

Capitolato tecnico – Parte Speciale

ID 2733 - GARA A PROCEDURA APERTA AI SENSI DEL D. LGS. 36/2023 E S.M.I., PER L’AFFIDAMENTO DI UN ACCORDO QUADRO AVENTE AD OGGETTO LA FORNITURA DI SOLUZIONI PER PROTEZIONE E RESILIENZA DELLE RETI E DEI SISTEMI INFORMATIVI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI – LOTTO 1

Classificazione Consip: Ambito Pubblico

Indice

1	PREMESSA	4
1.1	Scopo del documento	4
1.2	Oggetto	4
2	DESCRIZIONE DEI SERVIZI	5
2.1	Assessment dell'ecosistema dell'Amministrazione	5
2.2	Progettazione degli interventi e selezione dei prodotti	7
2.3	Monitoraggio della messa in esercizio dei prodotti	8
3	MODALITÀ DI EROGAZIONE DEI SERVIZI	10
3.1	Metrica di dimensionamento e modalità di remunerazione	10
3.2	Risorse da impiegare nell'esecuzione dei servizi	10
4	INDICATORI DI QUALITÀ	24
4.1	IQ01 – Rispetto di una scadenza contrattuale	24
4.2	IQ02 – Adeguatezza delle figure professionali proposte per l'erogazione dei servizi	26
4.3	IQ03 – Adeguatezza del personale impiegato nei ruoli contrattuali	27
4.4	IQ04 – Adeguatezza dei tempi di sostituzione delle figure professionali proposte per l'erogazione dei servizi	28
4.5	IQ05 - Turnover del personale impiegato nella fornitura	29
4.6	IQ06 – Impegni assunti in offerta tecnica	30
4.7	IQ07 – Tempestività di risposta per il servizio di Service Desk	31
4.8	IQ08 – Percentuale di chiamate in ingresso perse per il servizio di Service Desk	32
5	SCHEMA PER LA PRESENTAZIONE DEI CURRICULA	34

Indice delle tabelle

Tabella 1. Esperienza aggiuntiva da considerare come “cultura equivalente”	13
--	----

1 PREMESSA

1.1 Scopo del documento

Il presente Capitolato Tecnico Speciale ha l'obiettivo di descrivere i requisiti minimi relativi alle **attività di Technical Advising** per le Amministrazioni contraenti (di seguito anche Amministrazione) a supporto dell'eventuale acquisto nell'ambito dei Lotti 2, 3 e 4.

Se non diversamente specificato, i termini temporali espressi nel presente Capitolato sono tutti da intendersi come solari (di calendario).

Si rinvia agli acronimi e alle definizioni riportati nel Capitolato Tecnico Generale.

1.2 Oggetto

Oggetto del Lotto 1 è la stipula di un Accordo Quadro per l'affidamento dei Servizi di Technical Advising come strumento di supporto alle Amministrazioni per l'analisi della superficie d'attacco e della postura di sicurezza della singola PA, l'individuazione e la prioritizzazione delle aree di intervento e la messa in esercizio delle soluzioni oggetto dei Lotti di fornitura.

Sinteticamente, i servizi prevedono:

1. Assessment dell'ecosistema dell'Amministrazione;
2. Progettazione degli interventi e selezione delle soluzioni;
3. Monitoraggio della messa in esercizio delle soluzioni.

In particolare:

- i servizi di cui al precedente punto 1 potranno sempre essere acquistati dalle Amministrazioni, anche qualora il Contratto Esecutivo non abbia ad oggetto i servizi di cui ai precedenti punti 2 e 3;
- parimenti, i servizi di cui al precedente punto 3 potranno sempre essere acquistati dalle Amministrazioni, anche qualora il Contratto Esecutivo non abbia ad oggetto i servizi di cui ai precedenti punti 1 e 2;
- viceversa, i servizi di cui al precedente punto 2 dovranno sempre essere acquistati dalle Amministrazioni unitamente a quelli di cui al precedente punto 1.

Ciascuna Amministrazione potrà aderire al Lotto di Technical Advising esclusivamente in una logica di governo e coordinamento preventivo e contestuale degli acquisti oggetto dei Lotti 2, 3, 4.

2 DESCRIZIONE DEI SERVIZI

2.1 Assessment dell'ecosistema dell'Amministrazione

Il servizio è volto a supportare le Amministrazioni nella identificazione e prioritizzazione delle aree tecniche di scopertura dal punto di vista cyber.

Il Fornitore dovrà:

- adottare una metodologia consolidata e strumenti di acquisizione delle informazioni;
- garantire, a proprio carico, tutte le soluzioni operative e gli strumenti tecnologici necessari per lo svolgimento a regola d'arte delle attività di assessment.

Il servizio è articolato come segue.

Raccolta delle informazioni

In questa fase il Fornitore acquisirà tutte le informazioni funzionali all'identificazione del contesto dell'Amministrazione, supportato dal personale dell'Amministrazione stessa o da terzi da essa indicati. In particolare, in base a quanto di interesse dall'Amministrazione, il Fornitore acquisirà a titolo esemplificativo e non esaustivo:

- Perimetro di intervento e obiettivi dell'Amministrazione in termini di cybersicurezza;
- Risultanze di analisi del rischio, se presenti e di interesse;
- Risultanze di pregressi assessment, se presenti e di interesse;
- Risultanze in ambito continuità operativa, se presenti e di interesse;
- Valutazione della postura, se presente;
- Obblighi normativi cui la PA è sottoposta con impatti di natura tecnologica;
- Documentazione architetture e tecnica di interesse, se presente;
- Eventuali procedure interne di interesse;
- Se pertinenti, informazioni riguardo piani evolutivi in ambito tecnologico.

Il Fornitore, ove necessario, supporterà l'Amministrazione nell'identificare le informazioni da acquisire.

Al termine delle attività il Fornitore dovrà produrre un **documento di sintesi delle informazioni raccolte**, entro 7 giorni lavorativi o diversi termini concordati con l'Amministrazione, che non potranno eccedere i giorni prima indicati, e riportati nel Piano di Lavoro Generale.

Analisi AS – IS

Il Fornitore dovrà predisporre una mappatura dell'AS IS dei Sistemi ICT, con focus sulle soluzioni di sicurezza già in campo, comprensiva quindi anche degli elementi di rete di interesse e delle relazioni tra di essi e, dove necessario, dei processi che sottendono e dei dati trattati. Ad ogni elemento dovrà quindi essere associato un contenuto informativo che prevedrà (a titolo esemplificativo e non esaustivo):

- Identificativo dell'elemento tecnologico (nome e breve descrizione);
- Caratteristiche tecnologiche;
- Relazioni con gli altri elementi;
- Processi sottesi (se necessario e richiesto dall'Amministrazione);
- Dati trattati (se necessario e richiesto dall'Amministrazione);
- Filieri sottoposte al Perimetro di Cybersicurezza Nazionale (se necessario e richiesto dall'Amministrazione).

In alcuni casi le informazioni potranno essere ricavate direttamente dall'Amministrazione e/o da eventuali suoi fornitori di riferimento, oppure dal produttore e/o Fornitore del Sistema ICT, o da altre entità, se coinvolte, nella gestione delle infrastrutture e/o delle applicazioni ("società in house", società partecipate, enti consorziati, accordi di servizio, ...).

Al termine delle attività il Fornitore dovrà produrre, entro 10 giorni lavorativi o diversi termini concordati con l'Amministrazione, che non potranno eccedere i giorni prima indicati, e riportati nel Piano di Lavoro Generale, un **documento di Mappatura** in cui organizzare le informazioni prima indicate.

Individuazione delle aree di intervento

Il Fornitore analizzerà i risultati delle precedenti attività effettuando gli opportuni approfondimenti anche con l'Amministrazione o con terzi da essa individuati.

Saranno così individuate le aree di intervento e analizzate in base a importanza, urgenza e complessità realizzativa e stima dei costi per l'Amministrazione. Dovranno essere indicate, se fattibile, possibili soluzioni tra loro alternative/compensative, comprensive di una valutazione di alto livello di benefici attesi e problematiche possibili connesse.

Il Fornitore dovrà produrre un **documento di Gap Analysis** contenente le informazioni prima indicate, al fine di consentire all'Amministrazione di avere un quadro completo dello stato dell'arte, entro i tempi indicati nel Piano di Lavoro Generale, che comunque non possono superare i termini di seguito indicati come eventualmente migliorati in offerta tecnica: 20 giorni lavorativi.

Durante lo svolgimento delle attività prima indicate, il Fornitore dovrà condurre e formalizzare **SAL periodici settimanali**, o con diverse periodicità concordate con l'Amministrazione e riportata nel Piano di Lavoro Generale, sia con le strutture operative che con quelle direttive con contenuto rispettivamente di dettaglio ed executive.

I documenti indicati nel presente paragrafo saranno valutati dall'Amministrazione entro 5 gg lavorativi. In caso l'Amministrazione rilevi la necessità di un aggiornamento dei documenti, ne darà comunicazione al Fornitore entro i 5 giorni prima indicati. Il Fornitore dovrà adeguare la documentazione entro e non oltre i successivi 5 giorni lavorativi dalla comunicazione ricevuta, salvo diversa tempistica concordata con la PA.

2.2 Progettazione degli interventi e selezione dei prodotti

In base al documento di Gap Analysis, il Fornitore, per ogni area individuata, dovrà:

- individuare possibili azioni da intraprendere. A tal fine dovranno essere considerati sia possibili acquisti nell'ambito dei Lotti 2, 3 e 4, sia eventuali attività in capo all'Amministrazione;
- nei casi in cui tra le possibili azioni da intraprendere emerga l'esigenza di eventuali acquisti nell'ambito dei Lotti 2, 3, 4, il Fornitore dovrà individuare:
 - i prodotti da acquistare, il relativo dimensionamento, la modalità tecnologica più idonea all'ecosistema (tra appliance fisica, virtuale e SaaS). Resta inteso che, ove si renda necessario l'acquisto di prodotti di cui ai Lotti 2, 3, 4, l'individuazione dovrà essere orientata nell'ambito dei soli brand ivi previsti;
 - i servizi opzionali da attivare e la stima di massima;
 - le pianificazioni di massima delle attività legate ai prodotti, dall'acquisto fino alla messa in esercizio. In particolare, in questa fase dovranno essere identificate tutte le attività sia in capo ai Fornitori dei Lotti 2, 3, e 4, sia in capo all'Amministrazione, come, ad esempio, attività preparatorie o di supporto. Dovranno essere considerate, ove necessario, le tempistiche legate alle attività di verifica inerenti al perimetro di cybersicurezza nazionale (test CVCN/CV);
 - in caso di migrazioni tecnologiche, dovrà essere stimato anche l'effort legato alle attività di analisi delle configurazioni/personalizzazioni e successivo adattamento del nuovo prodotto;
 - eventuali interrelazioni con altri sistemi dell'Amministrazione che creino dei vincoli/propedeuticità di esecuzione (es. il nuovo prodotto è inserito in un particolare contesto e il suo inserimento richiede anche l'adattamento di altri oggetti a lui vicini).
- se possibile, evidenziare possibili scenari alternativi;
- rispetto ai punti precedenti, effettuare una valutazione costi / benefici, anche a scopo comparativo in caso di scenari alternativi;

- produzione di **SAL periodici**, entro le tempistiche concordate con l'Amministrazione e riportate nel Piano di Lavoro Generale, sia con le strutture operative che con quelle direttive.

Il Fornitore dovrà produrre un **documento analitico ed un documento di sintesi che indichi gli interventi** a copertura dei gap individuati, contenente le informazioni prima indicate, al fine di consentire all'Amministrazione di avere un quadro completo delle possibili linee d'azione da intraprendere e di effettuare una scelta consapevole entro i tempi indicati nel Piano di Lavoro Generale, che comunque non possono superare i termini di seguito indicati come eventualmente migliorati in offerta tecnica: entro 60 giorni.

Quanto prodotto in questa fase sarà di supporto all'Amministrazione per la compilazione del Piano dei fabbisogni relativo agli acquisti sui Lotti 2, 3 e 4.

I documenti indicati in tale paragrafo saranno valutati dall'Amministrazione entro 5 gg lavorativi. In caso l'Amministrazione rilevi la necessità di un aggiornamento dei documenti, ne darà comunicazione al Fornitore entro i 5 giorni prima indicati. Il Fornitore dovrà adeguare la documentazione entro e non oltre i successivi 5 giorni lavorativi dalla comunicazione ricevuta, salvo diversa tempistica concordata con la PA.

2.3 Monitoraggio della messa in esercizio dei prodotti

Nell'ambito delle attività di Monitoraggio, il Fornitore dovrà assicurare il supporto all'Amministrazione nella gestione della messa in esercizio dei prodotti acquistati, svolgendo almeno le seguenti attività:

- la definizione della pianificazione dettagliata degli interventi selezionati di cui al punto precedente, compresi, a titolo esemplificativo e non esaustivo, data di consegna del prodotto, installazione e configurazione, analisi relative a configurazioni avanzate (es playbook), integrazione nell'ecosistema, hardening, attività di migrazione. Tale pianificazione dovrà essere concordata con l'Amministrazione e il Fornitore del Lotto (2, 3, 4) di riferimento;
- nel caso in cui le attività interessino più progetti di installazione e/o dovessero essere particolarmente complesse, dovranno essere indicate anche le eventuali interdipendenze e le priorità tra le diverse attività, anche in funzione delle priorità dell'Amministrazione;
- il controllo della pianificazione e del budget definito per la messa in esercizio dei prodotti;
- il controllo costante dei servizi e dei relativi livelli di servizio complessivamente erogati dal Fornitore del Lotto (2, 3, 4) di riferimento;
- l'evidenziazione di possibili scostamenti con l'individuazione di workaround da sottoporre all'Amministrazione;
- la formalizzazione degli elementi che consentono di dimostrare il raggiungimento degli obiettivi istituzionali e strategici dell'Amministrazione supportati dai prodotti selezionati;

- la definizione di **SAL periodici**, entro le tempistiche concordate con l'Amministrazione, e comunque almeno settimanali, e riportate nel Piano di Lavoro Generale, sia con le strutture operative che con quelle direttive;
- la definizione di standard, metodologie e best practices, previa approvazione dell'Amministrazione, per il monitoraggio dei progetti.

Il Fornitore, laddove necessario nell'ambito del servizio, sarà tenuto a coordinare e gestire i rapporti, le informazioni e le comunicazioni con l'Amministrazione e/o con soggetti terzi da essa indicati.

Per realizzare il servizio di Pianificazione, il Fornitore dovrà rendere disponibile entro i termini concordati con l'Amministrazione e riportati nel Piano di Lavoro Generale, una **soluzione di pianificazione e gestione progettuale**, al fine di verificare la messa in esercizio dei prodotti dei Lotti 2, 3, 4 di riferimento (attività e relative tempistiche e dipendenze tra le stesse, risorse allocate, costi, controllo avanzamenti, monitoraggio degli scostamenti).

Tale soluzione potrà utilizzare anche dati e informazioni presenti su altri strumenti utilizzati dall'Amministrazione.

In particolare, tale soluzione dovrà essere almeno in grado di realizzare, per conto dell'Amministrazione:

- la pianificazione, la gestione ed il monitoraggio di:
 - tempi;
 - attività operative;
 - risorse;
 - aspetti economici e finanziari;
- la rendicontazione e il reporting delle attività.

Il Fornitore dovrà inoltre produrre, entro i tempi concordati con l'Amministrazione (che non potranno essere superiori a 15 giorni), e riportati nel Piano di Lavoro Generale un **documento di pianificazione** contenente tutti gli interventi. Tale documento dovrà essere aggiornato periodicamente, con cadenza almeno bisettimanale e comunque tempestivamente in base alle nuove esigenze derivanti dalle attività progettuali o su richiesta dell'Amministrazione. Tale documento rappresenterà il punto di riferimento delle attività realizzative e delle iniziative progettuali in capo all'Amministrazione.

Il documento dovrà contenere tutte le informazioni di sintesi, comprese anche le esigenze e i requisiti eventualmente emersi durante le attività di Assessment e Progettazione (ove acquistate congiuntamente al Servizio di monitoraggio) degli interventi, correlati ai relativi progetti e iniziative di riferimento.

In particolare, nell'ambito di tale documento, per ciascun progetto, dovranno essere evidenziati almeno i seguenti elementi:

- stati di avanzamento e milestone progettuali;
- deliverable di fornitura e output associati;
- eventuali non conformità e/o mancate accettazioni del servizio/prodotto.

Il documento di pianificazione dovrà essere costantemente disponibile ed allineato alle richieste dell'Amministrazione, soprattutto per quanto riguarda gli aspetti inerenti al governo complessivo dei progetti.

I documenti indicati in tale paragrafo saranno valutati dall'Amministrazione entro 3 gg lavorativi. In caso l'Amministrazione rilevi la necessità di un aggiornamento dei documenti, ne darà comunicazione al Fornitore entro i 3 giorni prima indicati. Il Fornitore dovrà adeguare la documentazione entro e non oltre i successivi 4 giorni lavorativi dalla comunicazione ricevuta.

3 MODALITÀ DI EROGAZIONE DEI SERVIZI

3.1 Metrica di dimensionamento e modalità di remunerazione

La metrica di dimensionamento di tutti i servizi è: **Giorno/Persona**.

La modalità di remunerazione di tutti i servizi è: **a tempo/spesa oppure a corpo**.

In fase di offerta è richiesto a ciascun concorrente di esprimere un prezzo per giorno/persona per ogni figura professionale prevista. I prezzi espressi saranno riferiti alle **8 ore lavorative** complessive nella fascia oraria feriale Lun-Sab 8.00-20.00 (fascia standard).

In sede di Piano dei fabbisogni, l'Amministrazione definirà i deliverables richiesti e le risorse necessarie, indicando quindi il mix necessario per le attività richieste, in un'ottica di coerenza e proporzionalità, come meglio indicato al successivo paragrafo 3.2.

3.2 Risorse da impiegare nell'esecuzione dei servizi

Con riferimento a ciascuno dei servizi oggetto del Lotto 1, tutte le risorse che il Fornitore impiegherà per l'erogazione dei servizi oggetto della fornitura dovranno essere adeguate al ruolo ricoperto e dovranno essere in possesso almeno dei requisiti minimi espressi dal presente Capitolato Tecnico Speciale, integrati con tutte le migliorie eventualmente indicate in Offerta Tecnica. Si precisa che tutte le figure di seguito indicate possono essere impiegate per i servizi oggetto del presente Lotto.

Nel Piano dei Fabbisogni la singola Amministrazione specificherà nel dettaglio le proprie esigenze, indicando le figure professionali richieste per ciascun servizio, tra quelle indicate nel seguito, e la

rispettiva quantità espressa in giorni persona. È facoltà dell'Amministrazione, in sede di Piano dei Fabbisogni, dettagliare le proprie esigenze precisando le competenze ed esperienze tra quelle indicate per ciascun profilo nell'ambito delle tabelle di seguito riportate. A tal fine, per ciascun profilo professionale le competenze ed esperienze indicate nelle tabelle di cui al presente paragrafo devono essere presenti nel complesso delle risorse professionali che il Fornitore metterà 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), l'anzianità lavorativa e le certificazioni dovranno essere posseduti da ciascuna risorsa. In ogni caso, fermo restando quanto sopra, l'Amministrazione può richiedere, nell'ambito di ogni specifico profilo, più risorse distinte, specializzate ciascuna in un determinato ambito tecnologico.

Con riferimento alle certificazioni:

- per le certificazioni migliorative eventualmente offerte, resta fermo quanto indicato in offerta tecnica;
- tutte le certificazioni possedute dalle risorse per ciascun ruolo dovranno essere mantenute aggiornate e in corso di validità per tutta la durata contrattuale.

Inoltre, il Piano dei Fabbisogni dell'Amministrazione sarà corredato dalla descrizione del contesto tecnologico attuale e futuro di riferimento.

Nell'ambito del Piano Operativo predisposto dal Fornitore, saranno declinati i profili professionali in coerenza con il suddetto contesto descritto dall'Amministrazione. Permane in ogni caso l'obbligo per il Fornitore di erogare i servizi richiesti anche a fronte di significative variazioni del suddetto 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.

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 e della normativa di riferimento, nonché degli standard, delle linee guida e best practices applicabili.

Nel presente documento, e laddove citati nel Capitolato Tecnico Generale, 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 ed esperienze delle figure che seguono non sono esaustive delle esigenze future. Infatti, le competenze ed esperienze iniziali potranno variare in funzione dell'evoluzione tecnologica e in relazione a ulteriori tematiche, prodotti, sistemi e metodologie che emergeranno durante la validità dell'Accordo Quadro e dei Contratti Esecutivi. A tal fine, le sottostanti tabelle potranno essere

aggiornate nel corso della vigenza dell'Accordo Quadro e dei Contratti Esecutivi, in accordo tra Consip e il Fornitore.

Per ogni profilo è richiesto il possesso di una anzianità 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 anzianità 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 indicato nella sottostante tabella.

In ogni caso, il titolo di studio posseduto deve essere almeno un diploma di scuola secondaria di secondo grado.

TITOLO DI STUDIO POSSEDUTO TITOLO DI STUDIO RICHIESTO	LAUREA MAGISTRALE IN DISCIPLINE TECNICO SCIENTIFICHE	LAUREA TRIENNALE IN DISCIPLINE TECNICO SCIENTIFICHE	LAUREA MAGISTRALE (ALTRE DISCIPLINE)	LAUREA TRIENNALE (ALTRE DISCIPLINE)	DIPLOMA DI PERITO TECNICO INDUSTRIALE IN INFORMATICA	DIPLOMA DI SCUOLA SECONDARIA DI SECONDO GRADO (DIVERSO DA PERITO TECNICO INDUSTRIALE IN INFORMATICA)
LAUREA MAGISTRALE IN DISCIPLINE TECNICO SCIENTIFICHE	-	+ 2 anni	+ 2 anni (o master 2° livello in cybersecurity)	+ 3 anni (o + 2 anni e master 1° livello in cybersecurity)	+ 5 anni	+ 7 anni
LAUREA TRIENNALE IN DISCIPLINE TECNICO SCIENTIFICHE	-	-	+ 1 anno (o master 1° livello in cybersecurity)	+ 2 anni (o + 1 anno e master 1° livello in cybersecurity)	+ 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 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 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 tecnologie informatiche" o "informatica" o "ingegneria dell'informazione (telecomunicazioni, informatica)" o "sicurezza informatica".

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 D.M. 1648 e 1649 del 19 dicembre 2023.

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.

FIGURA PROFESSIONALE	SECURITY PRINCIPAL
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 10 (dieci) anni nel settore ICT, di cui almeno 5 (cinque) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Possesso di almeno una certificazione in ambito program e project management, quali ad esempio: Prince2 Practitioner, PgMP, PMP, UNI 11648
COMPETENZE ED ESPERIENZE RICHIESTE	Conoscenza delle metodologie di program e project management
	Conoscenza approfondita della normativa nazionale ed europea in ambito ICT Security e Privacy
	Conoscenza approfondita dei processi di security governance e security management
	Conoscenza approfondita delle metodologie e dei processi in ambito ict security e privacy quali: risk management, business continuity, vulnerability assessment & penetration test, incident handling ed escalation per la gestione degli incidenti di sicurezza informatica, classificazione e gestione delle informazioni, gestione delle utenze, gestione degli end point, security audit, etc
	Conoscenza dei processi e delle procedure operative ICT
	Conoscenza ed esperienza sulle tecnologie principali per la sicurezza ict (si cita a titolo esemplificativo e non esaustivo NGFW, WAAP, IAM; DLP, SIEM, SOAR, etc)
	Conoscenza dei principali standard e framework di sicurezza e privacy quali: ISO /IEC 27001; ISO/IEC: 27017; ISO/IEC 27018; ISO 22301; ITIL, COBIT; CMMI; CISM; CISA; NIST, etc
	Esperienza di Project Management in progetti analoghi e in contesti di diversa complessità

FIGURA PROFESSIONALE	SECURITY PRINCIPAL
	Esperienza consolidata nella gestione di progetti/programmi in ambito ICT Security e Privacy
	Esperienza consolidata nel disegno e nella valutazione dei sistemi di gestione della sicurezza e della privacy delle informazioni, nonché nella gestione della continuità operativa

FIGURA PROFESSIONALE	SECURITY ARCHITECT
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 8 (otto) anni nel settore ICT, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi e componenti infrastrutturali
	Conoscenza di norme e standard adottati per l'hardening ed il patching dei sistemi operativi, servizi e applicazioni
	Conoscenza della normativa nazionale ed europea in ambito ICT Security e Privacy
	Conoscenza approfondita delle problematiche di sicurezza delle infrastrutture ICT e IT/OT
	Conoscenza delle metodologie e degli strumenti operativi richiesti per verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture ICT
	Conoscenza delle tecnologie principali per la sicurezza ICT, soprattutto in ambito sicurezza cloud e prodotti SaaS, minacce di nuova generazione e modalità di contenimento, utilizzo ml/ai nelle soluzioni adottate, ecc.
	Conoscenza dei sistemi di correlazione eventi, progettazione regole di correlazione e tuning

FIGURA PROFESSIONALE	SECURITY ARCHITECT
	sistemi di analisi eventi con esperienza di integrazione in contesti analoghi
	Buona conoscenza dei principi e dei sistemi di autenticazione, specialmente sistemi di Identity & Access Management, di Data Classification, di gestione certificati, con esperienza di integrazione su ambienti analoghi
	Conoscenza delle tecnologie in uso nel contesto di riferimento dei Lotti di fornitura dei prodotti, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate
	Conoscenza dei principali standard e framework di sicurezza e privacy quali: ISO /IEC 27001, ISO/IEC: 27017, ISO/IEC 27018, ISO 22301; CISSP, CCSP, CSSLP, CISM, NIST, OWASP, SANS/SEC-540, etc
	Consolidata esperienza nella progettazione della sicurezza ICT maturata in contesti analoghi
	Esperienza nell'analisi di un'infrastruttura ICT complessa volta all'individuazione di problematiche architetture che ne potrebbero compromettere la sicurezza
	Esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura ICT complessa
	Esperienza nell'identificazione di soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per traghettare la piena adozione delle contromisure previste

FIGURA PROFESSIONALE	SENIOR SECURITY CONSULTANT
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche

FIGURA PROFESSIONALE	SENIOR SECURITY CONSULTANT
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 7 (sette) anni nel settore ICT, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di coordinamento delle risorse Junior
	Buona conoscenza delle metodologie e dei processi in ambito ICT security e privacy quali: risk management, business continuity, vulnerability assessment & penetration test, Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica, classificazione e gestione delle informazioni, gestione delle utenze, gestione degli end point, Hardening e Patching, security audit, etc
	Buona 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
	Buona conoscenza delle principali tecnologie in ambito ICT Security (si cita a titolo esemplificativo e non esaustivo NGFW, WAAP, IAM; DLP, SIEM, SOAR, etc)
	Buona conoscenza delle metodologie e degli strumenti operativi richiesti per la gestione dei progetti
	Buona conoscenza dei processi e delle procedure operative IT
	Conoscenza di alcuni principali standard e framework di sicurezza e privacy quali: ISO/IEC 27001; ISO/IEC:27017; ISO/IEC 27005; ISO/IEC 27018; ISO 22301; ITIL; COBIT; CMMI; CISM; CISA; etc
	Buona conoscenza della normativa nazionale ed europea in ambito ICT Security e Privacy
	Esperienza sui sistemi di gestione della sicurezza delle informazioni (SGSI) e sulla continuità operativa

FIGURA PROFESSIONALE	SENIOR SECURITY CONSULTANT
	Esperienza nella gestione di progetti in ambito ICT Security e Privacy in contesti pubblici e privati (es adeguamento a normative)
	Esperienza nella gestione della continuità operativa e del disaster recovery
	Esperienza nella gestione degli eventi di sicurezza e Data Breach
	Esperienza nelle attività di analisi dei rischi e nella valutazione della security posture

FIGURA PROFESSIONALE	SENIOR SECURITY ANALYST
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 6 (sei) anni nel settore ICT, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di coordinamento delle risorse Junior
	Conoscenza dei processi e delle procedure operative ICT
	Conoscenza approfondita dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica
	Conoscenza approfondita dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi
	Conoscenza approfondita dei sistemi di rilevazione e analisi degli allarmi
	Conoscenza dei processi di reverse engineering dei malware ed esperienza consolidata nella analisi forense di malware mediante strumenti di analisi e attività di reverse
	Conoscenza approfondita dei protocolli di rete e della tipologia di traffico all'interno di un contesto complesso con esperienza consolidata nell'analisi forense del traffico di rete e nell'identificazione di

FIGURA PROFESSIONALE	SENIOR SECURITY ANALYST
	anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza
	Esperienza consolidata nella definizione di configurazioni e analisi di sicurezza
	Esperienza nella definizione di regole di correlazione e nel tuning delle stesse

FIGURA PROFESSIONALE	SECURITY SPECIALIST
TITOLO DI STUDIO	Laurea magistrale/specialistica in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 5 (cinque) anni nel settore ICT, di cui almeno 2 (due) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Capacità di comprendere il contesto tecnologico in analisi e di identificare le minacce cyber
	Capacità di identificare ed implementare le adeguate misure difensive
	Capacità di eseguire risk assessment
	Capacità di effettuare attività di Vulnerability Assessment e Penetration Test
	Conoscenza delle problematiche di sicurezza delle infrastrutture ICT
	Conoscenza delle tecnologie principali per la sicurezza ICT, compreso l'ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento, ML/AI, ecc.
	Ottima conoscenza sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione in contesti analoghi
	Buona conoscenza sistemi di autenticazione, specialmente sistemi di Identity & Access Management con esperienza di integrazione su ambienti analoghi

FIGURA PROFESSIONALE	SECURITY SPECIALIST
	Conoscenza delle tecnologie in uso nel contesto di riferimento, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate Conoscenza di alcuni principali standard e framework di sicurezza e privacy quali: ISO/IEC 27001; CISM; CCSK; CISSP; CompTIA Security+; CEH; PSI-DSS; Nist, etc Esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura ICT complessa Esperienza nell'analisi, nella valutazione e nell'implementazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (reti TCP/IP, NGFW, SIEM, DLP, soluzioni anti-malware, WAAP, soluzione cloud oriented per la sicurezza, IAM, ecc.) Esperienza nella progettazione e gestione della sicurezza ICT e delle relative soluzioni maturata in contesti analoghi Esperienza nell'analisi tecnica di incidenti e nella modalità di intervento Esperienza nelle attività di Hardening e Patching

FIGURA PROFESSIONALE	JUNIOR SECURITY CONSULTANT
TITOLO DI STUDIO	Laurea triennale in discipline scientifiche
ANZIANITÀ LAVORATIVA	Anzianità lavorativa di almeno 3 (tre) anni nel settore ICT, di cui almeno 2 (due) anni di provata esperienza nella specifica funzione
CERTIFICAZIONI	Nessuna certificazione
COMPETENZE ED ESPERIENZE RICHIESTE	Conoscenza dei processi e delle procedure operative ICT Conoscenza dei processi di: risk management, vulnerability assessment & penetration test, Incident Handling ed Escalation per la gestione

FIGURA PROFESSIONALE	JUNIOR SECURITY CONSULTANT
	degli incidenti di sicurezza informatica, classificazione e gestione delle informazioni, gestione delle utenze, gestione degli end point, Hardening e Patching, etc
	Conoscenza dei sistemi di rilevazione e analisi degli allarmi
	Conoscenza della modalità di intervento sulle postazioni client e sui server in caso di diffusione di malware di nuova generazione
	Conoscenza delle principali tecnologie in ambito ICT Security (si cita a titolo esemplificativo e non esaustivo NGFW, WAAP, IAM; DLP, SIEM, SOAR, etc)
	Conoscenza dei protocolli di rete e della tipologia di traffico all'interno di un contesto ICT
	Conoscenza di alcuni principali standard e framework di sicurezza e privacy quali: ISO/IEC 27001; ISO/IEC:27017; ISO/IEC 27005; ISO/IEC 27018; ISO 22301; ITIL; COBIT; Nist; etc
	Conoscenza della normativa nazionale ed europea in ambito ICT Security e Privacy
	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
	Esperienza nell'analisi tecnica di incidenti
	Esperienza di affiancamento e supporto nelle attività di Vulnerability Assessment e Penetration Test
	Esperienza in progetti in ambito security e privacy

I curriculum vitae delle figure professionali da impiegare nei vari servizi dovranno essere resi disponibili alle Amministrazioni rispettando lo schema indicato al capitolo 5. Sarà facoltà dell'Amministrazione indicare un diverso template. In ogni caso, dovranno essere particolarmente dettagliate le competenze ed esperienze tecniche al fine di verificare la corrispondenza con i requisiti minimi, gli eventuali requisiti migliorativi offerti e il contesto dell'Amministrazione.

Sulla base dei CV presentati l'Amministrazione procederà alla verifica che il personale proposto sia in linea con i requisiti minimi e gli eventuali requisiti migliorativi offerti, riservandosi la possibilità di procedere ad un colloquio di approfondimento per verificare la corrispondenza delle competenze elencate nel CV (in tal caso il Fornitore dovrà rendere disponibile al colloquio la risorsa **entro 3 giorni lavorativi** dalla richiesta). Per il personale ritenuto inadeguato, qualunque sia il ruolo, l'Amministrazione Contraente procederà alla richiesta formale di sostituzione inviando apposita richiesta di sostituzione, in cui indicherà puntualmente la risorsa che ritiene inadeguata, le relative motivazioni in riferimento ai requisiti minimi e/o migliorativi di gara, la "data prevista di sostituzione" ai fini degli indicatori di qualità. La presentazione del CV (e delle eventuali certificazioni) della nuova risorsa in sostituzione dovrà quindi avvenire secondo i termini indicati dall'Amministrazione (che non potranno superare i 5 giorni lavorativi). La richiesta di sostituzione potrà avvenire anche successivamente all'avvio del servizio, laddove l'Amministrazione riscontri che il personale impiegato non sia adeguato ad effettuare le attività richieste.

Il Fornitore, in caso necessiti di sostituire il personale allocato presso l'Amministrazione, dovrà darne opportuna comunicazione all'Amministrazione stessa entro 10 giorni lavorativi dalla sostituzione della stessa, indicando al contempo la nuova risorsa subentrante e inviando il relativo CV (e le eventuali certificazioni). La nuova risorsa dovrà possedere tutte le caratteristiche di quella in sostituzione. L'Amministrazione valuterà il nuovo CV, anche mediante colloquio, ai fini dell'autorizzazione alla sostituzione.

Ciascuna risorsa impiegata dovrà fornire, nel corso dell'esecuzione dei servizi, la propria esperienza sullo specifico ambito di competenza, a supporto dell'erogazione dei servizi medesimi, interagendo con l'Amministrazione e/o con i soggetti terzi da essa delegati e con i vari gruppi di lavoro coinvolti.

Oltre a tali attività, le risorse impiegate avranno il compito di divulgare all'interno dell'Amministrazione la conoscenza maturata sui progetti seguiti e sui servizi erogati, attraverso riunioni, presentazioni e documenti di best practices in modo da rendere il personale dell'Amministrazione consapevole di quanto realizzato in ambito cybersecurity e del valore aggiunto apportato all'Amministrazione medesima.

I Fornitori potranno offrire l'impiego, in fase di esecuzione, di personale in possesso di certificazioni in ambito *security* secondo quanto previsto nel Capitolato d'Oneri.

4 INDICATORI DI QUALITÀ

Il presente capitolo definisce il livello di qualità minimo atteso dei servizi dei singoli Contratti Esecutivi, attraverso la definizione degli obiettivi di qualità, la misura del loro raggiungimento e il dettaglio delle azioni contrattuali da applicare in caso di mancato rispetto dei valori soglia (indicatori di qualità).

Il Fornitore potrà integrare i presenti indicatori nell'ambito dell'Offerta Tecnica presentata ai fini dell'aggiudicazione dell'Accordo Quadro, secondo i criteri indicati nel Capitolato d'Oneri.

Il mancato rispetto dei valori di soglia migliorativi sarà sanzionato con la penale "Mancato rispetto degli impegni assunti in offerta tecnica".

Per gli indicatori di qualità di cui al presente capitolo, le conseguenti azioni contrattuali potranno essere esercitate dalle singole Amministrazioni od essere esercitate da Consip S.p.A., ove previsto, su richiesta delle Amministrazioni.

Su richiesta dell'Amministrazione, il Fornitore dovrà fornire i dati elementari utilizzati per il calcolo degli indicatori di cui al presente paragrafo.

Tali dati dovranno essere forniti in un formato elaborabile con i prodotti di office automation in uso presso l'Amministrazione. Inoltre, il Fornitore dovrà mettere a disposizione delle Amministrazioni, senza oneri aggiuntivi, uno strumento per la fruizione dei suddetti contenuti.

Relativamente alle penali per ritardo, si precisa inoltre che deve considerarsi ritardo anche il caso in cui il Fornitore esegua le prestazioni relative allo specifico indicatore in modo anche solo parzialmente difforme dalle disposizioni di cui al presente documento, all'Offerta tecnica e comunque alle indicazioni contenute nel Piano di Lavoro Generale. In tal caso, le Amministrazioni applicheranno al Fornitore le penali di cui allo specifico indicatore sino alla data in cui la fornitura inizierà ad essere eseguita in modo effettivamente conforme, fatto salvo il risarcimento del maggior danno.

4.1 IQ01 – Rispetto di una scadenza contrattuale

L'indicatore misura il rispetto di scadenze temporali derivanti dalla documentazione contrattuale (dell'Accordo Quadro e del Contratto Esecutivo), dal Piano di Lavoro Generale e comunque concordate con l'Amministrazione. La penale prevista nel presente paragrafo riveste carattere residuale rispetto ad altre penali da ritardo espressamente normate nel presente documento e in ogni caso nell'Accordo Quadro e relativi allegati, nonché nel Contratto Esecutivo, ossia verrà applicato tale indicatore se non ve ne sono altri specifici.

A titolo esemplificativo e non esaustivo si rappresentano di seguito alcuni documenti, il cui ritardo nella trasmissione può determinare l'applicazione di penali:

- Adempimenti relativi alle fasi di invio del Piano Operativo e di perfezionamento del Contratto Esecutivo di cui ai rispettivi paragrafi del Capitolato Tecnico Generale;

- Piani di qualità generale e specifico;
- Piano di lavoro Generale;
- CV delle risorse e dei responsabili tecnici con le relative certificazioni;
- Deliverable di fornitura.

ASPETTO DA VALUTARE	RISPETTO DI UNA SCADENZA CONTRATTUALE		
Unità di misura	Giorni lavorativi	Fonte dati	Comunicazioni Note Amministrazione Verbal di riunioni
Periodo di riferimento	Durata della fornitura Periodi di verifica di conformità	Frequenza di misurazione	Mensile o a scadenza se minore
Dati da rilevare	Per ciascuna scadenza vanno rilevati: – Data prevista (data_prev) – Data effettiva (data_eff) L'indicatore viene calcolato come sommatoria degli eventi rilevati nel periodo di misurazione (mensile)		
Regole di campionamento	Nessuna		
Formula	$IQ01 = \sum (data_eff - data_prev)$		
Regole di arrotondamento	Nessuna		
Valore di soglia	<i>$IQ01 = 1$, oppure $IQ01 = 0$ in caso di migliorativo offerto in sede di gara</i>		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà <u>per ogni giorno lavorativo di ritardo rispetto al valore soglia</u> l'applicazione della penale “Mancato rispetto di una scadenza contrattuale dell’Accordo Quadro”, pari a 5.000,00 (cinquemila/00). Il mancato rispetto del valore di soglia comporterà <u>per ogni giorno (solare o lavorativo a seconda di quanto indicato nel corrispondente paragrafo di riferimento)</u> di ritardo rispetto al valore soglia l'applicazione della penale “Mancato rispetto di una scadenza contrattuale del Contratto esecutivo”, pari all’0,6‰ (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione	Consip e Amministrazione Contraente		

Eccezioni	Nessuna
-----------	---------

4.2 IQ02 – Adeguatezza delle figure professionali proposte per l'erogazione dei servizi

L'indicatore misura il numero di figure professionali impiegate nell'erogazione dei servizi (diversi da Responsabile unico delle attività contrattuali e Responsabili tecnici del Fornitore per l'erogazione dei servizi) che, nel corso della fornitura, l'Amministrazione Contraente abbia ritenuto non rispondenti al profilo professionale richiesto, richiedendone la sostituzione;

ASPETTO DA VALUTARE	NUMERO DI RISORSE IMPIEGATE NELLA EROGAZIONE DEL SERVIZIO RITENUTE DALL'AMMINISTRAZIONE NON RISPONDENTI AI REQUISITI		
Unità di misura	Risorsa inadeguata	Fonte dati	E-mail Lettere Verbali
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile
Dati da rilevare	N_{ris_inad} = Numero di risorse sostituite su richiesta dell'Amministrazione perché non rispondenti ai requisiti		
Regole di campionamento	Nessuna		
Formula	$IQ02 = N_{ris_inad}$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ02 = 1$, oppure $IQ02 = 0$ in caso di migliorativo offerto in sede di gara		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà <u>per ogni risorsa eccedente il valore di soglia nel periodo di riferimento</u> l'applicazione della penale “Risorse Impiegate nell'erogazione del servizio non rispondenti ai requisiti” , pari all' 0,6% (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

4.3 IQ03 – Adeguatezza del personale impiegato nei ruoli contrattuali

L'indicatore misura il numero di risorse nei ruoli di Responsabile unico delle attività contrattuali (RUAC dell'Accordo Quadro) e di Responsabili tecnici del Fornitore che, nel corso della fornitura, Consip o l'Amministrazione Contraente abbia ritenuto non rispondente al profilo professionale richiesto nel Capitolato Tecnico Generale, richiedendone la sostituzione.

ASPETTO DA VALUTARE	NUMERO DI RISORSE RITENUTE INADEGUATE		
Unità di misura	Risorsa inadeguata	Fonte dati	E-mail Lettere Verbali
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile
Dati da rilevare	N_{ris_inad} = Numero di risorse sostituite per inadeguatezza su richiesta di Consip o dell'Amministrazione		
Regole di campionamento	Nessuna		
Formula	$IQ03 = N_{ris_inad}$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ03 = 0$		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per la sostituzione del RUAC dell'Accordo Quadro rispetto al valore soglia</u> l'applicazione della penale "Adeguatezza del personale impiegato nei ruoli contrattuali" pari a € 5.000,00 (cinquemila/00). Il mancato rispetto del valore soglia comporterà <u>per ogni risorsa di Responsabile tecnico del Fornitore sostituito rispetto al valore soglia</u> l'applicazione della penale "Adeguatezza del personale impiegato nei ruoli contrattuali" pari all'0,6‰ (zerovirgolasei per mille) dell'importo del Contratto esecutivo.		
Applicazione	Consip e Amministrazione Contraente		
Eccezioni	Nessuna		

4.4 IQ04 – Adeguatezza dei tempi di sostituzione delle figure professionali proposte per l'erogazione dei servizi

L'indicatore misura i giorni di ritardo nella sostituzione di figure professionali (diversi da Responsabile unico delle attività contrattuali e Responsabili tecnici del Fornitore per l'erogazione dei servizi) che eccedano quelli previsti nel Capitolato tecnico speciale.

ASPETTO DA VALUTARE	NUMERO DI GIORNI DI RITARDO NELLA SOSTITUZIONE DI RISORSE IMPIEGATE NELLA EROGAZIONE DEL SERVIZIO RITENUTE DALL'AMMINISTRAZIONE NON RISPONDENTI AI REQUISITI		
Unità di misura	Risorsa inadeguata	Fonte dati	E-mail Lettere Verbali
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile
Dati da rilevare	Per ciascuna risorsa vanno rilevati: – Data prevista sostituzione (data_prev) – Data effettiva sostituzione (data_eff) L'indicatore viene calcolato come sommatoria degli eventi rilevati nel periodo di misurazione (mensile)		
Regole di campionamento	Nessuna		
Formula	$IQ04 = \sum (data_eff - data_prev)$		
Regole di arrotondamento	Nessuna		
Valore di soglia	<i>$IQ04 = 5$, oppure $IQ04 = 4$ in caso di migliorativo offerto in sede di gara</i>		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà <u>per ogni giorno (solare o lavorativo a seconda di quanto indicato nel corrispondente paragrafo di riferimento) eccedente il valore di soglia nel periodo di riferimento</u> l'applicazione della penale “Adeguatezza dei tempi di sostituzione delle figure professionali proposte per la erogazione dei servizi” , pari all'0,6‰ (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

4.5 IQ05 - Turnover del personale impiegato nella fornitura

L'indicatore misura il numero di sostituzioni delle risorse impiegate (inclusi il RUAC e Responsabili tecnici del Fornitore dell'erogazione del servizio), su iniziativa del Fornitore e non autorizzate dall'Amministrazione Contraente.

ASPETTO DA VALUTARE	NUMERO DI RISORSE SOSTITUITE SU INIZIATIVA DEL FORNITORE		
Unità di misura	Risorse	Fonte dati	E-mail lettere verbali
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile
Dati da rilevare	Numero risorse sostituite su iniziativa del Fornitore (<i>Nrisorse_sostituite</i>)		
Regole di campionamento	Nessuna		
Formula	$IQ05 = Nrisorse_sostituite$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ05 = 1$		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni risorsa aggiuntiva rispetto al valore soglia</u> l'applicazione della penale "Turnover del personale impiegato nella fornitura" pari a € 1.000,00 (mille/00).		
Applicazione	Consip e Amministrazione Contraente		
Eccezioni	- Eventuali sostituzioni finalizzate ad un migliore funzionamento dei servizi/attività, purché preventivamente approvate dai referenti dell'Amministrazione, non contribuiscono al raggiungimento del valore soglia. - Eventuali sostituzioni operate a fronte di dimissioni/licenziamento di risorse impegnate nell'erogazione dei servizi non contribuiscono al raggiungimento del valore soglia <u>purché sia rispettata almeno una delle seguenti condizioni:</u> a) ciascuna sostituzione sia effettuata nel rispetto dei termini del preavviso previsti dal contratto di lavoro applicato;		

	b) ciascuna sostituzione deve essere preventivamente approvata dall'Amministrazione; c) ciascuna dimissione sia opportunamente documentata.
--	--

4.6 IQ06 – Impegni assunti in offerta tecnica

L'indicatore di qualità verifica il numero di impegni assunti dal Fornitore in offerta tecnica, afferenti obbligazioni contrattuali non adempiute nei tempi e/o nei modi rappresentati nel Contratto esecutivo e relativi allegati e/o tracciati sul Piani di lavoro Generale, qualora non presidiate da specifici indicatori.

ASPETTO DA VALUTARE	NUMERO DI IMPEGNI ASSUNTI DAL FORNITORE IN OFFERTA TECNICA NON ADEMPIUTI		
Unità di misura	Impegno	Fonte dati	Comunicazioni Note Amministrazione
Periodo di riferimento	Durata della fornitura	Frequenza di misurazione	Mensile o a scadenza se minore
Dati da rilevare	N_{IMP} = Numero impegni assunti dal Fornitore in offerta tecnica		
Regole di campionamento	Nessuna		
Formula	$IQ06 = N_{IMP}$		
Regole di arrotondamento	Nessuna		
Valore di soglia	$IQ06 = 0$		
Azioni contrattuali	Il mancato rispetto del valore di soglia comporterà <u>per ogni scostamento rispetto al valore soglia</u> l'applicazione della penale "Impegni assunti in offerta tecnica", pari all' 0,6‰ (zerovirgolasei per mille), dell'importo del Contratto esecutivo.		
Applicazione	Amministrazione Contraente		
Eccezioni	Nessuna		

4.7 IQ07 – Tempestività di risposta per il servizio di Service Desk

L'indicatore di qualità è definito come la percentuale, consolidata su base mensile, di chiamate risposte entro i 120 secondi nell'ambito della finestra di erogazione del servizio con operatore, misurati tra l'inizio della chiamata al servizio di Service Desk (o dalla eventuale selezione sul risponditore automatico dell'opzione per parlare con un operatore) e la risposta dell'operatore per Contratto Esecutivo.

ASPETTO DA VALUTARE	TEMPESTIVITÀ DI RISPOSTA PER IL SERVIZIO DI SERVICE DESK		
Unità di misura	Percentuale	Fonte dati	Comunicazioni Contratto Esecutivo Piano di Lavoro Strumenti di Tracciatura
Periodo di riferimento	Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	Mensile
Dati da rilevare	– Data e Ora (hh/mm/ss/dd) di avvio dell'interazione (<i>Data_avvio</i>) – Data e Ora (hh/mm/ss/dd) della effettiva risposta (<i>Data_risp</i>) – Numero totale interazioni pervenute nel periodo di riferimento (<i>Num_tot</i>)		
Regole di campionamento	Nessuna		
Formula	$IQ07 = \text{Num_interazioni} (T_ risp \leq T_ottimale) / \text{Num_tot}$ Dove: $T_ risp = \text{Data_ risp} - \text{Data_avvio}$ $T_ottimale = 120 \text{ secondi}$		
Regole di arrotondamento	Il risultato della misura va arrotondato al punto percentuale: - per difetto se la parte decimale è $\leq 0,5$ - per eccesso se la parte decimale è $> 0,5$		
Valore di soglia	IQ07 = 95%		
Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale in diminuzione rispetto al valore soglia</u> nel periodo di riferimento, l'applicazione della penale “Tempestività di risposta” pari a € 300,00 (trecento/00).		
Applicazione	Amministrazione Contraente		

Eccezioni	Nessuna
------------------	---------

4.8 IQ08 – Percentuale di chiamate in ingresso perse per il servizio di Service Desk

L'indicatore di qualità identifica la percentuale di chiamate in ingresso perse per Contratto Esecutivo. Si definisce chiamata persa quella telefonata:

- a cui segue il segnale di occupato;
- che viene messa in diretto contatto con la segreteria telefonica (soluzione ammessa solo per chiamate fuori orario di servizio con operatore).

Detto valore viene valutato considerando il numero delle chiamate consolidato su base mensile.

ASPETTO DA VALUTARE	CHIAMATE IN INGRESSO PERSE PER IL SERVIZIO DI SERVICE DESK		
Unità di misura	Percentuale	Fonte dati	Comunicazioni Contratto Esecutivo Piano di Lavoro Strumenti di Tracciatura
Periodo di riferimento	Durata della fornitura Periodi di verifiche di conformità	Frequenza di misurazione	Mensile
Dati da rilevare	– Numero di Chiamate cui segue il segnale di occupato (NC_Occ) – Numero di Chiamate inoltrate automaticamente alla segreteria telefonica (NC_Segr) – Numero totale di Chiamate realizzate (NC_Tot)		
Regole di campionamento	Vanno considerate tutte le richieste pervenute nel periodo di riferimento		
Formula	$IQ08 = NC_Inevase / NC_Tot$ Dove: $NC_Inevase = NC_Occ + NC_Segr$		
Regole di arrotondamento	Il risultato della misura va arrotondato al punto percentuale: – per difetto se la parte decimale è $\leq 0,5$ – per eccesso se la parte decimale è $> 0,5$		
Valore di soglia	$IQ08 = 4\%$		

Azioni contrattuali	Il mancato rispetto del valore soglia comporterà <u>per ogni punto percentuale in aumento rispetto al numero dei campioni di misura del parametro</u> nel periodo di riferimento, l'applicazione della penale “Percentuale di chiamate in ingresso perse” pari a € 1.000,00 (mille/00).
Applicazione	Amministrazione Contraente
Eccezioni	Nessuna

5 SCHEMA PER LA PRESENTAZIONE DEI CURRICULA

Di seguito viene presentato lo schema che il Fornitore dovrà utilizzare per la compilazione del 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 nel Capitolato Tecnico, a partire dalla più recente, fornendo una breve descrizione delle attività svolte, del ruolo ricoperto, della durata del progetto. È 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:</i> 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

Principali pubblicazioni	<i>(indicare le principali pubblicazioni)</i>	