APPENDICE 2

DESCRIZIONE DEI PROFILI PROFESSIONALI

PREINFORMATIVA PER L'AFFIDAMENTO DEI SERVIZI DI CONDUZIONE, MANUTENZIONE E SUPPORTO SPECIALISTICO PER LA GESTIONE E L'EVOLUZIONE DELL'INFRASTRUTTURA ICT DI INAIL

INDICE

1. PREMESSA

Di seguito si riporta la tabella di correlazione tra le figure professionali ed i servizi richiesti in gara.

È richiesto che il Fornitore indichi in Offerta il dimensionamento e la composizione dei diversi team di risorse che si impegna ad utilizzare per l'erogazione dei servizi di conduzione dell'infrastruttura ICT remunerati a canone, tenendo conto di quanto indicato nel Disciplinare di gara in relazione ai criteri di merito tecnico.

Qualunque sia l'organizzazione che il Fornitore intenda proporre per i suddetti team di risorse, nel formulare la propria offerta tenga presente tale tabella, ferma restando la facoltà per il Fornitore stesso di proporre il mix di figure professionali ritenuto più funzionale alle finalità e agli obiettivi di qualità della fornitura.

Si precisa che i servizi di conduzione e manutenzione degli impianti tecnologici, qualunque sia l'organizzazione che il Fornitore intenda proporre per l'erogazione dei servizi, dovranno essere svolti da figure professionali con le caratteristiche specificate al par. 4.2.24 del Capitolato Tecnico.

Lotto 1

Servizi	CT	CI	SP	SS	S
Conduzione infrastruttura ICT	x	x	x	x	x
Supporto specialistico all'implementazione dei progetti di IT Innovation	x	x	x	x	x

Servizi	CP	SCS	SCJ	SP	SPJ	SS	S
Supporto specialistico al Security Operation Center (SOC)	x	x	x	x	x	x	x

Lotto 2

Servizi	CT	CI	SP	EP	SS	S
Supporto alle strutture gestionali nel controllo operativo dei servizi					x	x
Supporto al System Test			x		x	x
Supporto specialistico su tecnologie, sistemi e reti	x		x		x	x
Supporto agli studi architetturali e ai progetti tecnologici	x	x	x		x	x
Supporto ai progetti applicativi		x	x		x	
Supporto alla definizione/revisione dei processi				x		

Legenda

CT: Consulente di evoluzione tecnologica

CI: Consulente di integrazione applicativa

SP: Specialista di prodotto (per SOC in ambito sicurezza)

SPJ: Specialista di prodotto junior (in ambito sicurezza)

SS: Sistemista Senior (per SOC in ambito sicurezza)

S: Sistemista (per SOC in ambito sicurezza)

CP: Capo Progetto (in ambito sicurezza)

SCS: Security Consultant senior

SCJ: Security Consultant junior

2. DESCRIZIONE DEI PROFILI PROFESSIONALI

Nei paragrafi seguenti è fornita la descrizione dei profili professionali minimi da impiegare nella fornitura.

Le figure professionali proposte dovranno fare riferimento ai profili descritti, fermo restando l'obbligo per il Fornitore ad 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, senza alcun onere aggiuntivo per INAIL.

I *curricula vitae* del personale da impiegare nei vari servizi dovranno essere resi disponibili a INAIL secondo quanto previsto dal Capitolato tecnico e dal contratto, rispettando il template riportato al paragrafo 3.

Per ogni profilo è richiesto il possesso di una esperienza lavorativa in ambito ICT.

Per ogni profilo è inoltre richiesto il possesso di uno specifico titolo di studio oppure di una "cultura equivalente", che corrisponde ad una esperienza lavorativa aggiuntiva rispetto a quella indicata nel profilo stesso. L'entità dell'esperienza aggiuntiva necessaria dipende dal titolo di studio posseduto dalla risorsa proposta rispetto a quello richiesto, come sintetizzato nella seguente tabella. Ad esempio, nel caso in cui fosse richiesta una laurea magistrale in discipline tecnico/scientifiche con esperienza in ambito ICT di 8 anni, il possesso di laurea triennale richiederebbe esperienza minima di 10 anni (8+2). In ogni caso, il titolo di studio posseduto deve essere almeno un diploma di scuola secondaria di secondo grado.

Esperienza aggiuntiva da considerare come "cultura equivalente"

Titolo di studio Posseduto / Titolo di studio Richiesto	Laurea triennale in discipline tecnico/scientifiche	Laurea magistrale (altre discipline)	Laurea triennale (altre discipline)	Diploma di perito tecnico Industriale in Informatica	Altro diploma di scuola secondaria di secondo grado
Laurea magistrale in discipline tecnico/scientifiche	+2 anni	+2 anni	+4 anni	+5 anni	+9 anni
Laurea triennale in discipline tecnico/scientifiche			+2 anni	+4 anni	+7 anni

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.

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.

Si precisa che:

- non è necessario che ciascuna risorsa possegga la totalità delle conoscenze richieste per il profilo professionale di riferimento: le tecnologie su cui sono richieste le competenze/certificazioni elencate nei profili possono essere intese come fra loro alternative, in funzione del servizio di assegnazione o delle esigenze progettuali;
- le certificazioni richieste, per i servizi di conduzione ICT remunerati a canone e per i servizi di supporto specialistico al SOC remunerati in giorni/persona, potranno eventualmente essere conseguite entro sei mesi dalla data di inizio attività;
- requisito fondamentale è individuare figure professionali con una forte propensione alla comunicazione e ai rapporti personali, con attitudine ad operare nella Pubblica Amministrazione.

2.1. Consulente di evoluzione tecnologica

Qualifica professionale	Consulente di evoluzione tecnologica
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 10 anni di cui almeno 5 nella funzione
Competenze/attitudini	- Esplora gli sviluppi tecnologici ICT e concepisce soluzioni innovative per integrare le nuove tecnologie nelle infrastrutture e nei servizi esistenti - Individua e propone soluzioni evolutive in termini di infrastrutture ICT - Definisce in autonomia le strategie di implementazione delle piattaforme tecnologiche
Esperienze consolidate	- Redazione di specifiche e documentazione di progetto - Redazione di documentazione e manualistica tecnica - Tecniche di gestione progetti - Progettazione test integrati - Analisi e risoluzione problemi
Conoscenze	- Dimensionamento infrastrutture ICT e capacity planning; - Progettazione, disegno, realizzazione e test di architetture tecnologiche complesse e di architetture tecnologiche a supporto dei servizi Cloud e di Disaster Recovery/Business Continuity - Progettazione, disegno, realizzazione e test di interventi evolutivi relativi alla logistica e all'attrezzaggio dei CED - Conoscenza delle principali tendenze evolutive delle architetture tecnologiche e analisi d'impatto della relativa implementazione sulle soluzioni in uso - Conoscenze approfondita ed integrata degli elementi tecnologici che costituiscono un sistema complesso, quali a titolo esemplificativo e non esaustivo: • Piattaforme di virtualizzazione e bilanciamento del carico • sistemi gestionali Java/Oracle • sistemi gestionali .NET/Microsoft SQL Server • sistemi di automation, orchestration, provisioning • sistemi di Project and Portfolio Management • sistemi di IT Infrastructure Management • sistemi conoscitivi e di data warehouse • sistemi di workflow, collaboration e gestione documentale • sistemi di Identity Management • infrastrutture di rete e sistemi di sicurezza • sistemi di storage management (Storage Area Network e Tape Area Network) • sistemi di monitoraggio e gestione delle performance • sistemi di Service Management • sistemi di integrazione EAI e EII
Certificazione	Ove l'attività e/o l'intervento lo richieda, nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze per le risorse professionali impiegate attraverso la produzione della certificazione, al massimo livello conseguibile, nelle piattaforme ovvero nei prodotti SW di riferimento per l'attività e/o l'intervento.

2.2. Consulente di integrazione applicativa

Qualifica professionale	Consulente di Integrazione applicativa
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 10 anni di cui almeno 5 nella funzione
Competenze/attitudini	- Esplora gli sviluppi tecnologici ICT e concepisce soluzioni innovative per lo sviluppo di nuove servizi e l'implementazione dei servizi esistenti - Partecipa alla valutazione e alla scelta delle soluzioni ICT - Partecipa alla definizione delle specifiche di progetto
Esperienze consolidate	- Redazione di specifiche e documentazione di progetto - Redazione di documentazione e manualistica tecnica - Tecniche di gestione progetti - Progettazione test integrati - Analisi e risoluzione problemi
Conoscenze	- Analisi delle necessità di impianto delle applicazioni in ambienti complessi e/o in ambienti Cloud e/o in regime di Disaster Recovery/Business Continuity - Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico - Controllo qualità del codice e rispetto degli standard di programmazione con l'uso di strumenti di profilazione - Ottimizzazione delle strutture dati - Integrazione applicativa con servizi federati (es. autenticazione, firme digitali, porta di dominio, ecc.) - Conoscenze consolidate degli ambiti tecnologici e applicativi che costituiscono un sistema complesso, quali a titolo esemplificativo e non esaustivo: • Piattaforme Cloud (on premises, pubbliche o ibride) e servizi da queste erogati • Piattaforme di virtualizzazione e bilanciamento del carico • Sicurezza delle applicazioni • Prodotti MW e applicativi in ambito gestionale, documentale, content management, Big Data, conoscitivo e BI • Piattaforme di collaboration e CTI • Piattaforme per il monitoraggio e controllo • Piattaforme a supporto della qualità del SW • Sistemi di deployment in ambienti Unix e Unix-like/J2EE e Microsoft .NET/Sharepoint • Strumenti di valutazione delle performance delle applicazioni e dei sistemi
Certificazione	Ove l'attività e/o l'intervento lo richieda, nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze per le risorse professionali impiegate attraverso la produzione della certificazione, al massimo livello conseguibile, nelle piattaforme ovvero nei prodotti SW di riferimento per l'attività e/o l'intervento.

2.3. Specialista di prodotto/Specialista di prodotto senior (ambito Sicurezza)

Qualifica professionale	Specialista di prodotto/ Specialista di prodotto senior (ambito Sicurezza)
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni di cui almeno 4 nella funzione
Competenze/attitudini	- Partecipa alla valutazione e alla scelta delle soluzioni ICT - Partecipa alla definizione delle specifiche di progetto - Verifica e analizza le performance delle infrastrutture e delle relative componenti ed individua le attività necessarie alla loro ottimizzazione
Esperienze consolidate	- Analisi e progettazione di sistemi informativi, package, procedure complesse - Redazione documentazione tecnica - Redazione di specifiche di progetto - Controllo e realizzazione procedure - Progettazione test integrati - Analisi e risoluzione problemi
Conoscenze	Conoscenze specialistiche su installazione, configurazione, personalizzazione, amministrazione, tuning, analisi di vulnerabilità e trouble shooting dei prodotti SW di mercato e/o open source e delle soluzioni che ne sfruttano le funzionalità, nei diversi ambiti tecnologici che costituiscono un sistema complesso, quali a titolo esemplificativo e non esaustivo: - Piattaforme Cloud, on premises, pubbliche o ibride, e servizi da esse erogati - Piattaforme di virtualizzazione e bilanciamento del carico - Sistemi operativi - Prodotti MW e applicativi in ambito gestionale, documentale, content management, Big Data, conoscitivo e BI - Piattaforme di collaboration e CTI - Piattaforme per il monitoraggio e controllo - Piattaforme per il Data Center Automation e per la gestione centralizzata dell'infrastruttura ICT - Sistemi di storage management (Storage Area Network e Tape Area Network) - prodotti di penetration test/vulnerability assessment - prodotti di accesso e autenticazione - prodotti/soluzioni di sicurezza (Firewall, IPS, VPN, sistemi di autenticazione forte, Antivirus, ecc.) - apparati di rete e relativi sistemi operativi In ambito Sicurezza, oltre alle conoscenze specialistiche sui prodotti e le soluzioni, con particolare riferimento alle soluzioni McAfee, è richiesta la conoscenza delle procedure di triage degli alert di sicurezza, di rilevamento delle intrusioni, di gestione degli eventi di rete e di information security.
Certificazione	Ove l'attività e/o l'intervento lo richieda, nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze per le risorse professionali impiegate attraverso la produzione della certificazione, al massimo livello conseguibile, nelle piattaforme ovvero nei prodotti SW di riferimento per l'attività e/o l'intervento.

2.4. Specialista di prodotto junior (ambito Sicurezza)

Qualifica professionale	Specialista di prodotto junior (ambito Sicurezza)
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 4 anni, di cui almeno 2 nella funzione
Competenze/attitudini	- Partecipa alla valutazione e alla scelta delle soluzioni ICT - Partecipa alla definizione delle specifiche di progetto - Verifica e analizza le performance delle infrastrutture e delle relative componenti ed individua le attività necessarie alla loro ottimizzazione
Esperienze consolidate	- Redazione documentazione tecnica - Redazione di specifiche di progetto - Controllo e realizzazione procedure - Analisi e risoluzione problemi
Conoscenze	Conoscenze specialistiche su installazione, configurazione, personalizzazione, amministrazione, tuning, analisi di vulnerabilità e trouble shooting dei prodotti SW di mercato e/o open source e delle soluzioni che ne sfruttano le funzionalità, negli ambiti tecnologici relativi alla sicurezza dei dati e delle informazioni, quali a titolo esemplificativo e non esaustivo: - prodotti di penetration test/vulnerability assessment - prodotti di accesso e autenticazione - prodotti/soluzioni di sicurezza (Firewall, IPS, VPN, sistemi di autenticazione forte, Antivirus, ecc.) Oltre alle conoscenze specialistiche sui prodotti e le soluzioni di sicurezza, con particolare riferimento alle soluzioni McAfee, è richiesta la conoscenza delle procedure di triage degli alert di sicurezza, di rilevamento delle intrusioni, di gestione degli eventi di rete e di information security.
Certificazione	Ove l'attività e/o l'intervento lo richieda, nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze per le risorse professionali impiegate attraverso la produzione della certificazione, al massimo livello conseguibile, nelle piattaforme ovvero nei prodotti SW di riferimento per l'attività e/o l'intervento.

2.5. Capo Progetto (ambito sicurezza)

Qualifica professionale	Capo Progetto (ambito sicurezza)
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Esperienza in ambito ICT	Minimo 12 anni di cui almeno 4 nella funzione
Competenze/attitudini	Oltre alle competenze/attitudini richieste per la figura professionale Security Consultant senior (vedi 2.6): - Dirige e coordina le attività del Security Operation Center (SOC) e ne gestisce le risorse professionali e la strategia tecnologica, assicurando il raggiungimento degli obiettivi della DCOD - Fornisce alla DCOD input e suggerimenti per la strategia di sicurezza globale - Funge da punto di riferimento organizzativo per gli incidenti critici
Esperienze consolidate	Oltre alle esperienze consolidate richieste per la figura professionale Security Consultant senior (vedi 2.6): - Conduzione di progetti in ambienti tecnologici complessi - Gestione di team di risorse ad elevata professionalità - Redazione di specifiche e documentazione di progetto - Tecniche di gestione progetti
Conoscenze	Sono richieste le conoscenze previste per la figura professionale Security Consultant senior (vedi 2.6)
Certificazioni richieste	E' richiesta la certificazione PMI Project Management Professional (PMP)

2.6. Security Consultant senior

Qualifica professionale	Security Consultant senior
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Esperienza in ambito ICT	Minimo 10 anni di cui almeno 5 nella funzione
Competenze/attitudini	- Esplora gli sviluppi tecnologici in ambito sicurezza ICT e concepisce soluzioni per integrare le nuove tecnologie nelle infrastrutture e nei servizi esistenti - Definisce in autonomia le strategie di implementazione delle piattaforme di sicurezza - Definisce ed implementa le politiche di sicurezza - Assicura che i rischi legati alla sicurezza siano analizzati e gestiti - Controlla e prende iniziative a fronte di intrusioni, frodi o falle della sicurezza - Rivede gli incidenti sulla sicurezza e fornisce raccomandazioni per applicare strategie e policy specifiche per un miglioramento continuo della sicurezza
Esperienze consolidate	- Analisi di infrastrutture IT complesse per l'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza - Definizione e progettazione di controlli di sicurezza su prodotti MW - Realizzazione di script per automatizzare la gestione della sicurezza ed integrarla in modelli di workflow, IT Automation o IT Orchestration - Implementazione di sistemi di Identity & Access Management per la gestione di flussi applicativi autenticati - Disegno, implementazione e tuning di sistemi di security monitoring e di analisi eventi

Qualifica professionale	Security Consultant senior
	- Progettazione di regole di correlazione - Erogazione e presidio di servizi "CERT", ricezione segnalazioni e analisi di eventi di cyber security, predisposizione di documenti inerenti gli eventi analizzati, gestione degli incidenti informatici, raccolta e analisi dei dati e delle informazioni per il miglioramento della security governance - Conduzione di security assessment e definizione/governo dei piani di rientro dai rischi identificati - Valutazione di sistemi SGSI in accordo con la norma ISO:27001 e definizione/governo dei piani di rientro dai rischi identificati - Redazione della documentazione a supporto per i processi di compliance e definizione/governo dei piani di rientro dai rischi identificati - Formazione, informazione e supporto sul tema della cybersecurity
Conoscenze	- Conoscenza approfondita: o delle reti e delle tecnologie/soluzioni di sicurezza di mercato o delle problematiche di sicurezza e delle best practice da adottare o delle metodologie di vulnerability assessment, penetration test, compliance management e security audit o dei processi di Security Governance e Security Management o delle metodologie e degli standard ISO in materia di IT audit o delle direttive AgID in materia di sicurezza delle informazioni e continuità operativa dei servizi o dei principali aspetti di IT security riguardanti la compliance o delle metodologie e tecniche di analisi forense in ambito informatico - Ottima conoscenza dei modelli di deploy Cloud (public, private e Hybrid) e dei principali punti di attenzione in ambito sicurezza e compliance - Ottima conoscenza dei possibili modelli architetturali, compresi quelli basati sui micro-servizi, e dei possibili modelli di erogazione (virtualizzazione, container, PaaS, ecc.) e delle peculiarità di sicurezza relative - Buona conoscenza dei modelli di esecuzione "serverless computing" e delle problematiche di sicurezza derivanti dall'astrazione dei livelli sottostanti - Conoscenza dei modelli di sviluppo sicuro delle applicazioni (SecureSDLC)
Certificazioni richieste	Ove l'attività e/o l'intervento lo richieda, nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze per le risorse professionali impiegate attraverso la produzione della certificazione, al massimo livello conseguibile, sulla tematica di sicurezza ovvero sulla tecnologia/prodotto SW di riferimento per l'attività e/o l'intervento.

2.7. Security Consultant junior

Qualifica professionale	Security Consultant junior
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Esperienza in ambito ICT	Minimo 6 anni di cui almeno 3 nella funzione
Competenze/attitudini	- Supporta la definizione delle strategie di implementazione delle piattaforme di sicurezza - Definisce ed implementa le politiche di sicurezza - Assicura che i rischi legati alla sicurezza siano analizzati e gestiti - Controlla e prende iniziative a fronte di intrusioni, frodi o falle della sicurezza - Rivede gli incidenti sulla sicurezza e fornisce raccomandazioni per applicare strategie e policy specifiche per un miglioramento continuo della sicurezza
Esperienze consolidate	- Analisi di infrastrutture IT per l'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza - Implementazione di controlli di sicurezza su prodotti MW - Realizzazione di script per automatizzare la gestione della sicurezza ed integrarla in modelli di workflow, IT Automation o IT Orchestration - Implementazione e tuning di sistemi di security monitoring e di analisi eventi - Progettazione di regole di correlazione - Erogazione e presidio di servizi "CERT", ricezione segnalazioni e analisi di eventi di cyber security, predisposizione di documenti inerenti gli eventi analizzati, gestione degli incidenti informatici, raccolta e analisi dei dati e delle informazioni per il miglioramento della security governance - Esecuzione di security assessment e supporto alla definizione/governo dei piani di rientro dai rischi identificati - Formazione, informazione e supporto sul tema della cybersecurity
Conoscenze	- Ottima conoscenza: o delle reti e delle tecnologie/soluzioni di sicurezza di mercato o delle problematiche di sicurezza e delle best practice da adottare o delle metodologie di vulnerability assessment, penetration test, compliance management e security audit o dei processi di Security Governance e Security Management o delle metodologie e degli standard ISO in materia di IT audit o delle direttive AgID in materia di sicurezza delle informazioni e continuità operativa dei servizi - Buona conoscenza dei modelli di deploy Cloud (public, private e Hybrid) e dei principali punti di attenzione in ambito sicurezza e compliance - Buona conoscenza dei possibili modelli architetturali, compresi quelli basati sui micro-servizi, e dei possibili modelli di erogazione (virtualizzazione, container, PaaS, ecc.) e delle peculiarità di sicurezza relative
Certificazioni richieste	Ove l'attività e/o l'intervento lo richieda, nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze per le risorse professionali impiegate attraverso la produzione della certificazione, al massimo livello conseguibile, sulla tematica di sicurezza ovvero sulla tecnologia/prodotto SW di riferimento per l'attività e/o l'intervento.

2.8. Esperto processi

Qualifica professionale	Esperto processi
Titolo di studio	Laurea magistrale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 8 anni, di cui almeno 4 maturata su progetti di IT Service Management
Competenze/attitudini	- Definisce nuovi modelli di servizio e nuove modalità di erogazione/fruizione dei servizi esistenti, assicurando la misurazione dei risultati attesi, sia in termini di benefici conseguiti che di livelli di servizio - Progetta e disegna nuovi processi ICT e misura l'efficacia di quelli esistenti - Sfrutta le proprie conoscenze e le proprie esperienze, anche in termini di metodologie/best practices/linee guida/norme/standard di mercato, per valutare processi e soluzioni esistenti, al fine di individuare ambiti di innovazione e proporne le relative roadmap evolutive - Valuta i potenziali impatti dei cambiamenti organizzativi e di processo, definendo ed indirizzando le possibili soluzioni per mitigarne gli effetti
Esperienze consolidate	- Definizione, disegno e documentazione di modelli di erogazione di servizi ICT e supporto alla relativa introduzione e diffusione in contesti di business complessi/innovativi - Analisi, definizione e redazione di documentazione di processo e delle relative procedure gestionali e operative e/o di workflow specifici - Gestione di progetti di medie/grandi dimensioni correlati all'introduzione di nuovi processi/evoluzione di processi esistenti - Erogazione di sessioni formative volte all'adozione/diffusione di nuovi processi e di nuove modalità operative e/o gestionali - Definizione di specifiche funzionali e supporto all'implementazione, configurazione, parametrizzazione e personalizzazione delle piattaforme gestionali ed operative in uso presso strutture di erogazione di servizi IT - Definizione di specifiche funzionali e supporto all'implementazione, configurazione, parametrizzazione e personalizzazione di strumenti a supporto del governo e controllo dei servizi IT (report/cruscotti/dashboard)
Conoscenze	- Metodologie di Project Management e BPMN - Tecniche di gap analysis e di formalizzazione di processi - Best Practices ITIL e normativa ISO 20000 - Metodologie per l'analisi, il disegno e la revisione dell'IT Service Management - Tecniche di implementazione e gestione della qualità di un servizio IT - Prodotti software di Project/Risk Management - Piattaforme di IT Service Management
Certificazioni	Per ciascuna risorsa professionale impiegata in questo ruolo, il Fornitore dovrà comprovare le summenzionate conoscenze attraverso la produzione della certificazione **ITIL Expert in IT Service Management**, nella versione più recente ovvero nella versione indicata da INAIL

2.9. Sistemista Senior/Sistemista di sicurezza senior

Qualifica professionale	Sistemista senior/Sistemista di sicurezza senior
Titolo di studio	Laurea triennale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 10 anni di cui almeno 5 nella funzione
Competenze/attitudini	- Opera efficacemente in ambienti complessi, individua in maniera proattiva problematiche che potrebbero influire sulla fruizione dei servizi e ne indirizza la risoluzione, guida e supporta i componenti meno esperti del proprio team, collabora in piena sinergia con tutti i team che concorrono all'erogazione dei servizi all'utenza - Valuta e pianifica i cambiamenti, esegue e documenta le attività tecniche e i test relativi, operando in maniera proattiva per mitigarne gli impatti sulla fruizione dei servizi e per garantirne la rispondenza ai requisiti - Assicura il rispetto degli standard interni, esterni, nazionali ed internazionali per garantire l'integrità, l'interoperabilità e la sicurezza dei sistemi, delle relative componenti e delle informazioni - Verifica e ottimizza le performance dei sistemi e delle relative componenti, esegue le verifiche tecniche relative all'integrazione di sistema e ne garantisce la validazione e la documentazione dell'esito favorevole - Interpreta incidenti/problemi, individua le possibili soluzioni e ne valuta i possibili effetti collaterali, basandosi sulle proprie conoscenze e sulle informazioni provenienti da bollettini, community, case produttrici, basi dati di conoscenza e documentazione in uso, implementa le soluzioni individuate, tracciando sugli appositi strumenti tutti gli eventi occorsi e le attività effettuate - Effettua controlli sistematici per individuare minacce/debolezze dell'ambiente, proponendo azioni, strategie e policy specifiche atte a mitigare i rischi legati alla sicurezza e a garantire un miglioramento continuo del livello di sicurezza dell'infrastruttura
Esperienze consolidate	- Pianificazione, progettazione, dimensionamento, realizzazione e conduzione di infrastrutture ICT in contesti complessi/innovativi - Progettazione, analisi e realizzazione di architetture di BC/DR - Redazione e controllo di studi di fattibilità, documentazione tecnico-architetturale, procedure e/o specifiche tecniche, manuali operativi, template e/o manualistica utente e rapporti statistici sui servizi - Best Practices ITIL - Problem determination/solving in ambienti complessi - Utilizzo di strumenti di trouble ticketing e di gestione della conoscenza - Pianificazione, progettazione e implementazione di test di sistema e di test integrati tra diversi/e piattaforme, sistemi operativi, middleware e sistemi di gestione dati - Pianificazione, progettazione e implementazione di test prestazionali, di analisi dinamica e di sicurezza delle applicazioni - Tecniche di gestione progetti - Tecniche e strumenti di monitoraggio

Qualifica professionale	Sistemista senior/Sistemista di sicurezza senior

Conoscenze	- Ottima conoscenza di tecniche di progettazione e realizzazione di architetture volte a erogare servizi agli utenti di riferimento, comprensive di tutte le componenti necessarie (sistemi elaborativi, networking, security, basi dati, ecc.)
	- Conoscenza approfondita su installazione, configurazione, gestione e problem determination/solving di:
	  - software di base
	  - prodotti Middleware
	  - sistemi di storage management (SAN e TAN)
	  - sistemi di backup/restore dei dati
	  - prodotti di virtualizzazione e bilanciamento del carico
	  - prodotti di realizzazione video/audio conference
	  - prodotti di collaboration e CTI
	  - prodotti per il monitoraggio e controllo
	  - prodotti di supporto alla qualità del sw
	  - prodotti di performance test
	  - prodotti di penetration test/vulnerability assessment
	  - prodotti di accesso e autenticazione
	  - prodotti/soluzioni di sicurezza (Firewall, IPS, VPN, sistemi di autenticazione forte, Antivirus, ecc.)
	  - apparati di rete e relativi sistemi operativi
	- Conoscenza approfondita su installazione, configurazione, personalizzazione, gestione e problem determination/solving di piattaforme di Cloud Computing, con particolare riferimento alle funzioni di automation, orchestration e provisioning
	- Conoscenza approfondita su installazione, configurazione, gestione e problem determination/solving in ambito networking (routing, bilanciamento, sistemi di management, ecc…), di protocolli e architettura di rete TCP/IP, di tecnologie LAN/WAN e WIFI
	- Ottima conoscenza di data modeling, disegno e sviluppo di procedure ETL
	- Buona conoscenza di metodologie di project management/risk management e di strumenti software a supporto
	
	In ambito Sicurezza, oltre alle conoscenze specialistiche sui prodotti e le soluzioni, con particolare riferimento alle soluzioni McAfee, sono richieste:
	- Conoscenza approfondita dei principali standard di sicurezza (ITSEC, BS7799), dei principali tipi di vulnerabilità/attacchi di rete e delle tecniche di implementazione di azioni/policy in casi di intrusioni, frodi e/o compromissioni di sicurezza
	- Conoscenza approfondita delle procedure di risposta agli incidenti di sicurezza e di escalation
	- Capacità avanzate di analisi dei log e di correlazione di eventi
	- Capacità avanzate di valutazione dei malware e dei relativi impatti
	- Ottime conoscenze di intelligence ed analisi delle minacce
	- Conoscenze approfondite in ambito investigazione forense
	- Conoscenze approfondite in ambito Web Application Firewall

Qualifica professionale	Sistemista senior/Sistemista di sicurezza senior
Certificazioni	Per le risorse professionali impiegate in questo ruolo nei diversi ambiti, compresi i servizi di conduzione ICT remunerati a canone, il Fornitore dovrà comprovare le summenzionate conoscenze attraverso la produzione delle seguenti certificazioni, nella versione più recente ovvero nella versione indicata da INAIL: - Sistemi/Windows: Certificazione Windows Server - Sistemi/Linux: Certificazione RedHat RHCSA - Sistemi/pSeries: Certificazione AIX, VSphere - Sistemi/Virtualizzazione: Certificazione VMWare, Certificazione Citrix - Database/Oracle: Certificazioni Oracle Database Administration, Oracle Certified Expert, Oracle Exadata Administrator - Database/SQL: Certificazione MCSA SQL Database Administration, MCSA Azure Database Administrator - Database/Opendb: Certificazione Postgres, MongoDB - Middleware/J2EE: Certificazione RedHat Certified JBoss Administrator RHCJA, Red Hat Certified Specialist in Messaging Administration - Reti: certificazione CCNA o CCIE, per le attività di conduzione almeno una risorsa con certificazione CCIE - Cloud: Certificazione Cloudera, MCSA Azure Administrator Per le risorse professionali impiegate in questo ruolo nei servizi di supporto specialistico al SOC, ove l'attività lo richieda nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze attraverso la produzione della certificazione, al massimo livello conseguibile, sulla tematica di sicurezza ovvero sulla tecnologia/prodotto SW di riferimento. Le suddette certificazioni, per i servizi di conduzione ICT remunerati a canone e per i servizi di supporto specialistico al SOC remunerati in giorni/persona, potranno essere conseguite entro sei mesi dalla data di inizio delle attività.

2.10. Sistemista/Sistemista di sicurezza

Qualifica professionale	Sistemista/Sistemista di sicurezza
Titolo di studio	Laurea triennale in discipline tecnico/scientifiche o cultura equivalente
Anzianità lavorativa	Minimo 6 anni di cui almeno 3 nella funzione
Competenze/attitudini	- Opera in maniera proattiva in contesti anche non strettamente tecnologici, garantendo il rispetto dei livelli di servizio definiti, individuando e gestendo problematiche che potrebbero influire sulla fruizione dei servizi, collaborando con i membri del proprio team nonché con i componenti di altri team che concorrono all'erogazione dei servizi all'utenza - Utilizza e alimenta i sistemi di tracciamento e di gestione della conoscenza, predispone documentazione e manualistica a supporto dell'erogazione dei servizi da parte del proprio team ovvero di team terzi - Supporta la valutazione e la pianificazione dei cambiamenti, esegue e documenta le attività tecniche e i test relativi, operando in modo da mitigarne gli impatti sulla fruizione dei servizi e garantirne la rispondenza ai requisiti - Opera in linea con gli standard interni, esterni, nazionali ed internazionali per garantire l'integrità, l'interoperabilità e la sicurezza dei sistemi, delle relative componenti e delle informazioni - Verifica e analizza le performance dei sistemi e delle relative componenti ed effettua le attività necessarie alla loro ottimizzazione sulla base delle indicazioni degli specialisti, collaborando all'esecuzione delle verifiche tecniche relative all'integrazione di sistema - Interpreta incidenti/problemi, individua le possibili soluzioni e ne valuta i possibili effetti collaterali, basandosi sulle proprie conoscenze e sulle informazioni provenienti da bollettini, community, case produttrici, basi dati di conoscenza e documentazione in uso, implementa le soluzioni individuate, tracciando sugli appositi strumenti tutti gli eventi occorsi e le attività effettuate - Effettua controlli sistematici per individuare minacce/debolezze dell'ambiente, supportando la definizione di azioni, strategie e policy specifiche atte a mitigare i rischi legati alla sicurezza ed effettuandone l'implementazione
Esperienze consolidate	- Realizzazione e conduzione di infrastrutture ICT in contesti complessi/innovativi - Redazione e controllo di studi di fattibilità, documentazione tecnico-architetturale, procedure e/o specifiche tecniche, manuali operativi, template e/o manualistica utente e rapporti statistici sui servizi - Best Practices ITIL - Problem determination/solving in ambienti complessi - Utilizzo di strumenti di trouble ticketing e di gestione della conoscenza - Implementazione ed esecuzione di test di sistema e di test integrati tra diversi/e piattaforme, sistemi operativi, middleware e sistemi di gestione dati - Implementazione ed esecuzione di test prestazionali, di analisi dinamica e di sicurezza delle applicazioni - Partecipazione a progetti volti all'impianto di infrastrutture ICT in contesti complessi/innovativi - Strumenti di monitoraggio

Qualifica professionale	Sistemista/Sistemista di sicurezza

Conoscenze	- Buona conoscenza di tecniche di progettazione e realizzazione di architetture volte a erogare servizi agli utenti di riferimento, comprensive di tutte le componenti necessarie (sistemi elaborativi, networking, security, basi dati, ecc.)
	- Ottima conoscenza su installazione, configurazione, personalizzazione, gestione e problem determination/solving di:
	  - software di base
	  - prodotti Middleware
	  - sistemi di storage management (SAN e TAN)
	  - sistemi di backup/restore dei dati
	  - prodotti di virtualizzazione e bilanciamento del carico
	  - prodotti di realizzazione video/audio conference
	  - prodotti di collaboration e CTI
	  - prodotti per il monitoraggio e controllo
	  - prodotti di supporto alla qualità del sw
	  - prodotti di performance test
	  - prodotti di penetration test/vulnerability assessment
	  - prodotti di accesso e autenticazione
	  - prodotti/soluzioni di sicurezza (Firewall, IPS, VPN, sistemi di autenticazione forte, Antivirus, ecc.)
	  - apparati di rete e relativi sistemi operativi
	- Buona conoscenza su installazione, configurazione, personalizzazione, gestione e problem determination/solving di piattaforme di Cloud Computing, con particolare riferimento alle funzioni di automation, orchestration e provisioning
	- Ottima conoscenza su installazione, configurazione, gestione e problem determination/solving in ambito networking (routing, bilanciamento, sistemi di management, ecc…), di protocolli e architettura di rete TCP/IP, di tecnologie LAN/WAN e WIFI
	- Buona conoscenza di data modeling, disegno e sviluppo di procedure ETL
	- Conoscenza di base di metodologie di project management/risk management e di strumenti software a supporto
	
	In ambito Sicurezza, oltre alle conoscenze specialistiche sui prodotti e le soluzioni, con particolare riferimento alle soluzioni McAfee, sono richieste:
	- Ottima conoscenza dei principali standard di sicurezza (ITSEC, BS7799), dei principali tipi di vulnerabilità/attacchi di rete e delle tecniche di implementazione di azioni/policy in casi di intrusioni, frodi e/o compromissioni di sicurezza
	- Ottima conoscenza delle procedure di risposta agli incidenti di sicurezza e di escalation
	- Buone capacità di analisi dei log e di correlazione di eventi
	- Buone capacità di valutazione dei malware e dei relativi impatti
	- Buone conoscenze di intelligence ed analisi delle minacce
	- Conoscenze di base in ambito investigazione forense
	- Buone conoscenze in ambito Web Application Firewall

Qualifica professionale	Sistemista/Sistemista di sicurezza
Certificazioni	Per le risorse professionali impiegate in questo ruolo nei diversi ambiti, compresi i servizi di conduzione ICT remunerati a canone, il Fornitore dovrà comprovare le summenzionate conoscenze attraverso la produzione delle seguenti certificazioni, nella versione più recente ovvero nella versione indicata da INAIL: - Sistemi/Windows: Certificazione Windows Server - Sistemi/Linux: Certificazione RedHat RHCSA - Sistemi/pSeries: Certificazione AIX, VSphere - Sistemi/Virtualizzazione: Certificazione VMWare, Certificazione Citrix - Database/Oracle: Certificazioni Oracle Database Administration, Oracle Certified Expert, Oracle Exadata Administrator - Database/SQL: Certificazione MCSA SQL Database Administration, MCSA Azure Database Administrator - Database/Opendb: Certificazione Postgres, MongoDB - Middleware/J2EE: Certificazione RedHat Certified JBoss Administrator RHCJA, Red Hat Certified Specialist in Messaging Administration - Reti: certificazione CCNA o CCIE - Cloud: Certificazione Cloudera, MCSA Azure Administrator Per le risorse professionali impiegate in questo ruolo nei servizi di supporto specialistico al SOC, ove l'attività lo richieda nonché su espressa indicazione di INAIL, il Fornitore dovrà comprovare le summenzionate conoscenze attraverso la produzione della certificazione, al massimo livello conseguibile, sulla tematica di sicurezza ovvero sulla tecnologia/prodotto SW di riferimento. Le suddette certificazioni, per i servizi di conduzione ICT remunerati a canone e per i servizi di supporto specialistico al SOC remunerati in giorni/persona, potranno essere conseguite entro sei mesi dalla data di inizio delle attività.

3. SCHEMA PER LA PRESENTAZIONE DEI CURRICULUM

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.

<table>
<tr><td>Nominativo</td><td colspan="4">(Inserire il Cognome e il Nome della risorsa)</td></tr>
<tr><td>Ruolo</td><td colspan="4">(Inserire il Ruolo attualmente ricoperto dalla risorsa)</td></tr>
<tr><td>Figura professionale</td><td colspan="4">(Indicazione della figura professionale tra quelle previste nonché eventuale ruolo rivestito nell’ambito della fornitura o indicazione di eventuali specifici ruoli aggiuntivi indicati in Offerta)</td></tr>
<tr><td>Servizio/attività</td><td colspan="4">(Fornire l’indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato o ad eventuali aspetti caratterizzanti l’Offerta tecnica)</td></tr>
<tr><td>Conoscenze</td><td colspan="4">(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)</td></tr>
<tr><td rowspan="11">Principali Esperienze Lavorative</td><td colspan="4">(Indicare le esperienze più significative per la gara in oggetto e comprovanti le competenze richieste nel Capitolato Tecnico, 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)</td></tr>
<tr><td colspan="2">Settore</td><td>Data inizio-Data fine</td><td>Esperienze</td></tr>
<tr><td colspan="2" rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2" rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2" rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>Competenze Tecniche</td><td colspan="4">(Indicare le competenze specifiche di cui si è in possesso)</td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td rowspan="3">Specializzazioni</td><td colspan="4">(Indicare eventuali specializzazioni, master, ecc.)</td></tr>
<tr><td>Anno</td><td colspan="2">Titolo</td><td>Descrizione</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="3">Certificazioni</td><td colspan="4">(Indicare eventuali certificazioni)</td></tr>
<tr><td>Anno</td><td colspan="2">Titolo</td><td>Descrizione</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
</table>

Istruzione	*(indicare i titoli di studio)*	
Lingue	*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)*	
	Lingue	Grado di conoscenza