CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO 2

CAPITOLATO TECNICO - PARTE GENERALE

ID 2174 – GARA PER L'AFFIDAMENTO DI UN ACCORDO QUADRO IN UN UNICO LOTTO AI SENSI DELL'ART 54 COMMA 4 LETT. C) DEL D.LGS. 50/2016 PER LA FORNITURA DI PRODOTTI PER LA GESTIONE DEGLI EVENTI DI SICUREZZA E DEGLI ACCESSI, LA PROTEZIONE DEI CANALI EMAIL, WEB E DATI ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI

Principali modifiche intervenute dalla pubblicazione del documento "ID 2174 - Condizioni di Fornitura - parte Generale" relativo all'avviso di preinformazione pubblicato sulla GUUE n. S-102 del 28/05/2021

Paragrafi	Ambito
1, 1.1 e 1.2	Modifiche inerenti l'entrata in vigore del D.L. 82/2021, del DPCM 81/2021 e del D.L. 77/2021

INDICE

1 Contesto di riferimento

Al fine di potenziare l'architettura nazionale cibernetica, con il Piano Nazionale per la protezione cibernetica e la sicurezza informatica di marzo 2017, AGID ha assunto il compito di *«dettare indirizzi, **regole tecniche e linee guida in materia di sicurezza informatica** e di omogeneità degli standard, **assicurare la qualità tecnica e la sicurezza dei sistemi informativi pubblici** e della loro rete di interconnessione e **monitorare i piani ICT delle amministrazioni pubbliche**».*

Attraverso il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020 – 2022 (in avanti nel presente documento anche solo "Piano Triennale"), AgID ha proseguito la propria attività per la regolamentazione della cyber security già avviata negli anni precedenti, evidenziando come *l'esigenza per la PA di contrastare le minacce cibernetiche sia divenuta fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA .*
Nel Piano Triennale **AGID fissa pertanto ulteriori obiettivi e relative linee di azione**, in capo ad AgID e al Dipartimento per la Trasformazione Digitale, nonché alle PA.

In tale contesto, si inserisce anche la pubblicazione, da parte di AgID, delle:

- «Misure minime di sicurezza ICT per le pubbliche amministrazioni (aprile 2017);
- «linee guida di sicurezza nello sviluppo delle applicazioni» (maggio 2020), per lo sviluppo del software sicuro nella PA;
- «linee guida di sicurezza nel procurement ICT» (maggio 2020), che raccolgono indicazioni tecnico-amministrative, buone prassi e strumenti operativi per garantire all'interno delle procedure di gara per l'approvvigionamento di beni e servizi ICT, la rispondenza di questi ad adeguati livelli di sicurezza.

In base alle disposizioni del CAD (D. Lgs n. 82/2005 e s.m.i.) e in linea con gli obiettivi descritti dal *Piano triennale*", AgID si occupa inoltre di "mantenere e sviluppare servizi di sicurezza preventivi e funzioni di accompagnamento utili per la crescita e la diffusione della cultura della sicurezza informatica".

Le attività di supporto alle PA **nella prevenzione e risposta agli incidenti informatici** svolte in passato dal CERT – PA, sono invece gestite, come previsto dal DPCM 8 agosto 2019, dallo **CSIRT Italia**, **il nuovo team per la cyber-difesa nazionale dapprima istituito presso il Dipartimento Informazioni per la Sicurezza (DIS) e trasferito, dal DL 82/2021** ("Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale") **presso l'Agenzia per la cybersicurezza nazionale (**in avanti nel presente documento anche solo "Agenzia").

La recente entrata in vigore (15/06/2021) del suddetto D.L., che ha decretato l'istituzione dell'Agenzia, ha aggiunto un altro importante tassello al contesto normativo cyber in forte evoluzione (D.L. n. 105/2019 convertito con modificazioni dalla Legge 133/2019, DPCM 131/2020, DPR 54/2021, DPCM 81/2021), rivedendo l'assetto organizzativo del Sistema di informazione per la sicurezza della Repubblica e le funzioni svolte dai vari Organi/Autorità, allo scopo di fronteggiare nel miglior modo possibile il rischio cibernetico, che può compromettere la sicurezza nazionale.
Secondo quanto previsto dal D.L. n. 82/2021 e, in particolare, in base a quanto disciplinato dal relativo art. 7, fra le funzioni ad essa assegnate, l'Agenzia assume tutte quelle già attribuite al DIS e al CVCN (Centro di valutazione e certificazione nazionale) dal D.L. 105/2019, nonché ai sensi del comma 1, lett. m) del succitato articolo, "*assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo*".

A ciò si aggiunge l'entrata in vigore (01/06/2021) del D.L. 77/2021 "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", che ha l'obiettivo di semplificare e agevolare la realizzazione del Piano Nazionale di Ripresa e Resilienza e che destina 620 milioni di euro alla cyber security delle PP.AA., considerando quindi questo un asset fondamentale a servizio della digitalizzazione del Paese.

In questo scenario di notevole fermento, il **Piano delle Gare Strategiche ICT, concordato tra Consip e AgID,** ha l'obiettivo, tra le altre cose, di mettere a disposizione delle PP.AA. delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza.

Consip S.p.A., in qualità di Stazione Appaltante, ha aggregato i fabbisogni e predisposto la procedura di gara per soddisfare le esigenze delle amministrazioni centrali e locali.

In tale contesto si inserisce la presente procedura, volta all'acquisizione di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni, strutturata in un unico lotto che darà origine a un **Accordo Quadro con più operatori economici,** ai sensi dell'art. 54, comma 4, lett. c) del D. Lgs. n. 50/2016.

1.1 Inquadramento Strategico

La presente iniziativa si colloca nell'ambito delle acquisizioni di beni e servizi strategici previsto da AgID ai fini dell'attuazione del Piano Triennale.

In particolare, il **Piano Triennale** vincola tutte le Pubbliche Amministrazioni al rispetto dell'indirizzo strategico ed operativo per la trasformazione digitale. L'Agenzia per l'Italia Digitale guida le Amministrazioni nella fase di adeguamento alle indicazioni contenute nel piano e successive versioni ed aggiornamenti, attraverso un'azione di coordinamento e monitoraggio.

L'attuazione del Piano triennale prevede un percorso graduale di coinvolgimento delle Pubbliche Amministrazioni:

- il **2017** è stato l'anno della costruzione, attraverso il consolidamento della strategia di trasformazione digitale e il completamento, del percorso di condivisione con le Pubbliche Amministrazioni;
- il **2018** è l'anno del consolidamento del Piano che sarà gestito anche attraverso strumenti on-line che consentiranno alle Pubbliche Amministrazioni di fornire i propri dati con semplicità. Essi permetteranno di gestire i piani triennali delle Amministrazioni in modo dinamico;
- il **2019** è l'anno di completamento delle azioni del primo ciclo triennale del processo,
- il **2020** e il **2022** sono gli anni della maturazione, della conclusione dei principali progetti avviati e dell'evoluzione di una visione orientata a cittadini e imprese.

Il Piano Triennale ricalca la stessa struttura del piano precedente e descrive il Modello strategico di evoluzione del sistema informativo della Pubblica Amministrazione ovvero le azioni di medio/lungo termine necessarie per un uso corretto, mirato, sicuro e consapevole delle tecnologie digitali.

I prodotti e i servizi oggetto della presente acquisizione sono quindi parte integrante del modello strategico di evoluzione digitale che dovrà essere adottato dalle Amministrazioni.

In ossequio alle previsioni del Piano Triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, sono previste la definizione e l'implementazione di misure di ***governance centralizzata***, mediante la costituzione di **Organismi di coordinamento e controllo, finalizzati alla direzione strategica e alla direzione tecnica della stessa**.

In particolare, le attività di direzione strategica prevedono il coinvolgimento di soggetti istituzionali, mentre nell'ambito delle attività di direzione tecnica saranno coinvolti anche soggetti non istituzionali, individuati nei Fornitori Aggiudicatari della presente acquisizione.

Si precisa che per "Organismi di coordinamento e controllo" si intendono i soggetti facenti capo alla Presidenza del Consiglio e/o al Ministero per l'Innovazione Tecnologica e la Digitalizzazione (es: Agid, Dipartimento per la trasformazione digitale per quanto concerne la direzione strategica), che, in base alle funzioni attribuite ex lege, sono ad oggi deputati, per quanto di rispettiva competenza, al monitoraggio e al controllo delle iniziative rientranti nel Piano Triennale per l'informatica nella Pubblica Amministrazione e/o nell'ambito della sicurezza informatica.

Nell'ambito di tali Organismi, è ricompresa altresì Consip S.p.A., per i compiti di propria competenza. Rimangono salve eventuali modifiche organizzative che interverranno a livello istituzionale nel corso della durata dell'Accordo Quadro che si stipulerà con gli aggiudicatari della presente gara.
Si precisa che, nell'ambito di tale iniziativa, potrebbe emergere la necessità di un coinvolgimento di ulteriori soggetti istituzionali con specifici ruoli nel settore della cyber security (DIS, CVCN trasferito presso l'Agenzia, …).

Gli **Organismi di coordinamento e controllo** saranno normati da appositi Regolamenti che, resi disponibili alla stipula dei contratti relativi alla presente iniziativa, esporranno gli aspetti operativi delle attività di coordinamento e controllo sia **tecnico** che **strategico**.

I meccanismi di governance sopra introdotti e applicati a tutte le iniziative afferenti al Piano Triennale riguarderanno:

- i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip;
- l'inquadramento o *categorizzazione* degli interventi delle Amministrazioni, realizzati mediante la sottoscrizione di uno o più contratti esecutivi afferenti alle iniziative del Piano Strategico, nel contesto del Piano Triennale;
- l'individuazione, da parte delle Amministrazioni, nell'insieme fornito in documentazione di gara, degli indicatori di digitalizzazione coi quali gli Organismi di coordinamento e controllo analizzeranno e valuteranno gli interventi realizzati dalle Amministrazioni con i contratti esecutivi afferenti alle Gare strategiche;
- la valutazione e l'attuazione della revisione dei prodotti/servizi previsti dagli Accordi Quadro e/o dei relativi prezzi, per le Gare Strategiche che lo prevedono in documentazione di gara e in funzione dell'evoluzione tecnologica del mercato e/o della normativa applicabile;
- l'analisi e la verifica di coerenza, rispetto al perimetro di ogni Gara Strategica, degli interventi delle Amministrazioni realizzati mediante contratti esecutivi afferenti alle Gare Strategiche;
- le modalità e le tempistiche con cui i fornitori dovranno consegnare i dati relativi ai contratti esecutivi, con particolare riferimento alla fase di chiusura degli Accordi Quadro.

1.2 Inquadramento Normativo

Si riportano di seguito le principali previsioni normative di riferimento che i Fornitori e le Amministrazioni Contraenti dovranno rispettare:

- D.Lgs. 7 marzo 2005, n. 82 e s.m.i ("*Codice dell'Amministrazione Digitale*")

- Piano Triennale per l'Informatica 2020 – 2022 (*"Piano triennale per l'informatica nella Pubblica Amministrazione"*)
- D.Lgs. 1 dicembre 2009, n. 177 ("*Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'articolo 24 della legge 18 giugno 2009, n. 69*")
- Legge 9 gennaio 2004, n. 4 ("*Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*")
- D.Lgs. 18 aprile 2016, n. 50 ("*Codice dei contratti pubblici*") e s.m.i. e relative prassi attuative
- normativa in materia di sicurezza sul luogo di lavoro di cui al D. Lgs. 9 aprile 2008, n. 81, come modificato ed integrato dal D.Lgs. 3 agosto 2009, n. 106;
- legge n. 46 del 05/03/1990: norme sulla sicurezza degli impianti, per quanto attiene all'installazione dei componenti e per quanto in vigore, nonché D.M. 22-1-2008 n. 37 (regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n. 248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici);
- Codice Civile;
- DPCM del 17/02/2017 («**Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali**») che delinea un'architettura istituzionale, attribuendo ruoli e responsabilità alle varie strutture coinvolte ai fini della realizzazione del quadro strategico nazionale;
- D. Lgs. 65/2018 e s.m.i., che attua la direttiva UE 2016/1148 (**Direttiva «NIS»**), intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, applicati agli «Operatori di Servizi Essenziali» (OSE) e ai «Fornitori di Servizi Digitali «(FSD);
- Legge n. 124/2007 ("Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto") e s.m.i.;
- Regolamento UE 2016/679 ("*Regolamento generale sulla protezione dei dati personali*")
- D.Lgs. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n. 101 ("*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*");
- D.L. 82/2021 (*"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*);
- D.L. 105/2019 (convertito con modificazioni dalla L. 18 novembre 2019, n. 133), come adeguato a sua volta dalla legge n. 8 del 28 febbraio 2020 e dal D.L. 82/2021, recante **disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica**, e i DPCM (tra cui il 131/2020, entrato in vigore il 5/11/2020) e regolamenti di successiva emanazione (alla data DPR 54/2021 e DPCM 81/2021), come previsti dalla menzionata legge. La disciplina di cui all'Accordo Quadro e relativi allegati (ivi compreso il Capitolato

Tecnico) potrà subire adeguamenti alla luce dei DPCM e regolamenti della richiamata normativa, che saranno emanati in seguito alla pubblicazione della presente iniziativa.

Il Fornitore comunque si impegna, ai sensi di quanto previsto dal DPCM 81/2021, del Regolamento di cui al DPR 54/2021, a porre in essere tutte le condizioni per il loro integrale recepimento tanto con riguardo alle caratteristiche, requisiti, standard e limiti delle forniture/servizi oggetto della presente iniziativa e sia con riguardo agli adempimenti, sempre in materia di sicurezza informatica, da porre in essere in ossequio alle disposizioni delle competenti Autorità.

In particolare, ai sensi di quanto previsto all'art. 1, comma 6 lett. a) del D.L. 105/2019, la cui efficacia è stata modificata dall'art. 16 comma 9, lett. a) del D.L. n. 82/2021, il Fornitore dovrà fornire pieno supporto alle Amministrazioni chiamate anche a collaborare con il CVCN (Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia) o i CV istituiti presso il Ministero dell'interno e il Ministero della difesa, all'effettuazione di verifiche preliminari e condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1 comma 2 lett. b) della L. 133/2019. Il Fornitore dovrà, pertanto, su richiesta dell'Amministrazione, mettere a disposizione il proprio know - how, i prodotti hardware e software oggetto di test, le risorse fisiche (ad es. componenti accessori, realizzazione di test bed, etc), logistiche (ad es. messa a disposizione di sedi idonee all'effettuazione dei test su richiesta dell'Amministrazione) e professionali (ad. es. figure professionali in grado di fornire il necessario supporto alle Amministrazioni sia nella fase che precede l'effettuazione dei test, che durante la loro esecuzione, nonché successivamente, per la produzione di eventuale documentazione tecnico - amministrativa che si rendesse necessaria);

- D.L. 77/2021 (*"Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*").

Si applicano inoltre tutte le previsioni del Piano Triennale e le norme italiane ed europee da questo richiamate.

1.3 Introduzione alla gara strategica e relativo perimetro

Nell'ambito delle gare strategiche, la presente iniziativa ha l'obiettivo di accelerare il procurement delle PA di prodotti di sicurezza ICT, da implementarsi presso le sedi delle Amministrazioni ordinanti, e i relativi servizi connessi alla fornitura.

I **prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni** consentiranno alle PA di dotarsi di soluzioni in grado di garantire il monitoraggio e la gestione degli eventi di sicurezza originati nell'ambito della propria

infrastruttura e di proteggere i canali mail e web e i propri dati, anche attraverso il tracciamento degli accessi maggiormente sensibili che operano nella gestione dei propri sistemi.

I prodotti richiesti sono:

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Database Security (DB Security)
- Data Loss Prevention (DLP)
- Privileged Access Management (PAM)
- Web Application Firewall (WAF).

A corredo di tali prodotti sono inoltre richiesti i seguenti servizi base connessi:

- installazione, configurazione
- formazione e affiancamento
- manutenzione
- Contact Center ed help desk
- hardening su client
- supporto specialistico.

Sono inoltre previsti i seguenti servizi aggiuntivi connessi:

- hardening su altri sistemi
- Data Assessment
- Privileged Account Assessment
- servizi professionali erogati dal vendor
- servizio di incident response.

1.4 Indicatori di digitalizzazione

Nell'ambito delle attività di governance ed in particolare della valutazione del livello di efficacia degli interventi operati dalle Amministrazioni attraverso l'utilizzo di contratti esecutivi afferenti alle Gare Strategiche, si intendono definite due tipologie di indicatori:

- Indicatori Generali, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale.

- Indicatori Specifici, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico Contratto Esecutivo in funzione dei prodotti/servizi acquisiti. In tale contesto è definito un indicatore (c.d. "indicatore di progresso" nel seguito descritto) che indica il livello di maturità della infrastruttura di sicurezza ICT delle Amministrazioni, sulla base del grado di mappatura degli interventi effettuati con le misure minime di sicurezza AGID (Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni» e successive modifiche e integrazioni).

Gli indicatori saranno utilizzati per il monitoraggio dei contratti e il raggiungimento dei relativi obiettivi, così come dettagliati nell'Appalto Specifico.

Ciascuna Amministrazione, nel proprio Appalto Specifico, assocerà almeno un Indicatore Generale per il quale fornirà, agli Organismi di coordinamento e controllo e/o ai soggetti da questi indicati, le misure di riferimento ex ante ed ex post rispetto al contratto esecutivo.

1.4.1 Indicatori generali

La seguente tabella riporta gli Indicatori Generali di digitalizzazione validi per tutte le Gare Strategiche:

Indicatori quantitativi	Indicatori qualitativi	Indicatori di collaborazione e riuso
Riduzione % della spesa per l'erogazione del servizio	Obiettivi CAD raggiunti con l'intervento	Riuso di processi per erogazione servizi digitali
Riduzione % dei tempi di erogazione del servizio	Infrastrutture immateriali integrate	Riuso soluzioni tecniche
Numero servizi aggiuntivi offerti all'utenza interna, esterna (cittadini), esterna (imprese), altre PA	Integrazione con Basi Dati di interesse nazionale	Collaborazione con altre Amministrazioni (progetto in co-working)

Gli elementi di dettaglio per la rilevazione degli indicatori generali saranno forniti alla stipula/attivazione dell'Accordo Quadro, o comunque secondo le modalità e i tempi concordati dall'Organismo di Coordinamento e Controllo finalizzato alla direzione strategica e/o secondo quanto più precisamente definito in corso d'opera all'atto della stipula/attivazione degli Accordi Quadro delle altre gare strategiche già pubblicate (Digital Transformation, Public Cloud IaaS e PaaS, Servizi Applicativi in ottica cloud e Data Management).

1.4.2 Indicatore specifico

1.4.2.1 Indicatore di progresso

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID (e successive modifiche e integrazioni), sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Appalto Specifico (acquisto di prodotti e/o servizi previsti nell'Appalto Specifico), che sarà determinato come da schema seguente:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Richiesta di Offerta dell'AS
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

2 Funzionamento dello strumento

2.1 Funzionamento dell'Accordo Quadro

L'Accordo Quadro avviene prevede **due fasi** procedimentali:

- **la prima fase**, che si conclude con l'aggiudicazione dell'Accordo Quadro e la sua stipula, a cura della Consip S.p.A. (così come disciplinato nel Capitolato d'Oneri);
- **la seconda fase**, che si caratterizza per l'affidamento di ciascun Contratto Esecutivo, a cura della singola Amministrazione contraente, tramite rilancio competitivo effettuato mediante **Appalto Specifico** ai sensi dell'art. 54, comma 4, lett. c) del Codice, il tutto, secondo i termini e le condizioni dell'Accordo Quadro.

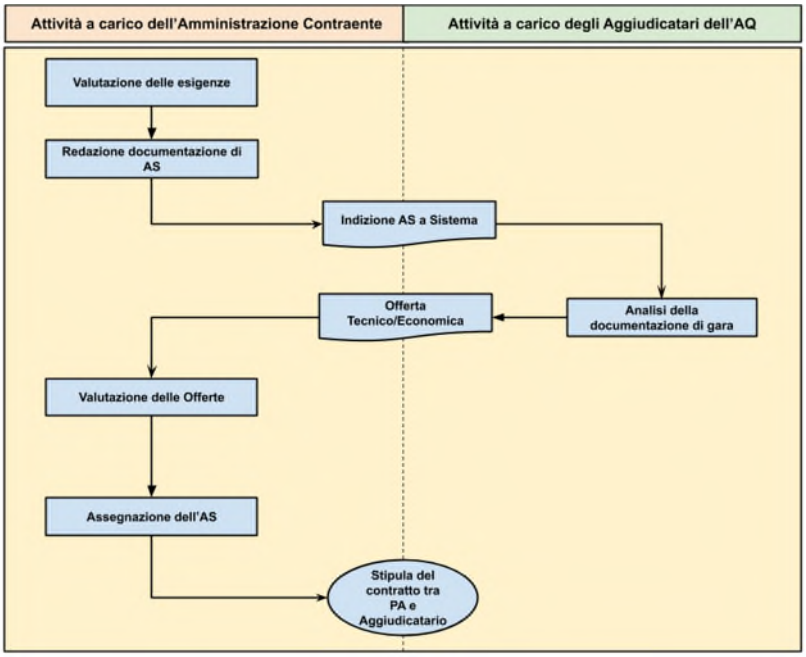
N. potenziali fornitori aggiudicatari	Accordo Quadro **multi fornitore** **Minimo numero di aggiudicatari pari a 2** **Massimo numero di aggiudicatari pari a 5**
Modalità di affidamento dei Contratti Esecutivi	Appalto Specifico (AS)
Condizioni contrattuali	Condizioni stabilite nel rilancio competitivo
Condizioni di adesione	Fabbisogno rientrante nel perimetro dei prodotti e servizi previsti

Al fine di utilizzare l'Accordo quadro, l'Amministrazione dovrà seguire l'*iter* procedurale descritto nei successivi paragrafi.

2.2 Adesione all'Accordo Quadro

Le Amministrazioni legittimate esperiranno gli **Appalti Specifici**, successivamente alla stipula dell'Accordo Quadro e per tutta la durata dello stesso, personalizzando i prodotti e i servizi richiesti in prima fase in linea con le condizioni stabilite nell'Accordo Quadro.

La realizzazione di ciascun Appalto Specifico avverrà attraverso il Sistema messo a disposizione da parte di Consip per mezzo del quale le Amministrazioni procederanno a realizzare la procedura indicando i prodotti e i servizi richiesti. La procedura di selezione è sinteticamente descritta nel diagramma seguente.



Si precisa che gli AS dovranno essere realizzati in accordo con i vincoli previsti nel Capitolato d'Oneri e nel Capitolato Tecnico speciale, a cui si rimanda per una descrizione puntuale delle modalità di realizzazione degli AS.

2.3 Categorizzazione degli interventi

Per ciascun Contratto Esecutivo, l'Amministrazione dovrà indicare gli ambiti (o layer) – cosiddetti di I livello - e i relativi obiettivi del Piano Triennale che essa prevede di mappare mediante le attività che saranno svolte con il Contratto esecutivo in oggetto.

Per ciascuno degli ambiti scelti, l'Amministrazione potrà selezionare, tra quelli presenti, uno o più obiettivi.

Tale categorizzazione dovrà essere riportata nella seguente documentazione contrattuale:

- Piano Operativo
- Contratto esecutivo.

Ambito (layer) – I livello	Obiettivi Piano Triennale
Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA
Dati	• Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese • Aumentare la qualità dei dati e dei metadati

	• Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
Piattaforme	• Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa • Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA • Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
Infrastrutture	• Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio) • Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud) • Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
Interoperabilità	• Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API • Adottare API conformi al Modello di Interoperabilità
Sicurezza Informatica	• Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA • Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

Fermo restando l'obbligo per le Amministrazioni di indicare gli ambiti di I livello e i relativi obiettivi del Piano Triennale, per le iniziative di Sicurezza Informatica ci si riserva la possibilità di definire prima della stipula dell'Accordo Quadro eventuali ambiti di II Livello più specifici per una mappatura più mirata degli interventi in ambito Cyber Security da parte delle PA.

2.4 Requisiti organizzativi

Il Fornitore è tenuto ad impiegare i referenti di seguito indicati, quali ruoli minimi di coordinamento delle attività contrattuali previste. In caso di inadeguatezza, impreparazione e/o incompetenza, il referente dovrà immediatamente essere sostituito con una figura rispondente ai requisiti minimi richiesti e con l'eventuale applicazione dei rilievi e/o delle penali contrattualmente previsti.

2.4.1 Ruoli di coordinamento richiesti

2.4.1.1 Responsabile unico delle attività contrattuali

Ai fini della gestione dell'Accordo Quadro, ogni Aggiudicatario dovrà indicare un Responsabile unico delle attività contrattuali (RUAC), che sarà il referente del Fornitore nei confronti di Consip S.p.A. per tutte le attività di gestione relative all'AQ. Il RUAC, inoltre, dovrà disporre di appositi poteri di firma tali da impegnare in maniera esecutiva il Fornitore nei confronti delle Amministrazioni.

Il RUAC dovrà almeno essere in possesso del Diploma di Scuola Media Superiore ed avere svolto, in aziende operanti nel settore dell'ICT, almeno 10 (dieci) anni di lavoro di cui 5 (cinque) anni di esperienza nello svolgimento di mansioni analoghe a quelle richieste.

Avrà la responsabilità delle seguenti attività:

- cura dei rapporti con la Consip S.p.A. e con AgID e suo diretto ed eventuale coinvolgimento su questioni riguardanti le singole Amministrazioni Contraenti, comunque per motivi di carattere straordinario, e su specifica richiesta di Consip/AgID;
- partecipazione agli incontri di allineamento con Consip/AgID;
- coordinamento dei Responsabili del Fornitore e supervisione delle attività a partire dal momento della stipula dei contratti;
- adozione di idonei strumenti per facilitare la comunicazione e lo scambio di informazioni tra i vari soggetti e attori coinvolti nella fornitura;
- assicurazione di un alto grado di sinergia tra le risorse impiegate nei diversi contratti esecutivi al fine di garantire un costante e adeguato grado di conoscenza e di attenzione ed evitando che medesime criticità possano ripetersi su più contratti;
- impostazione, organizzazione, pianificazione e controllo di tutte le azioni necessarie per garantire il rispetto delle prestazioni richieste, secondo i requisiti tecnici e nei tempi previsti, stabiliti anche con le Amministrazioni (ad esempio controllo del Piano Operativo, controllo dell'avanzamento delle prestazioni, verifica del pieno adempimento degli impegni assunti in offerta tecnica, pianificazione e impiego di risorse quantitativamente e qualitativamente adeguate, attività di valutazione e contenimento dei rischi, efficacia ed efficienza dell'attività di test, etc.);

- monitoraggio dell'andamento delle installazioni e controllo del rispetto dei piani concordati tra i Responsabili del Fornitore e le Amministrazioni Contraenti;
- proposta di eventuali azioni correttive a fronte di situazioni critiche;
- monitoraggio della qualità delle prestazioni erogate e dell'andamento dei livelli di servizio per tutto il periodo di efficacia dei contratti ed individuazione delle eventuali azioni correttive a fronte del mancato rispetto degli SLA previsti;
- reporting mensile, o comunque in ogni caso di esplicita richiesta da parte di Consip, sull'andamento dei contratti;
- gestione dei reclami/disservizi/segnalazioni da parte delle Amministrazioni Contraenti e/o della Consip S.p.A., prevedendo che le eventuali relative deduzioni dovranno essere sottoposte al cospetto del richiedente entro 3 giorni lavorativi dal ricevimento della segnalazione, pena l'applicazione delle penali secondo quanto stabilito nel Capitolato tecnico Speciale;
- gestione delle criticità e dei rischi complessivi di progetto risolvendo tutti i potenziali conflitti e/o eventuali disservizi;

2.4.1.2 Responsabili del Fornitore

I Responsabili del Fornitore sono i referenti operativi del Fornitore per le attività di fornitura e relativi servizi connessi. Il Fornitore dovrà rendere disponibile per ciascun Contratto esecutivo almeno un responsabile.

I suddetti responsabili dovranno garantire il corretto svolgimento delle attività, assicurando un elevato livello di qualità, nel pieno rispetto delle aspettative dell'Amministrazione contraente e dei livelli di servizio previsti dal Capitolato Tecnico.

Il Fornitore dovrà indicare, per ogni AS e prima della stipula dell'AS, i riferimenti del Responsabile del Fornitore (numero di telefono cellulare e un indirizzo di posta elettronica) e garantire la risposta ai quesiti posti dall'Amministrazione Contraente entro 3 giorni lavorativi dall'inoltro o dal contatto telefonico (cfr. par. 4.1.8 del Capitolato Tecnico parte Speciale).

Il responsabile dovrà essere almeno in possesso del Diploma di Scuola Media Superiore ed avere conseguito, in aziende operanti nel settore dell'ICT, almeno 10 (dieci) anni di lavoro di cui 3 (tre) anni di esperienza nello svolgimento di mansioni analoghe a quelle richieste.

In considerazione della natura delle attività da svolgere e a garanzia dell'operatività dei servizi, i Responsabili devono essere reperibili telefonicamente dal lunedì al venerdì, dalle ore 8 alle ore 20 e sempre tramite posta elettronica.

Il *Responsabile del Fornitore* deve essere inoltre disponibile presso l'Amministrazione ove necessario e/o richiesto per l'espletamento di tutte le attività contrattuali.

Il *Responsabile del Fornitore* avrà la responsabilità delle seguenti attività:

- risponderà in termini organizzativi/funzionali al RUAC condividendo ed attuando le impostazioni ricevute;
- risponderà all'Amministrazione Contraente per tutte le attività e le problematiche relative alle fasi di pianificazione, consegna, realizzazione, verifica di conformità della fornitura e di esecuzione dei servizi richiesti;
- parteciperà alle riunioni di avanzamento e/o a riunioni indette dalle Amministrazioni.
- coordinerà le risorse impiegate;
- implementerà le azioni necessarie per garantire il rispetto delle prestazioni richieste secondo i requisiti tecnici e nei tempi previsti, stabiliti anche con le Amministrazioni;
- risponderà per la risoluzione dei disservizi e la gestione dei reclami da parte delle Amministrazioni e/o della Consip S.p.A. prevedendo che le eventuali relative deduzioni dovranno essere sottoposte al cospetto del richiedente entro 3 giorni lavorativi dal ricevimento della segnalazione pena l'applicazione delle penali secondo quanto stabilito dall'Accordo Quadro;
- dovrà provvedere a informare l'Amministrazione Contraente attraverso la realizzazione di stati di avanzamento, predisponendo se necessario un *Piano Correttivo* a fronte di eventuali ritardi e/o problemi riscontrati, che l'Amministrazione avrà la facoltà di accettare, ovvero chiederne eventuali integrazioni o revisioni. Laddove il *Piano Correttivo* sia accettato dall'Amministrazione, il cronoprogramma di progetto riportato nel *Piano Operativo* dovrà essere aggiornato di conseguenza (cfr Capitolato Tecnico Speciale);
- riporterà puntualmente al RUAC l'andamento dei livelli di servizio dei contratti esecutivi gestiti;
- sarà responsabile delle comunicazioni e dei documenti formalizzati nei confronti dell'Amministrazione (ad esempio il "*Verbale di Fornitura*");
- eseguirà di concerto con il Responsabile dell'Amministrazione i controlli di qualità per assicurarsi che tutte le attività vengano realizzate a regola d'arte.

3 Fase di avvio dell'AQ e di conclusione dei contratti esecutivi

3.1 Adempimenti del Fornitore in fase di avvio

A partire dalla data di stipula dell'Accordo Quadro, il Fornitore dovrà mettere in campo tutte le azioni necessarie per garantire al proprio personale l'acquisizione di tutte le conoscenze indispensabili al corretto svolgimento della fornitura e dei servizi previsti contrattualmente, in funzione dei dimensionamenti previsti in fase di gara.

In tale fase e conformemente ai livelli di servizio e alle tempistiche di attivazione dei servizi previste, il Fornitore dovrà attuare e rendere pienamente operativo quanto previsto nel capitolato tecnico parte speciale e quanto dichiarato in sede di offerta tecnica per l'avvio della fase di esecuzione, compresivi di modelli organizzativi, modalità operative e strumenti richiesti nel capitolato tecnico e/o indicati in offerta tecnica dal concorrente.

3.2 Trasferimento Know-how

In base ai servizi connessi richiesti da parte dell'Amministrazione contraente (quali ad esempio il supporto specialistico), nella fase finale di esecuzione, secondo le indicazioni previste dal Contratto Esecutivo, il Fornitore dovrà predisporre un Piano di Trasferimento per le attività di passaggio di consegne di fine fornitura (*phase-out*), finalizzato al trasferimento all'Amministrazione, o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione delle attività.

L'Amministrazione contraente ha la facoltà di richiedere nel Piano Operativo, oppure durante il periodo di durata contrattuale, il passaggio di consegne di fine fornitura per ciascun Contratto esecutivo, per un periodo massimo di trenta giorni solari precedenti alla data di scadenza del Contratto Esecutivo.

Il passaggio di consegne di fine fornitura dovrà essere erogato dal Fornitore senza oneri aggiuntivi per l'Amministrazione, in accordo con i requisiti di qualità indicati nel presente capitolato.

Il Fornitore dovrà mettere a disposizione un apposito gruppo di lavoro, con un numero adeguato di risorse professionali, strumenti organizzativi e tecnologici.

Si fa presente che il trasferimento di know-how potrà essere richiesto anche durante l'erogazione dei servizi nel corso della durata contrattuale, direttamente al personale dell'Amministrazione tramite apposita comunicazione.

Rientrano nelle responsabilità generali del Fornitore le seguenti attività:

- il project management generale del progetto e le attività di governance complessiva;
- il coordinamento generale di tutti gli attori coinvolti e la supervisione delle attività di trasferimento;
- il supporto, per tutta la durata delle attività di trasferimento, a tutti gli attori coinvolti per lo svolgimento delle attività;
- lo svolgimento delle attività di propria pertinenza in conformità alla pianificazione definita;
- il reporting continuativo e conclusivo delle attività svolte al termine del trasferimento.

Il Fornitore, a supporto della specifica fase di transizione dovrà produrre un apposito Piano di Trasferimento (PTF) che prevede i seguenti contenuti minimi:

- l'oggetto del trasferimento,
- le attività e le relative modalità di esecuzione;
- i compiti e le responsabilità di ciascuna delle Parti;
- il programma temporale in base al quale le attività dovranno essere eseguite.

Il PTF sarà redatto dal Fornitore e sottoposto all'approvazione dell'Amministrazione almeno 30 giorni solari prima della scadenza del Contratto esecutivo, oppure entro trenta giorni solari successivi alla data di comunicazione dell'evento di cessazione delle attività oppure entro 15 giorni solari dalla data di richiesta dell'Amministrazione se il trasferimento è richiesto durante il periodo di durata contrattuale. Il documento prodotto dovrà essere gestito dal Fornitore ed aggiornato a seguito delle modifiche richieste dall'Amministrazione ovvero intervenute nel corso di svolgimento delle attività di trasferimento.

La responsabilità della gestione contrattuale viene mantenuta dal Fornitore fino al termine delle attività di Trasferimento del servizio in conformità di quanto previsto dal PTF.

Su richiesta dell'Amministrazione, il Fornitore dovrà registrare tutti gli effort delle risorse impegnate nelle attività di esecuzione del trasferimento per tutta la durata delle attività stesse e consegnarle unitamente al rapporto finale per consentire le verifiche da parte dell'Amministrazione.

4 Strumenti a supporto della fornitura

4.1 Portale di Fornitura

Il Fornitore dovrà rendere disponibile, senza oneri aggiuntivi, un **"Portale della Fornitura",** multicanale e raggiungibile tramite Internet (basato sull'utilizzo esclusivo del protocollo *HTTPS* configurato con certificati non *self-signed* in linea con le raccomandazioni *AgID-TLS e cipher suite*) che consenta alle singole Amministrazioni e agli Organismi di coordinamento e controllo di governare agevolmente la fornitura e di promuovere la condivisione e l'esperienza maturata nelle varie iniziative.

Il Portale deve dunque fungere anche da strumento di promozione per la PA e di comunicazione tra la PA e i cittadini/imprese, offrendo a questi ultimi servizi di informazione e monitoraggio circa l'andamento delle varie iniziative.

Nel realizzare il Portale, l'aggiudicatario pertanto dovrà prevedere come dotazione minima:

- strumenti e soluzioni di project management per la pianificazione e la gestione delle singole iniziative progettuali;
- strumenti di analisi ed esplorazione dei dati, orientati all'analisi multidimensionale e con funzionalità di creazione di grafici ed interrogazioni complesse e personalizzate, estrazioni ed esportazioni sui formati maggiormente diffusi per lo scambio dati (es. csv, xml, json, xls ecc.).
- cruscotti grafici riassuntivi, costituiti dai parametri di SLA ed i valori effettivamente conseguiti sulla base dei dati individuati per il raggiungimento degli obiettivi di monitoraggio ed attuazione di processi;
- strumenti di collaborazione e cooperazione, per la condivisione di documenti e contenuti digitali e la comunicazione social a supporto del confronto su esperienze e iniziative di interesse;

Il Portale dovrà quindi essere organizzato dal Fornitore nelle seguenti aree di fruizione:

- "Area Comunicazione": è l'area ad accesso pubblico del portale, contiene informazioni di carattere generale sull'AQ e informazioni e dati specifici sull'andamento della fornitura e dei servizi connessi; **(a partire dalla I release del portale).**
- "Area Informativa": è l'area di supporto riservata alla PA e contiene almeno le seguenti informazioni: documentazione aggiornata (normativa, tecnologica e operativa) di riferimento per i prodotti e servizi dell'AQ; la descrizione delle soluzioni migliorative offerte **(a partire dalla I release** del portale relativamente alla **documentazione normativa** e **nella versione completa** relativamente alla **documentazione tecnologica e operativa)**;
- "Area Project Management": è l'area ad accesso riservato e profilato per le singole Amministrazioni tramite la quale è possibile disporre degli strumenti di pianificazione e gestione delle singole iniziative progettuali; deve governare l'esecuzione dell'intero workflow operativo di ciascun Appalto Specifico dal Piano Operativo alla verifica di conformità finale ed eventuali rilevazioni nel periodo di garanzia; il

Fornitore quindi prevedrà in questa sezione anche le versioni eventualmente aggiornate del Piano Operativo (**a partire dalla I release del portale**).

- "Area Collaborazione e Monitoraggio": è l'area che contiene:
  - gli strumenti e le informazioni di controllo e governo della fornitura quali cruscotti statici e dinamici relativi ai dati di tutti i Piani Operativi e i Contratti Esecutivi;
  - reportistica sul rispetto dei livelli di servizio e degli indicatori di digitalizzazione; report statici e dinamici relativi ai valori economici dei Contratti Esecutivi con evidenza della capacità contrattuale residuale; i dati devono essere estraibili nei formati maggiormente diffusi per lo scambio dati (es. csv, xml, json, xls, ecc.).
  - gli strumenti di promozione di collaborazione e condivisione tra le PA.
- "Area Osservatori": è l'area che consente agli Organismi di coordinamento e controllo e alla Consip S.p.A. di svolgere le proprie funzioni di monitoraggio sulla qualità dei servizi erogati in AQ.

Il Fornitore deve organizzare la navigazione delle aree di interesse prevedendo l'accesso differenziato degli utenti in base alle seguenti tipologie:

- Non autenticato: utente generico del World Wide Web (WWW);
- Utente accreditato (ad esempio un fornitore di servizi);
- Pubblica Amministrazione: l'Amministrazione contraente che ha aderito (o intende aderire) ai prodotti/servizi oggetto della fornitura;
- Organismo di Coordinamento e Controllo e Consip S.p.A.;
- Utente accreditato facente parte della struttura organizzativa della Pubblica Amministrazione (Consip S.p.A e/o terzi soggetti da essa indicati, ecc.).

In particolare gli Organismi di coordinamento e controllo dovranno avere la possibilità, su loro richiesta, di accedere a tutte le aree sopra descritte in modo da visionare e analizzare la documentazione ivi presente. Il Fornitore dovrà pertanto prevedere per essi un accesso dedicato al Portale di Fornitura ed attivabile in funzione delle specifiche richieste e requisiti da essi indicati in corso d'opera.

Il Portale dovrà essere implementato utilizzando un'infrastruttura hardware e software che il fornitore stesso provvederà a realizzare e mantenere in esercizio. Il Portale deve essere gestito globalmente dal Fornitore che assume la responsabilità di garantire:

- hosting della piattaforma;
- gestione e manutenzione del portale;
- aggiornamento dei contenuti e la corretta alimentazione del sito;
- disponibilità in linea per le Amministrazioni, Consip S.p.A. e/o soggetti terzi da essa indicati;

- gestione degli accessi agli utenti abilitati mediante credenziali di riconoscimento (es., login e password);
- disponibilità di un manuale di utilizzo del portale e dei singoli sistemi integrati.

Il Fornitore dovrà procedere alla progettazione e realizzazione del sistema includendo le eventuali indicazioni provenienti da Consip nella fase di predisposizione del Portale.

Il Portale dovrà essere reso disponibile in una prima release funzionante all'attivazione dell'Accordo Quadro e nella versione completa all'attivazione dei servizi del primo Contratto Esecutivo di fornitura sottoscritto e dovrà essere reso disponibile con continuità alle Amministrazioni contraenti, a Consip S.p.A. e/o terzi soggetti da essa indicati, e ad eventuali strutture da essi delegate per tutta la durata contrattuale ed aggiornato con frequenza almeno mensile, entro il 15 del mese successivo al mese di riferimento.
Il Portale dovrà garantire i necessari livelli di riservatezza adeguati alla gestione di informazioni e dati che riguardano affidamenti diversi.

Tutta la reportistica prodotta relativa ai servizi dovrà essere archiviata e conservata a cura del Fornitore, attraverso un sistema di gestione della documentazione riservata.
Il Fornitore inoltre, dovrà garantire la Disponibilità del Portale secondo quanto stabilito nel Capitolato Tecnico parte Speciale, pena le applicazioni delle penali ivi previste.

5 Organismo di coordinamento e controllo finalizzato alla direzione tecnica

Come indicato al paragrafo 1.1, è previsto un Organismo di coordinamento e controllo finalizzato alla direzione tecnica, che si occuperà, fra l'altro, di valutare, in accordo con i soggetti istituzionali interessati, sia gli impatti che eventuali disposizioni possano avere nell'ambito dei prodotti e dei servizi previsti nell'iniziativa sia le evoluzioni tecnologiche che potrebbero consentire di migliorare la sicurezza informatica delle Pubbliche Amministrazioni.
Stante l'attuale evoluzione del quadro normativo di riferimento (cfr. paragrafo 1.2) non è possibile alla data di pubblicazione della presente iniziativa prevedere quali potranno essere in dettaglio ulteriori compiti specifici che tale Organismo dovrà contemplare.
I Fornitori Aggiudicatari, con la stipula dei relativi contratti, si impegnano in ogni caso a **recepire obbligatoriamente** le indicazioni fornite dall'Organismo nei limiti in cui tali le indicazioni derivino da **disposizioni normative cogenti e inderogabili**, **Regolamenti e Circolari adottate dai Soggetti Istituzionali competenti,** anche alla luce delle prescrizioni derivanti dai decreti attuativi di cui all'art. 1, commi 2 e 3, D.L. n. 105/2019, e loro rispettivi aggiornamenti, e/o del Regolamento di cui al DPR 54/2021. Tali indicazioni potranno riguardare, a titolo non esaustivo:

- **la modifica di specifiche fasce relative ai meta prodotti**;

- **l'inserimento di nuovi meta prodotti,** comunque complementari/supplementari a quelli previsti in gara, ad esempio nel caso in cui sia necessario adeguare l'offerta per recepire caratteristiche, requisiti e standard delle forniture oggetto della presente iniziativa, così come saranno prescritte dai decreti attuativi per le Amministrazioni che rientrano nel "Perimetro di sicurezza nazionale cibernetica";
- **recepire eventuali raccomandazioni** derivanti dall'Organismo e concernenti la fornitura e/o le modalità di erogazione dei servizi connessi e i relativi livelli di servizio, con le relative modifiche/integrazioni/variazioni che dovranno essere concordate ed autorizzate dall'Organismo stesso.

In particolare**,** in caso di **modifica di specifiche fasce relative ai meta prodotti:**

- l'Organismo potrà modificare/integrare/variare i requisiti migliorativi e le funzionalità aggiuntive richiedibili in seconda fase per i prodotti, al fine di recepire **disposizioni normative cogenti e inderogabili** sopraggiunte, quali quelle derivanti dai decreti attuativi della legge sul perimetro di sicurezza cibernetica. In tal caso, come previsto al paragrafo 1.2, i Fornitori Aggiudicatari dell'AQ dovranno porre in essere tutte le condizioni per l'integrale recepimento delle richieste dell'Organismo.

Nel caso di **inserimento di nuovi meta prodotti** ulteriori rispetto a quelli previsti dal Capitolato Tecnico Speciale, l'Organismo procederà con un'analisi tecnica comparativa fra i prodotti delle tecnologie rappresentative del mercato di riferimento, che potranno essere scelte fra le seguenti:

- tecnologie proposte dai Soggetti Istituzionali;
- tecnologie proposte dal Fornitore;
- tecnologie che potranno essere identificate a seguito di opportuna analisi di mercato.

L'Organismo effettuerà un'analisi economica volta a congruire, sulla base di una valutazione riguardante il mercato di riferimento, i prezzi dei nuovi meta prodotti. I prezzi congruiti per i nuovi ambiti merceologici costituiranno la base d'asta per la seconda fase.

I Fornitori si impegnano inoltre a:

T1. sottoscrivere il Regolamento dell'Organismo ed agire in linea con lo stesso, rispettando gli obblighi contrattuali assunti;
T2. partecipare agli incontri periodici dell'Organismo Tecnico di coordinamento e controllo, rendendo disponibili le informazioni e i dati di avanzamento delle attività e dei contratti, in funzione dell'Ordine del Giorno stabilito per l'incontro stesso;
T3. supportare l'Organismo Tecnico di coordinamento e controllo nelle attività di inserimento di nuovi meta prodotti;
T4. fornire all'Organismo Tecnico di coordinamento e controllo report descrittivi di tutte le iniziative progettuali eseguite;

T5. fornire all'Organismo proposte di inserimento di nuovi meta prodotti e/o di adeguamento della modalità di erogazione dei servizi connessi e dei relativi livelli di servizio sulla base di evidenze documentate dal Fornitore, mediante report specifici, analisi di mercato.

6 Organismo di coordinamento e controllo finalizzato alla direzione strategica

Tale Organismo sarà unico per tutte le Gare Strategiche ICT. In particolare, nell'ambito delle attività di coordinamento e controllo strategico, il Fornitore assume i seguenti obblighi:

S1. Supportare l'Organismo Strategico di coordinamento e controllo nell'analisi dei progetti ad alta criticità segnalati dagli Organismi Tecnici di coordinamento e controllo;

S2. Collaborare e Supportare l'Organismo Strategico di coordinamento e controllo nelle attività di propria competenza (ad esempio: analisi delle best practices in ambito cyber security, modelli, soluzioni, metriche, modalità di remunerazione dei servizi connessi, etc.);

S3. Fornire report che evidenzino processi/applicazioni/soluzioni/servizi ICT che sono stati impiegati presso molteplici Amministrazioni.