

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

CAPITOLATO TECNICO GENERALE

Classificazione Consip: Ambito pubblico

Indice

1.	SCOPO DEL DOCUMENTO	3
1.1.	Acronimi	4
1.2.	Definizioni	5
2.	CONTESTO DI RIFERIMENTO	7
2.1.	Contesto generale in ambito Cyber sicurezza	7
2.2.	Contesto normativo, Linee Guida e Standard di riferimento	10
3.	DURATA	13
4.	LUOGO DI ESECUZIONE DEI SERVIZI	14
5.	RAZIONALI PER L'UTILIZZO DELL'ACCORDO QUADRO	16
6.	MODELLO DI FUNZIONAMENTO	18
6.1.	Interazione tra i Lotti di servizi Managed Security Services e servizi di Governance, Analisi del Rischio e Controllo	18
6.2.	Adesione ai Lotti dell'Accordo Quadro	18
6.3.	Modalità di affidamento dei contratti esecutivi	19
6.3.1.	RPF (Richiesta Preliminare di Fornitura)	19
6.3.2.	Piano Operativo	22
6.3.3.	Contratto esecutivo	24
6.4.	Responsabilità ed obblighi dei fornitori	28
7.	REQUISITI ORGANIZZATIVI	29
7.1.	Requisiti di qualità	29
7.2.	Risorse impiegate	31
8.	RUOLI DI COORDINAMENTO RICHIESTI	32
8.1.	Responsabile unico delle attività contrattuali (RUAC)	32
8.2.	Responsabili tecnici per l'erogazione dei servizi	33
9.	COLLAUDO E TEST DEI SERVIZI	34
9.1.	Collaudo funzionale	35
9.2.	Collaudo di configurazione	36
10.	GOVERNANCE	36
11.	CLAUSOLA EX ART. 120, COMMA 1, LETT. A), DEL D.LGS. 36/2023	37
12.	PRESCRIZIONI COMUNI RELATIVE A SOLUZIONI CLOUD E INFRASTRUTTURE	40
12.1.	Qualificazione/Adeguamento	41
12.2.	Exit strategy e grace period	43
12.3.	Perdita della qualificazione/adequatezza	43
12.4.	Sostituzione di soluzioni cloud e infrastrutture	44
13.	PRESCRIZIONI COMUNI RELATIVE ALLA CYBERSICUREZZA	44

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

1. SCOPO DEL DOCUMENTO

La presente iniziativa si pone in continuità con l'AQ ID 2296 – Servizi di sicurezza da remoto in materia di servizi di cyber sicurezza. L'obiettivo dell'iniziativa è quello di mettere a disposizione delle PP.AA. un insieme di servizi finalizzati alla protezione dei perimetri, delle infrastrutture, dei dati e delle applicazioni in linea con il Piano triennale per l'informatica nella PA 2024-2026 di AgID e con la normativa in materia di cyber security.

L'iniziativa è suddivisa nei seguenti Lotti:

Numero Lotto	Oggetto del lotto	CIG
1	Servizi Managed Security Services gestiti da remoto - PAC	
2	Servizi Managed Security Services gestiti da remoto – PAL	
3	Servizi di Governance, Analisi del Rischio e Controllo – PAC	
4	Servizi di Governance, Analisi del Rischio e Controllo - PAL	

Tabella 1 – Elenco dei lotti

Il presente Capitolato Tecnico Generale ha lo scopo di descrivere il funzionamento e i requisiti comuni ai suddetti lotti oggetto della presente iniziativa.

Il presente documento è integrato:

- dall'Appendice 1 "Schema verifiche ispettive";
- dal Capitolato Tecnico Speciale Lotti 1 e 2 relativo ai Servizi di Sicurezza da remoto e relative Appendici;
- dal Capitolato Tecnico Speciale Lotti 3 e 4 relativo ai Servizi di Governance, Analisi del Rischio e Controllo e relative Appendici.

I Capitolati Tecnici Speciali disciplinano i contenuti di dettaglio e i requisiti minimi dei rispettivi lotti, in termini di quantità, qualità e indicatori di qualità.

Si chiarisce che tutti i requisiti minimi richiesti per i servizi di cybersicurezza dei rispettivi Lotti, oggetto della presente iniziativa, dovranno essere mantenuti in corso di validità per tutta la durata contrattuale e aggiornati anche di fronte ad evoluzioni del contesto tecnologico e normativo di riferimento, senza oneri aggiuntivi per le Pubbliche Amministrazioni beneficiarie.

Si chiarisce altresì che l'erogazione delle prestazioni oggetto di tutti i Lotti di cui alla presente iniziativa dovrà avvenire nel rispetto di tutte le normative, linee guida e prassi di settore, vigenti e applicabili, in materia di sicurezza cibernetica, di cui al par. 2.2.

Per agevolare la lettura del presente documento e di ciascun Capitolato Tecnico Speciale

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

vengono riportati di seguito gli acronimi e le definizioni più frequentemente utilizzati nell'ambito di tali documenti.

1.1. Acronimi

ACN: Agenzia per la Cyber sicurezza Nazionale

AgID: Agenzia per Italia Digitale

AQ: Accordo Quadro

API: Application Program Interface

CAD: Codice dell'Amministrazione Digitale

CI/CD: Integrazione continua/deployment continuo

CONSIP: Consip S.p.A.

CPE: Customer Premises Equipment

CSIRT: Computer Security Incident Response Team

CVCN: Centro di valutazione e certificazione nazionale

ENISA: Agenzia dell'Unione europea per la cibersicurezza

GDPR: General Data Protection Regulation - Regolamento generale sulla protezione dei dati

HTTP: Hyper Text Transport Protocol

HTTPS: HyperText Transfer Protocol Secure

ICT: Information and Communication Technology

IT: Information Technology

KPI: Key Performance Indicator

NIS: Network & Information Security

NIST: National Institute of Standards and Technology

MISP: Malware information Sharing Platform

OSSTMM: Open Source Security Testing Methodology Manual

OT: Operational Technology

PA/PP.AA.: Pubblica/le Amministrazione/i

PAC: Pubblica Amministrazione Centrale

PAL: Pubblica Amministrazione Locale

PCI: Payment Card Industry.

PMO: Project Management Office

PT: Piano Triennale per l'informatica nella PA 2024-2026

RUPA: Rete Unitaria della Pubblica Amministrazione

SIEM: Security information and event management

SOC: Security Operation Center

SPC: Sistema pubblico di connettività

SPID: Sistema pubblico di identità digitale

SAL: Stato Avanzamento Lavori

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

XioT: Extended Internet of Things

1.2. Definizioni

Accordo Quadro/AQ: l'Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A., per ciascun Lotto, all'esito della procedura di gara di prima fase, comprensivo di tutti i suoi Allegati, nonché dei documenti ivi richiamati, quale accordo concluso da Consip anche per conto delle Amministrazioni, da una parte, ed il Fornitore, dall'altra parte, con lo scopo di stabilire le clausole relative ai Contratti Esecutivi da affidare per tutta la durata del medesimo Accordo Quadro.

Aggiudicatario/Fornitore: se non diversamente indicato, l'"aggiudicatario" di ciascuno dei lotti della fornitura.

Amministrazione aggiudicatrice: Consip S.p.A.

Amministrazione/i o Amministrazione/i Contraente/i: le Stazioni Appaltanti, nonché gli altri soggetti che, ai sensi della normativa vigente e di quanto previsto al successivo capitolo 5, sono legittimati ad affidare Contratti Esecutivi nell'ambito dell'Accordo Quadro relativo a ciascun lotto.

Capitolato Tecnico Generale: il presente documento che definisce il funzionamento, le modalità di utilizzo e i requisiti comuni ai lotti oggetto della presente iniziativa.

Capitolati Tecnici Speciali: i documenti che integrano il presente documento, disciplinando i contenuti di dettaglio e i requisiti minimi della singola tipologia di servizio per ciascuna tipologia di lotto, in termini di quantità, qualità e livelli di servizio.

Contratto Esecutivo/di Fornitura: il contratto avente ad oggetto i servizi della presente gara, costituito dall'Ordine di Fornitura inviato a Sistema e dai rispettivi allegati.

Erosione Potenziale: erosione del massimale dell'Accordo Quadro calcolata sulla base delle richieste preliminari di fornitura (come di seguito definite).

Erosione Effettiva: erosione del massimale dell'Accordo Quadro calcolata sulla base dei Contratti Esecutivi perfezionati.

Ordine di Fornitura: l'ordine diretto inviato dall'Amministrazione, attraverso il Sistema, nei confronti del Fornitore.

Piano dei Fabbisogni: il documento preliminare inviato dall'Amministrazione al Fornitore, individuato sulla base di quanto previsto nel presente documento, nel quale dovranno essere riportate, tra l'altro, le specifiche esigenze dell'Amministrazione.

Piano Operativo: il documento inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione.

Prodotto della fornitura: tutto ciò che viene realizzato dal fornitore, compresa la documentazione contrattuale.

Richiesta Preliminare di Fornitura o RPF: richiesta preliminare inviata dall'Amministrazione, attraverso il Sistema, nei confronti del Fornitore, nel rispetto delle regole previste nel presente documento, contenente il Piano dei Fabbisogni.

Modalità di erogazione *da remoto*: servizio erogato - in modalità Managed Security Services- attraverso i Centri Servizi del Fornitore.

Modalità di erogazione *on-site*: servizio erogato presso le strutture dell'Amministrazione beneficiaria o altre strutture indicate dalla stessa o in alternativa presso la sede del Fornitore.

Milestone: in ingegneria del software e Project Management indica ciascun traguardo intermedio e il traguardo finale dello svolgimento del progetto. Sono i punti di controllo all'interno di ciascuna fase oppure di consegna di specifici deliverable o raggruppamenti di deliverable. Sono normalmente attività considerate convenzionalmente a durata zero che servono per isolare nella schedulazione i principali momenti di verifica e validazione. Di fatto ciascun punto di controllo serve per approvare quanto fatto a monte della milestone ed abilitare le attività previste a valle della milestone.

Sistema: il Sistema informatico predisposto dal MEF, tramite Consip, costituito da soluzioni e strumenti elettronici e telematici che consentono l'effettuazione delle procedure telematiche di approvvigionamento previste dagli Strumenti di Acquisto/Negoziato, nel rispetto della normativa vigente in materia di approvvigionamenti della Pubblica Amministrazione.

Sistema IT: la singola immagine del sistema operativo, comprensiva di tutte le periferiche fisiche e/o logiche e di tutti i prodotti e/o servizi necessari al corretto funzionamento delle applicazioni, oppure l'insieme delle componenti HW e SW inserite in un unico chassis atto alla interconnessione e l'estensione di reti TLC (ad esempio apparati che gestiscono i primi quattro livelli della pila ISO-OSI).

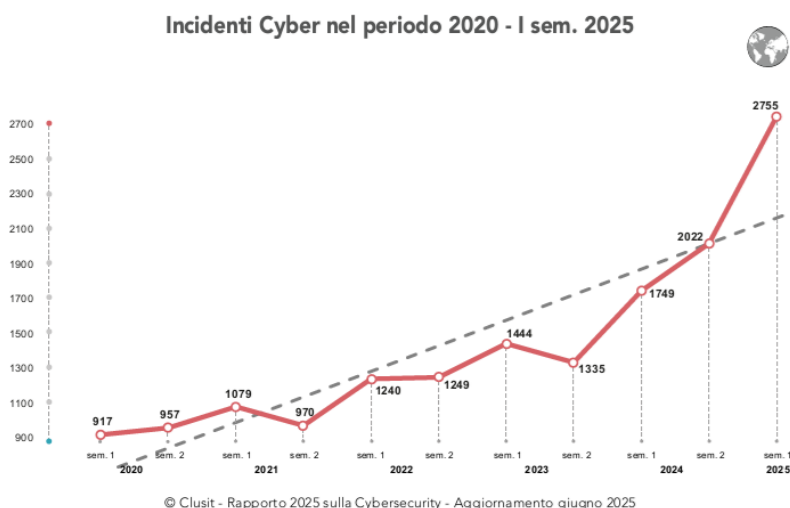
Centro servizi: la/e sede/i da cui l'Aggiudicatario eroga i servizi "da remoto" in modalità Managed Security Services di cui al Capitolato tecnico speciale Lotti 1 e 2.

2. CONTESTO DI RIFERIMENTO

2.1. Contesto generale in ambito Cyber sicurezza

Il contesto attuale della cyber sicurezza è caratterizzato da un aumento significativo delle minacce informatiche, con un'evoluzione continua delle tecniche di attacco e una maggiore attenzione alle vulnerabilità delle infrastrutture critiche e dei sistemi delle organizzazioni ed in particolare della PA. La crescente interconnessione dei dispositivi, l'adozione di nuove tecnologie e l'aumento della dipendenza da sistemi digitali rendono la cybersicurezza un'area fondamentale per la protezione delle informazioni e la continuità operativa.

Nel 2024 gli incidenti a livello mondiale erano aumentati del 36% rispetto al 2023 (quelli verso Italia del 20%). La tendenza globale del primo semestre 2025 mostra una ulteriore crescita, pari al +36% rispetto al semestre precedente (+13% verso l'Italia) Nel primo semestre 2025, secondo una tendenza ormai consolidata da diversi anni, non solo è aumentata la frequenza degli incidenti ma anche la loro gravità media. Nel 2024, gli incidenti con impatto "Critico" o "Alto" erano il 77% del totale (un aumento drammatico rispetto al 50% del 2020). Nella prima metà del 2025, l'impatto medio stimato a livello globale è cresciuto ulteriormente rispetto al 2024 (82% di incidenti con gravità critica o alta).



Nel 1° semestre del 2025 l'ambito per cui si rileva un maggior numero di incidenti cyber in Italia è quello Governativo / Militare / Law Enforcement, interessato da una significativa quota di eventi, pari

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

al 38% del totale, che in valore assoluto si traduce in una quantità di incidenti pari al 279% rispetto all'intero anno precedente. La crescita rispetto allo stesso periodo dello scorso anno (I sem. 2024) è pari a oltre il 600%.

Al secondo posto si trova invece l'ambito Transportation / Storage (17% del totale), solo ottavo a livello globale, che realizza in sei mesi oltre una volta e mezzo il numero degli incidenti di tutto l'anno precedente.

In questo contesto di minaccia crescente, il nostro Paese si colloca tra le nazioni che più risultano incapaci di contenere gli attacchi. Nel 2023 l'Italia ha registrato l'11,2% di tutti gli incidenti globali (un aumento netto dal 3,4% del 2021 e dal 7,6% del 2022) confermando il suo status di "maglia nera della cybersecurity" tra le principali economie mondiali. Anche nel 2024 è rimasta vittima del 9,9% degli incidenti a livello mondiale, e il 10,2% nel primo semestre 2025.

In proporzione al dato globale la percentuale di incidenti realizzati contro l'Italia risulta anomala, sia rispetto alla dimensione della popolazione che a quella del PIL nazionale, il che rappresenta uno svantaggio competitivo per il Paese.

I dati del 2025 mostrano come l'Italia (rispetto alla media globale) sia stata molto più colpita da incidenti di tipo DDoS realizzati da gruppi di sedicenti attivisti, per esempio NoName057(16), che in realtà sono sabotatori coordinati da strutture governative russe. Pur trattandosi di incidenti con impatti di livello tipicamente medio-basso, la loro frequenza rende necessarie azioni di mitigazione specifiche.

In generale, la tecnica prevalente a causa degli incidenti in Italia è quella dei DDoS, riprendendosi il primo posto in classifica come già avvenuto nel 2023. Gli incidenti DDoS si attestano al 54%, con un peso significativamente maggiore rispetto a quello occupato a livello globale, dove costituiscono solo il 9% del totale.

In risposta a tale scenario, dal 2023 si sono introdotte numerose novità a livello normativo che porteranno ripercussioni sulle organizzazioni e sull'ecosistema digitale. Gli enti regolatori hanno rafforzato il quadro giuridico su più fronti, ampliando il perimetro delle organizzazioni coinvolte, con l'obiettivo di tutelare i settori strategici, definire linee guida per lo sviluppo di nuove tecnologie e inasprire le conseguenze per i cybercriminali.

Le misure europee e nazionali a favore della cyber-security rappresentano un tassello della più complessa vision di un unico mercato digitale introdotto dalla Direttiva NIS del 2016 e consolidato dalla Direttiva NIS2 che mira a stabilire una strategia comune di cybersecurity per tutti gli Stati membri, elevando i livelli di sicurezza dei servizi digitali su scala europea. La NIS2 ha modernizzato il quadro giuridico esistente per tenere il passo con una maggiore digitalizzazione e un panorama in evoluzione delle minacce alla cibersicurezza. Con l'estensione dell'ambito di applicazione delle

norme in materia di cibersicurezza a nuovi settori ed organizzazioni, si migliora ulteriormente la resilienza e le capacità di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'UE nel suo complesso.

La NIS2 impone, in particolare, obblighi di cybersicurezza stringenti in capo a un'ampia platea di organizzazioni (Soggetti essenziali e Soggetti importanti) operanti in settori ritenuti critici per il funzionamento della società europea, tra cui tutte le grandi imprese, le piccole e microimprese (solo se operano in settori chiave per la società) e la Pubblica Amministrazione.

Le entità in perimetro NIS2 sono chiamate a **rispettare requisiti che spaziano dalla governance della cybersicurezza**, all'adozione di misure per la **gestione dei rischi** (inclusa la sicurezza della catena di fornitura), fino alla **gestione della continuità operativa e alla segnalazione degli incidenti**.

Il Nuovo regolamento UE sulla cybersicurezza, in vigore dal 7 gennaio 2024, include misure pensate per far raggiungere alle istituzioni un alto livello di conoscenza e consapevolezza in ambito cyber. Ogni Stato definisce un quadro di gestione, governance e controllo del rischio cyber e una maggiore operatività tra i soggetti istituzionali coinvolti.

In Italia, il *DDL Cybersecurity*, convertito nella legge n. 90/2024, risponde all'aumento dei cyber attacchi inasprendo le pene per i cybercriminali ed è finalizzato a innalzare il livello complessivo di sicurezza del Sistema Paese, soprattutto per quanto riguarda la PA.

In tale contesto, caratterizzato dal considerevole incremento della minaccia cyber, è continua l'azione dell'Agenzia per la cybersicurezza nazionale (ACN) per garantire la diffusione di informazioni sui rischi cyber oltre che per fornire assistenza ai soggetti sotto attacco cyber.

Attraverso il CSIRT Italia, organo dell'Agenzia per la cybersicurezza nazionale, viene fornito il supporto alle PA nella prevenzione e risposta agli incidenti informatici come previsto dal DPCM 8 agosto 2019. In particolare, il **CSIRT Italia** è il team per la cyber-difesa nazionale che promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Attraverso il CSIRT Italia, l'Agenzia ha potuto monitorare l'evoluzione delle minacce caratterizzate sempre più da eventi di tipo ransomware e DDoS – ma anche dalla diffusione di malware via e-mail e phishing – e indirizzata a diverse realtà pubbliche oltre che ad aziende attive nei settori più disparati (primi fra tutti telecomunicazioni, trasporti e servizi finanziari).

Nel Piano Triennale per l'Informatica nella PA di AgID, aggiornato al triennio 2024-2026, la sicurezza mantiene un ruolo strategico e trasversale. Il documento definisce **un percorso chiaro volto rafforzare la sicurezza informatica delle PA italiane**, attraverso:

- la distribuzione di Indicator of Compromise – IoC, indicatori di compromissione che si attivano quando ad esempio si verifica un incidente di web security fornendo le prove

(aggregate e caricate sui cd Sistemi Security event and event management – SIEM) dell'avvenuto data breach;

- il monitoraggio proattivo delle minacce cyber per innalzare il livello di sicurezza informatica all'interno del dominio delle Amministrazioni pubbliche.
- il rafforzamento della cyber sicurezza attraverso l'implementazione di strumenti di autovalutazione e il potenziamento delle attività formative;
- innalzamento dei livelli di resilienza, privacy, correttezza ed affidabilità dell'Intelligenza Artificiale per assicurare che sia progettata, sviluppata e impiegata in maniera sicura, anche in coerenza con le linee guida internazionali sulla sicurezza dell'Intelligenza Artificiale.

In questo contesto, **AgID svolge funzione di indirizzo strategico e governance centralizzata** di tutte le iniziative, anche mediante la costituzione di organismi di coordinamento e controllo, finalizzati alla direzione strategica e tecnica delle stesse.

2.2. Contesto normativo, Linee Guida e Standard di riferimento

Si riportano di seguito le principali previsioni normative e linee guida che governano la presente iniziativa:

- Codice Civile.
- Regolamento Generale sulla Protezione dei Dati (GDPR) n. 2016/679.
- D.Lgs. 31 marzo 2023, n. 36 (*"Codice dei contratti pubblici"*) e s.m.i. e relative prassi attuative.
- D.Lgs. 7 marzo 2005, n. 82 (*"Codice dell'Amministrazione Digitale"*) e s.m.i.
- Decreto Direttoriale n. 21007/24 del 27 giugno 2024 dell'ACN che introduce un nuovo quadro normativo per le infrastrutture digitali e i servizi cloud destinati alla Pubblica Amministrazione.
- DPCM 30 aprile 2025 recante *"Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale"*.
- AI Act – Regolamento UE 2024/1689.
- Legge 23 settembre 2025 n. 132 *"Disposizioni e deleghe al Governo in materia di intelligenza artificiale"*.
- Legge 28 giugno 2024, n. 90 recante *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"*.
- Legge 4 agosto 2021, n.109 recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"* che converte il decreto legge 14 giugno 2021, n. 82.

- Circolare ACN del 21 aprile 2022, n. 4336 recante *“Attuazione dell'articolo 29, comma 3, del decreto-legge 21 marzo 2022, n. 21. Diversificazione di prodotti e servizi tecnologici di sicurezza informatica”*.
- 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 relativi DPCM.
- D.L. n. 77/2021 recante *“Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure”*.
- D.L. n. 82/2021 recante *“Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale”*.
- DPCM n. 81/2021 recante *“Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza”*.
- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 recante *“Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale».*” G.U. 21 giugno 2008, n. 144.
- Regolamento UE 2016/679 (*“Regolamento generale sulla protezione dei dati”*) e s.m.i. e relativa normativa nazionale applicabile.
- Regolamento (UE) 2025/37 del Parlamento Europeo e del Consiglio del 19 dicembre 2024 che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti.
- Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828.
- Decreto Legislativo 18 maggio 2018, n. 65 - Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
- Direttiva sulle misure per un livello comune elevato di cybersicurezza in tutta l'Unione (direttiva NIS2) e suo decreto di recepimento.

- Decreto Legislativo 4 settembre 2024, n. 138, di “recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione”.
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 - Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - CSIRT italiano.
- Piano Nazionale per la Protezione Cibernetica 2017.
- Programma di abilitazione al Cloud (Cloud Enablement Program di cui al seguente link: <https://cloud.italia.it/>).
- Linee guida ACN per l'applicazione dei criteri di premialità di cui all'articolo 14 della legge n. 90/2024.
- Linee guida ACN adottate con Decreto direttoriale n. 12053 del 03 febbraio 2025 per l'attuazione nazionale del primo sistema europeo di certificazione della cibersicurezza EUCC (European Common Criteria).
- Linee Guida ACN per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90.
- Linee Guida ACN funzioni crittografiche – Funzioni di Hash.
- Linee Guida ACN funzioni crittografiche – Codici di Autenticazione di Messaggi (MAC).
- Linee Guida ACN funzioni crittografiche – Conservazione delle Password.
- Linee Guida ACN “Tassonomia Cyber dell'Agenzia per la Cibersicurezza Nazionale”.
- Linee guida AgID “Linee guida – La sicurezza nel procurement ICT”.
- Linee guida AgID per lo sviluppo del software sicuro.
- Linee Guida AgID per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali.
- Circolare AgID “Misure minime di sicurezza ICT per le Pubbliche Amministrazioni”.
- Standard ISO 27001.
- Standard ISO 27002.
- Standard ISO IEC 62443.
- NIST Cybersecurity Framework (CFS) 2.0 del 26/02/2024.
- Eventuali successive modificazioni delle norme e standard di riferimento.
- Ogni altra disposizione normativa e regolamentare applicabile.

Relativamente alle normative, linee guida tecnologiche e agli standard, il precedente elenco cita i principali documenti di riferimento in vigore alla data di pubblicazione della presente procedura. Le normative, linee guida e gli standard devono essere allineati alle ultime versioni disponibili.

Si applicano inoltre tutte le previsioni del Piano Triennale per l'informatica nella PA e le norme italiane ed Europee da questo richiamate.

3. DURATA

L'Accordo Quadro ha una durata di 24 mesi a decorrere dalla data di attivazione, ovvero la minore durata determinata dall'esaurimento dell'importo massimo stabilito nell'Accordo Quadro, eventualmente incrementato.

Per durata dell'Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno inviare gli Ordini di Fornitura agli operatori economici parti dell'Accordo Quadro.

Nel caso in cui il valore dell'AQ non sia stato ancora esaurito, la durata potrà essere prorogata fino ad ulteriori 6 (sei) mesi; ciò avverrà previa comunicazione scritta della Consip S.p.A. da inviarsi al Fornitore a mezzo PEC, con almeno 15 giorni di anticipo rispetto alla scadenza del termine.

Ciascun Contratto Esecutivo (stipulato all'esito della procedura individuata al paragrafo 6.3.3) dispiegherà i suoi effetti dal termine della fase di Presa in carico e startup di cui al Capitolato Tecnico Speciale Lotti 1 e 2 e al Capitolato Tecnico Speciale Lotti 3 e 4 e avrà una durata massima di 48 mesi.

4. LUOGO DI ESECUZIONE DEI SERVIZI

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

- i Managed Security Services, di cui ai Lotti 1 e 2, saranno erogati da remoto in modalità continuativa attraverso i Centri Servizi del Fornitore, ad eccezione del servizio di supporto specialistico che potrà essere erogato anche in modalità on-site presso le sedi indicate dall'Amministrazione;
- i Servizi di Governance, Analisi del Rischio e Controllo di cui ai Lotti 3 e 4, saranno erogati principalmente presso le sedi indicate dall'Amministrazione (che potranno anche essere dislocate presso una diversa Amministrazione, per esempio nel caso di Amministrazione che opera a favore di altra Amministrazione) e/o, ove specificato dall'Amministrazione stessa, presso la Sede del Fornitore.

Le caratteristiche ed i requisiti dei Centri Servizi sono descritti nel Capitolato Tecnico Speciale relativo ai Lotti 1 e 2.

Per l'erogazione dei servizi in modalità "on-site", nel Piano dei Fabbisogni (di cui al successivo paragrafo 6.3.1) l'Amministrazione, ove richiesto, specificherà le sedi effettive di erogazione. In tal caso sono a carico del Fornitore tutti gli oneri e rischi relativi ad eventuali spese di trasporto, di viaggio, di trasferta e di missione per il personale addetto all'esecuzione delle prestazioni, nonché i connessi oneri assicurativi.

Resta inteso che tutte le risorse professionali potranno essere chiamate a prestare servizio presso le sedi indicate dall'Amministrazione e, pertanto, il Fornitore dovrà tenerne conto nella formulazione della propria offerta tecnica ed economica.

Il Fornitore dovrà disporre di strumenti di collaborazione anche da remoto con l'Amministrazione e per la condivisione della attività al fine di garantire, per tutti i servizi e le attività, la partecipazione effettiva e trasparente in modo semplice ed immediato e senza costi aggiuntivi per l'Amministrazione. Tutti gli strumenti devono essere previsti nel Piano di Qualità generale di Lotto e attivati nel periodo di "Presa in carico e startup".

Il Fornitore dovrà garantire inoltre presso l'Amministrazione:

- per i Lotti 1 e 2 la presenza delle risorse professionali previste per l'erogazione del servizio di supporto specialistico, nonché le figure di coordinamento, sia per riunioni operative e/o di coordinamento, senza oneri aggiuntivi per l'Amministrazione rispetto a quanto previsto dal Contratto Esecutivo.
- per i Lotti 3 e 4 la presenza delle risorse professionali necessarie per l'erogazione dei servizi oggetto di fornitura, nonché le figure di coordinamento, sia per riunioni operative e/o di coordinamento, senza oneri aggiuntivi per l'Amministrazione rispetto a quanto previsto dal Contratto Esecutivo

L'Amministrazione stessa potrà eventualmente prevedere, con riferimento ai servizi in modalità "on-site", la disponibilità di posti di lavoro e postazioni presso la propria sede (tendenzialmente solo per Enti di dimensioni rilevanti dotati di una propria organizzazione ICT), specificandone le modalità di fruizione nel Piano dei Fabbisogni. In nessun caso, gli aggiudicatari potranno richiedere costi aggiuntivi relativi alla disponibilità di strumenti, attrezzature, corredo hardware e software.

5. RAZIONALI PER L'UTILIZZO DELL'ACCORDO QUADRO

Si rappresentano di seguito i razionali per l'individuazione delle Amministrazioni che possono aderire a ciascun lotto.

LOTTE 1 E 3 - PUBBLICHE AMMINISTRAZIONI CENTRALI (PAC):

I Lotti 1 e 3 sono rivolti a:

- tutti i soggetti presenti nell'“Elenco delle amministrazioni pubbliche inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm. (Legge di contabilità e di finanza pubblica)”, nei seguenti “raggruppamenti istituzionali”:
 - Amministrazioni Centrali;
 - Enti nazionali di previdenza e assistenza;
- gli Organismi di diritto pubblico, la cui influenza dominante sia esercitata da parte dei soggetti di cui ai punti precedenti;
- le Società partecipate - anche indirettamente, in via maggioritaria (in senso assoluto) dai soggetti di cui ai punti precedenti - qualificabili come stazioni appaltanti;
- ogni altra stazione appaltante e gli altri soggetti, che non abbiano rilevanza territoriale o locale, che ai sensi della normativa vigente sono legittimati ad aderire al presente Accordo Quadro;

I soggetti individuati nel precedente elenco potranno procedere ad acquisizioni per conto di altri soggetti nell'ambito della presente iniziativa solo nel caso in cui i soggetti per conto di cui procedono siano ricompresi nel detto elenco.

LOTTE 2 E 4 - PUBBLICHE AMMINISTRAZIONI LOCALI (PAL):

I Lotti 2 e 4 sono rivolti a:

- tutti i soggetti presenti nell'“Elenco delle amministrazioni pubbliche” inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm. (Legge di contabilità e di finanza pubblica)”, del seguente “raggruppamento istituzionale”:
 - Amministrazioni locali
- gli Organismi di diritto pubblico, la cui influenza dominante sia esercitata da parte dei soggetti di cui ai punti precedenti;
- le Società, partecipate, anche indirettamente, in via maggioritaria (in senso assoluto) dai soggetti di cui ai punti precedenti, qualificabili come stazioni appaltanti;
- ogni altra stazione appaltante, nonché gli altri soggetti di rilevanza regionale o locale, che ai sensi della normativa vigente sono legittimati ad aderire al presente Accordo Quadro.

I soggetti individuati potranno procedere ad acquisizioni per conto di altri soggetti nell'ambito della presente iniziativa solo se i soggetti per conto di cui procedono siano essi stessi ricompresi nel detto elenco.

6. MODELLO DI FUNZIONAMENTO

6.1. Interazione tra i Lotti di servizi Managed Security Services e servizi di Governance, Analisi del Rischio e Controllo

Lo scenario della presente iniziativa è caratterizzato dalla presenza di Lotti dedicati ai servizi Managed Security Services (lotti 1 e 2) e Lotti dedicati ai servizi di Governance, Analisi del Rischio e Controllo (lotti 3 e 4).

L'azione di controllo imparziale sulla esecuzione dei servizi dei Lotti 1 e 2 rende necessario differenziare il ruolo che assumono i fornitori di ciascuno dei due gruppi di Lotti.

In continuità con la precedente edizione, tale ruolo si innesta in considerazione dei diversi obiettivi a cui i diversi Lotti rispondono. In particolare:

- i Lotti di servizi Managed Security Services hanno l'obiettivo di mettere a disposizione delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati;
- i Lotti di servizi di Governance, Analisi del Rischio e Controllo hanno l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di salute della sicurezza del sistema informativo dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza relativi ai Lotti 1 e 2, sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

6.2. Adesione ai Lotti dell'Accordo Quadro

Per ciascun lotto, l'affidamento dei servizi oggetto dell'Accordo Quadro avviene all'esito dello svolgimento di due fasi procedurali:

- **la prima fase (I)**, che si conclude con l'aggiudicazione dell'Accordo Quadro e la sua stipula, a cura della Consip S.p.A.;
- **la seconda fase (II)**, che si caratterizza per l'affidamento dei singoli Contratti Esecutivi, a cura della singola Amministrazione contraente, come di seguito riportato.

Segnatamente, ciascun lotto ha ad oggetto l'affidamento di un Accordo Quadro con un solo operatore economico, ai sensi dell'art. 59, comma 3, del D.Lgs. 36/2023.

Successivamente alla stipula dell'Accordo Quadro, e per tutta la durata dello stesso, le Amministrazioni legittimate potranno affidare i Contratti Esecutivi in favore dell'unico operatore affidatario dell'Accordo Quadro entro i limiti e le condizioni fissate nell'Accordo Quadro stesso e comunque nel rispetto, ove applicabile, di quanto previsto dall'art. 1 comma 6, del D.L. n. 105/2019 (convertito in L. n. 133/2019), come meglio descritto nei successivi paragrafi.

6.3. Modalità di affidamento dei contratti esecutivi

L'affidamento di ciascun Contratto Esecutivo, nell'ambito di ciascun Lotto, avverrà con le modalità di seguito descritte ed operativamente con l'emissione di Ordini esperiti tramite la Piattaforma telematica Acquisti in Rete (<http://www.acquistinretepa.it>). La guida operativa per le Amministrazioni e il kit documentale a supporto, personalizzabile e comunque non vincolante, saranno messi a disposizione delle Amministrazioni successivamente all'attivazione. Le Amministrazioni potranno accedere a tale documentazione previa autenticazione sulla Piattaforma stessa.

In sintesi, l'Amministrazione dovrà eseguire i seguenti passi:

- a. Registrazione e abilitazione alla Piattaforma Acquisti in Rete;
- b. Accesso alla vetrina delle iniziative di acquisto tramite la sezione dedicata;
- c. Emissione della RPF, contenente il Piano dei Fabbisogni, nel rispetto di quanto indicato al successivo paragrafo 6.3.1;
- d. Emissione dell'Ordine di Fornitura. L'Ordine di Fornitura dovrà contenere, in allegato, il Piano dei Fabbisogni, il Piano operativo, l'eventuale schema di Contratto sottoscritto dall'Amministrazione e l'eventuale atto di nomina del Responsabile del trattamento dei dati (il Piano Operativo si considererà accettato con l'invio dell'Ordine di Fornitura).

Le comunicazioni e gli invii di documenti verso le Amministrazioni da parte dei Fornitori, descritti nei successivi paragrafi, avverranno a mezzo Area Comunicazioni del Sistema o, solo in caso di indisponibilità del Sistema medesimo, a mezzo PEC (resta fermo che, in ipotesi di malfunzionamento/indisponibilità che non consenta l'invio tempestivo della documentazione di cui ai successivi paragrafi tramite Sistema, è comunque obbligo dei Fornitori trasmettere tale documentazione a mezzo Sistema non appena tornato disponibile).

Per i dettagli si vedano i paragrafi seguenti.

6.3.1. RPF (Richiesta Preliminare di Fornitura)

L'Amministrazione trasmetterà, a mezzo Sistema, al Fornitore del lotto di riferimento, la RPF, alla quale dovrà essere necessariamente allegato il **Piano dei Fabbisogni**.

Il **Piano dei Fabbisogni** dovrà contenere: i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo (anche tenendo conto degli obblighi derivanti dalla normativa in materia di trattamento dei dati) e la descrizione delle attività dimensionate, al fine di permettere la identificazione e contestualizzazione dei servizi nonché la eventuale declinazione delle figure professionali e degli strumenti a supporto.

Fermo quanto sopra, si applicherà quanto segue:

1. l'erosione del massimale del singolo lotto verrà calcolata sulle Richieste Preliminari di Fornitura («Erosione Potenziale»). Pertanto, l'invio delle RPF determinerà la priorità di adesione da parte delle Amministrazioni;
2. qualora l'Erosione Potenziale terminasse prima della scadenza contrattuale di 24 mesi e il fornitore avesse residui non erosi perché alcune PA dopo la RPF non sono riuscite a perfezionare il contratto e quindi hanno liberato massimale (perdendo l'ordine di priorità), tali residui potranno essere recuperati entro e non oltre la scadenza dell'Accordo Quadro, eventualmente prorogata. I contratti esecutivi saranno stipulati rispettando l'ordine di graduatoria.

Fermo restando quanto indicato nel Capitolato Tecnico Speciale, il Piano dei fabbisogni conterrà, a titolo esemplificativo e non esaustivo, i seguenti elementi:

- se il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC;
- il comparto di appartenenza coerente con il lotto di riferimento (PAC/PAL);
- l'importo contrattuale e le quantità previste per i servizi oggetto di fornitura;
- solo in caso servizi cloud/infrastrutture digitali e per servizi cloud: la classificazione del dato trattato e il livello di qualificazione/adeguamento richiesto (l'Amministrazione potrà richiedere al Fornitore un livello di qualificazione/adeguamento superiore a quello dichiarato e comprovato ai fini della stipula dell'AQ. Si veda quanto previsto al par. 12 e relativi sottoparagrafi);
- l'indicazione dei requisiti di sicurezza, in attuazione della disciplina di cui al D.Lgs. 138/2024, relativi agli ambiti di interesse in ragione del proprio ruolo (soggetto NIS essenziale o importante), entro i limiti previsti dalle fonti di rango comunitario e nazionale e dai provvedimenti dell'ACN (tra i quali la Determina n. 379907/2025 s.m.i. e rispettivi allegati) ed eventuali indicazioni dell'Autorità di settore NIS, proporzionati all'oggetto del contratto, che il Fornitore è tenuto a rispettare;
- la data di attivazione di ciascun servizio oggetto di fornitura;
- la durata del Contratto esecutivo e dei singoli servizi;
- le sedi di erogazione dei servizi;
- l'orario di servizio dell'Amministrazione;
- le modalità di erogazione e consuntivazione dei servizi, nel rispetto delle previsioni dell'Accordo Quadro;
- la richiesta per i servizi che prevedono l'impiego di tecnologie avanzate di intelligenza artificiale che gli stessi siano erogati, in tutto o in parte, in modalità ibrida ovvero integralmente on-premise;
- per ciascun servizio richiesto, la metrica di misurazione, dimensionamento, la modalità di erogazione (da remoto oppure presso la PA), le caratteristiche specifiche del servizio

tra quelle previste. Si precisa che il dimensionamento è dedicato e specifico per ciascun servizio erogabile durante la durata del contratto esecutivo;

- per i servizi a consumo e a corpo eventualmente richiesti, i profili delle risorse professionali che verranno impiegate, con le relative competenze e certificazioni richieste, nel rispetto di quanto previsto nell'apposita appendice Profili professionali relativa al lotto di riferimento e comunque di quanto eventualmente offerto in termini migliorativi dal Fornitore nell'Offerta Tecnica di prima fase;
- ogni altra indicazione riportata nel Capitolato Tecnico Speciale inerente agli specifici servizi richiesti;
- eventuali precisazioni in merito alle modalità di fatturazione e pagamento;
- eventuali precisazioni, nel rispetto della disciplina contenuta nell'Accordo Quadro e relativi allegati, in merito alle modalità di svolgimento delle verifiche di conformità, anche ai fini di quanto previsto al paragrafo 9.2;
- per i Lotti 1 e 2, l'indicazione del/i referente/i tecnico/i;
- l'indicazione dell'eventuale intenzione di nominare l'aggiudicatario quale Responsabile del Trattamento dei Dati Personali.

Qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio fabbisogno sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lett. b), della legge n. 133/2019, l'Amministrazione stessa darà comunicazione dell'intenzione di procedere all'affidamento al Centro di Valutazione e certificazione nazionale (CVCN) istituito presso il Ministero dello Sviluppo Economico o ai Centri di Valutazione (CV) istituiti presso il Ministero dell'Interno e il Ministero della Difesa. Poiché tali organismi potranno riscontrare la comunicazione dell'Amministrazione prevedendo la necessità di effettuare verifiche preliminari e/o imporre 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 al comma 2 lett. b) legge 133/2019, l'Amministrazione prevederà nel Contratto Esecutivo clausole che condizionino, sospensivamente ovvero risolutivamente, il contratto medesimo al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN o dai CV.

Si precisa che, ove richiesto dall'Amministrazione, il Fornitore dovrà impegnarsi obbligatoriamente a supportare la stessa nella redazione del Piano dei fabbisogni e a mantenere quest'ultimo allineato in caso di eventuali modifiche e/o evoluzioni.

Nel caso di RPF inviate da un Soggetto Aggregatore, il Piano dei Fabbisogni inoltre:

- dovrà contenere l'indicazione di tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'affidamento;

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

- dovrà indicare gli importi e i quantitativi relativi ad ogni singola Amministrazione;
- potrà indicare le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni.

Alla RPF **potranno** inoltre essere eventualmente allegati:

- il testo dell'eventuale **ulteriore documento di contratto**, che potrà essere redatto sulla base dello schema di contratto messo a disposizione da Consip S.p.A. nell'ambito dell'apposito KIT e potrà contenere ogni eventuale ulteriore contestualizzazione delle previsioni dell'Accordo Quadro e/o elemento operativo rilevante per l'esecuzione del Contratto Esecutivo;

l'**atto di nomina del Responsabile del trattamento dei dati** (quest'ultimo nel rispetto dell'apposito allegato contrattuale), in bozza, personalizzato secondo le specifiche esigenze dell'Amministrazione esplicitate nel Piano dei Fabbisogni.

Si precisa che dalla trasmissione del Piano dei fabbisogni da parte dell'Amministrazione non scaturisce alcun obbligo per l'Amministrazione di procedere alla stipula del Contratto esecutivo con il Fornitore aggiudicatario.

Resta inteso in ogni caso che, ai sensi dell'art. 5 del D.Lgs. 36/2023, le Amministrazioni sono tenute a rispettare i principi di buona fede e di tutela dell'affidamento, in quanto, anche prima del perfezionamento del Contratto Esecutivo, sussiste un affidamento dell'operatore economico sul legittimo esercizio del potere e sulla conformità del comportamento amministrativo al principio di buona fede.

6.3.2. Piano Operativo

L'aggiudicatario selezionato, sulla base del Piano dei fabbisogni, predispone un "**Piano Operativo**". Entro un termine massimo di 15 giorni lavorativi dall'invio del Piano dei fabbisogni o dal maggiore termine eventualmente indicato dall'Amministrazione (comunque non superiore a 30 giorni solari), tale Piano Operativo dovrà essere trasmesso all'Amministrazione che ne abbia fatto richiesta, pena l'applicazione, da parte di Consip S.p.A., delle penali previste nell'Accordo Quadro.

Entro 2 giorni lavorativi dalla trasmissione del Piano Operativo, il Fornitore dovrà altresì procedere, ai fini del monitoraggio dell'andamento dell'Accordo Quadro, all'accettazione a Sistema del Piano dei fabbisogni, pena l'applicazione da parte di Consip S.p.A., su segnalazione della PA, delle penali di cui all'Accordo Quadro.

Inoltre, ferma l'applicazione delle suddette penali, la mancata accettazione a Sistema del Piano dei fabbisogni non avrà effetti sull'invio del Piano Operativo, che il Fornitore abbia già operato a mezzo Sistema/PEC, e non sarà ostativo rispetto alla successiva eventuale approvazione di quest'ultimo da parte dell'Amministrazione.

In particolare, fermo quanto previsto nel Capitolato Tecnico Speciale, il Piano Operativo dovrà analizzare/definire, a titolo esemplificativo e non esaustivo, i seguenti aspetti in coerenza al Piano dei Fabbisogni:

- l'importo contrattuale e le quantità previste per i servizi oggetto di fornitura (con indicazione del calcolo del contributo di cui all'art. 31 dell'Accordo Quadro che l'Amministrazione dovrà versare a Consip);
- l'identificativo del servizio;
- la data di attivazione del servizio;
- l'indicazione del/i luogo/ghi di esecuzione del servizio;
- la durata del Contratto esecutivo e dei servizi;
- l'esito della valutazione tecnica e l'eventuale accettazione ad erogare i servizi che prevedono l'impiego di tecnologie avanzate di intelligenza artificiale in tutto o in parte in modalità ibrida, ovvero integralmente on-premise.
- la configurazione (ove applicabile);
- i singoli costi dei servizi;
- impegno delle eventuali risorse professionali previste;
- specifiche di collaudo, contenenti le modalità di esecuzione dei test di collaudo, descritti tramite schede tecniche di dettaglio e le date di prevista disponibilità al collaudo;
- il nominativo e il relativo CV del RUAC del Contratto Esecutivo.
- la proposta operativa coerente rispetto al contesto tecnologico e applicativo indicato nel Piano dei Fabbisogni.

Compatibilmente con i tempi di elaborazione del Piano Operativo, con specifico riferimento ai servizi da svolgere presso la/le sede/i dell'Amministrazione, il Fornitore ha facoltà di condurre, con proprio personale tecnico o altro personale da lui stesso incaricato, e congiuntamente con i referenti dell'Amministrazione interessata, sopralluoghi sui siti, allo scopo di verificare gli impatti e le modalità dell'attivazione dei servizi nella sede in esame (secondo quanto richiesto dall'Amministrazione nel Piano dei Fabbisogni).

L'aggiudicatario deve approntare il calendario dei sopralluoghi necessari e deve indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato che effettuerà il sopralluogo, con gli estremi di un documento di riconoscimento e l'elenco delle verifiche da effettuare. Il calendario viene sottoposto all'approvazione dell'Amministrazione interessata.

Si precisa che dalla mera trasmissione del Piano Operativo da parte del Fornitore aggiudicatario verso l'Amministrazione non scaturisce obbligo per l'Amministrazione di procedere alla stipula del Contratto esecutivo con il medesimo Fornitore.

Resta fermo in ogni caso quanto previsto al precedente paragrafo 6.3.1. in relazione al principio di buona fede.

Le Amministrazioni saranno tenute a comunicare in forma scritta alla Consip S.p.A. tutte le ipotesi di mancato rispetto da parte del Fornitore selezionato del termine per la trasmissione del Piano Operativo.

Il Fornitore non potrà accettare, ossia dovrà rifiutare, la RPF (e quindi non dovrà predisporre il Piano Operativo) qualora la stessa:

- provenga da un soggetto non legittimato, in base alla normativa vigente e al precedente capitolo 5, a utilizzare il presente Accordo Quadro;
- riguardi ambiti merceologici e/o prestazioni diversi o non corrispondenti a quelli oggetto dell'Accordo Quadro.

Qualora ricorra una delle suddette casistiche, il Fornitore dovrà tempestivamente e comunque **entro quattro giorni lavorativi** dal ricevimento della RPF, pena l'applicazione da parte di Consip S.p.A. su segnalazione dell'Amministrazione di apposita penale, informare l'Amministrazione, spiegando le suddette ragioni del rifiuto. Si veda altresì quanto previsto all'art. 7, comma 19, dell'Accordo Quadro.

Qualora Consip S.p.A. venga a conoscenza del fatto che un'Amministrazione sia giunta sino al perfezionamento di un Contratto Esecutivo pur in presenza di uno dei casi di rifiuto della relativa RPF di cui al presente paragrafo, Consip S.p.A. avrà la facoltà in qualsiasi momento, previo apposito contraddittorio, di darne comunicazione all'Amministrazione e al Fornitore, rappresentando che il conseguente Contratto Esecutivo stipulato sarà considerato espunto dal perimetro del presente Accordo Quadro. A tal fine Consip S.p.A. si adopererà per addivenire alla decadenza dell'Ordine e di conseguenza della rispettiva RPF, sul Sistema, anche imponendo al Fornitore di chiedere all'Amministrazione tale decadenza entro e non oltre 2 giorni lavorativi dalla richiesta, pena l'applicazione di apposita penale.

Resta inteso che in tale ipotesi, Consip S.p.A. si riserva altresì la facoltà di risolvere l'Accordo Quadro nei confronti di tale Fornitore.

Se nel Piano dei Fabbisogni l'Amministrazione ha richiesto un livello di qualificazione dei servizi cloud e/o un livello di adeguamento delle rispettive infrastrutture digitali superiore rispetto a quello comprovato all'atto della stipula dell'Accordo Quadro, in conformità a quanto meglio disciplinato nel seguito (nell'apposito paragrafo), il Fornitore potrà alternativamente:

- legittimamente rifiutare il Piano dei Fabbisogni pervenuto;
- dichiarare di potersi dare seguito in quanto già in possesso del livello richiesto;
- rendersi disponibile a conseguire il livello richiesto mediante l'iter di "promozione" disciplinato nel Regolamento ACN.

6.3.3. Contratto esecutivo

L'Amministrazione, **entro 30 giorni solari** dalla ricezione del Piano Operativo, ha la facoltà:

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

- i) di approvare il Piano Operativo tramite il Sistema (mediante l'invio dell'Ordine di Fornitura");
- ii) di comunicare la richiesta di eventuali modifiche e/o integrazioni, nel rispetto del Piano dei fabbisogni. In tal caso il Fornitore dovrà apportare al documento presentato le modifiche e/o integrazioni richieste dall'Amministrazione. Il Fornitore dovrà inviare la versione definitiva del Piano Operativo **entro 10 giorni** solari dalla comunicazione di richiesta dell'Amministrazione, pena l'applicazione, da parte di Consip S.p.A., delle penali previste nell'Accordo Quadro. Dalla data di trasmissione del Piano Operativo aggiornato decorrerà nuovamente il termine di **30 giorni solari** entro i quali l'Amministrazione ha la facoltà di approvare il Piano Operativo medesimo.
- iii) di chiedere massimo ulteriori **15 giorni solari** per la verifica del Piano Operativo.

Contestualmente all'approvazione del Piano Operativo, mediante l'Ordine di Fornitura sul Sistema, l'Amministrazione invierà al Fornitore, sempre tramite il Sistema, i seguenti documenti, sottoscritti digitalmente dall'Amministrazione:

- il Piano dei Fabbisogni;
- il Piano Operativo firmato (che si intenderà così approvato);
- qualora li abbia predisposti e condivisi con il Fornitore ai sensi di quanto previsto al precedente paragrafo 6.3.1, l'apposito documento di contratto, eventualmente redatto sulla base dello schema di contratto messo a disposizione nel kit, e l'eventuale atto di nomina del Responsabile del trattamento dei dati, entrambi firmati;
- ogni ulteriore allegato al Piano dei Fabbisogni e al Piano Operativo approvato.

L'Ordine di Fornitura e i suddetti allegati costituiranno tutti parte integrante e sostanziale del Contratto Esecutivo.

Qualora siano decorsi 30 giorni solari dalla ricezione del Piano Operativo (contestualmente alla quale deve essere accettato da parte del Fornitore il piano dei fabbisogni a sistema), ovvero siano decorsi i termini temporali previsti al punto ii) ovvero non abbia richiesto gli ulteriori (massimo 15) giorni solari per la relativa verifica previsti al punto iii) il relativo Piano dei fabbisogni precedentemente trasmesso dall'Amministrazione, pur accettato dal Fornitore sul Sistema, si intenderà decaduto.

A parziale deroga rispetto a quanto sopra, unicamente nel caso in cui l'Amministrazione abbia richiesto un livello di qualificazione/adeguamento superiore a quello dichiarato e comprovato dal Fornitore ai fini della stipula dell'Accordo Quadro e quest'ultimo abbia dichiarato la propria disponibilità ad avviare l'iter di "promozione" del livello di qualificazione/adeguamento di cui dispone, fermo quanto previsto ai precedenti punti ii) e iii), il termine di 30 giorni solari per l'approvazione del Piano Operativo può essere prorogato per un massimo di ulteriori 60 giorni solari, trascorsi inutilmente i quali, in caso di mancato conseguimento del livello di qualificazione/adeguamento richiesto, il Piano dei Fabbisogni, ancorché eventualmente accettato dal Fornitore a Sistema, si intenderà decaduto.

Resta inteso che il Contratto esecutivo potrà essere stipulato solo previa verifica dell'avvenuto conseguimento del livello di qualificazione/adeguamento richiesto dall'Amministrazione.

Il Fornitore sarà obbligato a rifiutare gli Ordini di Fornitura tardivi rispetto ai termini sopra indicati.

Resta inteso che, qualora Consip S.p.A. venga a conoscenza del fatto che un Fornitore sia giunto sino al perfezionamento di uno o più Contratti Esecutivi (Ordini di Fornitura) pur in presenza di un ordine tardivo, Consip S.p.A. stessa si riserva le medesime facoltà previste al precedente paragrafo 6.3.2 (relativo al caso di perfezionamento di un Contratto Esecutivo pur in presenza di uno dei casi di rifiuto obbligatori della RPF). In tale ipotesi, Consip S.p.A. si riserva altresì la facoltà di risolvere l'Accordo Quadro nei confronti di tale Fornitore.

L'utilizzo dell'Accordo Quadro avviene esclusivamente attraverso il Sistema di e-Procurement della Pubblica Amministrazione. L'accesso e l'utilizzo del Sistema sono disciplinati dalle Regole del Sistema di e-Procurement della Pubblica Amministrazione, che le Amministrazioni e il Fornitore dichiarano di ben conoscere ed accettare integralmente.

Sono legittimate ad utilizzare l'Accordo Quadro, ai sensi della normativa vigente, le Amministrazioni come definite in premessa, sulla base delle indicazioni di cui al capitolo 5 in relazione a ciascun Lotto.

Per potere acquistare attraverso l'Accordo Quadro ed emettere validi Ordini di Fornitura, il Punto Ordinate dell'Amministrazione deve preventivamente abilitarsi al Sistema di e-Procurement. Resta inteso che l'abilitazione del Punto Ordinate non comporta, in capo alla Consip e/o al Ministero, una verifica dei poteri di acquisto attribuiti a ciascuna Unità Ordinate.

Le predette Amministrazioni, previa effettuazione di apposita abilitazione al Sistema di e-Procurement della Pubblica Amministrazione tramite il proprio Punto Ordinate attraverso l'apposita procedura prevista dal Sistema, utilizzano l'Accordo Quadro mediante Ordini di Fornitura. L'Ordine di Fornitura consiste in un documento informatico identificato con un apposito numero e generato automaticamente dal Sistema sulla base dei dati forniti dal Punto Ordinate, con le modalità di seguito descritte.

Affinché l'Ordine di Fornitura possa produrre effetti, esso deve assumere la forma di un documento informatico generato dal Sistema, sottoscritto con firma digitale dal Punto Ordinate e trasmesso al Fornitore attraverso il Sistema, unitamente agli allegati obbligatori indicati nel presente paragrafo (a seconda che sia o meno stata attivata dall'Amministrazione la procedura relativa alla Richiesta Preliminare di Fornitura). Non è consentito l'invio di Ordini di Fornitura con altre modalità. Il Fornitore prende atto e accetta che non dovrà in alcun modo dare seguito ad Ordini di Fornitura che non siano trasmessi nel rispetto delle modalità di cui sopra.

Qualora l'Ordine di Fornitura non sia completo in ogni sua parte necessaria, l'Ordine medesimo non avrà validità ed il Fornitore non dovrà darvi esecuzione; quest'ultimo, tuttavia, dovrà darne

tempestiva comunicazione alla Amministrazione, entro e non oltre **quattro giorni lavorativi** dal ricevimento dell'Ordine stesso. In tal caso, l'Amministrazione potrà emettere un nuovo Ordine di Fornitura, secondo le indicazioni sopra riportate.

Rimane fermo quanto previsto dall'art. 59 comma 5-bis del Codice, ove in sede di emissione degli Ordini di Fornitura non sia possibile preservare l'equilibrio contrattuale né ripristinarlo mediante rinegoziazione secondo oggettiva buona fede.

Per effetto dell'Ordine di Fornitura, il Fornitore sarà obbligato ad eseguire la fornitura richiesta, nell'ambito dell'oggetto contrattuale, restando inteso che in caso di mancata utilizzazione dell'Accordo Quadro da parte dei soggetti sopra indicati nulla potrà essere preteso a qualsiasi titolo dal medesimo Fornitore il quale, infatti, sarà tenuto a svolgere le attività, effettuare le forniture e prestare i servizi solo a seguito della ricezione degli Ordini di Fornitura, compilati ed inviati entro i termini ed in conformità alle condizioni sopra indicate.

I singoli Contratti Esecutivi si perfezionano il **quarto giorno lavorativo** successivo alla ricezione da parte del Fornitore degli Ordini di Fornitura inviati dalle medesime Amministrazioni. Spirato il predetto termine, l'Ordine di Fornitura è irrevocabile per le Parti e, per l'effetto, il Fornitore è tenuto a dare esecuzione completa alla fornitura richiesta entro il termine indicato nell'Ordine di Fornitura. Il Fornitore sarà comunque tenuto a trasmettere all'Amministrazione il Contratto Esecutivo sottoscritto per accettazione entro e non il **quarto giorno lavorativo** dalla ricezione dell'Ordine di Fornitura, pena l'applicazione di apposita penale da parte di Consip su segnalazione dell'Amministrazione.

Qualora il Fornitore non abbia autorizzato Consip alla pubblicazione delle generalità e del codice fiscale del/i delegato/i ad operare sul conto/i corrente/i dedicato/i, il Fornitore medesimo sarà tenuto a comunicare, entro e non oltre **due giorni** dalla conclusione del singolo Contratto Esecutivo i surrichiamati dati alle Amministrazioni ordinanti.

Il Fornitore prende atto, rinunciando ora per allora a qualsiasi pretesa di risarcimento o di indennizzo, che l'Amministrazione ha la facoltà di revocare l'Ordine di Fornitura, avvalendosi esclusivamente del Sistema, da esercitarsi entro un giorno lavorativo dall'emissione dell'Ordine di Fornitura.

Qualora venga richiesto da Consip, il Fornitore, entro **un giorno lavorativo** dalla richiesta, ha l'obbligo di dare riscontro alla medesima Consip, anche per via telematica, di ciascun Ordine di Fornitura divenuto irrevocabile.

Le Amministrazioni provvederanno, al momento dell'emissione del singolo Ordine di Fornitura, tra le altre cose: i) alla nomina del Responsabile Unico del Progetto, ai sensi e per gli effetti dell'art. 15 del Codice; ii) alla nomina del Direttore dell'esecuzione, laddove le relative funzioni non siano svolte dal Responsabile Unico del Progetto, nel rispetto dell'artt. 114 del Codice e del relativo Allegato II.14; iii) ai sensi e per gli effetti dell'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i., degli artt. 6 e 7 del Decreto Legge 12 novembre 2010, n. 187 nonché della Determinazione dell'A.N.A.C.) n. 8 del 18 novembre 2010, alla indicazione sul medesimo Ordine di Fornitura del CIG (Codice Identificativo

Gara) “derivato” rispetto a quello dell’Accordo Quadro e da esse richiesto nonché del CUP (Codice Unico Progetto) ove obbligatorio ai sensi dell’art. 11 della Legge 16 gennaio 2003 n. 3.

Le Amministrazioni Contraenti procedono ad inviare a Consip il certificato di verifica di conformità di cui all’art. 37 dell’Allegato II.14 del Codice, relativamente ai singoli Contratti Esecutivi. Resta salva la facoltà per Consip di svolgere verifiche ispettive e controlli sull’esecuzione delle singole prestazioni.

Nel corso dell’esecuzione del Contratto Esecutivo, l’Amministrazione potrà aggiornare il Piano dei Fabbisogni e richiedere aggiornamenti del Piano Operativo ogni qualvolta lo ritenga necessario, nel rispetto delle previsioni del Codice degli Appalti in merito alle modifiche dei contratti in fase di esecuzione.

Il Fornitore sarà tenuto alla fornitura e all’erogazione dei servizi in conformità ai processi, alle procedure ed alle responsabilità attribuite secondo le direttive dell’Amministrazione, che verranno definite e condivise nella fase di avvio della fornitura, nonché aggiornate durante il corso della fornitura in funzione delle eventuali evoluzioni.

Il Fornitore dovrà produrre, entro 10 giorni lavorativi dalla stipula del Contratto Esecutivo:

- un Piano di Lavoro Generale coerente con il fabbisogno, che rappresenta la totalità dei servizi richiesti e le attività propedeutiche all’attivazione dei servizi, e che potrà essere aggiornato successivamente alla stipula del Contratto esecutivo previo accordo con l’Amministrazione. Tale piano dovrà contenere al proprio interno anche il “Piano di Presa in carico e startup” come indicato nel Capitolato tecnico Speciale;
- un Piano della Qualità specifico di Contratto esecutivo (ad integrazione del Piano della Qualità Generale che dovrà essere trasmesso alla Consip S.p.A. contenente: i) l’organizzazione di ciascuno dei servizi (organigramma e responsabilità assegnate); ii) metodi tecniche e strumenti applicabili per ciascun servizio; iii) requisiti di qualità;
- ove previsto, i CV delle risorse professionali e dei responsabili tecnici che verranno impiegate per l’erogazione dei servizi, con le relative certificazioni richieste e/o proposte in offerta tecnica.

6.4. Responsabilità ed obblighi dei fornitori

La presente iniziativa si colloca nell’ambito delle acquisizioni di beni e servizi strategici previsto da AgID ai fini dell’attuazione del Piano Triennale per l’informatica nella Pubblica Amministrazione. Per quanto detto, ad essa si applicano i meccanismi e le previsioni del PT in termini di governance.

i Fornitori si impegnano fin d’ora:

- a mettere in campo le misure necessarie a supportare, agevolare e garantire il raggiungimento degli obiettivi della governance;
- a sottoscrivere, ove previsti, i regolamenti di pertinenza;

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

- ad agire in linea con gli stessi, rispettando gli obblighi contrattuali assunti negli Accordi Quadro.

In particolare, i Fornitori:

- nell'ambito della esecuzione dei servizi, si obbligano a rispettare i **Principi Guida** di cui al PT;
- nell'ambito della **gestione dei contratti, degli Ordini e delle attività progettuali**, assumono l'obbligo di fornire i dati e le informazioni relativi ai contratti esecutivi stipulati con le Amministrazioni, nelle modalità e nei tempi definiti dai Contratti di Accordo Quadro;
- Nell'ambito della **governance di cui al PT**, si obbligano:
 - a supportare Consip e/o ulteriori soggetti deputati nelle attività di analisi, verifica tecnica, approfondimento e verifica della applicazione dei Principi Guida, rilevazione periodica di misure a supporto della governance, valutazione delle evoluzioni tecnologiche e/o dei trend di digitalizzazione.
 - a partecipare a incontri, indetti da Consip o da ulteriori soggetti, 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;
 - a fornire a Consip e/o ulteriori soggetti report descrittivi di tutte le iniziative progettuali eseguite.

7. REQUISITI ORGANIZZATIVI

7.1. Requisiti di qualità

L'assicurazione della qualità dei servizi è l'insieme delle attività sistematiche e pianificate messe in campo dal Fornitore per dare evidenza all'Amministrazione che i servizi e i prodotti contrattualmente forniti siano conformi ai requisiti.

Pertanto, essa è parte integrante dell'esecuzione di un servizio e non un mezzo finalizzato alla sola consegna e accettazione del servizio medesimo.

Le attività di assicurazione della qualità sono implementate attraverso verifiche, ispezioni e consuntivi, svolte principalmente sui deliverable delle principali attività atte a garantire qualità nella fornitura, quali:

- la pianificazione della qualità (piano della qualità – generale e specifico);
- il controllo della qualità (verifiche, validazioni, riesami, ispezioni e collaudi);
- il controllo e monitoraggio dei livelli di servizio (indicatori di qualità e di servizio).

Il Fornitore dovrà assicurare la qualità della fornitura sia rispettando i criteri di qualità del proprio processo sia applicando il piano della qualità.

Il Fornitore dovrà assicurare la qualità dei servizi erogati, attraverso la presenza al suo interno di specifiche funzioni di verifica, validazione, riesame, assicurazione qualità sui prodotti e sui processi, che si devono basare sui principi prescritti dalle norme della serie ISO 9000.

Il Piano della Qualità Generale e il Piano della Qualità Specifico di Contratto esecutivo costituiranno il riferimento per le attività di verifica e validazione svolte dal Fornitore all'interno dei propri gruppi di lavoro.

Il Piano della Qualità Generale e i Piani della Qualità Specifici di Contratto esecutivo dovranno essere aggiornati a seguito di significativi cambiamenti di contesto in corso d'opera o, comunque, su richiesta della Consip/Amministrazione ogni qualvolta lo reputi/reputino opportuno, nonché in caso di nuovi standard, best-practice e disponibilità di strumenti in grado di migliorare l'assicurazione della qualità. Essi devono essere riconsegnati aggiornati a livello di intero documento, e non per le sole parti variate, e dovrà essere possibile individuare le modifiche effettuate.

Durante l'erogazione, tutti i dati rilevati e tutti quelli oggetto dei report periodici o per evento saranno archiviati a cura del Fornitore che ne dovrà garantire la fruizione alla Consip S.p.A. e all'Amministrazione per tutta la durata contrattuale.

Inoltre, il Fornitore si impegna a consegnare tutti i dati utilizzati per l'elaborazione degli indicatori di qualità secondo apposito formato standard che sarà indicato.

Su richiesta della Consip/Amministrazione, il Fornitore dovrà predisporre dei report sull'andamento della fornitura basandosi sui dati riportati nei rapporti indicatori di qualità della fornitura e di obiettivo anche al fine di effettuare analisi a vari livelli di dettaglio delle informazioni.

Gli indicatori di qualità che devono essere puntualmente rilevati dal fornitore, sono quelli indicati nelle apposite appendici ai Capitolati Tecnici Speciali.

Si precisa che tutte le prescrizioni del Capitolato Tecnico Generale e Speciali e rispettive appendici sono requisiti minimi, ai quali si aggiungono gli impegni assunti in offerta tecnica. Il mancato rispetto costituisce inadempimento.

Il Piano della Qualità Generale:

- contiene il riepilogo di tutti gli elementi migliorativi che caratterizzano l'offerta tecnica formulata dal Fornitore in AQ;
- fornisce lo strumento per collegare i requisiti specifici dei servizi contrattualmente richiesti, con le procedure generali del sistema qualità del fornitore già esistenti;
- esplicita disposizioni organizzative (ivi inclusi i responsabili tecnici) e metodologiche adottate dal fornitore, allo scopo di raggiungere gli obiettivi tecnici e di qualità contrattualmente definiti ivi incluso i livelli di qualità previsti nelle appendici relativi agli indicatori di cui ai Capitolati Tecnici Speciali;
- indica gli strumenti di collaborazione anche da remoto con l'Amministrazione e per la condivisione della attività;

- dettaglia i metodi di lavoro messi in atto dal fornitore, facendo riferimento o a procedure relative al proprio sistema, e perciò descritte nel manuale qualità, o a procedure sviluppate per lo specifico Accordo Quadro, a supporto delle attività in esso descritte, in questo caso da allegare al piano;
- garantisce il corretto e razionale evolversi delle attività contrattualmente previste, nonché la trasparenza e la tracciabilità di tutte le azioni messe in atto dalle parti in causa, il fornitore, la Consip e le Amministrazioni;
- garantisce un'efficace e rapido coordinamento con i Piani della Qualità specifici per i singoli Contratti Esecutivi.

Il Piano della Qualità generale dovrà essere consegnato alla Consip S.p.A., per ciascun lotto, entro e non oltre 30 giorni solari dalla stipula dell'Accordo Quadro, unitamente all'eventuale integrazione dell'Appendice 1 al rispettivo Capitolato Tecnico Speciale relativa agli indicatori di qualità completa di tutti gli indicatori migliorativi, degli strumenti di misurazione migliorativi o versioni di prodotto, proposti in sede di Offerta Tecnica di AQ, pena l'applicazione delle penali contrattualmente previste. Lo stesso dovrà essere approvato dalla Consip S.p.A. e il Fornitore dovrà recepire le eventuali osservazioni entro e non oltre i successivi 10 giorni solari, pena l'applicazione delle penali contrattualmente previste. Le successive versioni o revisioni del Piano della Qualità Generale saranno consegnate in funzione delle variazioni intervenute.

7.2. Risorse impiegate

Ferme restando le competenze professionali richieste nei Capitolati Tecnici Speciali e relative appendici e quelle eventualmente offerte, le risorse impiegate nei servizi oggetto dei lotti dovranno possedere elevate capacità tecniche in ambito sicurezza informatica e professionali (quali prontezza, precisione, affidabilità, competenza e perfetta conoscenza della documentazione contrattuale).

Il Fornitore dovrà garantire un elevato grado di flessibilità nel rendere disponibili le risorse professionali, e l'aggiornamento tecnico delle necessarie competenze.

Le risorse da impiegare/sostituire devono rispondere ai requisiti minimi indicati per i relativi profili professionali o a quelli migliorativi eventualmente indicati in Offerta Tecnica adeguati sulla base dell'evoluzione tecnologica e dell'aggiornamento di standard e linee guida nonché della normativa di riferimento relativa alla presente iniziativa. In caso di sostituzione le nuove risorse professionali devono avere attestati ed esperienze, in tipologia e durata, non inferiori alla risorsa da sostituire.

Si precisa inoltre che le competenze, conoscenze, abilità e certificazioni richiesti/offerti in fase di gara, dovranno essere posseduti per l'intera durata contrattuale. In caso di sostituzione di risorse certificate le nuove risorse dovranno possedere le medesime certificazioni o superiori.

Si rinvia in ogni caso alle previsioni contenute nelle appendici relative agli indicatori di qualità dei Capitolati Tecnici Speciali di ciascun lotto.

8. RUOLI DI COORDINAMENTO RICHIESTI

8.1. Responsabile unico delle attività contrattuali (RUAC)

Per ciascun Accordo Quadro e per ogni singolo Contratto esecutivo, il Fornitore dovrà indicare un Responsabile unico delle attività contrattuali (di seguito per brevità anche RUAC).

Per tutti i Lotti, il profilo professionale per la figura del RUAC, dovrà corrispondere al profilo Security Principal presente nell'appendice 2 al Capitolato tecnico speciale Lotti 3 e 4 specificatamente per le caratteristiche relative al Titolo di studio e alla Esperienza lavorativa.

Il nominativo, il CV e i contatti del RUAC dell'Accordo Quadro dovrà essere trasmesso a Consip S.p.A. tra i documenti della stipula dell'Accordo Quadro medesimo.

Unitamente al Piano operativo, il Fornitore dovrà fornire, all'Amministrazione, il nominativo, il relativo CV e i contatti per il RUAC del Contratto Esecutivo.

Il RUAC dovrà riferire, per quanto di competenza, alla Consip S.p.A. o alle Amministrazioni (in caso di RUAC del Contratto esecutivo) su tutte le tematiche contrattuali, quali ad esempio:

- la correttezza nell'esecuzione dei servizi (ad esempio, la stima, la pianificazione e la consuntivazione delle attività, gli adempimenti legati alla qualità, il controllo dell'avanzamento lavori, la verbalizzazione degli incontri con l'utenza, il controllo del Piano dei Fabbisogni e del Piano Operativo, le attività di valutazione e contenimento dei rischi, ecc.);
- il pieno adempimento degli impegni assunti in offerta tecnica;
- la correttezza e tempestività dell'utilizzo degli strumenti di supporto alle Amministrazioni e degli strumenti in uso presso l'Amministrazione e/o proposti in offerta tecnica;
- le predisposizioni e variazioni dei Piani di lavoro della fornitura;
- la predisposizione dei Piani della Qualità Specifici di Contratto esecutivo e garanzia del rispetto del Piano della Qualità Generale e delle specificità dei servizi richiesti;
- la verifica dei livelli di servizio sulle attività oggetto della fornitura ed individuazione delle eventuali azioni correttive a fronte del mancato rispetto delle soglie previste e/o a fronte di rilievi;
- la verifica dei risultati sugli indicatori di qualità;
- le problematiche relative a eventuale mancata aderenza delle risorse impiegate rispetto ai profili professionali richiesti con particolare riferimento, ad esempio, alle certificazioni richieste o a competenze di tematica;
- le eventuali azioni da intraprendere per migliorare l'erogazione dei servizi e valutarne i risultati ottenuti;

- la pianificazione ed impiego di risorse quantitativamente e qualitativamente adeguate.

Inoltre, dovrà svolgere i seguenti compiti:

- gestire le criticità e i rischi complessivi di progetto resolvendo tutti i potenziali conflitti e/o eventuali disservizi;
- riferire sul coordinamento fra i gruppi ed i referenti tecnici per garantirne il massimo grado di sinergia e omogeneità d'azione, ottimizzando in particolare la distribuzione delle risorse fra i gruppi a fronte di picchi d'attività e/o di esigenze e urgenze specifiche;
- garantire unitarietà, integrazione, omogeneità e sinergia nell'erogazione dei servizi;
- adottare idonei strumenti per facilitare la comunicazione e lo scambio di informazioni tra i vari attori coinvolti nella Fornitura;
- assicurare un alto grado di sinergia tra le risorse impiegate nei servizi core e quelle impiegate negli altri servizi al fine di garantire un costante e adeguato grado di conoscenza e di attenzione evitando discontinuità;
- proporre azioni correttive a fronte di situazioni critiche.
- rendere disponibili alla Consip S.p.A., su richiesta, documenti periodici di sintesi sull'andamento dei contratti e sulle attività di supporto alle Amministrazioni.

Inoltre, il RUAC dell'Accordo Quadro e del Contratto esecutivo dovranno, per quanto di rispettiva competenza:

- garantire, per il lotto di riferimento, il supporto alle Amministrazioni richiedenti;
- presentare, su richiesta della Consip, reportistica sull'andamento delle forniture nonché garantire l'uniformità e standardizzazione delle metodologie e degli strumenti;
- gestire a livello territoriale quanto previsto per la figura del RUAC, interfacciandosi, ove necessario, con i Responsabili tecnici per l'erogazione dei servizi.

Il RUAC dell'AQ dovrà inoltre riferire, per quanto di competenza, all'Organismo di coordinamento e controllo di cui al successivo paragrafo 10.1.

Il RUAC, dovrà avere una qualifica dirigenziale, con poteri di firma tali da impegnare in maniera esecutiva l'impresa/RTI/Consorzio nei confronti, rispettivamente, di Consip o dell'Amministrazione, a seconda che si tratti di RUAC dell'Accordo Quadro o di RUAC del Contratto Esecutivo.

8.2. Responsabili tecnici per l'erogazione dei servizi

I Responsabili Tecnici per l'erogazione dei servizi sono le figure del Fornitore responsabili delle attività di erogazione dei servizi.

I Responsabili tecnici devono essere reperibili telefonicamente nelle fasce orarie di erogazione del servizio e in caso di estensione dell'orario stesso tramite posta elettronica, senza oneri aggiuntivi.

Per ciascun Lotto, il Fornitore dovrà mettere a disposizione un responsabile tecnico per ciascun Contratto esecutivo e comunque per ciascuna Amministrazione per tutti i servizi indicati nel Capitolato Tecnico Speciale.

I suddetti responsabili tecnici dovranno garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori previsti dal Capitolato Tecnico Speciale e relative appendici.

I Responsabili tecnici, in relazione alle varie tipologie di servizi oggetto di fornitura, a titolo esemplificativo, dovranno:

- svolgere il coordinamento delle attività e delle risorse impiegate negli specifici servizi, nel rispetto dei piani di qualità e del piano di lavoro;
- verificare che l'erogazione delle attività di tutte le risorse coinvolte nei servizi, sia conforme ai requisiti minimi di qualità della fornitura;
- partecipare alle riunioni di avanzamento e/o a riunioni indette dalle Amministrazioni.
- interagire con i referenti tecnici, ove presenti, dell'altro lotto e/o di altre gare e/o di altri contratti laddove necessario e richiesto dalle Amministrazioni.

Per tutti i Lotti, il profilo professionale per la figura di responsabile tecnico dovrà corrispondere al Security Principal presente nell'appendice 2 al Capitolato Tecnico Speciale Lotti 3 e 4 specificatamente per le caratteristiche relative al Titolo di studio e alla Esperienza lavorativa.

Il Fornitore è tenuto ad impiegare i responsabili tecnici quali ruoli minimi di coordinamento delle attività contrattuali previste. In caso di inadeguatezza, impreparazione e/o incompetenza, il responsabile 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.

Per tutti i responsabili tecnici richiesti e/o offerti, il Fornitore dovrà indicare un numero di telefono cellulare e un indirizzo di posta elettronica attivo durante l'orario di lavoro richiesto per la fornitura.

I responsabili tecnici devono essere disponibili ad operare presso l'Amministrazione ove necessario e/o richiesto per l'espletamento di tutte le attività contrattuali.

I responsabili tecnici non dovranno comportare alcun onere aggiuntivo per l'Amministrazione e non potranno far parte di alcuno dei gruppi di lavoro relativi ai servizi oggetto della fornitura.

9. COLLAUDO E TEST DEI SERVIZI

Si descrivono di seguito le procedure di collaudo che il Fornitore dovrà obbligatoriamente attuare ai fini della verifica della completa funzionalità dei servizi oggetto di fornitura.

In particolare, la fornitura dei servizi descritti nel presente capitolato tecnico è soggetta alle procedure di collaudo di seguito descritte:

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

- collaudo funzionale (Test Bed): richiesto da Consip, successivamente alla stipula dell'Accordo Quadro nel corso dell'intera durata contrattuale; si tratta di prove mirate a verificare le modalità con le quali il Fornitore erogherà i servizi oggetto della presente gara.
- collaudo di configurazione, svolto dalla singola Amministrazione contraente, volto a verificare la corretta erogazione dei servizi acquisiti.

9.1. Collaudo funzionale

Il Fornitore dovrà mettere a disposizione una piattaforma di Test Bed presso sedi individuate congiuntamente con Consip utilizzate per l'erogazione dei servizi, strutturandola in modo tale da consentire l'esecuzione delle verifiche funzionali per i servizi richiesti. Nell'ambito della predisposizione del Test Bed, il Fornitore dovrà fornire anche il personale necessario all'esecuzione delle prove.

Il test bed dovrà garantire verifiche su:

- i servizi oggetto di erogazione in termini di requisiti minimi e migliorativi offerti e le infrastrutture hardware e software e le modalità organizzative.
- gli strumenti di monitoraggio e controllo della fornitura (incluso il Service Desk per i Lotti 1 e 2) inclusi.

Ai fini dell'esecuzione delle prove di Collaudo, il Fornitore dovrà rendere disponibile entro 30 giorni lavorativi dalla richiesta di Consip un documento intitolato "Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (*test bed*)" contenente almeno:

- la descrizione dell'architettura di test bed;
- il sistema di misura dei livelli di servizio e di generazione della reportistica;
- la modalità di svolgimento delle prove di collaudo.

A partire dal 15esimo giorno successivo alla ricezione della documentazione di cui sopra da parte di Consip, il fornitore dovrà rendersi disponibile all'avvio dei collaudi.

Consip si riserva di chiedere adeguamenti al documento di cui sopra, che il Fornitore dovrà recepire e formalizzare in una nuova versione entro 15 giorni dalla richiesta.

Il buon esito del collaudo sarà comunicato da Consip mediante verbale, sottoscritto anche dal Fornitore.

Qualora dagli accertamenti effettuati in sede di primo collaudo, i servizi non risultassero conformi alle specifiche di dettaglio previste nelle prove di collaudo, il fornitore dovrà eliminare i vizi accertati entro i termini fissati da Consip, e comunque entro 5 (cinque) giorni lavorativi. Decorso detto termine, si potrà procedere ad una seconda prova di collaudo in test bed.

Consip si riserva di effettuare attività di verifica sui servizi secondo le modalità ed i tempi sopra espressi anche nel corso della fornitura, con l'obiettivo di accertare la permanenza dei requisiti richiesti.

Consip si riserva di verificare la rispondenza dei Centri Servizi, ove previsti, ai requisiti minimi, con una particolare attenzione a quanto concerne le policy di sicurezza adottate.

Consip si riserva inoltre la facoltà di svolgere ispezioni sulle sedi messe a disposizione dal Fornitore o degli eventuali sub-fornitori, per l'erogazione dei servizi, con un preavviso minimo di 3 (tre) giorni lavorativi, per verificare il permanere, dei requisiti richiesti nel periodo di vigenza contrattuale.

9.2. Collaudo di configurazione

In seguito alla stipula del Contratto esecutivo, l'Amministrazione contraente potrà richiedere prove di collaudo atte a verificare la conformità di ogni singolo servizio contrattualizzato rispetto a:

- “Piano dei fabbisogni”, redatto dall'Amministrazione contraente;
- “Piano operativo”, redatto dal Fornitore;
- Specifiche e requisiti dei servizi, contenuti nel Capitolato Tecnico Speciale.

Il collaudo è volto ad accertare, periodicamente nel corso della fornitura, che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale e conformi alla documentazione tecnica di gara e all'offerta tecnica presentata. La responsabilità del collaudo è dell'Amministrazione; il Fornitore esegue l'attività di collaudo in contraddittorio con l'Amministrazione.

L'Amministrazione può procedere, a sua discrezione, ad un collaudo a campione.

Il Fornitore dovrà obbligatoriamente:

- fornire il supporto all'Amministrazione contraente in tutte le attività necessarie alle suddette prove di collaudo.
- consegnare (entro i tempi previsti nel Piano Operativo) all'Amministrazione contraente un documento intitolato “Specifiche di dettaglio delle prove di collaudo” che descrive la tipologia delle prove di collaudo previste e la pianificazione temporale delle stesse.
- qualora richiesto dall'Amministrazione, impegnarsi a svolgere ulteriori prove integrative.

10. GOVERNANCE

Nell'ambito di ciascun Lotto sarà costituito, successivamente all'attivazione dell'Accordo Quadro o comunque appena possibile, apposito Organismo di coordinamento e controllo, composto da referenti, rispettivamente, di Consip S.p.A., di AgID e del Fornitore (la composizione e il dettaglio degli aspetti operativi nonché le tempistiche delle attività dell'Organismo di coordinamento e controllo saranno precisati nell'ambito di apposito Regolamento che sarà reso disponibile successivamente all'attivazione dell'Accordo Quadro).

Nell'ambito delle attività dell'Organismo di coordinamento e controllo il **Fornitore assume i seguenti obblighi:**

- i. Partecipare agli incontri periodici dell'Organismo di coordinamento e controllo, rendendo disponibili, le informazioni e i dati di avanzamento delle attività e dei contratti, le penali applicate e le criticità, in funzione dell'Ordine del Giorno stabilito per l'incontro stesso;
- ii. Supportare l'Organismo di coordinamento e controllo nella eventuale **verifica di congruità tecnico/economica e all'analisi di progetti analoghi implementati, nell'ambito degli stessi contratti, da Amministrazioni diverse;**
- iii. Collaborare, su richiesta dell'Organismo di coordinamento e controllo, alle attività di analisi e approfondimento *ad hoc* individuate dall'Organismo stesso;
- iv. Fornire, secondo la periodicità dettagliata nei regolamenti, **report con proposte di standardizzazione di processi e/o sistemi e/o soluzioni ICT** (in funzione del proprio ambito di fornitura), fornendo supporto per l'analisi e gli approfondimenti all'Organismo di coordinamento e controllo;
- v. Fornire all'Organismo di coordinamento e controllo, secondo la periodicità dettagliata nei regolamenti, **report descrittivi di tutte le iniziative progettuali eseguite, motivando i casi in cui i processi/le soluzioni sviluppate si sono differenziate da pregresse analoghe;**
- vi. Predisporre ed inviare all'Organismo di coordinamento e controllo, con le modalità e le tempistiche che saranno riportate nel Regolamento, **un documento che illustri l'evoluzione tecnologica e/o i trend di digitalizzazione sul mercato dei servizi oggetto del proprio contratto con eventuali proposte di evoluzione e/o adeguamento dei servizi stessi;**

Le informazioni relative all'andamento della fornitura dovranno essere rese disponibili dal fornitore tramite cruscotto condiviso con Consip ed Agid e aggiornate su base mensile; l'aggiornamento dovrà avvenire entro il quindicesimo giorno solare successivo al mese di riferimento. Il cruscotto dovrà essere implementato con certificato per la navigazione esclusiva in HTTPS navigazione esclusiva in HTTPS configurato con certificati *non self-signed*. utilizzando un'infrastruttura hardware e software che il Fornitore stesso provvederà a realizzare e mantenere in esercizio.

Il cruscotto dovrà essere accessibile tramite credenziali utente dedicate a Consip e Agid e dovrà essere reso disponibile all'attivazione dei servizi del primo Contratto esecutivo di fornitura sottoscritto per ciascun Lotto.

11.CLAUSOLA EX ART. 120, COMMA 1, LETT. A), DEL D.LGS. 36/2023

Nel corso della vigenza dell'Accordo Quadro sarà possibile, ai sensi dell'art. 120, comma 1, lett. a), del D.Lgs. 36/2023, l'ampliamento degli ambiti di fornitura indicati nel Capitolato Tecnico Speciale di ciascun Lotto.

Il contesto di fornitura del presente Accordo Quadro, infatti, si caratterizza per la particolare dinamicità del contesto cyber, sia in ragione della costante e rapida evoluzione normativa in materia, tanto a livello comunitario che nazionale, che implica l'introduzione di specifici obblighi e requisiti, sia in considerazione della circostanza per cui gli attacchi informatici sono connotati da un livello di pervasività via via crescente. Pertanto, al fine di garantire la costante efficacia delle misure di

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

sicurezza informatica e di assicurare la resilienza dei Sistemi informativi della Pubblica Amministrazione, mediante l'adeguamento continuo delle soluzioni di sicurezza all'evoluzione delle minacce informatiche e ad eventuali interventi normativi in materia, l'Accordo Quadro potrà essere oggetto di ampliamento degli ambiti di fornitura, ai sensi dell'art. 120, comma 1, lett. a), del D. Lgs. 36/2023, nei limiti e alle condizioni di seguito indicate.

Presupposti dell'ampliamento

L'ampliamento potrà essere disposto qualora, nel corso della durata dell'Accordo Quadro, si manifestino esigenze imprevedibili, o comunque non prevedibili in termini certi, derivanti:

- dall'evoluzione del contesto cyber e dall'incremento della pervasività e sofisticazione degli attacchi informatici;
- da sopravvenienze normative e regolamentari, a livello nazionale o eurounitario, che introducano nuovi obblighi, requisiti o standard di sicurezza;
- dalla disponibilità sul mercato di strumenti, funzionalità o servizi di sicurezza più efficaci e performanti, idonei a garantire un livello di protezione adeguato all'evoluzione delle minacce.

Oggetto dell'ampliamento

L'ampliamento potrà riguardare, alternativamente o cumulativamente:

- l'introduzione di nuove funzionalità e/o nuovi servizi analoghi, connessi o complementari rispetto a quelli previsti nel lotto di riferimento;
- la modifica delle modalità di esecuzione delle prestazioni contrattuali e/o l'introduzione di nuove modalità esecutive, purché coerenti con l'oggetto dell'Accordo Quadro e funzionali al miglioramento della sicurezza dei sistemi.

Vincoli all'ampliamento

Ferme le condizioni innanzi indicate, l'ampliamento potrà essere disposto unicamente laddove ricorrano i seguenti presupposti:

- l'ampliamento complessivo (da intendersi come l'insieme di tutti gli ampliamenti) non potrà determinare in nessun caso il superamento del valore massimo del lotto;
- l'ampliamento dovrà necessariamente conseguire alla manifestazione, da parte delle Amministrazioni Contraenti, di esigenze imprevedibili (o comunque non prevedibili in termini certi) di dotarsi di servizi con specifiche/funzionalità di sicurezza più performanti.

Procedura di ampliamento

Ciascuna delle parti componenti l'Organismo di coordinamento e controllo avrà la facoltà di portare all'attenzione dello stesso le esigenze di ampliamento manifestate da una o più Amministrazioni Contraenti.

Sulla base di tali esigenze, se le nuove funzionalità/servizi/modalità di esecuzione idonee a soddisfarle risultano nella disponibilità del Fornitore, l'Organismo di coordinamento e controllo chiederà a quest'ultimo apposito documento di "specifiche tecniche" (contenente i requisiti da garantire), nonché l'eventuale quotazione delle nuove funzionalità/servizi/modalità di esecuzione richieste.

L'Organismo di coordinamento e controllo, quindi, acquisita la suddetta documentazione, svolgerà, anche tramite i propri componenti secondo quanto pattuito nel rispettivo Regolamento, le seguenti valutazioni:

- valutazione di ammissibilità, al fine di verificare la sussistenza dei presupposti espressi nel presente paragrafo; la valutazione si baserà almeno sui seguenti parametri:
 - riconducibilità con l'Accordo Quadro: oggetto del Lotto e categorie di servizi;
 - imprevedibilità della esigenza: evoluzione minacce cyber, aggiornamenti normativi, innovazione tecnologica disponibile;
 - domanda effettiva: numero PA coinvolte, tipologia esigenza (sistemica o specifica).
 - vincoli economici: non superamento del massimale contrattuale del Lotto;
- valutazione di congruità tecnica, la valutazione si baserà almeno sui seguenti parametri:
 - coerenza architetture: compatibilità con i servizi oggetto di fornitura, impatto su infrastrutture della PA;
 - incremento del livello di sicurezza: mitigare nuove minacce, migliore protezione degli asset;
 - conformità: compliance con normative (NIS2, normativa ACN), compliance con standard (ad es. ISO, NIST);
 - maturità della soluzione: disponibile, sperimentale, da sviluppare;
 - scalabilità e riusabilità: riusabilità presso più PA, capacità di standardizzazione.
- valutazione di congruità economica: la valutazione si baserà almeno sui seguenti parametri:
 - coerenza con i prezzi dell'AQ: confronto con servizi analoghi già presenti, prezzi unitari esistenti;
 - benchmark di mercato: confronto con prezzi di mercato o di progetti analoghi;
 - proporzionalità costo/beneficio: rapporto costo atteso/incremento livello di sicurezza;
 - sostenibilità complessiva: impatto sul massimale del Lotto, capacità di utilizzo da parte delle PA.

Una volta svolte le suddette valutazioni, le stesse saranno oggetto di approvazione da parte dell'Organismo di coordinamento e controllo e, in tal caso, diventeranno automaticamente "appendici" alla documentazione relativa al lotto di riferimento pubblicata all'attivazione dell'Accordo Quadro. Conseguentemente, verranno aggiornati altresì i prezzi contenuti nell'Offerta economica. Consip S.p.A. metterà tali appendici e l'Offerta economica aggiornate a disposizione delle

Amministrazioni, le quali, a decorrere dalla messa a disposizione, potranno iniziare ad approvvigionarsi con le nuove prestazioni contrattuali.

Il Fornitore si obbliga irrevocabilmente a erogare i servizi secondo quanto approvato dall'Organismo di coordinamento e controllo, con le modalità e alle condizioni dallo stesso stabilite, e comunque nel rispetto di quanto previsto dall'Accordo Quadro.

Tenuto conto della suddivisione dei lotti per comparto, qualora le esigenze delle Amministrazioni siano portate all'attenzione dell'Organismo di coordinamento e controllo di uno dei due lotti di comparto, Consip S.p.A. e/o AgID avranno la facoltà di segnalare l'esigenza anche all'Organismo di coordinamento e controllo dell'altro lotto di comparto.

In tal caso, prima di dare seguito alla richiesta del documento di "specifiche tecniche" al fornitore, l'Organismo di coordinamento e controllo del secondo lotto svolgerà una valutazione preliminare volta a valutare se l'esigenza manifestata dall'Amministrazione del comparto del primo lotto possa essere di interesse anche per le Amministrazioni del comparto del secondo.

In caso positivo, una volta acquisita la documentazione del Fornitore, si darà seguito anche nel secondo lotto alla procedura di valutazione, ed eventuale approvazione sopra descritta, fermo restando che, ai fini della verifica di sussistenza del presupposto dell'imprevedibilità dell'esigenza, potrà farsi riferimento all'esigenza adottata dall'Amministrazione del primo lotto.

12. PRESCRIZIONI COMUNI RELATIVE A SOLUZIONI CLOUD E INFRASTRUTTURE

Con riferimento alle soluzioni cloud eventualmente offerte e alle infrastrutture digitali e cloud, nonché, per i lotti 1 e 2, ai Centri servizi impiegati per l'erogazione dei servizi, troveranno applicazione le rispettive regole e livelli di servizio previsti dal Decreto Direttoriale n. 21007/24 del 27 giugno 2024 di ACN, Regolamento Unico per le infrastrutture e i servizi cloud per la PA, che armonizza il quadro regolatorio vigente e definisce le misure tecnico-organizzative e le modalità di qualificazione e adeguamento di servizi e infrastrutture (di seguito per brevità anche Regolamento ACN).

In particolare, il Fornitore necessariamente ricorrerà alla qualificazione/adeguamento:

- con riferimento alle soluzioni cloud eventualmente offerte per l'erogazione o comunque a supporto dei servizi e alle rispettive infrastrutture (in coerenza con la definizione di cui alla lettera p) dell'art 1 del Regolamento sia le infrastrutture fornite da un Cloud Service Provider (CSP), sia, nei casi di cui ai lotti 1 e 2, le infrastrutture fornite dal concorrente stesso ubicate nel proprio ambiente di private Cloud del Centro Servizi, laddove queste ultime rientrino, a loro volta, nella definizione di "infrastrutture dei servizi cloud per le PA" di cui alla lettera n) dell'art. 1 del Regolamento succitato. Ne consegue che sia le infrastrutture del CSP sia quelle fornite dal concorrente stesso saranno soggette alla disciplina di adeguamento nel rispetto della catena di adeguamento/qualificazione);
- per i lotti 1 e 2, con riferimento all'infrastruttura relativa al Centro Servizi.

A tal fine, prima della stipula dell'Accordo Quadro, sarà richiesto all'aggiudicatario di ciascun lotto:

- di indicare tutti le eventuali soluzioni cloud offerte per l'erogazione o comunque a supporto dei servizi;
- di dimostrare:
 - con riferimento a tutte le soluzioni cloud, il possesso del livello di qualificazione previsto per il trattamento dei dati ordinari, ossia il livello di qualificazione QC1 per (nonché il livello di adeguamento AI1 per le rispettive infrastrutture);
 - per i lotti 1 e 2, il possesso del livello di adeguamento AI1 per le infrastrutture relative al Centro Servizi.

Si precisa che, nel caso in cui l'Amministrazione, in sede di Piano dei Fabbisogni, evidenzi la necessità di un livello di qualificazione/adeguamento superiore, troveranno applicazione le disposizioni contenute nei seguenti paragrafi, oltre a quelle specifiche sul punto di cui al precedente paragrafo 6.3 e relativi sottoparagrafi.

I Livelli di servizio relativi ai servizi erogati in modalità Cloud per i lotti 1 e 2 sono quelli specificamente previsti nell'appendice 1 al Capitolato Tecnico Speciale Lotti 1 e 2 al paragrafo 3.10.

12.1. Qualificazione/Adeguamento

Il livello di qualificazione/adeguatezza previsto per l'esecuzione delle prestazioni di cui all'Accordo Quadro dovrà essere mantenuto per tutta la durata della medesima e dei Contratti Esecutivi. In caso di avvio del procedimento di revoca della qualificazione/dichiarazione di inadeguatezza da parte dell'ACN o in prossimità della scadenza della validità della qualificazione è onere e responsabilità esclusiva del Fornitore di adoperarsi per tempo al fine di evitare soluzioni di continuità nell'erogazione dei servizi anche, ove possibile, prestando la necessaria collaborazione al CSP/Produttore del servizio Cloud (di seguito per brevità anche solo "Produttore").

- a) Nel caso in cui, nel corso di esecuzione contrattuale, la qualificazione e/o l'adeguatezza dovesse essere prossima alla scadenza e non fosse già intervenuto il relativo rinnovo, è obbligo del Fornitore trasmettere tramite PEC alla Amministrazione e alla Consip S.p.A. entro e non oltre il termine di scadenza originale l'eventuale provvedimento, rilasciato da ACN ai sensi dell'articolo 19, comma 9, del Regolamento ACN, di autorizzazione ad operare in continuità fino alla data di conclusione del procedimento di rinnovo, pena l'applicazione della relativa penale.
- b) Nel caso in cui l'ACN comunichi l'avvio del procedimento di revoca della qualificazione/declaratoria di inadeguatezza ai sensi dell'art. 20 del Regolamento ACN è obbligo del Fornitore darne comunicazione tramite PEC alla Amministrazione e alla Consip entro 5 giorni solari dalla ricezione della notifica o, qualora il Fornitore sia diverso dal CSP/Produttore, entro 5 giorni solari dalla ricezione della comunicazione da parte del CSP/Produttore, pena l'applicazione di apposita penale. Resta salvo il diritto dell'Amministrazione e della Consip di acquisire le predette informazioni anche d'ufficio, con la conseguenza che, laddove emergesse

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

che ACN abbia comunicato o, qualora il Fornitore sia diverso dal CSP/Produttore, il CSP/Produttore, a seguito della comunicazione da parte di ACN, abbia comunicato, l'avvio del procedimento di revoca della qualificazione/declaratoria di inadeguatezza senza che il Fornitore ne abbia dato comunicazione all'Amministrazione e alla Consip nel termine sopra riportato, si applicheranno le sanzioni previste nell'articolo Penali dell'Accordo Quadro.

Gli obblighi di comunicazione di cui sopra sono applicabili a ciascun servizio cloud di cui al precedente paragrafo 6.2.

- c) Nel caso in cui l'ACN comunichi la revoca della qualificazione/declaratoria di inadeguatezza ai sensi dell'art. 21 del Regolamento ACN è obbligo del Fornitore darne comunicazione tramite PEC all'Amministrazione e alla Consip entro 5 giorni solari dalla ricezione della notifica, qualora il Fornitore sia diverso dal CSP/Produttore, entro 5 giorni solari dalla ricezione della comunicazione da parte del CSP/Produttore, pena l'applicazione di apposita penale. Resta salvo il diritto dell'Amministrazione e della Consip di acquisire le predette informazioni anche d'ufficio, con la conseguenza che, laddove emergesse che ACN abbia comunicato o, qualora il Fornitore sia diverso dal CSP/Produttore, il CSP/Produttore, a seguito della comunicazione da parte di ACN, abbia comunicato, la revoca della qualificazione/declaratoria di inadeguatezza senza che il Fornitore ne abbia dato comunicazione all'Amministrazione e alla Consip nel termine sopra riportato, sarà applicata apposita penale. Resta inteso che, in caso di revoca della qualificazione/dichiarazione di inadeguatezza di cui all'art. 21 del Regolamento ACN, si applicherà quanto previsto ai successivi paragrafi 12.2 e 12.3.

Qualora, in corso di esecuzione contrattuale, per esigenze imprevedibili e sopravvenute derivanti da sopraggiunti provvedimenti normativi e/o regolamentari che comportino l'attribuzione di nuove competenze alla singola Amministrazione o la variazione dei livelli di classificazione di una o più tipologie di dati, dovesse verificarsi, in tutto o in parte, una modifica nella classificazione dei dati trattati che renda necessario il possesso di un livello di qualificazione, ovvero di un livello di adeguatezza della rispettiva infrastruttura, superiore a quello richiesto ai fini della stipula dell'Accordo Quadro, la singola Amministrazione Contraente:

- qualora l'esigenza si manifesti prima del perfezionamento del Contratto Esecutivo, dovrà darne atto nel Piano dei Fabbisogni, come previsto al precedente paragrafo 6.3.1 e troverà applicazione quanto previsto sul punto al precedente paragrafo 6.3 e relativi sottoparagrafi;
- qualora invece il Contratto Esecutivo sia già in corso di esecuzione, dovrà darne immediata comunicazione al Fornitore tramite PEC, chiedendo a quest'ultimo di fornire la propria disponibilità ad avviare, eventualmente per il tramite del CSP/Produttore, l'iter di qualificazione e/o adeguatezza corrispondente, qualora non ne sia già in possesso. A seguito di tale comunicazione:

- I. nel caso in cui il Fornitore acconsenta, lo stesso, eventualmente, per il tramite del CSP/Produttore, è obbligato ad avviare, entro un termine concordato con l'Amministrazione Contraente, l'iter per il conseguimento del livello superiore di qualificazione e/o di

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

adeguatezza. In caso di mancato conseguimento del livello superiore, si applica quanto previsto al successivo punto II.;

- II. nel caso in cui il Fornitore opponga rifiuto, la singola Amministrazione avrà il diritto di recedere dal Contratto Esecutivo per giusta causa, ferma la facoltà di proseguire il rapporto contrattuale, anche solo in parte, ove ne ricorrano i presupposti.

12.2. Exit strategy e grace period

Al termine della durata del Contratto Esecutivo, per un periodo pari a 30 giorni, altrimenti detto grace period, il Fornitore si obbliga, senza oneri aggiuntivi, a mettere a disposizione dell'Amministrazione Contraente i dati di quest'ultima, ai fini del relativo recupero. Il Fornitore si obbliga a dare idonee garanzie dell'eliminazione e/o avvenuta inaccessibilità dei dati dell'Amministrazione Contraente. In ogni caso, il Fornitore si impegna a dare supporto all'Amministrazione Contraente per il grace period, senza oneri aggiuntivi (Exit strategy).

Preliminarmente alla fase di Exit strategy, il Fornitore si obbliga a esportare i dati in un formato che andrà stabilito in accordo con l'Amministrazione Contraente e, comunque, idoneo a consentire il trasferimento dei dati stessi e dei servizi.

Al termine di tale periodo di recupero, e a meno che non sia espressamente richiesto dalla legge, i dati dell'Amministrazione Contraente verranno cancellati e/o comunque resi inaccessibili. A tal fine, il Fornitore si obbliga a fornire tutte le idonee garanzie a dimostrazione della eliminazione dei dati nonché la disponibilità a far eseguire verifiche in tal proposito da parte dell'Amministrazione Contraente o di soggetti terzi da questa designati. In caso di revoca della qualificazione o di dichiarazione di inadeguatezza, trova applicazione quanto previsto dall'art. 21, comma 4, del Regolamento ACN.

Le previsioni del presente articolo trovano applicazione anche nel caso di recesso/cessazione parziale del rapporto contrattuale.

12.3. Perdita della qualificazione/adeguatezza

Nel caso in cui, con riferimento alle soluzioni cloud e alle infrastrutture di cui al precedente paragrafo 12, la qualificazione/dichiarazione di adeguatezza dell'infrastruttura venga a scadenza, senza che sia rinnovata, ovvero venga revocata, troverà applicazione quanto segue.

In particolare, ove ciò non comporti una modifica dell'offerta originariamente formulata, il Fornitore potrà, dandone comunicazione a Consip S.p.A. o direttamente all'Organismo di coordinamento e controllo, con le modalità di cui al successivo paragrafo 12.4, e alle Amministrazioni con cui abbia contratti in essere, proporre soluzioni e/o infrastrutture cloud diversi, ma comunque con funzionalità equivalenti o superiori rispetto a quelle minime ed eventualmente migliorative delle soluzioni cloud/infrastrutture offerti e comunque in possesso dei requisiti richiesti nella *lex specialis* di gara. In tal caso la sostituzione potrà diventare operativa solamente a seguito di apposita approvazione da

parte dell'Organismo di coordinamento e controllo, che opererà con le modalità di cui al successivo paragrafo 12.4.

Qualora la sostituzione di cui sopra non sia possibile, Consip e le Amministrazioni contraenti, per quanto di rispettiva competenza, potranno risolvere l'Accordo Quadro e il Contratto Esecutivo (limitatamente ai servizi cloud in questione), fermo quanto previsto dall'art. 21, comma 5, del Regolamento ACN.

12.4. Sostituzione di soluzioni cloud e infrastrutture

Nelle ipotesi di cui al precedente paragrafo 12.3 (ma anche negli ulteriori casi previsti nella documentazione contrattuale, ivi compresa la casistica di cui ai paragrafi 4.3 e 4.4 del Capitolato Tecnico Speciale relativo ai lotti 1 e 2 e di cui al paragrafo 4.3 del Capitolato Tecnico Speciale relativo ai lotti 3 e 4), su richiesta del Fornitore, sarà possibile la sostituzione delle soluzioni cloud e delle infrastrutture proposte.

L'Organismo di coordinamento e controllo chiederà al Fornitore apposito documento di "specifiche tecniche", contenente i requisiti della nuova soluzione/infrastruttura, al fine di dimostrarne l'equivalenza a quella eventualmente indicata in offerta tecnica, nonché comunque il possesso dei requisiti richiesti nei Capitolati tecnici speciali e relative appendici e di quelli migliorativi eventualmente offerti.

L'Organismo di coordinamento e controllo, quindi, acquisita la suddetta documentazione, svolgerà, anche tramite i propri componenti secondo quanto pattuito nel rispettivo Regolamento, le seguenti valutazioni:

- valutazione di ammissibilità, al fine di verificare la sussistenza dei presupposti espressi nel presente paragrafo;
- valutazione di congruità tecnica, nell'ambito della quale potrà svolgere ogni approfondimento ritenuto più opportuno, anche in contraddittorio con il Fornitore.

Una volta svolte le suddette valutazioni, le stesse saranno oggetto di approvazione da parte dell'Organismo di coordinamento e controllo e, in tal caso, diventeranno automaticamente "appendici" alla documentazione relativa al lotto di riferimento pubblicata all'attivazione dell'Accordo Quadro.

Tenuto conto delle nuove soluzioni/infrastrutture, sarà nuovamente svolto il collaudo secondo le modalità di cui al capitolo 9.

13. PRESCRIZIONI COMUNI RELATIVE ALLA CYBERSICUREZZA

I servizi oggetto dell'Accordo Quadro sono riconducibili, a seconda del lotto, alle seguenti categorie dell'Allegato 2 del DPCM 30 Aprile 2025 (*"Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale"*), come modificato al DPCM 2 ottobre 2025 (*"Modifica del decreto del Presidente del Consiglio dei ministri 30 aprile 2025"*):

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

Lotti 1 e 2

ID Servizio	Servizio	Categorie di cui all'Allegato II al DPCM 30 aprile 2025
Lx.S1	Security Operation Center (SOC)	Categoria 5, 18, 19, 20
Lx.S2	Next Generation Firewall (NGFW)	Categoria 11, 18, 19, 20
Lx.S3	Web Application Firewall and API protection (WAAP)	Categoria 11, 18, 19, 20
Lx.S4	Secure Web Gateway (SWG)	Categoria 11, 18, 19, 20
Lx.S5	Secure E-mail Gateway (SEG)	Categoria 11, 18, 19, 20
Lx.S6	Cloud Access Security Broker (CASB)	Categoria 1, 18, 19, 20
Lx.S7	Zero Trust Network Access (ZTNA)	Categoria 1, 18, 19, 20
Lx.S8	End Point Protection (EPP)	Categoria 2, 18, 19, 20
Lx.S9	Server Protection Platform (SPP)	Categoria 2, 18, 19, 20
Lx.S10	Anti-Advanced Persistent Threat (anti-APT)	Categoria 2, 18, 19, 20
Lx.S11	Threat Intelligence & Vulnerability Data Feed	Categoria 18, 19, 20
Lx.S12	Supporto specialistico	Categoria 18, 20

Lotti 3 e 4

ID Servizio	Servizio	Categorie di cui all'Allegato II al DPCM 30 aprile 2025
Lx.S16	Cyber Risk Management	Categoria 19, 20
Lx.S18	Vulnerability Assessment	Categoria 19, 20
Lx.S19	Penetration Testing	Categoria 19, 20
Lx.S20	Analisi del codice – Statico	Categoria 19, 20
Lx.S21	Analisi del codice – Dinamico	Categoria 19, 20
Lx.S22	Analisi del codice – Mobile	Categoria 19, 20
Lx.S23	Controllo terze parti (supply-chain di approvvigionamento)	Categoria 20

Con riferimento a entrambe le tabelle di cui sopra, la categoria 19 si intende associata allo specifico servizio, solo laddove siano state offerte dal Fornitore soluzioni cloud necessarie all'erogazione del servizio medesimo.

Tenuto conto che la presente iniziativa potrà essere impiegata per l'erogazione di prestazioni rientranti in un «contesto di impiego connesso alla tutela degli interessi nazionali strategici», per tutti i servizi richiamati, per ciascun lotto, nelle tabelle di cui sopra, il Fornitore dovrà garantire, nel corso della durata contrattuale e senza oneri aggiuntivi, il pieno rispetto di quanto previsto dall'Allegato 1, "Elementi essenziali di cybersicurezza dei beni e dei servizi informatici" del suddetto DPCM.

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

In particolare, per le categorie 1, 2, 5, 11 e 19: il Fornitore deve adottare tutte le misure necessarie affinché le caratteristiche dei servizi risultino conformi al Regolamento (UE) 2024/2847 del Parlamento Europeo e del Consiglio del 23 ottobre 2024 (Cyber Resilience Act, CRA) relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali. Si precisa che tale Regolamento ha modificato i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla cyberresilienza). La conformità dovrà essere garantita nei tempi e secondo le fasi previste dal periodo transitorio stabilito dal Regolamento, man mano che le relative disposizioni diventeranno obbligatorie.

Per tutte le suddette categorie (comprese le categorie 18 e 20), su richiesta di Consip S.p.A., possono essere istituiti appositi tavoli tecnici con il Fornitore ed eventuali interlocutori istituzionali, mediante l'eventuale coinvolgimento dell'Organismo di coordinamento e controllo, finalizzati a individuare congiuntamente le modalità operative di espletamento di tali verifiche. Nella richiesta di istituzione dei Tavoli tecnici, Consip può indicare tempistiche stringenti (comunque non inferiori a 5 giorni lavorativi) di riscontro da parte del Fornitore, e in caso di mancato rispetto delle stesse può trovare applicazione apposita penale applicata da Consip.

In linea con quanto previsto dal DPCM 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025 e in considerazione delle Linee guida per l'applicazione dei criteri di premialità di cui all'articolo 14 della legge n. 90/2024, per i servizi erogati nell'ambito della presente iniziativa di gara è previsto il criterio di valutazione n° C22 (lotti 1 e 2) n° C20 (lotti 3 e 4) di cui al par. 17.1 del Capitolato d'oneri. Tale criterio insiste su tutte le precedenti categorie con esclusione delle categorie 4 e 7 in quanto, per questa specifica iniziativa di gara, si rileva che non sono preposte a funzioni di sicurezza informatica attinenti alla tutela del dato e delle informazioni.

In linea con quanto previsto della legge n. 90/2024, articolo 14, comma 2, lettera b), per i servizi erogati nell'ambito della presente iniziativa è previsto il criterio di valutazione n° C17 (lotti 1 e 2) n° C15 (lotti 3 e 4) di cui al par. 17.1 del Capitolato d'Oneri.

In coerenza con quanto previsto al capitolo 6 delle Linee Guida dell'ACN, eventuali difformità che dovessero successivamente emergere, come ad esempio in sede di scrutinio tecnologico effettuato da ACN ai sensi dell'art. 1, comma 6, lett. a), del decreto-legge n. 105/2019, potranno costituire causa di risoluzione contrattuale, comportando una violazione del principio di fiducia di cui all'art. 2 del decreto legislativo n. 36/2023, ferma restando ogni altra conseguenza stabilita dallo stesso codice ai sensi dell'art. 98, comma 2, e dell'art. 96, comma 15, anche relativamente all'obbligo di segnalazione all'ANAC.