedure forensi e norme che tutelano i dati personali e i patrimoni informativi. • Conoscenze approfondite sul crimine informatico. • Tool di analisi forense quali X-Ways, Magnet Axiom, FTK Forensics Toolkit. • Tool di analisi di mobile forensic.
Abilità	<ul style="list-style-type: none"> • Essere in grado di analizzare e catalogare i dati raccolti. • Essere in grado di esaminare i dati per individuare elementi probatori, come comunicazioni, attività sospette o prove di crimini informatici. Lavorare sia autonomamente che in team, in modalità multitasking anche in situazione di forte stress. • Essere in grado di lavorare in modo etico senza influenze di attori interni o esterni.
Certificazioni	<p>Possesso di almeno una tra le seguenti certificazioni:</p> <ul style="list-style-type: none"> • GIAC – Certification Forensic Examiner (GCFE). • Certified Cyber Forensic Professional (GCFP) <p>per almeno il 60% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche e/o giuridiche o cultura equivalente.
Esperienza lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.

12. RISK MANAGER

Titolo del profilo	RISK MANAGER		
Riferimento profilo ECSF	Cybersecurity Risk Manager		
Descrizione sintetica	Figura che si occupa della gestione dei rischi e dello sviluppo di strategie di mitigazione degli stessi.		
Missione	<ul style="list-style-type: none"> Valutare rischi e vulnerabilità relativi alla cybersicurezza ed elaborare strategie efficaci per eliminarli in modo definitivo, o comunque per minimizzarli e renderli il meno impattanti possibile. 		
Principali Task	<ul style="list-style-type: none"> Implementare standard, metodologie e framework di gestione del rischio di cybersicurezza e garantire il rispetto di normative e linee guida. Analizzare e consolidare le pratiche di gestione del rischio dell'organizzazione. Sviluppare e implementare misure di sicurezza per mitigare i rischi individuati. Creare e implementare piani per gestire gli incidenti di sicurezza. Sviluppare programmi di formazione per il personale. Monitorare l'efficacia delle strategie di gestione del rischio introdotte e adattarle, se necessario. Redigere resoconti per informare l'organizzazione e gli stakeholder. 		
Competenze e-CF assegnate	E.3.	Gestione del Rischio	Livello e-4
	E.5.	Miglioramento dei processi	Livello e-3
	E.7.	Gestione del cambiamento del business	Livello e-4
	E.8.	Governo dei sistemi informativi	Livello e-4
Conoscenze	<ul style="list-style-type: none"> Standard, metodologie e framework relativi alla gestione del rischio. Raccomandazioni, buone pratiche, strumenti e processi relativi alla gestione del rischio. Minacce cyber e vulnerabilità dei sistemi informatici. Soluzioni e controlli relativi alla cybersicurezza. Rischi relativi alla cybersicurezza. Criteri di valutazione della sicurezza e dell'affidabilità delle terze parti. Processi di valutazione, monitoraggio e testing di efficacia dei controlli di cybersicurezza per la protezione di un'organizzazione contro le minacce informatiche. Framework delle certificazioni relative alla cybersicurezza. 		

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)
 Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

	<ul style="list-style-type: none"> • Tecnologie, anche emergenti, relative alla cybersicurezza. • Leggi, regolamenti e norme relative alla cybersicurezza e privacy. • Principi e processi relativi alla Supply Chain e ai rischi connessi.
Abilità	<ul style="list-style-type: none"> • Essere in grado di analizzare grandi quantità di dati per identificare trend, schemi e potenziali minacce. • Essere in grado di sviluppare piani di gestione del rischio in linea con gli obiettivi dell'organizzazione. • Essere in grado di analizzare i processi dell'organizzazione per individuare potenziali minacce operative, finanziarie, legali o reputazionali • Essere in grado di lavorare sia autonomamente che in team, in modalità multitasking anche in situazione di forte stress.
Certificazioni	<p>Possesso della seguente certificazione:</p> <ul style="list-style-type: none"> • Certified in Risk and Information Systems Control (CRISC) per il 100% delle risorse appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.
Titolo di studio	Laurea magistrale specialistica in materie tecnico-scientifiche e/o giuridiche o cultura equivalente.
Esperienza lavorativa	Minimo 5 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 3 nella funzione.

13. SECURITY AUDITOR SENIOR

Titolo del profilo	SECURITY AUDITOR SENIOR		
Riferimento profilo ECSF	Cybersecurity Auditor		
Descrizione sintetica	Figura professionale che svolge audit di cybersicurezza all'interno dell'organizzazione.		
Missione	<ul style="list-style-type: none"> Assicurare la compliance con i requisiti imposti dai regolamenti, dalla normativa, dagli standard di settore e dai requisiti di cybersicurezza. Individuare i possibili punti vulnerabili di un sistema informativo. 		
Principali Task	<ul style="list-style-type: none"> Seguire ed applicare standard, metodologie e framework relativi agli audit. Applicare strumenti e tecniche di auditing. Analizzare i processi organizzativi e valutare la sicurezza software / hardware, nonché i controlli tecnici e organizzativi. Scomporre e analizzare i sistemi per identificare le vulnerabilità ed eventuali controlli inefficaci. Diffondere, spiegare e adattare i requisiti legali e normativi alle necessità dell'organizzazione. Raccogliere, valutare, mantenere e proteggere le informazioni relative agli audit. Condurre gli IT audit. Completa i giornali di audit documentando test e risultati dell'audit. Pianificare ed eseguire il monitoraggio della sicurezza di reti, applicazioni ed utenti che compongono il sistema in esame. Rilevare eventuali abusi e violazioni sia accidentali che dolosi. Produrre resoconti che sintetizzano i risultati raggiunti. Valutare i sistemi ISMS in accordo con la norma ISO:27001. Utilizzare metodologie e linee guida ISO in materia di IT audit e applicare le stesse in funzione dei criteri di audit identificati. Utilizzare le linee guida ISO sui controlli di sicurezza in ambito Enterprise e Cloud. 		
	B.3.	Testing	Livello e-4
	B.5.	Produzione di documentazione	Livello e-5
	E.3.	Gestione del rischio	Livello e-4
	E.6.	Gestione della qualità IT	Livello e-5

	E.8.	Gestione della sicurezza delle informazioni	Livello e-4
Conoscenze		<ul style="list-style-type: none"> Soluzioni e controlli relativi alla cybersicurezza. Principi, raccomandazioni e buone pratiche relativi alla cybersicurezza. Requisiti di compliance a regolamenti, normative e buone pratiche relative alla cybersicurezza. Monitoraggio, test e valutazione dell'efficacia dei controlli di cybersicurezza. Standard, metodologie e framework relativi alle verifiche di conformità agli audit di cybersicurezza. Framework relativo alle certificazioni relative all'auditing e alla cybersicurezza. Requisiti, framework e modelli relativi al Risk Management. Principi e pratiche relative al ciclo di vita dei sistemi. 	
Abilità		<ul style="list-style-type: none"> Essere in grado di organizzare e lavorare in modo sistematico e deterministico basandosi sulle evidenze raccolte. Essere in grado di condurre gli IT audit con integrità, imparzialità e indipendenza. Essere in grado di adottare processi e delle procedure operative IT. Essere in grado di applicare metodologie e linee guida ISO in materia di IT audit. Essere in grado di applicare linee guida ISO sui controlli di sicurezza in ambito Enterprise e Cloud. Essere in grado di valutare sistemi ISMS in accordo con la norma ISO:27001. Essere in grado di valutare la compliance in materia Privacy. Essere in grado di definire e governare piani di rientro. 	
Certificazioni		<p>possesso della seguente certificazione:</p> <ul style="list-style-type: none"> Certified Information System Auditor (CISA) <p>per il 100% delle risorse appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>	
Titolo di studio		Laurea magistrale specialistica in materie tecnico-scientifiche o cultura equivalente.	
Esperienza lavorativa		Minimo 10 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 5 nella funzione.	

14. SECURITY MANAGER

Titolo del profilo	SECURITY MANAGER		
Riferimento profilo ECSF	Chief Information Security Officer		
Descrizione sintetica	Figura professionale che definisce la strategia di cybersicurezza di un'organizzazione.		
Missione	<ul style="list-style-type: none"> • Garantire la sicurezza delle risorse informative, dei sistemi informatici e delle reti aziendali. • Definire e pianificare strategie per la gestione dei rischi informatici. 		
Principali Task	<ul style="list-style-type: none"> • Sviluppare le politiche di sicurezza delle informazioni. • Pianificare e implementare le strategie per la gestione dei rischi informatici. • Supervisionare l'implementazione di controlli di sicurezza, come l'accesso alle informazioni, la crittografia dei dati e la protezione delle reti. • Collaborare con le altre strutture organizzative per garantire la conformità alle normative sulla privacy e sulla sicurezza dei dati. • Definire, implementare, gestire e mantenere un programma di governance della sicurezza delle informazioni. • Creare una struttura di gestione della sicurezza dell'informazione. • Creare un quadro per il monitoraggio della governance della cybersicurezza tenendo conto delle analisi costi/benefici dei controlli e del ROI (Return on Investment). • Identificare e selezionare le risorse necessarie per implementare e mantenere efficacemente i controlli sui sistemi informativi. • Comprendere il processo di audit IT e avere familiarità con gli standard di audit IT. • AUtilizzare tecniche di audit IT per esaminare e testare le tecnologie e le applicazioni dei sistemi informativi. • Eseguire il processo di audit secondo gli standard stabiliti e interpretare i risultati in base a criteri definiti per assicurare che i sistemi informativi siano protetti, controllati ed efficaci nel supportare gli obiettivi dell'organizzazione. 		
Competenze e-CF assegnate	A.7.	Monitoraggio dei trend tecnologici	Livello e-4
	B.5.	Produzione di documentazione	Livello e-4

	D.1.	Sviluppo della strategia per la Sicurezza informatica	Livello e-5
	E.3.	Gestione del rischio	Livello e-5
	E.8.	Gestione della sicurezza dell'informazione	Livello e-4
	E.9.	Governance dei sistemi informativi	Livello e-5
Conoscenze		<ul style="list-style-type: none"> • Policy e procedure di cyber security. • Standard, metodologie e framework di cyber security. • Raccomandazione e buone pratiche di cybersecurity. • Leggi, regolamenti e normative della cybersecurity. • Framework delle certificazioni relative alla cybersecurity. • Requisiti per la cybersicurezza etica. • Modelli di misurazione della maturità relativi alla cybersecurity. • Standard, metodologie, processi e framework relativi al Risk management. • Normativa in materia di privacy. 	
Abilità		<ul style="list-style-type: none"> • Essere in grado di comprendere il processo di audit IT e avere familiarità con gli standard di audit IT. • Essere in grado di individuare le risorse necessarie per l'attuazione del piano di gestione dei rischi • Avere visione dei rischi e delle minacce che potrebbero compromettere la business continuity dell'organizzazione. • Avere capacità di project management. • Essere in grado di comunicare in maniera efficace. • Essere in grado di promuovere il lavoro di squadra. 	
Certificazioni		possesso di almeno una delle seguenti certificazioni: <ul style="list-style-type: none"> • Certified Information Security Manager (CISM). • Certified information systems security professional (CISSP); per almeno il 60% 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 tecnico-scientifiche e/o giuridiche o cultura equivalente.	
Esperienza lavorativa		Minimo 10 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 5 nella funzione.	

15. PENETRATION TESTER SENIOR

Titolo del profilo	PENETRATION TESTER SENIOR		
Riferimento profilo ECSF	Penetration Tester		
Descrizione sintetica	Figura che si occupa della valutazione dell'efficacia dei controlli di cybersicurezza e dell'identificazioni di vulnerabilità dei sistemi e delle infrastrutture.		
Missione	<ul style="list-style-type: none"> Tentare di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. 		
Principali Task	<ul style="list-style-type: none"> Sviluppare script e programmi per verificare la cybersicurezza di sistemi, reti e applicazioni. Svolgere attività di ingegneria sociale. Identificare ed essere in grado di sfruttare le vulnerabilità. Condurre attività di "Ethical Hacking". Utilizzare i tool di Penetration testing. Condurre analisi tecniche e reporting. Analizzare i sistemi per identificare le vulnerabilità e i controlli inefficaci. Eseguire analisi statica/dinamica/mobile del codice e delle configurazioni di sistema. Gestire processi di hardening di sistemi e di piattaforme middleware. Valutare la validità dei pattern di sviluppo sicuro del software attraverso la ricerca di vulnerabilità nelle applicazioni e nei sistemi. Utilizzare tecniche di penetration testing, strumenti software ed exploit disponibili. Analizzare le vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi. Documentare gli attacchi condotti, affinché siano ripetibili. Verificare l'efficacia delle misure applicate come remediation alla fine dell'engagement. 		
Competenze assegnate e-CF	B.2.	Integrazione delle componenti	Livello e-4
	B.3.	Testing	Livello e-4
	B.4.	Rilascio di soluzioni	Livello e-2
	B.5.	Produzione di documentazione	Livello e-3
	E.3.	Gestione del Rischio	Livello e-4
Conoscenze	<ul style="list-style-type: none"> Procedure relative agli attacchi informatici. 		

Gara a procedura aperta ai sensi del D.Lgs. 36/2023 e s.m.i., per la conclusione di un Accordo Quadro per ogni Lotto avente ad oggetto l'affidamento di servizi Managed Security Services da remoto, di Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (ID 2737)

Appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 – Profili professionali

	<ul style="list-style-type: none"> • Applicazioni di Information technology (IT) e Operational technology (OT). • Procedure offensive e difensive. • Sicurezza e protocolli relativi ai sistemi operativi e alle reti. • Procedure di Penetration testing. • Standard, metodologie e framework relative ai Penetration test. • Strumenti per effettuare Penetration test. • Programmazione informatica. • Minacce e vulnerabilità dei sistemi informatici. • Policy, raccomandazioni e buone pratiche relative alla cybersecurity. • Framework delle certificazioni relative alla cybersecurity. • Leggi, regolamenti e norme relative alla cybersecurity. • Processo di hardening di sistemi e piattaforme middleware.
<p>Abilità</p>	<ul style="list-style-type: none"> • Essere in grado di identificare e risolvere i problemi di cybersicurezza. • Essere in grado di coordinare figure professionali Junior. • Essere in grado di operare simulando i comportamenti sia del ruolo di attaccante, contestualmente rispettando le regole di ingaggio, che del ruolo utente target. • Essere in grado di comprendere l'importanza per il management delle informazioni recuperate, individuando velocemente potenziali punti utili a condurre ulteriori attacchi. • Essere in grado di utilizzare modalità, tecniche e strumenti di penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware. • Essere in grado di attuare le modalità di disegno e di valutazione dei sistemi di gestione per la sicurezza. • Essere in grado di adottare pattern di sviluppo sicuro del codice. • Essere in grado di eseguire 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.
<p>Certificazioni</p>	<p>Possesso di almeno una tra le seguenti certificazioni:</p> <ul style="list-style-type: none"> • Offsec Certified Professional (OSCP). • OSSTMM Professional Security Tester (OPST). • Certified Etical Hacher (CEH) <p>per almeno il 60% delle risorse (arrotondato all'unità superiore), appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo.</p>

Titolo di studio	Laurea magistrale specialistica in materie scientifiche o cultura equivalente.
Esperienza lavorativa	Minimo 10 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 5 nella funzione.

16. PENETRATION TESTER JUNIOR

Titolo del profilo	PENETRATION TESTER JUNIOR		
Riferimento profilo ECSF	Penetration Tester		
Descrizione sintetica	Figura che si occupa della valutazione dell'efficacia dei controlli di cybersicurezza e dell'identificazioni di vulnerabilità dei sistemi e delle infrastrutture.		
Missione	<ul style="list-style-type: none"> Tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. 		
Principali Task	<ul style="list-style-type: none"> Partecipare allo sviluppo di script e programmi per verificare la cybersicurezza di sistemi, reti e applicazioni. Contribuire allo svolgimento di attività di ingegneria sociale. Partecipare ad attività di "Ethical Hacking". Utilizzare i tool di Penetration testing. Partecipare alla conduzione di analisi tecniche e reporting. Contribuire all'analisi dei sistemi per identificare le vulnerabilità. Partecipare all'esecuzione di analisi statica/dinamica/mobile del codice e delle configurazioni di sistema. Partecipare alla gestione di processi di hardening di sistemi e di piattaforme middleware. Contribuire alla validazione di pattern di sviluppo sicuro del codice. Partecipare all'attuazione di tecniche di penetration testing Utilizzare strumenti software di penetration testing ed exploit disponibili. Analizzare le vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi. Documentare gli attacchi condotti, affinché siano ripetibili. Contribuire alla verifica dell'efficacia delle misure applicate come remediation alla fine dell'engagement. 		
Competenze e-CF assegnate	B.2.	Integrazione delle componenti	Livello e-2
	B.3.	Testing	Livello e-3
	B.4.	Rilascio di soluzioni	Livello e-1
	B.5.	Produzione di documentazione	Livello e-2
	E.3.	Gestione del Rischio	Livello e-2
Conoscenze	<ul style="list-style-type: none"> Procedure relative agli attacchi informatici. 		

	<ul style="list-style-type: none"> • Applicazioni di Information Technology (IT) e Operational Technology (OT). • Procedure offensive e difensive. • Sicurezza e protocolli relativi ai sistemi operativi e alle reti. • Procedure relative a Penetration test. • Standard, metodologie e framework relative ai Penetration testing. • Strumenti per effettuare Penetration testing. • Programmazione informatica. • Minacce e vulnerabilità dei sistemi informatici. • Policy, raccomandazioni e buone pratiche relative alla cybersecurity. • Framework delle certificazioni relative alla cybersecurity. • Leggi, regolamenti e norme relative alla cybersecurity. • Processo di hardening di sistemi e piattaforme middleware.
Abilità	<ul style="list-style-type: none"> • Essere in grado di utilizzare strumenti di analisi statiche e dinamiche del codice sorgente o delle configurazioni di sistema. • Essere in grado di collaborare nell'adozione al processo di hardening di sistemi e piattaforme middleware. • Essere in grado di collaborare all'utilizzo dei pattern di sviluppo sicuro del codice. • Essere in grado di collaborare nell'esecuzione degli attacchi informatici, attraverso l'uso di strumenti software, tool ed exploit disponibili pubblicamente. • Essere in grado di collaborare nella stesura di documentazione degli attacchi condotti, affinché siano ripetibili • Essere in grado di partecipare alla verifica dell'efficacia delle misure applicate come remediation alla fine dell'engagement.
Certificazioni	N/A
Titolo di studio	Laurea triennale in materie tecnico-scientifiche o cultura equivalente
Esperienza lavorativa	Minimo 3 anni da computarsi successivamente al conseguimento del titolo di studio requisito del profilo, di cui almeno 2 nella funzione.

17. SCHEMA PER LA PRESENTAZIONE DEI CURRICULA

Di seguito viene presentato lo schema che il fornitore dovrà utilizzare per la compilazione dei curriculum vitae. Si sottolinea che nella redazione dei contenuti dovranno essere privilegiati gli aspetti di interesse per la fornitura e che orientativamente il documento non dovrà superare le 3 pagine.

Nominativo	<i>(Inserire il Cognome e il Nome della risorsa)</i>		
Ruolo	<i>(Inserire il Ruolo attualmente ricoperto dalla risorsa)</i>		
Figura professionale	<i>(Indicazione del ruolo assegnato alla risorsa in funzione delle figure professionali richieste nel capitolato tecnico).</i>		
Servizio/attività	<i>(Fornire l'indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato Tecnico)</i>		
Conoscenze	<i>(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)</i>		
Principali Esperienze Lavorative	<i>(Indicare le esperienze più significative per la gara in oggetto e comprovanti le competenze richieste nell'Appendice 2, a partire dalla più recente, fornendo una breve descrizione delle attività svolte, del ruolo ricoperto, della durata del progetto. E' necessario suddividere le esperienze per anno e per settore (Es: Pubblica Amministrazione, Bancario, Telecomunicazioni))</i>		
	Settore	Data inizio- Data fine	Esperienze
Competenze Tecniche	<i>(Indicare le competenze specifiche di cui si è in possesso)</i>		
Specializzazioni	<i>(Indicare eventuali specializzazioni, master, ecc.)</i>		
	Anno	Titolo	Descrizione

Certificazioni	<i>(Indicare eventuali certificazioni)</i>		
	Anno	Titolo	Descrizione
Istruzione	<i>(indicare i titoli di studio)</i>		
Lingue	<i>Per ogni lingua straniera, indicare il grado di conoscenza, dove: 1 - in grado di leggere 2 - in grado di leggere e scrivere 3 - in grado di leggere, parlare e scrivere in maniera più che comprensibile 4 - fluente sia nello scritto che nell'orale 5 - madrelingua - (native language)</i>		
	Lingue	Grado di conoscenza	
Principali pubblicazioni	<i>(indicare le principali pubblicazioni)</i>		