PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296

CONDIZIONI DI FORNITURA

INDICE

1 PREMESSA

La presente iniziativa è suddivisa nelle seguenti due tipologie di servizi:

- Servizi di sicurezza da remoto;
- Servizi di Compliance e controllo.

Nella tabella seguente si riporta la suddivisione in lotti:

Tabella 1.1 Lotti di suddivisione dell'iniziativa

Numero Lotto	Oggetto del lotto	CIG
1	Servizi di Sicurezza da remoto	
2	Servizi di Compliance e Controllo	

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

Il presente documento è integrato, rispettivamente:

- dall'Appendice 1 "Governance";
- dall'Appendice 2 "Lotto 1 - Contesto Tecnico" e relative appendici 2A (Indicatori di Qualità) e 2B (Profili Professionali);
- dall'Appendice 3 "Lotto 2 - Contesto Tecnico" e relative appendici 3A (Indicatori di Qualità) e 3B (Profili Professionali).

Le Appendici 2 e 3 disciplinano i contenuti di dettaglio e i requisiti minimi dei singoli lotti, in termini di quantità, qualità e livelli di servizio.

1.1 Suddivisione dei servizi per lotto di fornitura

Nella tabella seguente si riporta l'elenco dei servizi oggetto di fornitura:

Tabella 1.2 Servizi oggetto di fornitura

Lotto 1 – Servizi di sicurezza da remoto	
ID Servizio	**Servizio**
L*1*.S1	Security Operation Center
L*1*.S2	Next Generation Firewall
L*1*.S3	Web Application Firewall
L*1*.S4	Gestione continua delle vulnerabilità di sicurezza
L*1*.S5	Threat Intelligence & Vulnerability Data Feed
L*1*.S6	Protezione navigazione Internet e Posta elettronica
L*1*.S7	Protezione end point
L*1*.S8	Certificati SSL
L*1*.S9	Formazione e security awareness
L*1*.S10	Gestione dell'identità e l'accesso utente
L*1*.S11	Firma digitale remota
L*1*.S12	Sigillo elettronico
L*1*.S13	Timbro elettronico
L*1*.S14	Validazione temporale elettronica qualificata

L*1*.S15	Servizi specialistici
Lotto 2 - Servizi di Compliance e controllo	
ID Servizio	**Servizio**
L*2*.S16	Security Strategy
L*2*.S17	Vulnerability Assessment
L*2*.S18	Testing del codice – Statico
L*2*.S19	Testing del codice – Dinamico
L*2*.S20	Testing del codice – Mobile
L*2*.S21	Supporto all'analisi e gestione degli incidenti
L*2*.S22	Penetration Testing
L*2*.S23	Compliance normativa

Il codice identificativo di ciascun Servizio (ID) è una stringa così composta:

Lx; ove x è l'identificativo del numero del Lotto;
Sn; ove n è il numero progressivo del Servizio.

1.2 Acronimi

Per agevolare la lettura del presente documento e delle Appendici vengono riportati di seguito gli acronimi e le definizioni più frequentemente utilizzati nell'ambito di tali documenti:

AgID: Agenzia per Italia Digitale
AQ: Accordo Quadro
CAD: Codice dell'Amministrazione Digitale
CONSIP: Consip S.p.A.
CVCN: Centro di valutazione e certificazione nazionale
GDPR: General Data Protection Regulation - Regolamento generale sulla protezione dei dati
HTTP: Hyper Text Transport Protocol
HTTPS: Secure HyperText Markup Language
ICT: Information and Communication Technology
IT: Information Technology
KPI: Key Performance Indicator
OSSTMM: Open Source Security Testing Methodology Manual
PA: Pubblica Amministrazione
PAC: Pubblica Amministrazione Centrale
PAL: Pubblica Amministrazione Locale
PCI: abbreviazione per Payment Card Industry.
PMO: Project Management Office
PT: Piano triennale
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

1.3 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.

Aggiudicatario/Fornitore: se non diversamente indicato vanno intesi gli aggiudicatari previsti per ciascun AQ per ciascuno dei Lotti della fornitura.

Amministrazioni: Pubbliche Amministrazioni.

Amministrazione aggiudicatrice: Consip S.p.A.

Amministrazione/i Contraente/i: Pubbliche Amministrazioni che hanno siglato o intendono affidare un contratto esecutivo con il Fornitore per l'erogazione di uno dei servizi oggetto dell'Accordo Quadro.

Condizioni di fornitura: il presente documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa.

Collaudo e verifica di conformità, effettuati dall'Amministrazione e corrispondenti alla valutazione con verifica di merito dei prodotti consegnati

Componente: Il singolo elemento della configurazione di un sistema sottoposto a monitoraggio.

Contratto esecutivo: il Contratto avente ad oggetto rispettivamente:

1) Servizi di Sicurezza da remoto che si perfeziona con le modalità indicate al paragrafo 6.3 del presente documento.
2) Servizi di Compliance e controllo, che si perfeziona con le modalità indicate al paragrafo 6.5 del presente documento.

Piano dei Fabbisogni: il documento inviato dall'Amministrazione al Fornitore, al quale l'Amministrazione medesima affida il singolo Contratto Esecutivo e nel quale dovranno essere riportate, tra l'altro, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore;

Piano Operativo: il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel presente documento;

Prodotto della fornitura: tutto ciò che viene realizzato dal fornitore. Comprende tutta la documentazione contrattuale e gli artefatti come definiti nell'appendice Livelli di servizio.

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

Modalità di erogazione *On-site*: servizio erogato presso le strutture dell'Amministrazione contraente 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: Per Sistema si intende 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 in modalità "da remoto" di cui al presente documento per lo specifico Lotto di fornitura.

Perimetro di sicurezza nazionale cibernetica: ai sensi del DL. Del 21 settembre 2002 n.105, il Perimetro è composto dai sistemi informativi e dai servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione

di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali.

2 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.
Resta inteso che, per durata dell'Accordo Quadro, si intende il termine entro il quale le Amministrazioni Contraenti potranno affidare i singoli Contratti Attuativi.
Ciascun Contratto Esecutivo (stipulato all'esito della procedura individuata al paragrafo 6.3) dispiegherà i suoi effetti dalla data di stipula e avrà una durata massima di 48 mesi, decorrenti dalla data di conclusione delle attività di Presa in carico come meglio descritto nell'Appendice 2 "Contesto tecnico – Lotto 1" e Appendice 3 "Contesto tecnico - Lotto 2".

3 LUOGO DI ESECUZIONE DEI SERVIZI

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

- per i servizi erogati da remoto: presso i Centri Servizi del Fornitore;
- per i servizi on-site: presso le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa; in alternativa presso la Sede del Fornitore.

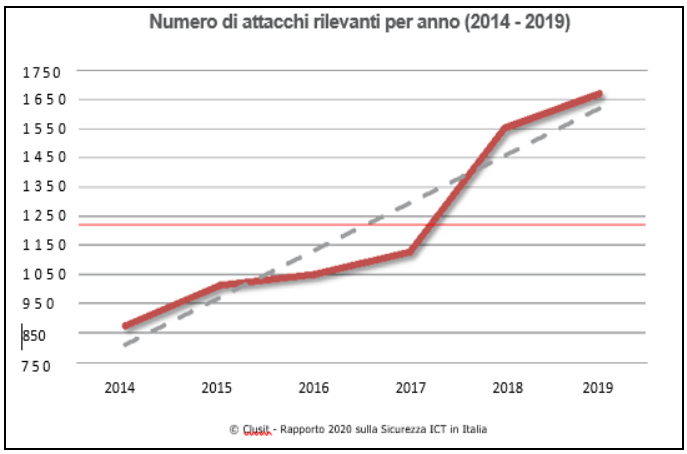
Le caratteristiche ed i requisiti dei Centri Servizi sono descritti nell'Appendice 2 "Contesto tecnico - Lotto 1".
Per l'erogazione dei servizi in modalità "on-site" previste nel Piano dei Fabbisogni, l'Amministrazione, ove richiesto specificherà le sedi effettive di erogazione. In tal caso sono a carico 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 per la 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".

4 CONTESTO

4.1 Contesto generale di riferimento

Nel contesto attuale la minaccia cibernetica cresce continuamente in quantità e qualità e i servizi informatici e telematici erogati dalla Pubblica Amministrazione diventano sempre più cruciali per il funzionamento del sistema Paese.
Dal rapporto ClusIT del 2020 sulla sicurezza dell'ICT in Italia, si rileva che il 2019 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, sia dal punto di vista quantitativo che da quello qualitativo, evidenziando un trend persistente di crescita degli attacchi, della loro gravità e dei danni conseguenti. Gli attaccanti non sono più "hackers", e nemmeno gruppetti effimeri di "artigiani" del cyber-crime: sono decine e decine di gruppi criminali organizzati trans-nazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari ed unità di mercenari che hanno come campo di battaglia, arma e bersaglio le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging, su scala globale, 365 giorni all'anno, 24 ore al giorno.

Già nel 2018 si è assistito a livello mondiale ad una crescita del 77,8% degli attacchi informatici di particolare gravità rispetto al 2014 e del 37,7% rispetto al 2017, attacchi aventi sempre più l'obiettivo non solo di interferire nella vita privata dei cittadini, ma anche di incidere sul piano finanziario e geopolitico.
Il «Cyber-crime» e il «Cyber Espionage» fanno registrare il numero di attacchi più elevato degli ultimi 8 anni; il primo è finalizzato alla monetizzazione dell'informazione sottratta indebitamente, il secondo è finalizzato allo spionaggio geopolitico, industriale e al furto della proprietà intellettuale. L'unica categoria di attacchi che registra un decremento nel 2018 è l'«hacktivism» (-22,8% rispetto al 2017), ovvero sia attacchi con finalità politiche o sociali.
I settori «Government» e «Health» hanno registrato nel 2018 un incremento degli attacchi pari rispettivamente al 40,8% e 98,8% rispetto al 2017.
Nel grafico seguente si riporta l'andamento del numero degli incidenti di sicurezza ritenuti più significativi avvenuti a livello globale nel 2019.



Le misure nazionali a favore della cyber-security rappresentano un tassello della più complessa vision di un unico mercato digitale che assicuri un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, adottato come criterio ispiratore della Direttiva NIS.
In ottemperanza agli obblighi imposti a livello sovranazionale dall'art. 7 Direttiva NIS (Direttiva (UE) 2016/1148 secondo cui "Ogni Stato membro adotta una strategia nazionale in materia di sicurezza della rete e dei sistemi

informativi che definisce gli obiettivi strategici e le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi e contempla almeno i settori di cui all'allegato II e i servizi di cui all'allegato III", rispettivamente, di Operatori di Servizi Essenziali (OSE) e di Fornitori di Servizi Digitali (FSD), il legislatore nazionale è di recente intervenuto, con il Decreto Legge n. 105/2019, per definire il perimetro di sicurezza nazionale cibernetica.
La legge n. 133/2019 (adeguamento del DL n.105/2019) prevede che con decreto del Presidente del Consiglio dei Ministri saranno identificati "le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati" inclusi nel perimetro di sicurezza nazionale cibernetica.

Le attività di supporto alle PA **nella prevenzione e risposta agli incidenti informatici** svolte in passato dal CERT – PA, sono invece gestite, come previsto dal DPCM 8 agosto 2019, dallo **CSIRT Italia, il nuovo team per la cyber-difesa nazionale dapprima istituito presso il Dipartimento Informazioni per la Sicurezza (DIS) e trasferito, dal DL 82/2021** ("Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale") **presso l'Agenzia per la cybersicurezza nazionale (**in avanti nel presente documento anche solo "Agenzia").
La recente entrata in vigore (15/06/2021) del suddetto D.L., che ha decretato l'istituzione dell'Agenzia, ha aggiunto un altro importante tassello al contesto normativo cyber in forte evoluzione (D.L. n. 105/2019 convertito con modificazioni dalla Legge 133/2019, DPCM 131/2020, DPR 54/2021, DPCM 81/2021), rivedendo l'assetto organizzativo del Sistema di informazione per la sicurezza della Repubblica e le funzioni svolte dai vari Organi/Autorità, allo scopo di fronteggiare nel miglior modo possibile il rischio cibernetico, che può compromettere la sicurezza nazionale.
Secondo quanto previsto dal D.L. n. 82/2021 e, in particolare, in base a quanto disciplinato dal relativo art. 7, fra le funzioni ad essa assegnate, l'Agenzia assume tutte quelle già attribuite al DIS e al CVCN (Centro di valutazione e certificazione nazionale) dal D.L. 105/2019, nonché ai sensi del comma 1, lett. m) del succitato articolo, "*assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo".*
A ciò si aggiunge l'entrata in vigore (01/06/2021) del D.L. 77/2021 "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", che ha l'obiettivo di semplificare e agevolare la realizzazione del Piano Nazionale di Ripresa e Resilienza e che destina 620 milioni di euro alla cyber security delle PP.AA., considerando quindi questo un asset fondamentale a servizio della digitalizzazione del Paese.

Anche nel Piano Triennale per l'Informatica della PA, aggiornato al triennio 2020-2022, la sicurezza assume un ruolo strategico e trasversale, comprendendo tutte le attività per la regolazione e regolamentazione della sicurezza nella Pubblica Amministrazione che sono state assegnate ad AgID, in particolare dal Quadro Strategico Nazionale e dalla Direttiva del Presidente del Consiglio del 1 agosto 2015. Oltre a questi vi sono anche tutti gli aspetti che concorrono a rendere sicuri e affidabili i sistemi informatici della PA, sotto il punto di vista del rispetto della normativa sulla protezione dei dati personali (GDPR). Viene raccomandata l'adozione in tutti i progetti di un approccio "security by default", imponendo alle Pubbliche Amministrazioni di rendersi conformi alle Misure minime di sicurezza ICT. La sicurezza informatica riveste pertanto un ruolo fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma anche la resilienza della macchina amministrativa. Essa è inoltre direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico.

4.2 Piano Triennale per l'Informatica della Pubblica Amministrazione

Il **Piano Triennale per l'informatica della Pubblica Amministrazione** è uno strumento essenziale per promuovere la trasformazione digitale dell'amministrazione italiana e del Paese e, in particolare quella della Pubblica Amministrazione italiana.

Tale trasformazione dovrà avvenire nel contesto del mercato unico europeo di beni e servizi digitali, secondo una strategia che in tutta la UE si propone di migliorare l'accesso online ai beni e servizi per i consumatori e le imprese e creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi per massimizzare il potenziale di crescita dell'economia digitale europea.

In tale contesto dove quindi i servizi digitali rappresentano un elemento indispensabile per il funzionamento di un Paese, la PA ne è parte fondamentale e indispensabile. E' ampiamente noto che la minaccia cibernetica è sempre più attiva e cresce continuamente in qualità e quantità minacciando infrastrutture critiche, processi digitali e rappresentando anche un elevato rischio di natura militare visto l'utilizzo che è sempre più diffuso verso quello che chiamiamo il perimetro di sicurezza cibernetico.

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

Il Piano mantiene l'attenzione rispetto al passato ponendosi anche il cruciale problema della protezione del dato. Questo elemento è fondamentale perché tale protezione è strettamente connessa alla sua qualità e agire correttamente consente di attuare anche gli obblighi normativi europei in materia di protezione dei dati personali (GDPR).

Il Piano si focalizza sulla Cyber Security Awareness, poiché tale consapevolezza fa scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche.

Nella PA ci sono frequenti attacchi a portali che bloccano i servizi erogati e costituiscono danno di immagine. E' in crescita anche il fenomeno denominato data breach (violazione dei dati) che rappresenta anche una grave violazione del GDPR.

Le azioni stabilite nel Piano sono tutte indispensabili rispetto allo scenario possibile. Oltre agli attori coinvolti nel Piano resta indispensabile e cruciale il supporto del Garante per la protezione dei dati personali quantomeno per verificare se la PA ha nominato un adeguato DPO (figura obbligatoria per il GDPR) ed è organizzata, almeno ai minimi termini, in linea con le regole del GDPR (Regolamento europeo 679/2016).

Il Piano affida a Linee guida e regole specifiche ma anche alle strutture specifiche di AgID il supporto alle PPAA.

In particolare **AgID** ha concordato l'indirizzo strategico per la progettazione della presente iniziativa con particolare riferimento sui contenuti tecnici e sui meccanismi di coordinamento e controllo dell'utilizzo dello strumento di acquisizione; **Consip S.p.A.**, in qualità di soggetto Stazione Appaltante, ha aggregato i fabbisogni e predisposto la procedura di gara e gestirà la stipula dei contratti per le amministrazioni centrali e locali.

Le PA devono intraprendere misure ed azioni per l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi definiti nel Piano Triennale.

In capo ai Fornitori è la responsabilità di supportare le Amministrazioni mediante i servizi resi disponibili dalla presente iniziativa e supportare i soggetti deputati al coordinamento e controllo, secondo quanto previsto dalla documentazione di gara.

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

In particolare, le attività di direzione strategica prevedono il coinvolgimento di soggetti istituzionali, mentre nell'ambito delle attività di direzione tecnica saranno coinvolti anche soggetti non istituzionali, individuati nei Fornitori Aggiudicatari della presente acquisizione.
Si precisa che per "Organismi di coordinamento e controllo", si intendono i soggetti facenti capo alla Presidenza del Consiglio e/o al Ministero per l'Innovazione tecnologica e la Digitalizzazione (es: Agid, Team Digitale), che, in base alle funzioni attribuite ex lege, sono ad oggi deputati, per quanto di rispettiva competenza, al monitoraggio e al controllo delle iniziative rientranti nel Piano Triennale per l'informatica nella Pubblica Amministrazione.
Nell'ambito di tali Organismi è ricompresa altresì Consip S.p.A., per i compiti di propria competenza. Rimangono salve eventuali modifiche organizzative che interverranno a livello istituzionale nel corso della durata del presente Accordo Quadro.
Gli Organismi di coordinamento e controllo saranno normati da appositi Regolamenti che, resi disponibili alla stipula dei contratti relativi alla presente iniziativa o appena possibile, definiranno gli aspetti operativi delle attività di coordinamento e controllo, sia tecnico che strategico.
I meccanismi di governance sopra introdotti e applicati anche a tutte le iniziative afferenti al Piano Triennale riguarderanno:

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

L'Organismo di controllo, nel momento in cui svolge attività di governo del contratto quadro, coinvolge i Fornitori aggiudicatari. Con specifico riferimento a tale aspetto, si rimanda al capitolo 8 per il dettaglio dei compiti demandati agli Organismi di coordinamento e controllo per la presente iniziativa.

4.3 Inquadramento dell'iniziativa

Nella logica di continuità di servizio con il Contratto Quadro SPC Cloud - Lotto 2, l'iniziativa **Sicurezza da remoto** viene bandita ai sensi dell'art. 4, comma 3 quater del d.l. 95/2012, ove Consip S.p.A. svolge altresì le attività di centrale di committenza relative alle Reti telematiche delle pubbliche amministrazioni, al Sistema pubblico di connettività ai sensi del decreto legislativo 7 marzo 2005, n. 82, e alla Rete internazionale delle pubbliche amministrazioni ai sensi del decreto medesimo nonché ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311.
Tale iniziativa si affianca alle gare strategiche previste da AgID ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese.
Storicamente il Sistema Pubblico di Connettività (SPC) ha seguito la rete unitaria della pubblica amministrazione (RUPA), nata con l'intento di connettere le pubbliche amministrazioni, almeno quelle centrali. Il Sistema Pubblico di Connettività (SPC), è posto alla base delle infrastrutture materiali dell'architettura disegnata nel Piano Triennale l'informatica nella Pubblica Amministrazione 2017-2019 di AgID, il cosiddetto Modello Strategico. È un sistema

composto da molti servizi stratificati, dalla connettività ai servizi Cloud, ed è stato aggiornato nel 2016 con nuove gare Consip SPC2, SPC Cloud ampliando il portafoglio dei servizi e delle infrastrutture.

L'iniziativa **Sicurezza da remoto** si pone un duplice obiettivo:

- quello di garantire la continuità e l'evoluzione dei servizi già previsti nella precedente iniziativa SPC Cloud – Lotto 2 avente ad oggetto servizi di sicurezza volti alla protezione dei sistemi informativi in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema pubblico di connettività;
- quello di rendere disponibili alle Amministrazioni servizi con carattere di innovazione tecnologica per l'attuazione del Codice dell'Amministrazione Digitale, nonché del Piano Triennale ICT della PA.

L'iniziativa Sicurezza da remoto si affianca alle iniziative strategiche relative alla fornitura di beni e servizi di Sicurezza in modalità "on-premise" come previsto nel Piano gare AgID in attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione, i cui perimetri di fornitura afferiscono a diverse modalità di gestione della sicurezza IT. L'iniziativa Sicurezza «on premise» si basa infatti sulla fornitura di componenti hardware e software da utilizzare presso le infrastrutture della PA. L'iniziativa Sicurezza da remoto si basa sull'utilizzo di servizi, che verranno erogati remotamente alle PA mediante un Centro Servizi del fornitore.
I servizi oggetto della presente iniziativa integrano il modello strategico di evoluzione digitale che dovrà essere adottato dalle Amministrazioni.
Con la partecipazione alla presente procedura di gara, gli operatori economici si impegnano a orientare il proprio futuro operato di erogatori di servizi in conformità con le disposizioni dell'attuale Piano Triennale ICT e con le normative in materia di Cyber security di riferimento ed adeguarsi alle dinamiche evolutive, utilizzando la tecnologia per accompagnare il processo di trasformazione digitale della PA.

4.4 Ruolo di AgID

AgID mantiene e sviluppa servizi di sicurezza preventivi e funzioni di accompagnamento utili per la crescita e la diffusione della cultura della sicurezza informatica, in linea con le disposizioni del CAD e con gli obiettivi descritti dal "Piano triennale per l'informatica nella pubblica amministrazione"
L'art. 51, comma 1-bis del CAD (Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni) indica che AgID svolge un ruolo significativo nella tutela della sicurezza nazionale in ambito di sicurezza cibernetica, di prevenzione e di diffusione della cultura di sicurezza informatica nella pubblica amministrazione.
AgID in tale ambito ha il compito di definire raccomandazioni, strategie, norme tecniche per sensibilizzare e informare le amministrazioni sui temi della sicurezza informatica e delle emergenze ad essa collegate.
Inoltre promuove intese con le analoghe strutture internazionali; segnala al Ministro per la semplificazione e la pubblica amministrazione il mancato rispetto, da parte delle pubbliche amministrazioni, delle regole tecniche di cui al comma 1, Art.51 del CAD.
L'art 14-bis, comma 2 del CAD, indica che AgID, tra l'altro, svolge le funzioni di emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea.
Il **«Piano Nazionale per la protezione cibernetica e la sicurezza informatica» (marzo 2017)** ha stabilito la roadmap per l'adozione da parte dei soggetti pubblici e privati delle misure prioritarie per l'implementazione del Quadro Strategico Nazionale, affida ad AGID il compito di ***«dettare indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità degli standard, ad assicurare la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione e a monitorare i piani ICT delle amministrazioni pubbliche».***

Infine attraverso **il Piano triennale sull'ICT,** AgID fissa obiettivi e relative linee di azione con lo scopo di assolvere alla mission affidatale, che comprende le attività per la regolamentazione della cybersecurity nella PA.
In tale contesto, si inserisce anche la pubblicazione, da parte di AgID, delle:

- «linee guida di sicurezza nel procurement ICT» che raccolgono indicazioni tecnico-amministrative, buone prassi e strumenti operativi per garantire all'interno delle procedure di gara per l'approvvigionamento di beni e servizi ICT, la rispondenza di questi ad adeguati livelli di sicurezza;
- «linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali», che hanno l'obiettivo di introdurre un modello organizzativo ed operativo per la costituzione e l'avvio di CERT regionali nell'ambito della PA.

Il CERT-AgID

Sulla base delle esperienze e delle conoscenze maturate principalmente nell'ambito delle funzioni svolte dal CERT-PA ed in virtù degli attuali compiti istituzionali l'Agenzia per l'Italia Digitale ha riorganizzato la predetta struttura denominandola CERT-AgID.
Il CERT-PA, attivo dal mese di marzo 2014 fino al 6 maggio 2020, ha operato all'interno di AgID con il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica.
E' stato censito presso ENISA (European Network and Information Security Agency), l'agenzia dell'Unione Europea che supporta la creazione della rete Europea dei CERT e la loro collaborazione.
Dal 19 luglio 2016 ha ottenuto lo status di "Team accreditato" presso Trusted Introducer, la rete di fiducia dei CERT mondiali fondata in Europa nel 2000. L'accreditamento è il secondo dei tre livelli di partecipazione previsti da Trusted Introducer, e prevede tra l'altro che ciascun Team si impegni formalmente a rispettare vincoli di sicurezza, obblighi deontologici, e impegni di cooperazione verso l'intera comunità.
Dal 6 maggio 2020, recependo il DPCM 8 agosto 2019, "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team - CSIRT italiano", il CERT-PA termina l'erogazione di servizi reattivi e di risposta agli incidenti informatici dedicati alla PA; il Cert-AgID si riposiziona per poter svolgere all'interno di AgID il supporto su tutti i temi riguardanti trasversalmente gli aspetti di sicurezza informatica relativi ai progetti interni ed esterni a cui AgID partecipa in maniera diretta o indiretta.

4.5 Spesa ICT in ambito Cyber Security

I costi generati dal cyber-crime aumentano di anno in anno: il rapporto Clusit 2020 evidenzia che tali costi ammontano complessivamente, a livello globale, a 500 milioni di dollari all'anno e che l'Italia nel 2016 abbia subito danni derivanti da attività di cyber-crime per quasi 10 miliardi di euro.
Dalla ricerca dell'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano viene confermato che nel 2019 la spesa in security è cresciuta per il terzo anno consecutivo. La spesa per la sicurezza informatica in Italia continua a crescere. Il 2019 è stato il terzo anno consecutivo di crescita del settore, con percentuali sempre sopra alla doppia cifra. Nel 2017 il settore era cresciuto del 12%, nel 2018 +9%, mentre nel 2019 l'information security è cresciuta dell'11%, per un valore complessivo di spesa pari a 1,317 miliardi di euro.
La spesa in sicurezza si concentra soprattutto in soluzioni tecnologiche per la security, che raccolgono il 52% degli investimenti, a fronte del 48% nei servizi che però crescono maggiormente (sono in aumento per il 45% delle aziende). La tecnologia che si pone con maggiore interesse è l'Artificial intelligence, già impiegata per la gestione della sicurezza dal 45% delle grandi imprese. I servizi più finanziati sono quelli offerti da fornitori esterni all'azienda per progetti specifici (professional services, 54%), ma quelli più in crescita sono i servizi offerti in maniera continuativa da provider esterni all'organizzazione per garantire il supporto e la manutenzione dei sistemi informativi aziendali (in aumento nel 45% delle organizzazioni).
La spesa in sicurezza ICT in Italia nel 2018 è risultata pari a circa 1,47 miliardi di euro, suddivisi in 787 mln di euro di soluzioni merceologiche e 685 mln di euro di servizi (rispettivamente pari al 53,5% e 46,5% del valore complessivo), con un aumento percentuale rispetto al 2017 pari al 6,3% per le soluzioni merceologiche e al 4,4%

per i servizi. La spesa per il 2019 si attesta su 1,56 miliardi di euro, in crescita, con un +6,7% per le soluzioni merceologiche e + 4,5% per i servizi rispetto al 2018.
In particolare nel mercato Italia l'ambito dei servizi «on-service» e dei servizi di «compliance e controllo», nel 2019, è risultato pari a 675,7 mln di euro, rappresentando circa il 43% del mercato Italia (≈ 1,56 miliardi di euro).
In ambito Pubblica Amministrazione, nel 2019 la spesa per la sicurezza informatica è stata pari a circa 392 milioni di euro, di cui la quota di spesa per servizi di sicurezza «on-service» e servizi di «compliance e controllo» è risultata pari a 161,5 mln di euro, rappresentando circa il 41%**.**

4.6 Contesto normativo e standard di riferimento

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

- Regolamento Generale sulla Protezione dei Dati (*GDPR*) n. 2016/679
- D.Lgs. 18 aprile 2016, n. 50 ("*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 del Presidente del Consiglio dei Ministri 1 aprile 2008 "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
- 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
- Il Regolamento UE n° 910/2014 – eIDAS
- Determinazione Commissariale AgID N. 63/2014
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 - Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - CSIRT italiano
- D.L. 105/2019 (convertito con modificazioni dalla L. 18 novembre 2019, n. 133), come adeguato a sua volta dalla legge n. 8 del 28 febbraio 2020 e dal D.L. 82/2021, recante **disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica,** e i DPCM (tra cui il 131/2020, entrato in vigore il 5/11/2020) e regolamenti di successiva emanazione (alla data DPR 54/2021 e DPCM 81/2021), come previsti dalla menzionata legge. La disciplina di cui all'Accordo Quadro e relativi allegati (ivi compresa la documentazione tecnica) potrà subire adeguamenti alla luce dei DPCM e regolamenti della richiamata normativa, che saranno emanati in seguito alla pubblicazione della presente iniziativa.
- Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133
- D.L. n. 77/2021 "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure";
- D.L. n. 82/2021 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale";
- DPCM n. 81/2021 "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";
- Piano Nazionale per la Protezione Cibernetica 2017
- Carta dei principi per la condotta tecnologica e relativi documenti ivi richiamati
- Linee guida AgID per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD

- Linee guida AgID di sicurezza nel procurement ICT
- Linee guida AgID per lo sviluppo del software sicuro
- Linee Guida AgID per adeguare la sicurezza del software di base
- Linee Guida AgID per la modellazione delle minacce e individuazione delle azioni di mitigazione
- Linee Guida AgID per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali
- Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Standard ISO 27002:2007 che stabilisce che la sicurezza dell'informazione è caratterizzata da integrità, riservatezza e disponibilità
- Standard ISO 27001:2005 che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle tecnologie dell'informazione
- Standard ISO IEC 62443 standard mondiale di protezione dei sistemi di controllo industriale
- Eventuali successive modificazioni delle norme e standard di riferimento
- Ogni altra disposizione normativa e regolamentare applicabile

4.7 Indicatori di digitalizzazione

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

- Indicatori Generali, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale;
- Indicatori Specifici, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti. In tale contesto, è definito un indicatore (cd. "indicatore di progresso" in seguito descritto) che indica il livello di maturità della infrastruttura di sicurezza ICT delle Amministrazioni, sulla base del grado di mappatura degli interventi effettuati con le misure minime di sicurezza AGID (Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»).

Gli indicatori saranno utilizzati per il monitoraggio dei contratti e del raggiungimento dei relativi obiettivi.

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

4.7.1 Indicatori generali

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

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

In aggiunta, per le gare strategiche inerenti la sicurezza informatica, sarà previsto l'"indicatore di progresso" descritto al paragrafo successivo.

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

4.7.1.1 Indicatore di progresso

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

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

5 RAZIONALI PER L'UTILIZZO DEI LOTTI

Questo capitolo, rivolto alle Pubbliche Amministrazioni, riporta le regole e le modalità con cui le stesse possono accedere a ciascun lotto della presente iniziativa.

Entrambi i Lotti (Lotto 1 - Servizi di Sicurezza da remoto e Lotto 2 - Servizi di Compliance e controllo) sono destinati alle Pubbliche Amministrazioni Centrali (PAC) e alle Pubbliche Amministrazioni Locali (PAL).

Rientrano nelle **Pubbliche Amministrazioni Centrali**:

- Organi costituzionali e di rilievo costituzionale
- Presidenza del Consiglio dei Ministri
- Ministeri, ivi compresi gli uffici periferici
- Agenzie fiscali
- Enti di regolazione dell'attività economica
- Enti produttori di servizi economici
- Autorità amministrative indipendenti
- Enti a struttura associativa
- Enti produttori di servizi assistenziali, ricreativi e culturali
- Enti e Istituzioni di ricerca
- Enti nazionali di previdenza e assistenza sociale
- Commissari straordinari di governo
- Comitati interministeriali
- Agenzia per i servizi sanitari regionali (AGENAS)
- Banca d'Italia
- Commissione nazionale per le società e la borsa (CONSOB)
- Istituto per la vigilanza sulle assicurazioni (IVASS)
- Autorità per l'energia elettrica e il gas e il sistema idrico (AEEGSI)
- Enti pubblici esercenti attività di collegamento con le organizzazioni internazionali (enti che svolgono attività di collegamento con tra il Governo Italiano e le organizzazioni internazionali quali a titolo meramente esemplificativo:
    - Comitato nazionale italiano Organizzazione Nazioni Unite per l'alimentazione e l'agricoltura (FAO)
    - Commissione nazionale per l'Unesco
- Ordini professionali nazionali e relativi uffici periferici/collegi territoriali
- Ogni altra Amministrazione e/o Ente di rilevanza nazionale
- Organismi di diritto pubblico e le Società, partecipati, anche indirettamente, dai soggetti di cui a tutti i punti precedenti qualificabili come stazioni appaltanti (in caso di società partecipate da soggetti di tipologie diverse - es. partecipati contestualmente da soggetti rientranti nella PAC e da soggetti rientranti nella PAL – si intenderanno ricompresi nella PAC, ai fini della presente iniziativa, gli Organismi di diritto pubblico e le Società partecipati in misura maggioritaria, anche indirettamente, dai soggetti di cui ai punti precedenti)
- Società in-house partecipate al 100% dai soggetti di cui ai punti precedenti

Rientrano nelle **Pubbliche Amministrazioni Locali**:

- Regioni
- Province autonome
- Province
- Città metropolitane
- Comuni

- Comunità montane
- Unioni di Comuni
- Istituti zooprofilattici sperimentali
- Agenzie, Enti e Consorzi per il diritto allo studio universitario
- Agenzie ed Enti per il turismo
- Agenzie ed Enti regionali per il lavoro
- Agenzie ed Enti regionali e provinciali per la formazione, ricerca ed ambiente
- Agenzie regionali per la rappresentanza negoziale
- Agenzie regionali per l'erogazione in agricoltura
- Agenzie regionali sanitarie e aziende ed enti di supporto all'S.S.N.
- Enti di governo dei servizi idrici e/o dei rifiuti (ex AATO)
- Autorità di sistema portuale
- Aziende ospedaliere, aziende ospedaliero-universitarie, policlinici ed istituti di ricovero e cura a carattere scientifico pubblici
- Aziende sanitarie locali
- Camere di commercio, industria, artigianato e agricoltura e unioni regionali
- Consorzi di bacino imbrifero montano
- Consorzi tra amministrazioni locali
- Parchi nazionali, consorzi ed enti gestori di parchi ed aree naturali protetti
- Consorzi interuniversitari di ricerca
- Agenzie ed Enti regionali di sviluppo agricolo
- Fondazioni lirico-sinfoniche
- Teatri nazionali e di rilevante interesse culturale
- Università e Istituti di istruzione universitaria pubblici
- Altre Amministrazioni locali
- Consorzi di funzione ed associazioni tra enti locali non esercenti attività economiche
- Comunità isolane e di arcipelago
- Enti pubblici a carattere regionale e locale
- Ogni altra Amministrazione e/o Ente di rilevanza regionale o locale
- Organismi di diritto pubblico e le Società, partecipati, anche indirettamente, dai soggetti di cui a tutti i punti precedenti qualificabili come stazioni appaltanti (in caso di società partecipate da soggetti di tipologie diverse - es. partecipati contestualmente da soggetti rientranti nella PAC e da soggetti rientranti nella PAL – si intenderanno ricompresi nella PAL, ai fini della presente iniziativa, gli Organismi di diritto pubblico e le Società partecipati in misura maggioritaria, anche indirettamente, dai soggetti di cui ai punti precedenti).

6 MODELLO DI FUNZIONAMENTO

6.1 Interazione tra i Lotti di servizi di Sicurezza da remoto e servizi di Compliance e Controllo

Lo scenario della presente iniziativa è caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo (come riportato nella Tabella 6.1).
Tale specializzazione si innesta in considerazione dei diversi obiettivi a cui i due Lotti rispondono. In particolare:

- il Lotto di servizi di Sicurezza da remoto ha 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;
- il Lotto di servizi di Compliance e controllo ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – 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 del Lotto 1 nonchè sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

6.2 Funzionamento dei lotti

L'Amministrazione in funzione dell'oggetto del proprio fabbisogno e sulla base di quanto indicato al precedente capitolo 5, dovrà seguire l'*iter* procedurale descritto nei successivi paragrafi per utilizzare l'Accordo Quadro ed attivare i servizi.

Si riporta di seguito lo schema di funzionamento dei lotti.

Tabella 6.2 Schema di funzionamento dei lotti

ELEMENTI	LOTTO SERVIZI DI SICUREZZA DA REMOTO	LOTTO SERVIZI DI COMPLIANCE E CONTROLLO
Strumento	Accordo Quadro multi-fornitore	Accordo Quadro multi-fornitore
Lotto	1	2
Modalità di affidamento dei Contratti Attuativi	Ordinativo di fornitura	Ordinativo di fornitura
Condizioni contrattuali	Condizioni tutte fissate	Condizioni tutte fissate

6.3 Comunicazione preventiva al CVCN

Il Decreto Legge 21 settembre 2019 n.105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, indica che i soggetti rientranti nel Perimetro di sicurezza nazionale cibernetica che procederanno ad affidamenti di forniture di beni, sistemi e servizi ICT, anche mediante ricorso a centrali di committenza, destinati a essere impiegati nel Perimetro ne dovranno dare comunicazione, ai sensi di quanto previsto all'art. 1, comma 6 lett. a) del D.L. 105/2019, la cui efficacia è stata modificata dall'art. 16 comma 9, lett. a) del D.L. n. 82/2021, al CVCN (Centro di valutazione e certificazione nazionale istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 presso l'Agenzia) o i CV istituiti presso il Ministero dell'interno e il Ministero della difesa il quale può effettuare verifiche e imporre test di hardware e software.
Pertanto tali soggetti rientranti nel Perimetro di sicurezza, beneficiari dei servizi oggetto di fornitura del Lotto 1 e del Lotto 2 della presente iniziativa, ai sensi dell'art 3 del **Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133,** dovranno trasmettere al CVCN

per via telematica le informazioni richieste.
Il CVCN svolge il procedimento di verifica e valutazione il cui esito viene comunicato al soggetto rientrante nel perimetro e al fornitore.

6.4 Adesione al Lotto 1 - Servizi di Sicurezza da remoto dell'Accordo Quadro

Nel caso di adesione all'Accordo Quadro per i servizi di Sicurezza da remoto, le Amministrazioni legittimate affideranno i Contratti attuativi, successivamente alla stipula dell'Accordo Quadro e per tutta la durata dello stesso, alle medesime condizioni (economiche e tecnico-prestazionali) stabilite nell'Accordo Quadro ai Fornitori aggiudicatari ai sensi dell'art. 54, comma 3, del D. Lgs. n. 50/2016.
In particolare, per l'AQ verrà attribuita in sede di aggiudicazione:

- una quota pari al 60% del massimale del Lotto 1 all'Operatore economico risultato 1° nella graduatoria di merito (Amministrazioni beneficiarie PAL);
- una quota pari al 40% del massimale del Lotto 1 all'Operatore economico risultato 2° nella graduatoria di merito (Amministrazioni beneficiarie PAC).

L'affidamento di ciascun Contratto esecutivo avverrà con le modalità di seguito descritte.

6.4.1 Piano dei Fabbisogni

L'Amministrazione trasmetterà, a mezzo PEC, al fornitore aggiudicatario per il comparto di riferimento, e contestualmente alla Consip S.p.A. (e/o a terzi dalla stessa indicati), il "**Piano dei Fabbisogni**" (o "**Ordinativo di fornitura**"), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo 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.
In particolare, il "Piano dei fabbisogni" conterrà, a titolo esemplificativo e non esaustivo, i seguenti elementi:

- Indicazione 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;
- la categorizzazione dell'intervento;
- il comparto di appartenenza (PAC/PAL);
- l'importo contrattuale e le quantità previste per i servizi oggetto di fornitura;
- la data di attivazione di ciascun servizio oggetto di fornitura;
- la durata del Contratto esecutivo e dei singoli servizi;
- le modalità di erogazione e consuntivazione dei servizi di fornitura;
- 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 della fornitura;
- ogni altra eventuale indicazione riportata nell'Appendice 2 inerente agli specifici servizi richiesti, come ad esempio un documento allegato con il contesto tecnologico e applicativo;
- l'eventuale cronoprogramma ai fini dell'anticipazione del prezzo, ove applicabile.

Si precisa che, ove richiesto dall'Amministrazione, il Fornitore dovrà impegnarsi obbligatoriamente a supportare la stessa nella redazione del Piano dei fabbisogni.

Con specifico riferimento ai servizi da svolgere presso i siti delle Amministrazioni, 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).
Il Fornitore dovrà approntare, ove necessario ed entro 15 gg lavorativi dalla richiesta (o salvo diverso accordo tra le parti), il calendario dei sopralluoghi necessari, che dovrà indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal Fornitore 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 trasmissione del Piano dei fabbisogni da parte dell'Amministrazione verso il Fornitore selezionato non scaturisce alcun obbligo per l'Amministrazione di procedere alla stipula del Contratto esecutivo con il Fornitore aggiudicatario.

6.4.2 Piano Operativo

Il fornitore aggiudicatario, 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, a mezzo PEC, all'Amministrazione che ne abbia fatto richiesta, nonché a Consip S.p.A. e/o terzi da essa indicati.
In particolare, fermo quanto previsto nell'Appendice 2 dei servizi di sicurezza da remoto, il Fornitore aggiudicatario, mediante il "Piano Operativo", dovrà formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti.

Il Piano Operativo dovrà indicare, a titolo esemplificativo e non esaustivo, i seguenti aspetti in coerenza al Piano dei Fabbisogni:

- la categorizzazione dell'intervento;
- il comparto di appartenenza (PAC/PAL);
- l'importo contrattuale e le quantità previste per i servizi oggetto di fornitura;
- l'identificativo del servizio;
- la data di attivazione del servizio di fornitura;
- l'indicazione del/i luogo/ghi di esecuzione della fornitura;
- la durata del Contratto esecutivo e dei servizi;
- 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;
- quota e prestazioni che intenderà subappaltare nel rispetto di quanto indicato nel Piano dei fabbisogni.

Il Piano Operativo, inoltre, dovrà contenere:

- un piano di lavoro generale coerente con il fabbisogno, che rappresenta la totalità dei servizi richiesti e rappresenta le attività propedeutiche all'attivazione dei servizi, e che potrà essere aggiornato successivamente alla stipula del Contratto esecutivo previo accordo con l'Amministrazione. Come previsto nell'Appendice 2 relativo al lotto di servizi di sicurezza da remoto, tale piano dovrà contenere al proprio interno anche il piano di Presa in carico;
- un Piano della Qualità specifico di Contratto esecutivo (ad integrazione del Piano della Qualità Generale che dovrà essere trasmesso alla Consip S.p.A. ai sensi del successivo paragrafo 7.1.1),

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 che verranno impiegate per l'erogazione dei servizi, con le relative certificazioni richieste e/o proposte in offerta tecnica;
- la proposta operativa coerente rispetto al documento di contesto tecnologico e applicativo allegato al Piano dei Fabbisogni.

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.
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 ai fini dell'applicazione della relativa penale.

6.4.3 Contratto esecutivo

L'Amministrazione, entro 30 giorni solari dalla relativa ricezione, ha la facoltà di approvare il "Piano Operativo", ovvero di comunicare la richiesta di eventuali modifiche e/o integrazioni, nel rispetto del Piano dei fabbisogni. In tal caso l'aggiudicatario dovrà apportare al documento presentato le modifiche e/o integrazioni richieste.
L'aggiudicatario dovrà inviare la versione definitiva del Piano Operativo entro 10 giorni solari dalla comunicazione di richiesta dell'Amministrazione Contraente.
Da tale data decorrerà nuovamente il termine di 30 giorni solari di cui al periodo precedente.
Qualora, decorsi 30 giorni solari dalla ricezione del Piano Operativo, l'Amministrazione non lo abbia approvato ovvero non ne abbia richiesto la modifica ovvero non abbia richiesto ulteriori giorni per la relativa verifica, il relativo Piano dei fabbisogni precedentemente trasmesso dall'Amministrazione si intenderà decaduto.

Il Contratto si perfeziona in seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione del Piano operativo da parte dell'operatore economico sulla base dell'apposito schema allegato alla documentazione di gara. Esso conterrà altresì ogni altro aspetto rilevante per l'esecuzione del singolo contratto, in ragione di quanto stabilito nel presente documento e nelle Appendici
Nel caso di Contratto esecutivo affidato da un Soggetto Aggregatore, il medesimo inoltre:
- dovrà contenere l'indicazione di tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'affidamento;
- 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.

Il Fornitore dovrà produrre, all'Amministrazione, entro 10 giorni lavorativi dalla sottoscrizione del Contratto esecutivo, idonea reportistica volta a documentare il rispetto dell'impegno eventualmente assunto con riguardo al criterio C18, pena l'applicazione delle penali del relativo indicatore di qualità di cui all'Appendice 2A.
Nel corso dell'esecuzione del Contratto esecutivo, l'Amministrazione potrà aggiornare il Piano dei fabbisogni e richiedere aggiornamenti del Piano Operativo in termini di tipologia di servizi e quantità ogni qualvolta lo ritenga necessario, nel rispetto delle previsioni di cui all'art. 106 del D.Lgs. 50/2016, del Comunicato ANAC 13 marzo 2021 nonché dell'importo massimo dell'Accordo Quadro.

6.5 Adesione al Lotto 2 - Servizi di Compliance e Controllo dell'Accordo Quadro

Nel caso di adesione all'Accordo Quadro per i servizi di Compliance e controllo, affideranno i Contratti Attuativi, successivamente alla stipula dell'Accordo Quadro e per tutta la durata dello stesso, alle medesime condizioni (economiche e tecnico-prestazionali) stabilite nell'Accordo Quadro ai Fornitori aggiudicatari ai sensi dell'art. 54, comma 3, del D. Lgs. n. 50/2016.

In particolare, per l'AQ verrà attribuita in sede di aggiudicazione:

- una quota pari al 60% del massimale del Lotto 2 all'Operatore economico risultato 1° nella graduatoria di merito (Amministrazioni beneficiarie PAL);
- una quota pari al 40% del massimale del Lotto 2 all'Operatore economico risultato 2° nella graduatoria di merito (Amministrazioni beneficiarie PAC).

L'affidamento di ciascun Contratto esecutivo avverrà con le modalità di seguito descritte.

6.5.1 Piano dei Fabbisogni

L'Amministrazione trasmetterà, a mezzo PEC, al fornitore aggiudicatario, e contestualmente alla Consip S.p.A. (e/o a terzi dalla stessa indicati), il "**Piano dei Fabbisogni**" (o "**Ordinativo di fornitura**"), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo 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.
In particolare, il "Piano dei fabbisogni" conterrà, a titolo esemplificativo e non esaustivo, i seguenti elementi:

- Indicazione 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;
- la categorizzazione dell'intervento;
- il comparto di appartenenza (PAC/PAL);
- l'importo contrattuale e le quantità previste per i servizi oggetto di fornitura;
- la data di attivazione di ciascun servizio oggetto di fornitura;
- la durata del Contratto esecutivo e dei singoli servizi;
- le modalità di erogazione e consuntivazione dei servizi di fornitura;
- per ciascun servizio richiesto, la metrica di misurazione, dimensionamento, luogo 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 della fornitura;
- ogni altra eventuale indicazione riportata nell'Appendice 3 inerente agli specifici servizi richiesti, come ad esempio un documento allegato con il contesto tecnologico e applicativo;
- l'eventuale cronoprogramma ai fini dell'anticipazione del prezzo, ove applicabile.

Si precisa che, ove richiesto dall'Amministrazione, il Fornitore dovrà impegnarsi obbligatoriamente a supportare la stessa nella redazione del Piano dei fabbisogni.
Con specifico riferimento ai servizi da svolgere presso i siti delle Amministrazioni, 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).
Il Fornitore dovrà approntare, ove necessario ed entro 15 gg lavorativi dalla richiesta (o salvo diverso accordo tra le parti), il calendario dei sopralluoghi necessari, che dovrà indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal Fornitore 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 trasmissione del Piano dei fabbisogni da parte dell'Amministrazione verso il Fornitore selezionato non scaturisce alcun obbligo per l'Amministrazione di procedere alla stipula del Contratto esecutivo con il Fornitore aggiudicatario.

6.5.2 Piano Operativo

Il Fornitore, 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, a mezzo PEC, all'Amministrazione che ne abbia fatto richiesta, nonché a Consip S.p.A. e/o terzi da essa indicati.
In particolare, fermo quanto previsto nell'Appendice 3 del Lotto di servizi di Compliance e controllo, il Fornitore aggiudicatario, mediante il "Piano Operativo", dovrà formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti.
Il Piano Operativo dovrà indicare, a titolo esemplificativo e non esaustivo, i seguenti aspetti in coerenza al Piano dei Fabbisogni:

- la categorizzazione dell'intervento;
- il comparto di appartenenza (PAC/PAL);
- l'importo contrattuale e le quantità previste per i servizi oggetto di fornitura;
- l'identificativo del servizio;
- la data di attivazione del servizio di fornitura;
- l'indicazione del/i luogo/ghi di esecuzione della fornitura;
- la durata del Contratto esecutivo e dei servizi;
- 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;
- quota e prestazioni che intenderà subappaltare, nel rispetto delle previsioni di quanto indicato nel Piano dei fabbisogni.

Il Piano Operativo, inoltre, dovrà contenere:

- un piano di lavoro generale coerente con il fabbisogno, che rappresenta la totalità dei servizi richiesti e rappresenta le attività propedeutiche all'attivazione dei servizi, e che potrà essere aggiornato successivamente alla stipula del Contratto esecutivo previo accordo con l'Amministrazione. Come previsto nell'Appendice 3 relativa al lotto di servizi di Compliance e controllo, tale piano dovrà contenere al proprio interno anche il piano di Presa in carico;
- un Piano della Qualità specifico di Contratto esecutivo (ad integrazione del Piano della Qualità Generale che dovrà essere trasmesso alla Consip S.p.A. ai sensi del successivo paragrafo 7.1.1), 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 che verranno impiegate per l'erogazione dei servizi, con le relative certificazioni richieste e/o proposte in offerta tecnica;
- la proposta operativa coerente rispetto al documento di contesto tecnologico e applicativo allegato al Piano dei Fabbisogni.

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.
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 ai fini dell'applicazione della relativa penale.

6.5.3 Contratto esecutivo

L'Amministrazione, entro 30 giorni solari dalla relativa ricezione, ha la facoltà di approvare il "Piano Operativo", ovvero di comunicare la richiesta di eventuali modifiche e/o integrazioni, nel rispetto del Piano dei fabbisogni. In tal caso l'aggiudicatario dovrà apportare al documento presentato le modifiche e/o integrazioni richieste.
L'aggiudicatario dovrà inviare la versione definitiva del Piano Operativo entro 10 giorni solari dalla comunicazione di richiesta dell'Amministrazione Contraente.
Da tale data decorrerà nuovamente il termine di 30 giorni solari di cui al periodo precedente.
Qualora, decorsi 30 giorni solari dalla ricezione del Piano Operativo, l'Amministrazione non lo abbia approvato ovvero non ne abbia richiesto la modifica ovvero non abbia richiesto ulteriori giorni per la relativa verifica, il relativo Piano dei fabbisogni precedentemente trasmesso dall'Amministrazione si intenderà decaduto.
Il Contratto si perfeziona in seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione del Piano operativo da parte dell'operatore economico sulla base dell'apposito schema allegato alla documentazione di gara. Esso conterrà altresì ogni altro aspetto rilevante per l'esecuzione del singolo contratto, in ragione di quanto stabilito nel presente documento e nelle Appendici.
Nel caso di Contratto esecutivo affidato da un Soggetto Aggregatore, il medesimo Contratto esecutivo inoltre:

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

Il Fornitore dovrà produrre, all'Amministrazione, entro 10 giorni lavorativi dalla sottoscrizione del Contratto esecutivo, idonea reportistica volta a documentare il rispetto dell'impegno eventualmente assunto con riguardo al criterio P15, pena l'applicazione delle penali del relativo indicatore di qualità di cui all'Appendice 3A.

Nel corso dell'esecuzione del Contratto esecutivo, l'Amministrazione potrà aggiornare il Piano dei fabbisogni e richiedere aggiornamenti del Piano Operativo in termini di tipologia di servizi e quantità ogni qualvolta lo ritenga necessario, nel rispetto delle previsioni di cui all'art. 106 del D.Lgs. 50/2016, del Comunicato ANAC 13 marzo 2021 nonché dell'importo massimo dell'Accordo Quadro.

6.6 Categorizzazione degli interventi

All'atto di definizione del Piano dei Fabbisogni, l'Amministrazione individuerà e censirà l'ambito del Piano Triennale di riferimento per la specifica acquisizione, definendo ove possibile:

- l'ambito di I livello,
- Uno o più ambiti di II livello, indicando come primo il prevalente.

Tale categorizzazione dovrà essere riportata in tutta la documentazione contrattuale:

- Piano dei Fabbisogni,
- Piano Operativo,
- Contratto esecutivo.

Ambito (layer)	Obiettivi PT
Servizi	• Servizi al cittadino • Servizi a imprese e professionisti • Servizi interni alla propria PA • Servizi verso altre PA

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

7 Requisiti Organizzativi

7.1 Aspetti organizzativi di carattere generale

Il Fornitore di ogni lotto dovrà assicurare una quota pari almeno al 30% (quota migliorabile in accordo al criterio C18 o P15 di cui alle Informazioni sulla Procedura) delle assunzioni necessarie per l'esecuzione dei contratti esecutivi finanziati, 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, o per la realizzazione di attività ad essi connesse o strumentali, all'occupazione femminile e di giovani di età inferiore a 36 anni. In caso di inadempimento sarà prevista l'azione contrattuale di cui all'art. 47, comma 6, D.L. n. 77/2021.

7.1.1 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 fornire, su richiesta della Consip/Amministrazione, la base dati di dettaglio secondo apposito formato standard che sarà indicato, contenente tutti i dati rilevati, utilizzata per la valorizzazione degli indicatori di qualità.
Su richiesta della Consip/Amministrazione, il Fornitore dovrà predisporre delle rappresentazioni dell'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 2A e 2B.
Si precisa che tutte le prescrizioni del presente documento e delle appendici sono requisiti minimi, ai quali si aggiungono gli impegni assunti in offerta tecnica. Il mancato rispetto costituisce inadempimento.

***

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 delle Appendici 2A e 3A relative ai livelli di servizio e 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.
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 referenti 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 2A e 3A relative agli indicatori di qualità;
- dettaglia i metodi di lavoro messi in atto dal fornitore, facendo riferimento o a procedure relative al proprio sistema, e per ciò 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, le Amministrazioni e il Organismo tecnico di Coordinamento e Controllo (per il Lotto ove è previsto);
- garantisce un'efficace e rapido coordinamento con i Piani della Qualità specifici di Contratto esecutivo richiesti per i singoli Contratti Attuativi.

7.1.2 Risorse impiegate

Ferme restando le competenze professionali richieste nell'Appendice 2 "Contesto tecnico - Lotto 1" e nell'Appendice 3 "Contesto tecnico - Lotto 2" e relative loro 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, nonché nel garantire 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 aggiornati 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 i titoli e le 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 2A e 3A relative agli indicatori di qualità di ciascun lotto.

7.2 Ruoli di coordinamento richiesti

Il Fornitore è tenuto ad impiegare i referenti tecnici di seguito indicati, quali ruoli minimi di coordinamento delle attività contrattuali previste. In caso di inadeguatezza, impreparazione e/o incompetenza, il referente dovrà immediatamente essere sostituito con una figura rispondente ai requisiti minimi richiesti e con l'eventuale applicazione dei rilievi e/o delle penali contrattualmente previsti.
Per tutti i referenti 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.
Si fa presente inoltre che tutti i referenti tecnici devono essere disponibili ad operare presso l'Amministrazione ove necessario e/o richiesto per l'espletamento di tutte le attività contrattuali, secondo quanto esposto ai paragrafi successivi.
Tali presenze non dovranno comportare alcun onere aggiuntivo per l'Amministrazione e, pertanto, tutti i referenti tecnici richiesti e/o offerti non potranno far parte di alcuno dei gruppi di lavoro relativi ai servizi oggetto della fornitura.

7.2.1 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). Il RUAC dovrà riferire, per quanto di competenza, alla Consip S.p.A. e/o (ove richiesto) al Organismo tecnico di Coordinamento e Controllo (in caso di RUAC dell'Accordo Quadro) o alle Amministrazioni (in caso di RUAC del Contratto esecutivo) su tutte le tematiche contrattuali, quali ad esempio:

- 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.);

- pieno adempimento degli impegni assunti in offerta tecnica;
- correttezza e tempestività dell'utilizzo del Portale della fornitura, degli strumenti di supporto alle Amministrazioni e degli strumenti in uso presso l'Amministrazione e/o proposti in offerta tecnica;
- predisposizioni e variazioni dei Piani di lavoro della fornitura;
- predisposizione dei Piani della Qualità Specifici di Contratto esecutivo e garanzia del rispetto del Piano della Qualità Generale e delle specificità dei servizi richiesti;
- 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;
- verifica dei risultati sugli indicatori di qualità;
- 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;
- eventuali azioni da intraprendere per migliorare l'erogazione dei servizi e valutarne i risultati ottenuti;
- pianificazione ed impiego di risorse quantitativamente e qualitativamente adeguate;
- gestione delle criticità e dei rischi complessivi di progetto risolvendo tutti i potenziali conflitti e/o eventuali disservizi;
- 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;
- garanzia di unitarietà, integrazione, omogeneità e sinergia nelle singole erogazioni dei servizi;
- adozione di idonei strumenti per facilitare la comunicazione e lo scambio di informazioni tra i vari attori coinvolti nella Fornitura;
- assicurazione di 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;
- eventuali azioni correttive proposte a fronte di situazioni critiche.

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

- garantire il presidio su tutto il comparto di riferimento del lotto attraverso il pronto supporto alle Amministrazioni richiedenti;
- raccogliere, condividere e presentare, almeno trimestralmente, agli Organismi di coordinamento e controllo l'andamento delle forniture, nonché garantire l'uniformità e standardizzazione delle metodologie e degli strumenti;
- rendere disponibili alla Consip S.p.A. e all'Organismo tecnico di Coordinamento e Controllo visite periodiche di sintesi sull'andamento dei contratti e sulle attività di supporto alle Amministrazioni;
- gestire a livello territoriale quanto previsto per la figura del RUAC, interfacciandosi, ove necessario con i Responsabili tecnici per l'erogazione dei servizi.

Il profilo professionale minimo per la figura del RUAC dell'Accordo Quadro e dei RUAC dei Contratti Esecutivi dovrà corrispondere al Security Principal.
Il RUAC dell'Accordo Quadro, inoltre, dovrà avere una qualifica dirigenziale, con appositi poteri di firma tali da impegnare l'impresa/RTI/Consorzio nei confronti della Consip S.p.A.
Il RUAC del singolo Contratto esecutivo dovrà disporre di poteri di firma tali da impegnare in maniera esecutiva l'impresa/RTI/Consorzio nei confronti delle Amministrazioni.
Unitamente al Piano operativo il Fornitore dovrà fornire il nominativo e il relativo CV per il RUAC del Contratto esecutivo.

7.2.2 Referenti tecnici per l'erogazione dei servizi

I Referenti Tecnici per l'erogazione dei servizi sono le figure del Fornitore responsabili delle attività di erogazione dei servizi.
In considerazione della natura delle attività da svolgere e a garanzia dell'operatività dei servizi, i Referenti tecnici devono essere reperibili telefonicamente nelle fasce orarie di erogazione del servizio e in caso di estensione dello stesso sempre tramite posta elettronica, senza oneri aggiuntivi.
Il Fornitore dovrà mettere a disposizione i seguenti Referenti Tecnici:

- Servizi di sicurezza da remoto (Lotto 1): un referente tecnico per ciascun Contratto esecutivo e comunque per ciascuna Amministrazione per tutti i servizi indicati nell'Appendice 2 relativa al suddetto Lotto.
- Servizi di Compliance e Controllo (Lotto 2): un referente tecnico per ciascun Contratto esecutivo e comunque per ciascuna Amministrazione per tutti i servizi indicati nell'Appendice 3 relativa al suddetto Lotto.

I suddetti referenti 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 dall'Appendice 2 "Contesto tecnico - Lotto 1" e dall'Appendice 3 "Contesto tecnico - Lotto 2" e relative loro Appendici.
A titolo esemplificativo si riportano le attività principali in carico alle diverse tipologie di referenti tecnici.

I Referenti tecnici, in relazione alle varie tipologie di servizi oggetto di fornitura, 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.

Il profilo professionale minimo per la figura di responsabile del servizio dovrà corrispondere al Security Principal.

7.3 Collaudo 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 documento potrà essere soggetta alle seguenti procedure di collaudo:

- collaudo funzionale (Test Bed) svolto da Consip/AgID che, successivamente alla stipula di ciascun Contratto Quadro, potranno richiedere nel corso della durata contrattuale delle prove mirate a verificare le modalità con le quali il Fornitore erogherà i servizi oggetto della presente gara. Tale richiesta è inerente i servizi elencati nel paragrafo 1.1, ferma restando la facoltà di Consip/Agid di integrare tale elenco;
- collaudo di configurazione, svolto dalla singola Amministrazione contraente e volto a verificare la corretta erogazione dei servizi acquisiti dall'Amministrazione.

7.3.1 Collaudo funzionale

Il Fornitore dovrà mettere a disposizione una piattaforma di Test Bed presso sedi individuate congiuntamente con CONSIP/AgID 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:

- il portale della fornitura;
- i servizi oggetto di erogazione in termini di infrastrutture hardware e software;
- gli strumenti di monitoraggio e controllo della fornitura.

Ai fini dell'esecuzione delle prove di Collaudo, il Fornitore dovrà predisporre un documento intitolato "Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (*test bed*)" contenente almeno:

- il sistema di misura dei livelli di servizio e di generazione della reportistica;
- la modalità di svolgimento delle prove di collaudo.

Il Documento sopra descritto dovrà essere reso disponibile dal Fornitore entro 30 giorni lavorativi dalla richiesta di Consip/AgID. A partire dal 15esimo giorno successivo alla ricezione della documentazione di cui sopra da parte di Consip/AgID, il fornitore dovrà rendersi disponibile all'avvio dei collaudi.
Consip/AgID si riservano di chiedere adeguamenti al documento di cui sopra, che il Fornitore dovrà recepire e formalizzare in una nuova versione del documento entro 15 giorni dalla richiesta.
Il buon esito del collaudo sarà comunicato da Consip/AgID 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 dalla stazione appaltante, e comunque non inferiori a 5 (cinque) giorni lavorativi. Decorso detto termine, si potrà procedere ad una seconda prova di collaudo in test bed.
Consip/AgID si riservano 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.

Nel collaudo funzionale, Consip/AgID si riservano 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/AgID si riservano 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, nel periodo di vigenza contrattuale, dei requisiti richiesti.

7.3.2 Collaudo di configurazione e di conformità

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 nell'Appendice 2 e nell'Appendice 3.

Le verifiche di conformità delle prestazioni sono volte ad accertare, periodicamente nel corso della fornitura, che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale. La responsabilità dell'esecuzione della Verifica di conformità è dell'Amministrazione, che esegue l'attività con il supporto del fornitore.
Il Fornitore dovrà obbligatoriamente effettuare quanto segue.
Il Fornitore dovrà fornire il supporto all'Amministrazione contraente in tutte le attività necessarie alle suddette prove di collaudo e alle verifiche di conformità.
Il Fornitore dovrà consegnare (entro i tempi previsti nel Piano dei Fabbisogni) all'Amministrazione 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.

Il Fornitore dovrà altresì impegnarsi, qualora richiesto dall'Amministrazione, a svolgere ulteriori prove integrative. L'Amministrazione può procedere, a sua discrezione, ad un collaudo a campione.

7.4 Verifiche e test ai sensi del DL 105/2019

Il D.L. 105/2019 convertito in Legge n. 133/2019 «recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica», prevede l'istituzione di un perimetro di sicurezza nazionale cibernetica, finalizzato ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione o la prestazione di un servizio essenziale dello Stato e dal cui malfunzionamento/interruzione possa derivare un pregiudizio per la sicurezza nazionale.

In riferimento al suddetto Decreto Legge e al Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 ed ai regolamenti di successiva emanazione, il Centro di Valutazione e Certificazione Nazionale (CVCN) istituito presso il Ministero dello Sviluppo Economico e trasferito dal D.L. 82/2021 presso **l'Agenzia Nazionale per la Cybersicurezza** o il Centro di Valutazione (CV) istituito presso il Ministero dell'Interno o della Difesa o **Laboratori Accreditati di Prova (LAP)** accreditati dal CVCN**,** potranno effettuare verifiche preliminari, ed eventualmente imporre condizioni e test di sicurezza su hardware e software, secondo un approccio gradualmente crescente, dei servizi oggetto di fornitura, nonché verifiche e ispezioni.
Procedure, modalità e termini relative alle verifiche e test sono stabilite mediante il suddetto regolamento ai sensi dell'art. 1 comma 6, legge n. 133/2019. Il Fornitore dovrà fornire il supporto al CVCN/ CV/LAP in tutte le attività necessarie alle suddette verifiche e test; in particolare si indicano a titolo indicativo e non esaustivo:

a. fornire evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni sulla base dei requisiti di sicurezza espressi dalla normativa
b. provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio;
c. fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni;
d. fornire una descrizione delle funzioni di sicurezza implementate nell'oggetto di valutazione;
e. fornire una descrizione dei test funzionali e di sicurezza eventualmente già eseguiti dal fornitore, dal produttore o da terza parte, comprensivi dei relativi risultati.

Per le spese a carico del fornitore in conseguenza delle attività di valutazione svolte da CVCN e CV e per le attività di test svolte dai LAP si dovrà fare specifico riferimento alla normativa specifica.

8 GOVERNANCE

8.1 Organismo tecnico di coordinamento e controllo - Compiti operativi

Come indicato al paragrafo 4.2, è previsto un Organismo tecnico di coordinamento e controllo, il quale, per la presente iniziativa avrà dei compiti specifici per i diversi lotti, fermo restando i compiti generali previsti al summenzionato paragrafo.
In tal caso, l'Organismo tecnico coinvolgerà i fornitori aggiudicatari che nomineranno in via ufficiale uno o più rappresentanti, restando inteso che per ogni seduta solo un membro avrà diritto di voto.
Ogni decisione vincolante potrà essere presa soltanto a maggioranza assoluta dei membri.
I rappresentanti dei fornitori dovranno essere dotati di adeguati poteri di firma, come dimostrato da apposita documentazione inviata a Consip S.p.A., a seguito di specifica richiesta alla quale dovranno rispondere entro 10 gg lavorativi.
Le sessioni dell'Organismo tecnico saranno convocate con almeno 5 gg solari di preavviso e tramite mail dal Presidente dell'Organismo, che l'Organismo stesso nominerà a maggioranza semplice nella prima seduta e con specifico ed esclusivo riferimento alle funzioni operative di cui al seguente paragrafo. La prima seduta sarà convocata da Consip S.p.A.

8.2 Compiti specifici - Lotto 1

Allo scopo di armonizzare l'indirizzo strategico e le misure di governance della fornitura, l'Organismo tecnico di Coordinamento e Controllo potrà attuare specifiche attività di direzione tecnica per verificare i risultati attesi dalla erogazione dei servizi di sicurezza da remoto. In particolare:

i. supervisione del funzionamento complessivo dei servizi previsti nell'Accordo Quadro e valutazione, con periodicità annuale, dell'adeguatezza delle disposizioni dell'Accordo Quadro ed eventuale formulazione di proposte di emendamento da sottoporre alle parti;
ii. verifica, con periodicità trimestrale, dello stato di avanzamento dell'Accordo Quadro;
iii. facoltà di modificare le modalità di esecuzione della fornitura, di introdurre nuove modalità, di definire/modificare gli attuali standard, anche in corso d'opera.
iv. verifica con periodicità trimestrale dei Livelli di Servizio;
v. riesamina i livelli di servizio; il riesame potrà derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli indicatori di qualità che sono risultate non efficaci.
vi. proposta di inserimento di nuovi prodotti/servizi, complementari ai servizi già oggetto della presente fornitura nel rispetto dei massimali contrattuali, che potranno essere resi dal Fornitore alle Amministrazioni, come da procedura definita nel successivo paragrafo 8.2.1 del presente documento;
vii. proposta dei prezzi dei nuovi servizi di cui al precedente punto;

Inoltre, l'Organismo tecnico di Coordinamento e Controllo potrà eseguire:

viii. verifica della rispondenza dei Piani Operativi secondo quanto disposto nel Capitolati Tecnico Generale e Speciale;
ix. esame del Piano Operativo di servizi su richiesta dell'Amministrazione interessata;
x. esame degli interventi di manutenzione programmata che comportino l'interruzione della fornitura dei servizi.
xi. la verifica del possesso delle certificazioni e l'utilizzo delle risorse certificate nell'ambito dei contratti esecutivi come dichiarato dal concorrente in offerta tecnica.

L'Organismo tecnico di coordinamento e controllo potrà pertanto, tramite accesso dedicato al Portale di Fornitura o autonomamente, richiedere ed acquisire tutta la documentazione inerente i servizi ed i progetti di sicurezza. Potrà inoltre effettuare attività di analisi e verifica della documentazione prodotta dal Fornitore secondo quanto richiesto nella documentazione di gara ed in particolare: Piano di Fabbisogni, Piano Operativo e tutti i deliverable di fornitura, compresi i documenti eventualmente già in possesso dell'Amministrazione.

8.2.1 Inserimento nuovi servizi

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d.lgs. n. 50/2016.
L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dei due aggiudicatari dell'Accordo Quadro, richiederà agli stessi, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

8.3 Compiti specifici - Lotto 2

8.3.1 Analisi e verifica documentazione

Allo scopo di armonizzare l'indirizzo strategico e le misure di governance della fornitura, l'Organismo tecnico di Coordinamento e Controllo potrà attuare specifiche attività di direzione tecnica per verificare i risultati attesi dalla erogazione dei servizi di compliance e controllo. In particolare:

i. supervisione del funzionamento complessivo dei servizi previsti nell'Accordo Quadro e valutazione, con periodicità annuale, dell'adeguatezza delle disposizioni dell'Accordo Quadro ed eventuale formulazione di proposte di emendamento da sottoporre alle parti;
ii. verifica, con periodicità trimestrale, dello stato di avanzamento dell'Accordo Quadro;
iii. facoltà di modificare le modalità di esecuzione della fornitura, di introdurre nuove modalità, di definire/modificare gli attuali standard, anche in corso d'opera.
iv. verifica con periodicità trimestrale dei Livelli di Servizio;
v. riesamina i livelli di servizio; il riesame potrà derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli indicatori di qualità che sono risultate non efficaci.

Inoltre, l'Organismo tecnico di Coordinamento e Controllo potrà eseguire:

vi. verifica della rispondenza dei Piani Operativi secondo quanto disposto nel Capitolati Tecnico Generale e Speciale;
vii. esame del Piano Operativo di servizi su richiesta dell'Amministrazione interessata;
viii. la verifica del possesso delle certificazioni e l'utilizzo delle risorse certificate nell'ambito dei contratti esecutivi come dichiarato dal concorrente in offerta tecnica.

L'Organismo tecnico di coordinamento e controllo potrà pertanto, tramite accesso dedicato al Portale di Fornitura o autonomamente, richiedere ed acquisire tutta la documentazione inerente i servizi ed i progetti di sicurezza. Potrà inoltre effettuare attività di analisi e verifica della documentazione prodotta dal Fornitore secondo quanto richiesto nella documentazione di gara ed in particolare: Piano di Fabbisogni, Piano Operativo e tutti i deliverable di fornitura, compresi i documenti eventualmente già in possesso dell'Amministrazione.

8.4 Responsabilità dei fornitori

I Fornitori Aggiudicatari, con la stipula dei relativi contratti, si impegnano in ogni caso a recepire obbligatoriamente le indicazioni fornite dall'Organismo tecnico di coordinamento e controllo nei limiti in cui tali le indicazioni derivino **da disposizioni normative cogenti e inderogabili, Regolamenti e Circolari adottate dai Soggetti Istituzionali competenti**, anche alla luce delle prescrizioni future derivanti dall'adozione dei decreti attuativi di cui all'art. 1, commi 2 e 3, D.L. n. 105/2019, e loro rispettivi aggiornamenti, e/o del Regolamento di cui al successivo comma 6 del medesimo articolo.

In relazione alle responsabilità poste a carico del fornitore si faccia riferimento all'Appendice 1 "Governance delle iniziative afferenti al Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 – 2021".

9 STRUMENTI A SUPPORTO DELLA FORNITURA

9.1 Portale della Fornitura

Il Fornitore dovrà rendere disponibile un "Portale della Fornitura", multicanale e raggiungibile tramite Internet, che consenta alle singole Amministrazioni e agli Organismi di coordinamento e controllo di governare agevolmente la fornitura e di promuovere la condivisione e l'esperienza maturata nelle varie iniziative.

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

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

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

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

- "Area Comunicazione": è l'area ad accesso pubblico del portale, contiene informazioni di carattere generale sull'AQ e informazioni e dati specifici dei servizi in erogazione e sull'andamento della fornitura; (a partire dalla I release)
- "Area Informativa": è l'area di supporto riservata alle Amministrazioni e contiene almeno le seguenti informazioni: documentazione aggiornata (normativa, tecnologica e operativa) di riferimento per i servizi dell'AQ; la guida alla misurazione degli effort progettuali per singolo servizio; la descrizione delle soluzioni migliorative offerte. (a partire dalla I release)
- "Area Project Management": è l'area ad accesso riservato e profilato per le singole Amministrazioni contraenti tramite la quale è possibile disporre degli strumenti di attivazione, pianificazione e gestione delle singole attività; dovrà governare l'esecuzione dell'intero workflow operativo di ciascun servizio/attività. (a partire dalla I release)
- "Area Collaborazione e Monitoraggio" è l'area che contiene:
  - gli strumenti e le informazioni di controllo e governo della fornitura quali cruscotti statici e dinamici relativi ai dati di tutti i Piani di Fabbisogno predisposti dall'Amministrazione, i Piani Operativi ed i Contratti Attuativi;
  - reportistica sul rispetto dei livelli di servizio e degli indicatori di digitalizzazione, report statici e dinamici relativi ai valori economici dei Contratti Esecutivi con evidenza della capacità contrattuale residuale; i dati devono essere estraibili nei formati maggiormente diffusi per lo scambio dati (es. csv, xml, json, xls, ecc.).
- "Area Osservatorio": è l'area che consente alla Consip/AgID di svolgere le proprie funzioni di monitoraggio sulla qualità dei servizi erogati in AQ.

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

- Non autenticato: utente generico del World Wide Web (WWW);

- Utente accreditato: ad esempio un fornitore di servizi;
- Amministrazione: l'Amministrazione che ha aderito (o intende aderire) ai servizi oggetto della fornitura;
- Consip e AgID.

Il Portale dovrà essere implementato con certificato perla navigazione esclusiva in HTTPS utilizzando un'infrastruttura hardware e software che il Fornitore stesso provvederà a realizzare e mantenere in esercizio. Il Fornitore procederà alla realizzazione del Portale sulla base di quanto proposto nell'Offerta Tecnica.

Il Portale dovrà essere reso disponibile in una prima release funzionante alla stipula dell'Accordo Quadro e nella versione completa all'attivazione dei servizi del primo Contratto esecutivo di fornitura sottoscritto. Esso dovrà essere reso disponibile con continuità alle Amministrazioni contraenti, a AgID, a Consip S.p.A. nonché a terzi soggetti da essa indicati, e ad eventuali strutture da essi delegate per tutta la durata contrattuale ed aggiornato con frequenza almeno mensile, entro il 15 del mese successivo al mese di riferimento.

Il portale dovrà essere gestito globalmente dal Fornitore che assume la responsabilità di garantire:

- hosting della piattaforma;
- gestione e manutenzione del portale;
- aggiornamento dei contenuti e la corretta alimentazione del sito;
- disponibilità in linea per le Amministrazioni, AgID, Consip e/o soggetti terzi da essa indicati;
- gestione degli accessi agli utenti abilitati mediante credenziali di riconoscimento (es., login e password);
- presenza di un manuale di utilizzo del portale e dei singoli sistemi integrati;
- disponibilità di un servizio di supporto tecnico e funzionale agli utenti.

Tutta la reportistica prodotta relativa ai servizi dovrà essere archiviata e conservata a cura del Fornitore, attraverso un sistema di gestione della documentazione riservata.

Il Portale dovrà esporre almeno:

- il Piano dei Fabbisogni;
- il Piano Operativo;
- il Contratto esecutivo;
- lo stato di ciascuna iniziativa;
- workflow operativi di ciascun servizio.

Ad avvenuta attivazione di un Contratto esecutivo il Portale consentirà, attraverso gli strumenti disponibili, il governo della fornitura, con la consultazione dei piani di lavoro aggiornati, la reportistica dei livelli di qualità, la pianificazione di riunioni e incontri di SAL, le notifiche sulle scadenze.

Per garantire la consistenza e l'attualizzazione delle informazioni presenti nel Portale il Fornitore dovrà integrarlo con gli strumenti in uso presso l'Amministrazione, quali ad esempio sistemi di ticketing e/o di rilevazione delle performance.