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 2B - PROFILI PROFESSIONALI LOTTO 1

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 sicurezza da remoto 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 e nell'Appendice 2, 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 2, 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.
Missione	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.

<table>
<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.
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.</td></tr>
</table>

	• 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 organizzazione.
Principali Task	• 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.

<table>
<tr><td></td><td colspan="3">

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 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.

</td></tr>
</table>

	• 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.		
Principali Task	• 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.		
Competenze e-CF assegnate	B.2.	Integrazione dei componenti	Livello 4
	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 3
	E.8.	Gestione della sicurezza dell'informazione	Livello 4
	E.9.	Governance dei sistemi informativi	Livello 4
Conoscenze	• 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. • 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