AGENZIA REGIONALE PROTEZIONE AMBIENTALE DELLA CAMPANIA

DELIBERAZIONE DEL DIRETTORE GENERALE N. 566 DEL 14/11/2024

IL RUP LA VIA

OGGETTO: AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006. NUOVA ADESIONE ACCORDO QUADRO "SERVIZI DI SICUREZZA DA REMOTO, COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296, LOTTO 1 "SERVIZI DI SICUREZZA DA REMOTO". CIG B4225E190D.

L'anno duemilaventiquattro, il giorno quattordici del mese di Novembre presso la sede dell'A.R.P.A.C. alla stregua dell'istruttoria compiuta dal RUP e della dichiarazione di completezza e regolarità resa dal medesimo

PREMESSO CHE

- con deliberazione n. 532 del 14.11.2018 l'ARPAC ha nominato il Responsabile per la Transizione al Digitale, ai sensi dell'articolo 17 del rinnovato decreto legislativo 82/2005 (Codice dell'Amministrazione Digitale), individuandolo nella dott.ssa Loredana La Via, dirigente della UO Sistemi Informativi e Informatici, cui sono affidati i compiti di conduzione del processo di transizione alla modalità operativa digitale e dei conseguenti processi di riorganizzazione, finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
- tra i compiti affidati al RTD rientra quello inerente indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi ed alle infrastrutture, anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, c. 1 del citato CAD;
- la nuova direttiva europea NIS 2 (Direttiva n. 2022/2555, entrata in vigore il 17 gennaio 2023 << … *relativa a misure per un livello comune elevato di cybersicurezza nell'Unione,….* > che abroga la precedente Direttiva (UE) 2016/1148 - "Direttiva NIS 1"), recepita in Italia con il novello D. Lgs. 138/2024 ed entrata in vigore a partire dal 16.10.2024, mira a garantire l'aumento del livello di sicurezza informatica delle Pubbliche Amministrazioni del Paese ed introduce, tra l'altro, misure più stringenti e specifiche in termini di cyber risk management e di segnalazione e *condivisione* delle informazioni relative agli incidenti di sicurezza, al fine di garantire un livello elevato di sicurezza informatica in ambito nazionale e contribuire ad incrementare il livello della stessa in Unione Europea in modo da migliorare il funzionamento del mercato interno;
- secondo l'Osservatorio Cybersecurity & Data Protection la protezione contro i rischi di tipo cyber sta diventando sempre più una priorità di investimento in Italia, con il 67% delle imprese italiane ad aver segnalato un incremento dei casi di attacco, molti dei quali andati a segno;
- in questo scenario l'*endpoint* (che si tratti di laptop, tablet, PC o smartphone o di periferiche associate come le stampanti) è il "cuore" del problema, essendo questi dispositivi un punto di accesso privilegiato per gli hacker: infatti, l'84% dei responsabili della sicurezza afferma

che l'endpoint è il focus della maggior parte delle minacce e dove si verificano le più gravi violazioni informatiche per le Aziende;

- in attesa di alcune decisioni inerenti un SOC centralizzato da parte di Regione Campania, con deliberazione n. 731 del 21.12.2023 l'Agenzia ha aderito all'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296 – Lotto 1*, per solo n. 6 mesi, relativamente ai seguenti servizi:
  - L1.S1: Servizio SOC - Security Operation Center
  - L1.S15: Servizi specialistici;
- non avendo avuto più notizie del SOC centralizzato di cui sopra, nelle more della predisposizione del Piano dei Fabbisogni per l'adesione all'AQ con scadenza definitiva, con nota prot. n. 49579 del 02.08.2024 indirizzata alla Mandataria dell'RTI si è resa necessaria ed indispensabile la richiesta di proroga dei suddetti servizi, in scadenza al 31.08.2024, per garantire continuità e copertura all'Agenzia in materia di cybersicurezza, proroga prevista appunto per il tempo necessario a stilare un nuovo Piano dei Fabbisogni agenziale completo, con previsione della copertura dai rischi cyber per 48 mesi;
- in data 30.08.2024 è pervenuto, da parte della società Accenture S.p.A, il riscontro positivo alla suddetta istanza (nota prot. n. 53671 del 30.08.2024);
- con deliberazione n. 518 del 18.10.2024 è stata quindi formalizzata la proroga tecnica per un periodo pari a 2 mesi e ½, pertanto fino alla data del 15 novembre 2024;
- l'Agenzia per la Cybersicurezza Nazionale – ACN – con determina prot. n. 5959 del 26 febbraio 2024 recante «*Avviso Pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5*», ha approvato gli atti costituenti l'Avviso 08/2024 in materia di Cybersicurezza, a cui l'Agenzia ha presentato domanda di partecipazione con nota prot. n. 23488 del 12.04.2024;
- con determina ACN prot. n. 30550 del 23.09.2024 è stato approvato l'aggiornamento degli elenchi predisposti dalla Commissione di valutazione e, conseguentemente, la graduatoria definitiva a valere sull'Avviso 8/2024, di cui costituisce parte integrante e sostanziale l'Allegato A **"**Graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili" tra le quali risulta presente la proposta di progetto di ARPA Campania, ammessa a finanziamento per l'intero importo richiesto, ossia € 1.262.713,42 IVA inclusa;

CONSIDERATO CHE

- la UO Sistemi Informativi e Informatici ha redatto il nuovo, definitivo, Piano dei Fabbisogni contenente le indicazioni sulla tipologia dei servizi, il loro dimensionamento e le quantità richieste per una durata di 48 mesi, come da tempistiche dell'Accordo Quadro in questione, e lo ha trasmesso al RTI Fornitore in data 22.10.2024 con prot. n. 65598;
- il RTI Fornitore ha predisposto e trasmesso all'Agenzia, in data 05.11.2024 con prot. n. 68592, il 'Piano Operativo' esplicativo dei servizi richiesti dall'Ente, corredati dei costi ottenuti applicando i prezzi unitari di cui all'Accordo Quadro;
- come da progetto ARPAC ammesso al finanziamento PNRR, la prima annualità (2025) di servizi in Accordo Quadro ID 2296, Lotto 1, è coperta tramite i fondi inerenti l'Avviso ACN

n. 8/2024 relativi a Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” – Codice d’investimento M1C1I1.5;

- l’Accordo Quadro recita che il ‘Piano dei Fabbisogni’ potrà essere variato e/o aggiornato dall’Amministrazione ogni qualvolta questa lo ritenga necessario;
- il RTI Fornitore dovrà di conseguenza, in tali eventualità, aggiornare il ‘Piano Operativo’ nei tempi e modi come da Contratto;

RITENUTO CHE

- l’Agenzia, in quanto Pubblica Amministrazione, rimane soggetta a tutto quanto disposto dalla Circolare AgID n. 2/2017, recante *“Misure minime di sicurezza ICT per le pubbliche amministrazioni”* ed alla Direttiva NIS2;
- c’è l’esigenza immediata ed improcrastinabile di continuare con i servizi di monitoraggio ed ‘alerting’ degli eventi/minacce di sicurezza al fine di consentire una gestione degli incidenti di sicurezza, dalla fase di identificazione e notifica dell’evento fino alle azioni di contenimento, ripristino e prevenzione, e di prevedere un’adeguata quantità di giornate di servizi specialistici da parte di team di esperti di cybersecurity per dare supporto, gestire e trattare gli eventi di cui sopra;
- il Piano Operativo, prot. n. 68592 del 05.11.2024 inviato dal RTI Fornitore, sia adeguato da un punto di vista prestazionale andando a soddisfare pienamente le esigenze agenziali come sopra specificate;
- si debba procedere, pertanto, all’approvazione dello schema di “Contratto Esecutivo” e del nuovo “Piano Operativo”;

ATTESO CHE tutti gli atti richiamati nella presente deliberazione sono depositati presso l'ufficio proponente;

VISTI

- il Regolamento Europeo sulla Protezione dei Dati Personali (UE 679/2016);
- la Direttiva NIS2 – Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14.12.2022 relativa a misure per un livello comune elevato di cybersicurezza nell’Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 che abroga la Direttiva (UE) 2016/1148;
- il D. Lgs. 36/2023;
- il D. Lgs. n. 138 del 04.09.2024;
- la determina di ACN di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse con aggiornamento del circuito finanziario – n. protocollo 30550 del 23.09.2024;
- la Circolare AgID n. 2/2017, recante *“Misure minime di sicurezza ICT per le pubbliche amministrazioni”;*
- la L. R. 10/98 ed il vigente Regolamento sull'Organizzazione di ARPAC;
- la deliberazione n. 760/2023 di approvazione di Bilancio di previsione esercizio 2024 e pluriennale per il triennio 2024/2026.

Per tutto quanto premesso e considerato si propone di adottare la seguente

DELIBERAZIONE

Per le motivazioni espresse in narrativa che qui si intendono integralmente riportate e trascritte:

- di aderire all'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296 – Lotto 1 "Servizi di Sicurezza da Remoto"*, per un periodo pari a n. 48 mesi (15.11.2024 – 15.11.2028) per l'acquisizione dei seguenti servizi:
  - L1.S1: Security Operation Center (SOC)
  - L1.S5: Threat Intelligence & Vulnerability Data Feed (a partire dal 15.11.2025)
  - L1.S7: Protezione degli end-point
  - L1.S15: Servizi Specialistici;
- di individuare il RTI composto da:
  - Accenture S.p.A.
  - Fastweb S.p.A.
  - Fincantieri NexTech S.p.A.
  - Difesa e Analisi Sistemi S.p.A.

  come Fornitore per la realizzazione esecutiva delle esigenze agenziali in materia di Cybersicurezza;
- di approvare lo "Schema di Contratto esecutivo" per la fornitura dei servizi di sicurezza di cui al Lotto 1 dell'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296* che, allegato alla presente, ne costituisce parte integrante e sostanziale;
- di approvare l'allegato "Piano Operativo", comprensivo dei canoni e dell'utilizzo di figure professionali 'a consumo' per la fornitura, per un periodo di 48 mesi, dei servizi di seguito dettagliati:
  - L1.S1: Security Operation Center (SOC)
  - L1.S5: Threat Intelligence & Vulnerability Data Feed (a partire dal 15.11.2025)
  - L1.S7: Protezione degli end-point
  - L1.S15: Servizi Specialistici;
- di precisare che la presente fornitura, nello specifico relativamente ai servizi da erogare per il primo anno, nel periodo 15.11.2024 – 15.11.2025, è pagabile con parte del finanziamento PNRR - Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5" di cui sopra, per un totale pari ad € 150.000,00 IVA esclusa;
- di puntualizzare, inoltre, che la somma di € 183.000,00 (IVA compresa) è stata impegnata con impegno n. 534/2024 – Capitolo 10563, esercizio 2024;
- di precisare altresì che la somma di € 183.000,00 è stata accertata con accertamento n. 166/2024 – Capitolo 61128, esercizio 2024;
- di impegnare sul capitolo n. 10519 la somma totale di € 871.843,04 (IVA inclusa) così suddivisa per annualità:
  - € 17.484,26 (IVA inclusa) per l'anno 2025;
  - € 293.716,66 (IVA inclusa) per l'anno 2026;
  - € 280.321,06 (IVA inclusa) per le annualità 2027
  - € 280.321,06 (IVA inclusa) per le annualità 2028

a favore del RTI Accenture S.p.A./Fincantieri Nextech S.p.A./Fastweb S.p.A./Deas – Difesa e Analisi Sistemi S.p.A;

- di impegnare sul Capitolo n. 10502 “Utenze” del Bilancio di competenza 2024 e pagare, ai sensi dell’art. 4, c. 3-quater, del D. L. 6 luglio 2012, n. 95, convertito con modificazioni in L. 7 agosto 2012, n. 135, il contributo di cui all’art. 18, c. 3, D. Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010, a favore di CONSIP SpA nella misura dell’8 per mille del valore del contratto esecutivo (IVA esclusa), pari pertanto ad € 6.917,00, da pagare tramite bonifico bancario specificando nella causale “Accordo Quadro per *l’Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – ID2296 – Lotto 1*”;
- di dare atto che gli impegni di spesa di cui sopra sono soggetti alle disposizioni di cui all’art. 56 del D. Lgs. 118/2011;
- di affidare alla UO Sistemi Informativi e Informatici la verifica della regolarità del servizio nonché, a seguito di parere favorevole, l’autorizzazione della proposta di liquidazione trasmessa dall’U.O Bilancio Contabilità e Finanze, previa acquisizione del DURC;
- di precisare che la presente fornitura, per tipologia di prestazione, non è classificabile secondo il Catalogo dei servizi SNPA in quanto trattasi di spesa a carattere generale;
- di demandare alla UO AGCO di procedere con la sottoscrizione del contratto, il cui schema è approvato con la presente deliberazione;
- di disporre, ai sensi dell’art. 3 della L. 136/2010 che tutti i pagamenti a favore del RTI Accenture S.p.A./Fincantieri Nextech S.p.A./Fastweb S.p.A./Deas – Difesa e Analisi Sistemi S.p.A relativi al presente affidamento debbano essere eseguiti tramite conto corrente dedicato di cui al comma 1 dell’art. 3 della Legge n. 136/2010 e mediante bonifico bancario o postale ovvero altri strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni;
- di nominare quale Direttore dell’Esecuzione la dott.ssa La Via Loredana.

Napoli, 05 novembre 2024

IL RUP
dott.ssa Loredana La Via

La proposta di deliberazione è accolta.

Napoli, 14/11/2024

Il Direttore Generale
Avv. Luigi Stefano SORVINO

OGGETTO: AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006. NUOVA ADESIONE ACCORDO QUADRO "SERVIZI DI SICUREZZA DA REMOTO, COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296, LOTTO 1 "SERVIZI DI SICUREZZA DA REMOTO". CIG B4225E190D.

PARERE DI REGOLARITA' AMMINISTRATIVA

Sulla suesposta proposta, avente ad oggetto "AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006. NUOVA ADESIONE ACCORDO QUADRO "SERVIZI DI SICUREZZA DA REMOTO, COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296, LOTTO 1 "SERVIZI DI SICUREZZA DA REMOTO". CIG B4225E190D.", in ordine alla regolarità amministrativo-contabile ed alla copertura finanziaria, si esprime parere favorevole.

Data **14/11/2024**

Il Direttore Amministrativo a.i.

Luca Antonio Esposito / InfoCert S.p.A.

DELIBERAZIONE N° 566 DEL 14/11/2024

ATTESTAZIONE DI PUBBLICAZIONE

Si dichiara che la presente deliberazione è stata affissa all'Albo di questa Agenzia dal giorno 14/11/2024 e vi resterà per gg 15 (quindici) .

Napoli, **14/11/2024**

Il Funzionario Incaricato
Anna De Caprio / InfoCert S.p.A.

DELIBERAZIONE N° 566 DEL 14/11/2024

ATTESTAZIONE DI IMMEDIATA ESEGUIBILITA'

La presente Deliberazione è stata dichiarata immediatamente eseguibile per l'urgenza

Napoli data **14/11/2024**

Il Direttore Generale
Avv. Luigi Stefano SORVINO

Luigi Stefano Sorvino / InfoCert S.p.A.

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO F

ID 2296

SCHEMA DI CONTRATTO ESECUTIVO – LOTTO 1

INDICE

CONTRATTO ESECUTIVO

TRA

_____, con sede in _____, Via _____, C.F. _____, nella persona nella persona di _____, in qualità di _____, giusta i poteri conferitigli da _____in data _____ (nel seguito per brevità anche "***Amministrazione***"),

E

_____, sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, Via ___, in persona del ___ e legale rappresentante Dott. ___, giusta poteri allo stesso conferiti da ___ (nel seguito per brevità anche "Fornitore");

OPPURE

- _____, sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, Via ___, in persona del ___ e legale rappresentante Dott. ___, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa la mandante _____ ___ con sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, via ___, e la mandante ___, con sede legale in ___, Via ___, capitale sociale Euro ___=, iscritta al Registro delle Imprese di ___ al n. ___, P. IVA ___, domiciliata ai fini del presente atto in ___, via ___, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in _____ dott. _____ repertorio n. _____;

(nel seguito per brevità congiuntamente anche "Fornitore" o "Impresa")

PREMESSO CHE

(A) l'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, ha stabilito che Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311";

(B) L'articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip S.p.A. di concludere Accordi Quadro a cui le Stazioni Appaltanti, possono fare ricorso per l'acquisto di beni e di servizi.

(C) Peraltro, l'utilizzazione dello strumento dell'Accordo Quadro e, quindi, una gestione in forma associata della procedura di scelta del contraente, mediante aggregazione della domanda di più soggetti, consente la razionalizzazione della spesa di beni e servizi, il supporto alla programmazione dei fabbisogni, la semplificazione e standardizzazione delle procedure di acquisto, il conseguimento di economie di scala, una maggiore trasparenza delle procedure di gara, il miglioramento della responsabilizzazione e del controllo della spesa, un incremento della specializzazione delle competenze, una maggiore efficienza nell'interazione fra Amministrazione e mercato e, non ultimo, un risparmio nelle spese di gestione della procedura medesima.

(D) In particolare, in forza di quanto stabilito dall'art. 1, comma 514, della legge 28 dicembre 2015, n.208 (Legge di stabilità 2016) ,"Ai fini di cui al comma 512," – e quindi per rispondere alle esigenze delle amministrazioni pubbliche e delle società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 19 – "Consip S.p.A. o il soggetto aggregatore interessato sentita l'Agid per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. […] Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni".

(E) L'art. 20, comma 4, del D.L. n. 83/2012, come convertito con modificazioni dalla Legge 7 agosto 2012, n. 134, ha affidato a Consip S.p.A., a decorrere dalla data di entrata in vigore della legge di conversione del decreto medesimo, "le attività amministrative, contrattuali e strumentali già attribuite a DigitPA, ai fini della realizzazione e gestione dei progetti in materia, nel rispetto delle disposizioni del comma 3".

(F) Ai fini del perseguimento degli obiettivi di cui al citato Piano triennale per l'informatica nella Pubblica Amministrazione, e che in esecuzione di quanto precede, Consip S.p.A., in qualità di stazione appaltante e centrale di committenza, ha indetto con Bando di gara pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. ____ del _____ e nella Gazzetta Ufficiale dell'Unione Europea n. _____ del _____, una procedura aperta per la stipula di un Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, ai sensi dell'art. 54, comma 4, lett. a) del D. Lgs. n. 50/2016, con più operatori.

(G) Il Fornitore è risultato aggiudicatario della quota PAL del Lotto 1 della predetta gara, ed ha stipulato il relativo Accordo Quadro in data _____.

(H) In applicazione di quanto stabilito nel predetto Accordo Quadro, ciascuna Amministrazione Contraente utilizza il medesimo per la stipula di Contratti esecutivi, secondo quanto disciplinato nell'Accordo Quadro stesso.

(I) L'Amministrazione Contraente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto esecutivo, in conformità alle previsioni di cui al Capitolato Tecnico Generale.

(J) Il Fornitore dichiara che quanto risulta dall'Accordo Quadro e dai suoi allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico (Generale e Speciale) dell'Accordo Quadro, nonché dal presente Contratto esecutivo e dai suoi allegati, definisce in modo adeguato e completo gli impegni assunti con la firma del presente Contratto, nonché l'oggetto dei prodotti e dei servizi connessi da fornire e, in ogni caso, che ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica degli stessi e per la formulazione dell'offerta che ritiene pienamente remunerativa;

(K) il CIG del presente Contratto Esecutivo è il seguente: _____;

(L) <*ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3*> il CUP (Codice Unico Progetto) del presente Contratto Esecutivo è il seguente: _____;

TUTTO CIÒ PREMESSO SI CONVIENE E SI STIPULA QUANTO SEGUE:

1. DEFINIZIONI

1.1 I termini contenuti nel presente Contratto esecutivo hanno il significato specificato nell'Accordo Quadro e nei relativi Allegati, salvo che il contesto delle singole clausole disponga diversamente.

1.2 I termini tecnici contenuti nel presente Contratto esecutivo hanno il significato specificato nel Capitolato Tecnico Generale e Speciale, salvo che il contesto delle singole clausole disponga diversamente.

1.3 Il presente Contratto esecutivo è regolato:

a) dalle disposizioni del presente atto e dai suoi allegati, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti tra il Fornitore e l'Amministrazione relativamente alle attività e prestazioni contrattuali;
b) dalle disposizioni dell'Accordo Quadro e dai suoi allegati;
c) dalle disposizioni del D.Lgs. 50/2016 e s.m.i. e relative prassi e disposizioni attuative;
d) dalle disposizioni di cui al D.Lgs. n. 82/2005;
e) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato.

2. VALORE DELLE PREMESSE E DEGLI ALLEGATI

2.1 Le premesse di cui sopra, gli atti e i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Contratto esecutivo.

2.2 Costituiscono, altresì, parte integrante e sostanziale del presente Contratto esecutivo:

- l'Accordo Quadro,
- gli Allegati dell'Accordo Quadro,
- l'**Allegato 1** "Piano Operativo" approvato, l'**Allegato 2** "Piano dei Fabbisogni", di cui al paragrafo 6.4 del Capitolato Tecnico Parte Generale (Allegato all'Accordo Quadro).

2.3 In particolare, per ogni condizione, modalità e termine per la prestazione dei servizi oggetto del presente Contratto Esecutivo che non sia espressamente regolata nel presente atto, vale tra le Parti quanto stabilito nell'Accordo Quadro, ivi inclusi gli Allegati del medesimo, con il quale devono intendersi regolati tutti i termini del rapporto tra le Parti.

2.4 Le Parti espressamente convengono che il predetto Accordo Quadro, ha valore di regolamento e pattuizione per il presente Contratto esecutivo. Pertanto, in caso di contrasto tra i principi dell'Accordo Quadro e quelli del Contratto esecutivo, i primi prevarranno su questi ultimi, salvo diversa espressa volontà derogativa delle parti manifestata per iscritto.

3. OGGETTO DEL CONTRATTO ESECUTIVO

3.1 Il presente Contratto esecutivo definisce i termini e le condizioni che, unitamente alle disposizioni contenute nell'Accordo Quadro, regolano la prestazione in favore

dell'Amministrazione da parte del Fornitore dei seguenti servizi: _____, come riportati nel Piano Operativo approvato di cui all'Allegato 1 e nel Piano dei Fabbisogni di cui all'Allegato 2 al presente documento.

3.2 I predetti servizi dovranno essere erogati con le modalità ed alle condizioni stabilite nel presente Contratto esecutivo e nell'Accordo Quadro e relativi allegati.

3.3 È designato quale Responsabile unico del procedimento ai sensi dell'art. 31 del D.Lgs. n. 50/2016 e Direttore dell'esecuzione, ai sensi dell'art. 101 del D. Lgs. n. 50/2016, il Dott. _____. <*in alternativa*: Sono designati quale Responsabile unico del procedimento, ai sensi dell'art. 31 del D. Lgs. n. 50/2016 il Dott. _____ e Direttore dell'esecuzione ai sensi dell'art. 101 del D. Lgs. n. 50/2016 il Dott. _____>.

3.4 L'affidatario si impegna a rispettare tutti i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale in ottemperanza al principio di non arrecare un danno significativo all'ambiente "Do No Significant Harm" (DNSH), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.

3.5 *<In caso di Contratto esecutivo affidato da un Soggetto Aggregatore, indicare tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'Affidamento>.*

4. EFFICACIA E DURATA

4.1 Il presente Contratto esecutivo spiega i suoi effetti dalla data della sua sottoscrizione ed avrà termine allo spirare di _____ <*indicare la durata contrattuale in ragione di quanto previsto al par. 2 del Capitolato Tecnico Generale*> mesi dalla data di conclusione delle attività di presa in carico.

4.2 Le Amministrazioni possono, nei limiti di quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016, chiedere al Fornitore prestazioni supplementari rispetto al Contratto esecutivo, che si rendano necessarie, ove un cambiamento del contraente produca entrambi gli effetti di cui all'art. 106, comma 1, lettera b), D. Lgs. n. 50/2016; l'Amministrazione comunicherà ad ANAC tale modifica entro i termini di cui all'art. 106, comma 8, del medesimo decreto.

4.3 Le Amministrazioni possono apportare modifiche al contratto esecutivo ove siano soddisfatte tutte le condizioni di cui all'art. 106, comma 1, lettera c), D. Lgs. 50/2016, fatto salvo quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016. Al ricorrere delle condizioni di cui all'art. 106, comma 14, del D. Lgs. 50/2016 l'Amministrazione comunicherà ad ANAC tale modifica entro i termini e con le modalità ivi indicati. In entrambi i casi sopra descritti, l'Amministrazione eseguirà le pubblicazioni prescritte dall'art. 106, comma 5, del D. Lgs. n. 50/2016.

4.4 Le Amministrazioni potranno apportare le modifiche di cui art. 106, comma 1, lett. d), del D. Lgs. n. 50/2016, nel pieno rispetto di tale previsione normativa.

4.5 Ai sensi dell'art. 106, comma 12, del D.Lgs. n. 50/2016, ove ciò si renda necessario in corso di esecuzione, l'Amministrazione potrà imporre al Fornitore affidatario del Contratto esecutivo un aumento o una diminuzione delle prestazioni fino a concorrenza di un quinto dell'importo del contratto alle stesse condizioni ed agli stessi prezzi unitari previsti nel presente contratto. In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.

5. GESTIONE DEL CONTRATTO ESECUTIVO

5.1 Ai fini dell'esecuzione del presente Contratto esecutivo, il Fornitore ha nominato come Responsabile Unico delle Attività Contrattuali (RUAC) e come Referente/i Tecnico/i per l'erogazione dei servizi: il/i dott._____

5.2 I compiti demandati alle suddette figure del Fornitore sono declinati al paragrafo 7.2 del Capitolato Tecnico Generale dell'Accordo Quadro.

5.3 Le attività di supervisione e controllo della corretta esecuzione del presente Contratto esecutivo, in relazione ai servizi richiesti, sono svolte dall'Amministrazione, eventualmente d'intesa con i soggetti indicati nell'Allegato Governance al Capitolato Tecnico Generale dell'Accordo Quadro.

6. PRESA IN CARICO E TRASFERIMENTO DEL KNOW HOW

6.1 Il Fornitore, a decorrere dalla data di stipula del presente Contratto esecutivo, dovrà procedere alla attività di presa in carico con le modalità indicate nel Capitolato Tecnico Speciale dell'Accordo Quadro.

6.2 L'attivazione dei servizi avverrà nei tempi e nei modi di cui al Capitolato Tecnico Generale e Speciale dell'Accordo Quadro, al Piano dei Fabbisogni ed al Piano Operativo.

6.3 In base ai servizi richiesti da parte dell'Amministrazione contraente, alla scadenza del presente Contratto esecutivo o in caso di risoluzione o recesso dallo stesso, il Fornitore si impegna a porre in essere tutte le attività per il passaggio di consegne di fine fornitura (phase-out), finalizzato al trasferimento all'Amministrazione, o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione delle attività, secondo quanto previsto nel paragrafo 7.3 del Capitolato Tecnico Speciale (2A).

7. LOCALI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE CONTRAENTE

7.1 L'Amministrazione Contraente provvede ad indicare e mettere a disposizione del Fornitore, in comodato gratuito ed in uso non esclusivo, locali idonei alla installazione degli eventuali apparati del Fornitore necessari all'erogazione dei servizi richiesti, con le modalità indicate nel Piano dei Fabbisogni e nel Piano Operativo.

7.2 L'Amministrazione Contraente garantisce al Fornitore:

- lo spazio fisico necessario per l'alloggio delle apparecchiature ed idoneo ad ospitare le apparecchiature medesime;
- l'alimentazione elettrica delle apparecchiature di adeguata potenza; sarà cura del Fornitore provvedere ad adottare ogni misura per la garantire la continuità della alimentazione elettrica.

7.3 Il Fornitore provvede a visitare i locali messi a disposizione dall'Amministrazione Contraente ed a segnalare, prima della data di disponibilità all'attivazione, l'eventuale inidoneità tecnica degli stessi.

7.4 L'Amministrazione Contraente consentirà al personale del Fornitore o a soggetti da esso indicati, muniti di documento di riconoscimento, l'accesso ai propri locali per eseguire eventuali operazioni rientranti nell'oggetto del presente Contratto esecutivo. Le modalità dell'accesso saranno concordate fra le Parti al fine di salvaguardare la legittima esigenza

di sicurezza dell'Amministrazione Contraente. Il Fornitore è tenuto a procedere allo sgombero, a lavoro ultimato, delle attrezzature e dei materiali residui.

7.5 L'Amministrazione Contraente, successivamente all'esito positivo delle verifiche di conformità a fine contratto, porrà in essere quanto possibile affinché gli apparati del Fornitore presenti nei suoi locali non vengano danneggiati o manomessi, pur non assumendosi responsabilità se non quelle derivanti da dolo o colpa grave del proprio personale.

8. VERIFICHE DI CONFORMITA'

8.1 Nel periodo di efficacia del presente Contratto esecutivo, ciascuna Amministrazione Contraente procederà ad effettuare la verifica di conformità delle prestazioni oggetto di ciascun Contratto esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali, con le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico Generale e Speciale ad esso allegati.

9. PENALI

9.1 L'Amministrazione potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nell'Accordo Quadro, qui da intendersi integralmente trascritte.

9.2 Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 12 dell'Accordo Quadro.

10. CORRISPETTIVI

10.1 Il corrispettivo complessivo, calcolato sulla base del dimensionamento dei servizi indicato del Piano dei Fabbisogni e nel Piano Operativo, è pari a <*inserire importo in cifre*> € _____,___ <*eventuale*> così suddiviso _____.

10.2 I corrispettivi unitari per singolo servizio, dovuti al Fornitore per la fornitura dei servizi prestati in esecuzione del presente Contratto esecutivo sono determinati in ragione dei prezzi unitari stabiliti nell'Allegato "C" all'Accordo Quadro "Corrispettivi e Tariffe".

10.3 Il corrispettivo contrattuale si riferisce alla esecuzione dei servizi a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.
<nel caso di Contratto Esecutivo affidato da un Soggetto Aggregatore, dovranno essere indicati gli importi e i quantitativi relativi ad ogni singola Amministrazione>

10.4 I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore medesimo di ogni relativo rischio e/o alea. Il Fornitore non potrà vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.

10.5 Tali corrispettivi sono dovuti dall'Amministrazione Contraente al Fornitore a decorrere dalla "Data di accettazione" della fornitura e successivamente all'esito positivo della verifica di conformità della singola prestazione.

11. FATTURAZIONE E PAGAMENTI

11.1 La fattura relativa ai corrispettivi maturati secondo quanto previsto al precedente art. 10

viene emessa ed inviata dal Fornitore con cadenza _____.

11.2 Ciascuna fattura dovrà essere emessa nel rispetto di quanto prescritto nell'Accordo Quadro.

<nel caso di Contratto Esecutivo affidato da un Soggetto Aggregatore, dovranno essere indicate le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni>

11.3 Nel caso in cui risulti aggiudicatario del Contratto un R.T.I., le singole Società costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione, potranno provvedere ciascuna alla fatturazione "pro quota" delle attività effettivamente prestate. Le Società componenti il Raggruppamento potranno fatturare solo le attività effettivamente svolte, corrispondenti alla ripartizione delle attività. La società mandataria del Raggruppamento medesimo è obbligata a trasmettere, in maniera unitaria e previa predisposizione di apposito prospetto riepilogativo delle attività e delle competenze maturate, le fatture relative all'attività svolta da tutte le imprese raggruppate. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi / attività / fasi / prodotti a cui si riferisce.

11.4 I corrispettivi saranno accreditati, a spese del Fornitore, sul conto corrente n. _____, intestato al Fornitore presso _____, Codice IBAN _____; il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i all'Amministrazione all'atto del perfezionamento del presente Contratto Esecutivo.

11.5 Ove applicabile in funzione della tipologia di prestazioni, ai sensi dell'art. 35, comma 18, del Codice, così come novellato dal D.L. 32/2019, il fornitore può ricevere, entro 15 giorni dall'effettivo inizio della/e prestazione/i contrattuali un'anticipazione del prezzo di ciascun Contratto Esecutivo pari al 20 per cento del valore del Contratto Esecutivo stesso. L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore dell'Amministrazione Contraente beneficiaria della prestazione, rilasciata dai soggetti indicati all'art. 35, comma 18, del Codice, di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma (o altro documento equivalente tipo SLA) della prestazione che indicato nel Capitolato Tecnico relativo all'Appalto Specifico

11.6 L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento della/e prestazione/i, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.

11.7 Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione della/e prestazione/i, non procede, per ritardi a lui imputabili, secondo il cronoprogramma concordato. Sulle somme restituite sono dovuti gli interessi legali con decorrenza dalla data di erogazione dell'anticipazione.

12. GARANZIA DELL'ESATTO ADEMPIMENTO

12.1 Il Fornitore ha prestato garanzia definitiva rilasciata in data _____ dalla _____ avente n. _____ di importo pari ad Euro _____= (_____/00) che copre le

obbligazioni assunte con il presente contratto, il risarcimento dei danni derivanti dall'eventuale inadempimento delle stesse obbligazioni, nonché il rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'appaltatore, nonché, ove esistente, le obbligazioni assunte con il Patto di integrità.

12.2 L'Amministrazione ha inoltre il diritto di valersi della garanzia definitiva, nei limiti dell'importo massimo garantito: i) per l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione del contratto disposta in danno dell'esecutore; ii) per provvedere al pagamento di quanto dovuto dal Fornitore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene eseguito il contratto ed addetti all'esecuzione dell'appalto.

12.3 L'Amministrazione ha diritto di incamerare la garanzia, in tutto o in parte, per i danni che essa affermi di aver subito, senza pregiudizio dei suoi diritti nei confronti del Fornitore per la rifusione dell'ulteriore danno eventualmente eccedente la somma incamerata.

12.4 La garanzia prevede espressamente la rinuncia della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, nonché l'operatività della garanzia medesima entro 15 giorni, a semplice richiesta scritta.

12.5 Il Fornitore si impegna a tenere valida ed efficace la garanzia, mediante rinnovi e proroghe, per tutta la durata del presente contratto e, comunque, sino al perfetto adempimento delle obbligazioni assunte in virtù del presente contratto, pena la risoluzione di diritto del medesimo.

12.6 L'Amministrazione può richiedere al Fornitore la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte entro il termine di 10 (dieci) giorni dalla richiesta; in caso di inottemperanza, l'Amministrazione conseguirà la reintegrazione trattenendo quanto necessario dai corrispettivi dovuti al Fornitore.

12.7 La garanzia sarà progressivamente svincolata a misura dell'avanzamento dell'esecuzione contrattuale, nel limite massimo dell'80 per cento dell'iniziale importo garantito, secondo quanto stabilito dall'art. 103, comma 5, del D. Lgs. n. 50/2016, previa deduzione di crediti dell'Amministrazione verso il Fornitore e subordinatamente alla preventiva consegna, da parte del Fornitore all'Istituto garante, di un documento, in originale o copia autentica, attestante l'avvenuta esecuzione delle prestazioni contrattuali. Tale documento è emesso periodicamente dall'Amministrazione in ragione delle verifiche di conformità svolte. Il fornitore dovrà inviare per conoscenza all'Amministrazione la comunicazione che invia al Garante ai fini dello svincolo. Il Garante dovrà comunicare all'Amministrazione il valore dello svincolo. L'Amministrazione si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.

12.8 L'ammontare residuo della garanzia definitiva deve permanere fino alla data di emissione del certificato di verifica di conformità attestante la corretta esecuzione del Contratto esecutivo.

12.9 Resta fermo tutto quanto previsto dall'art. 103 del D. Lgs. n. 50/2016.

13. SUBAPPALTO *<OVE PREVISTO>*

13.1 L'Impresa si è riservata di affidare in subappalto, nella misura di_____, l'esecuzione delle seguenti prestazioni: _____ , salvo quanto previsto dall'art. 105, comma 12, del d. lgs. n. 50/2016.

13.2 L'Impresa si impegna a depositare presso Consip S.p.A., almeno venti giorni prima della data di effettivo inizio dell'esecuzione delle attività oggetto del subappalto: i) l'originale o la copia autentica del contratto di subappalto che deve indicare puntualmente l'ambito operativo del subappalto sia in termini prestazionali che economici; ii) dichiarazione attestante il possesso da parte del subappaltatore dei requisiti richiesti dalla documentazione di gara, per lo svolgimento delle attività allo stesso affidate, ivi inclusi i requisiti di ordine generale di cui all'articolo 80 del D. Lgs. n. 50/2016; iii) dichiarazione dell'appaltatore relativa alla sussistenza o meno di eventuali forme di controllo o collegamento a norma dell'art. 2359 c.c. con il subappaltatore; se del caso, v) documentazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione/certificazione prescritti dal D. Lgs. n. 50/2016 per l'esecuzione delle attività affidate.

13.3 In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, Consip S.p.A. procederà a richiedere al Fornitore l'integrazione della suddetta documentazione. Resta inteso che la suddetta richiesta di integrazione comporta l'interruzione del termine per la definizione del procedimento di autorizzazione del subappalto, che ricomincerà a decorrere dal completamento della documentazione.

13.4 I subappaltatori dovranno mantenere per tutta la durata del presente contratto, i requisiti richiesti per il rilascio dell'autorizzazione al subappalto. In caso di perdita dei detti requisiti Consip S.p.A. revocherà l'autorizzazione.

13.5 L'impresa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato nonché siano variati i requisiti di qualificazione o le certificazioni deve acquisire una autorizzazione integrativa.

13.6 Ai sensi dell'art. 105, comma 4, lett. a) del D. Lgs. n. 50/2016 e s.m.i. non sarà autorizzato il subappalto ad un operatore economico che abbia partecipato alla procedura di affidamento dell'Accordo Quadro.

13.7 Per le prestazioni affidate in subappalto: il subappaltatore, ai sensi dell'art. 105, comma 14, del Codice, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconoscere ai lavoratori un trattamento economico e normativo non inferiore a quello che avrebbe garantito il contraente principale, inclusa l'applicazione dei medesimi contratti collettivi nazionali di lavoro, qualora le attività oggetto di subappalto coincidano con quelle caratterizzanti l'oggetto dell'appalto ovvero riguardino le lavorazioni relative alle categorie prevalenti e siano incluse nell'oggetto sociale del contraente principale;

13.8 L'Amministrazione contraente, sentito il direttore dell'esecuzione, provvede alla verifica dell'effettiva applicazione degli obblighi di cui al presente comma. Il Fornitore è solidalmente responsabile con il subappaltatore degli adempimenti, da parte di questo ultimo, degli obblighi di sicurezza previsti dalla normativa vigente.

13.9 Il Fornitore e il subappaltatore sono responsabili in solido, nei confronti dell'Amministrazione Contraente, in relazione alle prestazioni oggetto del contratto di subappalto.

13.10 L'Impresa è responsabile in solido con il subappaltatore nei confronti dell'Amministrazione contraente dei danni che dovessero derivare ad essa o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività. In particolare, il Fornitore e il subappaltatore si impegnano a manlevare e tenere indenne la Consip e l'Amministrazione da qualsivoglia pretesa di terzi per fatti e colpe imputabili al subappaltatore o ai suoi ausiliari derivanti da qualsiasi perdita, danno, responsabilità, costo o spesa che possano originarsi da eventuali violazioni del Regolamento 679/2016.

13.11 Il Fornitore è responsabile in solido dell'osservanza del trattamento economico e normativo stabilito dai contratti collettivi nazionale e territoriale in vigore per il settore e per la zona nella quale si eseguono le prestazioni da parte del subappaltatore nei confronti dei suoi dipendenti, per le prestazioni rese nell'ambito del subappalto. Il Fornitore trasmette all'Amministrazione contraente prima dell'inizio delle prestazioni la documentazione di avvenuta denunzia agli enti previdenziali, inclusa la Cassa edile, ove presente, assicurativi e antinfortunistici, nonché copia del piano della sicurezza di cui al D. Lgs. n. 81/2008. Ai fini del pagamento delle prestazioni rese nell'ambito dell'appalto o del subappalto, la stazione appaltante acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.

13.12 Il Fornitore è responsabile in solido con il subappaltatore in relazione agli obblighi retributivi e contributivi, ai sensi dell'art. 29 del D. Lgs. n. 276/2003, ad eccezione del caso in cui ricorrano le fattispecie di cui all'art. 105, comma 13, lett. a) e c), del D. Lgs. n. 50/2016.

13.13 Il Fornitore si impegna a sostituire i subappaltatori relativamente ai quali apposita verifica abbia dimostrato la sussistenza dei motivi di esclusione di cui all'articolo 80 del D. Lgs. n. 50/2016.

13.14 L'Amministrazione Contraente corrisponde direttamente al subappaltatore, al cottimista, al prestatore di servizi ed al fornitore di beni o lavori, l'importo dovuto per le prestazioni dagli stessi eseguite nei seguenti casi: a) quando il subappaltatore o il cottimista è una microimpresa o piccola impresa; b) in caso di inadempimento da parte dell'appaltatore; c) su richiesta del subappaltatore e se la natura del contratto lo consente. In caso contrario, salvo diversa indicazione del direttore dell'esecuzione, il Fornitore si obbliga a trasmettere all'Amministrazione contraente entro 20 giorni dalla data di ciascun pagamento da lui effettuato nei confronti dei subappaltatori, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.

13.15 L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.

13.16 In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti commi, l'Amministrazione può risolvere il Contratto esecutivo, salvo il diritto al risarcimento del danno.

13.17 Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016, il Fornitore si obbliga a comunicare all'Amministrazione il nome del subcontraente, l'importo del contratto, l'oggetto delle prestazioni affidate.

13.18 Il Fornitore si impegna a comunicare all'Amministrazione, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione del contratto, il nome del sub-contraente, l'importo del sub-contratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto.

13.19 Non costituiscono subappalto le fattispecie di cui al comma 3 dell'art. 105 del d. lgs. n. 50/2016 e s.m.i.. Nel caso in cui l'Impresa intenda ricorrere alle prestazioni di soggetti terzi in forza di contratti continuativi di cooperazione, servizio e/o fornitura gli stessi devono essere stati sottoscritti in epoca anteriore all'indizione della procedura finalizzata all'aggiudicazione del contratto e devono essere consegnati all'Amministrazione prima o contestualmente alla sottoscrizione del Contratto.

13.20 Per tutto quanto non previsto si applicano le disposizioni di cui all'art. 105 del D.Lgs. 50/2016.

13.21 Restano fermi tutti gli obblighi e gli adempimenti previsti dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973 nonché dai successivi regolamenti.

13.22 L'Amministrazione provvederà a comunicare al Casellario Informatico le informazioni di cui alla Determinazione dell'Autorità di Vigilanza sui Contratti Pubblici (ora A.N.AC) n. 1 del 10/01/2008.

14. *<EVENTUALE>* CONDIZIONI E TEST RICHIESTI DAL CVCN

<Eventuale inserire condizioni/test in considerazione del riscontro del CVCN ai sensi dell'art. 1, comma 6, Legge n. 133/2019>

15. RISOLUZIONE E RECESSO

15.1 Le ipotesi di risoluzione del presente Contratto esecutivo e di recesso sono disciplinate, rispettivamente, agli artt. 14 e 15 dell'Accordo Quadro, cui si rinvia, nonché agli artt. "SUBAPPALTO" "TRASPARENZA DEI PREZZI", "TRACCIABILITÀ DEI FLUSSI FINANZIARI" e "TRATTAMENTO DEI DATI PERSONALI" del presente Documento.

15.2 *<Eventuale inserire le ipotesi di risoluzione o sospensione in accordo con quanto previsto nel precedente articolo 14>*

16. FORZA MAGGIORE

16.1 Nessuna Parte sarà responsabile per qualsiasi perdita che potrà essere patita dall'altra Parte a causa di eventi di forza maggiore (che includono, a titolo esemplificativo, disastri naturali, terremoti, incendi, fulmini, guerre, sommosse, sabotaggi, atti del Governo, autorità giudiziarie, autorità amministrative e/o autorità di regolamentazione indipendenti) a tale Parte non imputabili.

16.2 Nel caso in cui un evento di forza maggiore impedisca la prestazione dei servizi da parte del Fornitore, l'Amministrazione, impregiudicato qualsiasi diritto ad essa spettante in base alle disposizioni di legge sull'impossibilità della prestazione, non dovrà pagare i corrispettivi per la prestazione dei servizi fino a che i servizi non siano ripristinati e, ove

possibile, avrà diritto di affidare l'erogazione dei servizi in questione ad altro fornitore assegnatario per una durata ragionevole secondo le circostanze.

16.3 L'Amministrazione si impegna, inoltre, in tale eventualità a compiere le azioni necessarie al fine di risolvere tali accordi, non appena il Fornitore le comunichi di essere in grado di erogare nuovamente i servizi.

17. RESPONSABILITA' CIVILE *<eventuale>* E POLIZZA ASSICURATIVA

17.1 Fermo restando quanto previsto dall'Accordo Quadro, il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

<ove prevista>

17.2 A fronte dell'obbligo di cui al precedente comma, il Fornitore ha presentato polizza/e assicurativa/e conforme/i ai requisiti indicati nella Richiesta di Offerta (conformi all'allegato di gara dell'AQ).

17.3 Resta ferma l'intera responsabilità del Fornitore anche per danni coperti o non coperti e/o per danni eccedenti i massimali assicurati dalle polizze di cui al precedente comma 2.

17.4 Con specifico riguardo al mancato pagamento del premio, ai sensi dell'art. 1901 del c.c., l'Amministrazione si riserva la facoltà di provvedere direttamente al pagamento dello stesso, entro un periodo di 60 giorni dal mancato versamento da parte del Fornitore ferma restando la possibilità dell'Amministrazione di procedere a compensare quanto versato con i corrispettivi maturati a fronte delle attività eseguite.

17.5 Qualora il Fornitore non sia in grado di provare in qualsiasi momento la piena operatività delle coperture assicurative di cui al precedente comma 2 e qualora l'Amministrazione non si sia avvalsa della facoltà di cui al precedente comma 4, il Contratto potrà essere risolto di diritto con conseguente ritenzione della garanzia prestata a titolo di penale e fatto salvo l'obbligo di risarcimento del maggior danno subito.

17.6 Resta fermo che il Fornitore si impegna a consegnare, annualmente e con tempestività, all'Amministrazione, la quietanza di pagamento del premio, atta a comprovare la validità della polizza assicurativa prodotta per la stipula del contratto o, se del caso, la nuova polizza eventualmente stipulata, in relazione al presente contratto.

18. TRASPARENZA DEI PREZZI

18.1 L'Impresa espressamente ed irrevocabilmente:

a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione del presente contratto;

b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le Imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione del contratto stesso;

c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del

presente contratto rispetto agli obblighi con esse assunti, né a compiere azioni comunque volte agli stessi fini;

d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.Lgs. n. 50/2016 al fine di evitare situazioni di conflitto d'interesse.

18.2 Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma per tutta la durata del contratto lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'art. 1456 cod. civ., per fatto e colpa del Fornitore, che sarà conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione e con facoltà dell'Amministrazione di incamerare la garanzia prestata.

19. ONERI FISCALI E SPESE CONTRATTUALI

19.1 Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto, come previsto all'art. 28 dell'Accordo Quadro.

19.2 Così come previsto dall'art. 29 del Accordo Quadro, ai sensi dell'art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010. Pertanto, le Amministrazioni Beneficiarie sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del presente Contratto esecutivo, il predetto contributo nella misura prevista dall'art. 2, lettera a) (8 per mille del valore del contratto esecutivo sottoscritto se non superiore ad € 1.000.000,00) o lettera b) (5 per mille del valore del contratto esecutivo sottoscritto se superiore ad € 1.000.000,00), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del presente Contratto Esecutivo.

19.3 Il valore complessivo del presente Contratto Esecutivo è quello espressamente indicato al precedente paragrafo 10.1. Di conseguenza, il valore del contributo dovuto dall'Amministrazione Beneficiaria ammonta ad €_____(Euro_____).

19.4 In caso di incremento (entro il 20% dell'importo iniziale) del valore del Contratto esecutivo a seguito di una modifica del Piano dei Fabbisogni e del Piano Operativo approvato dall'Amministrazione Beneficiaria ai sensi dell'articolo 6 dell'Accordo Quadro, quest'ultima è tenuta a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall'art. 2, lettera c) (3 per mille sull'incremento tra il valore del contratto esecutivo ed il valore dell'atto aggiuntivo), del D.P.C.M. 23 giugno 2010.

A tal fine, nei casi di cui al precedente periodo, il Fornitore provvederà a comunicare all'Amministrazione e per conoscenza a Consip, entro il termine di 10 (dieci) giorni solari dalla data di approvazione del Piano Operativo incrementato, il valore aggiornato del Piano Operativo e il valore del contributo dovuto in ragione del relativo incremento.

19.5 Il pagamento del contributo, deve essere effettuato tramite bonifico bancario sul seguente IBAN: Banca: Intesa San Paolo - IBAN: IT 27 X 03069 05036 100000004389

Detti contributi sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972 e pertanto non è prevista nessuna emissione di fattura; gli stessi non rientrano nell'ambito di applicazione della tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136.

20. TRACCIABILITÀ DEI FLUSSI FINANZIARI

20.1 Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.

20.2 Ferme restando le ulteriori ipotesi di risoluzione previste dal presente contratto, si conviene che l'Amministrazione, in ottemperanza a quanto disposto dall'art. 3, comma 9 bis della Legge 13 agosto 2010 n. 136, senza bisogno di assegnare previamente alcun termine per l'adempimento, potrà risolvere di diritto il presente contratto ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa con raccomandata a/r qualora le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136.

20.3 Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, secondo periodo della Legge 13 agosto 2010 n. 136, ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136.

20.4 Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui alla norma sopra richiamata è tenuto a darne immediata comunicazione all'Amministrazione e la Prefettura – Ufficio Territoriale del Governo della provincia ove ha sede l'Amministrazione.

20.5 Il Fornitore, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari.

20.6 L'Impresa è tenuta a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i qualsivoglia variazione intervenuta in ordine ai dati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il codice fiscale delle persone delegate ad operare su detto/i conto/i.

20.7 Ai sensi della Determinazione dell'AVCP (ora A.N.AC.) n. 10 del 22 dicembre 2010, il Fornitore, in caso di cessione dei crediti, si impegna a comunicare il/i CIG/CUP al cessionario, eventualmente anche nell'atto di cessione, affinché lo/gli stesso/i venga/no riportato/i sugli strumenti di pagamento utilizzati. Il cessionario è tenuto ad utilizzare conto/i corrente/i dedicato/i, nonché ad anticipare i pagamenti al Fornitore mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i del Fornitore medesimo riportando il CIG/CUP dallo stesso comunicato.

21. FORO COMPETENTE

21.1 Per tutte le questioni relative ai rapporti tra il Fornitore e l'Amministrazione, la competenza è determinata in base alla normativa vigente.

22. TRATTAMENTO DEI DATI PERSONALI

<specificare, nella Piano dei Fabbisogni e nei rispettivi documenti allegati, un sufficiente dettaglio sul contesto tecnologico e procedurale nel quale il Fornitore dovrà operare, anche con specifico riferimento alle misure tecniche e organizzative necessarie per garantire il rispetto degli obblighi di cui all'art. 32 del regolamento UE, coordinando tali informazioni con quanto indicato nell'atto di nomina del Fornitore a Responsabile del trattamento >

22.1 Con la sottoscrizione del presente contratto il Fornitore è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito anche "Normativa in tema di trattamento dei dati personali") e delle istruzioni nel seguito fornite.

22.2 Il Fornitore/Responsabile ha presentato garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.

22.3 Le finalità del trattamento sono: _____ (motivi per cui il fornitore tratta i dati) <*Valorizzare in ragione dell'oggetto del contratto*>

22.4 Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati comuni (es. dati anagrafici e di contatto ecc..) ; ii) dati sensibili (dati sanitari, opinioni politiche ecc.); iii) dati giudiziari. <*Valorizzare in ragione dell'oggetto del contratto*>

22.5 Le categorie di interessati sono: es. dipendenti e collaboratori, utenti dei servizi, ecc… <*Valorizzare in ragione dell'oggetto del contratto*>

22.6 Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;

- ricevano la formazione necessaria in materia di protezione dei dati personali;

- trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default).

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive < *si precisa che tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato o includa il trattamento di dati sensibili di cui all'articolo 9, paragrafo 1, o i dati giudiziari di cui all'articolo 10*>, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE.

j) adottare le misure minime di sicurezza ICT per le P.A. di cui alla circolare Agid n. 2/2017 del 18 aprile 2017.

22.7 Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso <*personalizzare in ragione dell'oggetto del contratto*>:

- la pseudonimizzazione e la cifratura dei dati personali;

- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

22.8 La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.1) (Autorizzazione generale) Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente il Titolare del trattamento di ogni nomina e/o sostituzione dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.

<*Oppure*> 2) (Autorizzazione specifica) Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento. Nel caso in cui per le prestazioni del Contratto che comportano il trattamento di dati personali il Fornitore/ Responsabile ricorra a subappaltatori o subcontraenti è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al titolare.

Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà al Fornitore/Responsabile Inziale del trattamento la penale di cui all'Accordo Quadro e diffiderà lo stesso a far adottar al sub-Responsabile del trattamento tutte le misure più

opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, l'Amministrazione potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno;

Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori.

22.9 Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 23 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.

22.10 Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile del trattamento e/o di suoi sub-Responsabili.

22.11 Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto;

22.12 Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, , o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione l'Amministrazione applicherà la penale di cui all'Accordo Quadro e diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza

fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 c.c. l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

22.13 Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

22.14 Al termine della prestazione dei servizi oggetto del contratto, il Responsabile su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

22.15 Il Responsabile si impegna a attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" nonché Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.

22.16

22.17 In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.

22.18 Su richiesta del Titolare, il Responsabile si impegna ad adottare, nel corso dell'esecuzione del Contratto, ulteriori garanzie quali l'applicazione di un codice di condotta approvato o di un meccanismo di certificazione approvato di cui agli articoli 40 e 42 del Regolamento UE, quando verranno emanati. L'Amministrazione potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

22.19 Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

22.20 Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.

22.21 Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

22.22 Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

Letto, approvato e sottoscritto
Roma, lì _____

_____ _____
(per l'Amministrazione) (per il Fornitore)

Ai sensi e per gli effetti dell'art. 1341 c.c. il Fornitore dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti: Art. 1 Definizioni, Art. 3 Oggetto del Contratto esecutivo, Art. 4 Efficacia e durata, Art. 5 Gestione del Contratto esecutivo, Art. 6 Presa in carico e trasferimento del Know How, Art. 7 Locali messi a disposizione dell'Amministrazione contraente, Art. 8 Verifiche di conformità, Art. 9 Penali, Art. 10 Corrispettivi, Art. 11 Fatturazione e pagamenti, Art. 12 Garanzia dell'esatto adempimento, *<ove previsto>,* Art. 13 Subappalto, *<ove previsto>,* Art. 14 Condizioni e Test richiesti dal CVCN, Art. 15 Risoluzione e Recesso, Art. 16 Forza Maggiore, Art. 17 Responsabilità civile *<ove prevista>* e polizza assicurativa, Art. 18 Trasparenza dei prezzi, Art. 19 Oneri fiscali e spese contrattuali, Art. 20 Tracciabilità dei flussi finanziari Art. 21 Foro competente, Art. 22 Trattamento dei dati personali

Letto, approvato e sottoscritto

Roma, lì

_____
(per il Fornitore)

Accordo quadro avente ad oggetto l'affidamento
di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

ID 2296 - **LOTTO** 1

Piano Operativo

accenture | FASTWEB | FINCANTIERI Nextech | DEAS

Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Rev.	Data	Descrizione delle modifiche	Autore
01	04/11/2024	Prima emissione	RTI

Tabella 1 – Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

L' Agenzia Regionale per la Protezione dell'Ambiente- Campania (nel seguito anche "ARPAC" o "Amministrazione") si avvale di un'infrastruttura digitale complessa attraverso la quale eroga servizi a un'ampia area metropolitana. L'adozione di nuovi paradigmi di costruzione ed erogazione dei servizi digitali (cloud computing, mobile workplace), la crescita costante di attacchi cyber sempre più sofisticati, l'adeguamento del quadro normativo alle nuove esigenze di privacy e protezione delle infrastrutture critiche, rendono necessaria una profonda rivalutazione degli aspetti concettuali, tecnici e organizzativi legati alla cybersicurezza, soprattutto in relazione alla estrema dinamicità e complessità delle sue manifestazioni.

1.1 Scopo

L'Amministrazione rileva un forte deficit di strumenti per la gestione efficace del rischio cyber determinato da minacce sofisticate e in continua evoluzione. La casistica recente degli incidenti relativa ad amministrazioni pubbliche che attuano una gestione della sicurezza digitale analoga a quella dell'Agenzia Regionale per la Protezione dell'Ambiente, evidenzia la necessità di dotarsi quanto prima possibile delle competenze e degli strumenti necessari a riportare il rischio cyber a un livello accettabile e compatibile con la missione dell'Amministrazione.

Le criticità rilevate riguardano i seguenti aspetti:

- Corretta gestione e correlazione dei Log.
- Monitoraggio delle vulnerabilità e delle minacce.

Gli interventi previsti indirizzano in maniera diretta le criticità elencate, e si calano in un contesto organizzativo che prevede un deciso potenziamento delle Security Operation con l'obiettivo di conseguire una gestione efficace del rischio cyber in tutti i suoi aspetti.

1.2 Ambito di Applicabilità

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 (PA) 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.

È 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 Pubbliche Amministrazioni 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. È 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 Pubbliche Amministrazioni.

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.

L'RTI ha basato il modello di tali servizi sul National Institute of Standards and Technology (NIST) Cyber Security Framework (principale standard di sicurezza in ambito cyber, anche il framework nazionale si basa su di esso), arricchito dai principali standard e best practice di settore (ISO 27001, NERC-CIP, MITRE ATT&CK, ISF, SANS, ITIL e COBIT), integrando i requisiti normativi co-genti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al Framework Nazionale per la Cybersecurity e la Data Protection.

In particolare, nella figura sottostante è riportata la mappatura dei servizi offerti al Framework, al fine di illustrare come tali servizi siano funzionali a ciascuna area del Framework.

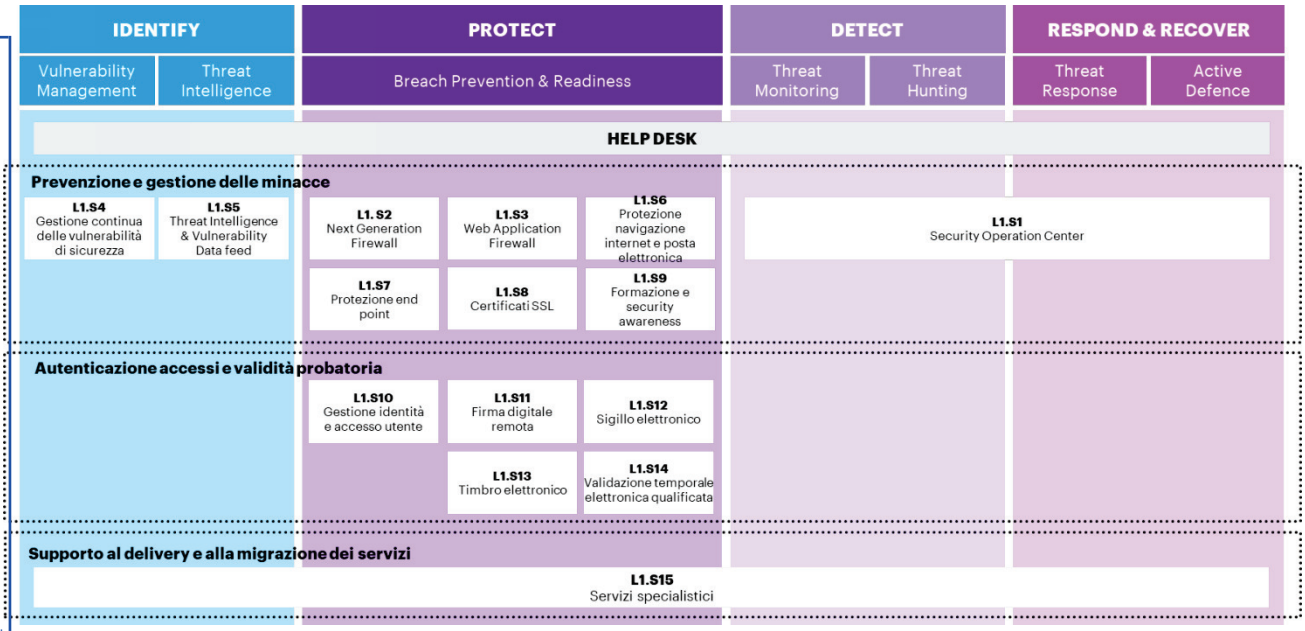

Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

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'iniziativa in oggetto 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.

Lo scenario è contestualmente caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo. 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 (Lotto 1)** 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 (Lotto 2)** 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 nonché sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

In riferimento a quanto sopra riportato, **ARPAC**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

Nell'ambito di tale lotto, si riportano di seguito i **servizi fruibili**, così come previsto dall'Accordo Quadro:

- L1.S1 - Security Operation Center (SOC)
- L1.S2 - Next Generation Firewall
- L1.S3 - Web Application Firewall
- L1.S4 - Gestione continua delle vulnerabilità di sicurezza
- L1.S5 - Threat Intelligence & Vulnerability Data Feed
- L1.S6 - Protezione navigazione Internet e Posta elettronica

- L1.S7 - Protezione degli endpoint
- L1.S8 - Certificati SSL
- L1.S9 - Servizio di Formazione e Security awareness
- L1.S10 - Gestione dell'identità e l'accesso utente
- L1.S11 - Firma digitale remota
- L1.S12 - Sigillo elettronico
- L1.S13 - Timbro elettronico
- L1.S14 - Validazione temporale elettronica qualificata
- L1.S15 - Servizi specialistici

A tal fine, **ARPAC**, ha individuato il Raggruppamento Temporaneo di Imprese (RTI) composto da Accenture S.p.A. (Accenture, impresa mandataria), Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri), e Difesa e Analisi Sistemi S.p.A. (DEAS) , quale aggiudicatario dell'Accordo Quadro che effettuerà la prestazione, sulla base di decisione motivata in relazione alle specifiche esigenze dell'amministrazione e in relazione a quanto stipulato nell'Accordo Quadro di riferimento.

1.3 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra ARPAC e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

Tabella 1 - Assunzioni

2 RIFERIMENTI

2.1 Normativa di riferimento

Trovano applicazione le normative e gli standard internazionali riportate al “Capitolato Tecnico Generale” (§ 4.6) [DA-1].

2.2 Documenti Applicabili

Rif.	Titolo
DA-1.	ALLEGATO 1 - CAPITOLATO TECNICO GENERALE - Gara a 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.
DA-2.	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
DA-3.	Accordo Quadro
DA-4.	Offerta Tecnica – Lotto 1 GARA A 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
DA-5.	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
DA-6.	Piano dei Fabbisogni nominato: “AQ2296_Lotto 1_Sicurezza da Remoto_Piano dei fabbisogni_ARPAC_rev22ott_v1.pdf” PEC del 22/10/2024

Tabella 2 - Documenti Applicabili

3 DEFINIZIONI E ACRONIMI

3.1 Acronimi

Definizione	Descrizione
Accordo Quadro (AQ)	L'Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A. 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
Capitolato Tecnico Generale	Documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa
Capitolati Tecnici Speciali	Integrano il Capitolato Tecnico Generale e definiscono i contenuti di dettaglio e i requisiti minimi in termini di quantità, qualità e livelli di servizio, relativamente al Lotto 1 avente ad oggetto i Servizi di Sicurezza da remoto e al Lotto 2 avente ad oggetto i Servizi di Compliance e controllo
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 Servizi di Sicurezza da remoto, di Compliance e di Controllo per le Pubbliche Amministrazioni (Lotto 1)
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 lavoro *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 (CS)	La/e sede/i da cui l'Aggiudicatario eroga i servizi in modalità "da remoto" di cui al presente Capitolato 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

Tabella 3 - Definizioni

Vocabolo	Titolo
AgID	Agenzia per l'Italia Digitale
AQ	Accordo Quadro

Vocabolo	Titolo
BC	Business Continuity
CE	Contratto Esecutivo
CS	Centro Servizi
CTS	Capitolato Tecnico Speciale
DA	Documenti Applicabili
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
HVAC	Heating, Ventilation and Air Conditioning
HW	Hardware
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LRP	Livello di Rischio Previsto
LRR	Livello di Rischio Residuo
MGMT	Management
MPLS	MultiProtocol Label Switching
NDA	Non-Disclosure Agreement
OLO	Other Licensed Operators
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PMO	Project Management Office
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Impresa
RTO	Recovery Time Objective
SAN	Storage Area Network
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SIEM	Security Information and Event Management
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SSL	Secure Sockets Layer
SW	Software
UPS	Uninterruptible Power Supply
UTD	Unified Threat Protection
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

L'approccio organizzativo che il RTI propone è volto a garantire:

- la gestione dell'Accordo Quadro (AQ) nel suo complesso, con ruoli di organizzazione, indirizzo e controllo dei diversi Contratti Esecutivi (CE) attivati (Governo dell'AQ);
- il coordinamento dei singoli CE e l'erogazione dei servizi richiesti per ciascuno di essi (Gestione dei CE);
- la capacità di adattarsi dinamicamente alle necessità della singola PA in base, ad esempio, alla maturità della stessa in ambito Cybersecurity, alle dimensioni, al contesto tecnologico, alla tipologia di dati trattati, alla distribuzione geografica e all'appartenenza del Perimetro di Sicurezza Cibernetico Nazionale.

L'organizzazione del RTI proposta per la conduzione dell'Accordo Quadro è mostrata nella figura di seguito riportata:

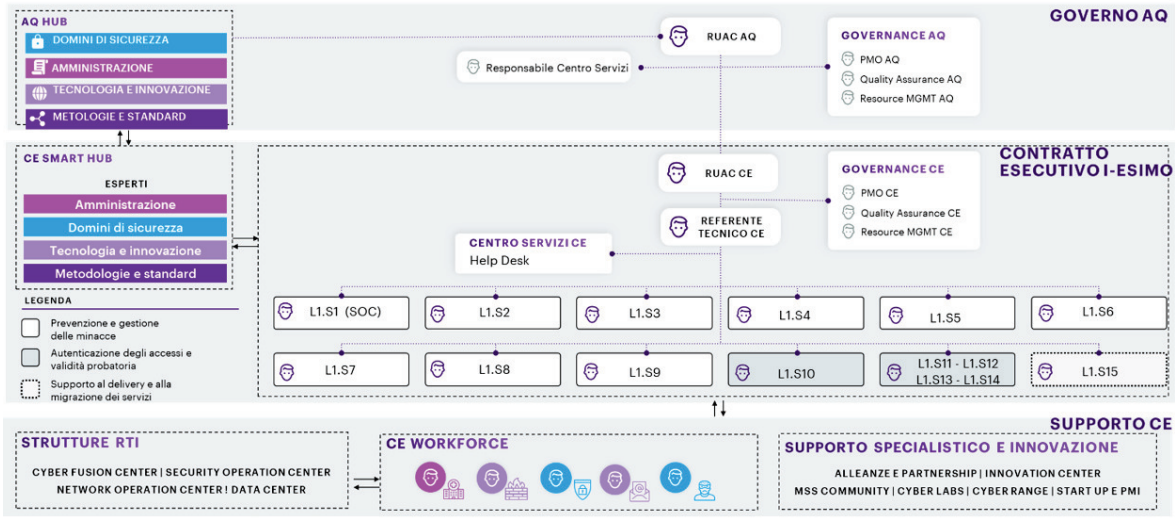

Figura 2 - Organizzazione dell'AQ proposta dal RTI

L'organigramma proposto prevede che il coordinamento delle attività del presente Accordo Quadro venga svolto dal Responsabile Unico della Attività Contrattuali dell'Accordo Quadro.

Il modello proposto si articola sui tre livelli di seguito illustrati:

- **Livello di Governo dell'AQ -** rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera fornitura. È presieduto dal Responsabile Unico delle Attività Contrattuali dell'AQ (RUAC AQ), che svolge un'azione di indirizzo e controllo strategico in ottica di gestione unitaria dei CE. Il RUAC AQ è designato dalla mandataria, presiede il Comitato di Coordinamento del RTI composto da figure manageriali delle aziende in esso contenute e dal Responsabile del Centro Servizi, che insieme definiscono la strategia di AQ e assicurano una visione unica e integrata dell'andamento dei servizi oggetto di gara, garantendo al tempo stesso la qualità complessiva dei CE per conseguire la piena soddisfazione delle PA.
  Il RUAC AQ è il principale riferimento del RTI per Consip, rappresenta inoltre il RTI all'interno dell'Organismo Tecnico di Coordinamento e Controllo ed è quindi la principale interfaccia verso i soggetti istituzionali su tutte le tematiche contrattuali. È supportato dal team di Governance AQ che include strutture/ruoli aggiuntivi (offerti senza oneri aggiuntivi) quali: Project Management Office, Quality Assurance e Resource Management.
- **Livello dei Contratti Esecutivi -** è progettato per adattarsi alle diverse tipologie di PA che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi. A tale livello sono coordinati ed erogati i servizi previsti per ogni CE ed è prevista la presenza di:
  - un Responsabile unico delle attività contrattuali del CE (RUAC CE);
  - un Referente Tecnico CE;
  - un team di Governance CE;
  - un Help Desk dedicato all'assistenza dei Referenti identificati dall'Amministrazione,

- team responsabili dell'erogazione dei servizi previsti.

Il RUAC CE ha una responsabilità speculare a quella del RUAC AQ e rappresenta la principale interfaccia verso le singole PA per tutte le tematiche contrattuali, avendo allo stesso tempo compiti di raccordo tra i due livelli.
Il Referente Tecnico CE è responsabile del corretto svolgimento delle attività e dei servizi e il relativo livello di qualità di erogazione per il singolo CE ed è supportato dal team di Governance CE (PMO CE, Quality Assurance CE e Resource Management CE).
I Team responsabili dell'erogazione dei servizi, composti da professionisti di settore, hanno l'ulteriore supporto dei maggiori esperti di tematica del RTI (Subject Matter Expert) per assicurare omogeneità di metodologie e innovazione continua in base all'evoluzione del contesto.

- **Livello Supporto CE -** garantisce due tipi di supporto:
  - *Scalabilità* - La CE Workforce comprende le strutture di appartenenza delle risorse assegnate ai CE, quali Cyber Fusion Center/Security Operation Center/Network Operation Center/Data Center, la cui dimensione garantisce flessibilità e scalabilità adeguata alle esigenze (es. aumento della domanda, complessità progettuale, contesto tecnologico, sensibilità dei dati);
  - *Supporto specialistico e innovazione* - Garantito da:
    - i CdC tecnologici (es. infrastruttura, rete, applicazioni, DB, S.O., sistemi di virtualizzazione e HW);
    - i Cyber Labs di Accenture, operanti a livello globale per introdurre nuove tecnologie di sicurezza tramite prove di laboratorio che ne facilitano l'integrazione sui sistemi cliente, e i centri di ricerca e sviluppo in ambito cyber di Fastweb (FDA-Fastweb Digital Academy), Fincantieri e DEAS;
    - il network di start-up e PMI innovative;
    - le partnership con i principali vendor in materia sicurezza;
    - le MSS COMMUNITY, specializzate per ambito (es. Application Security, Digital Identity, Threat Operations, Cloud Security, Continuous Risk Management), tecnologia delle soluzioni offerte e/o presenti presso le PA richiedenti, tematica (es. ambiti Difesa, Sanità);
    - i Cyber Range (Poligoni Cibernetici) di Accenture e DEAS;
    - i laboratori di test plant di Fastweb utilizzati per testare gli apparati di sicurezza, così come nella verifica della conformità dei prodotti effettuata dai CVCN (Centro di Valutazione e Certificazione Nazionale) e CV. In particolare, per la capacità del RTI di supportare Consip, le PA e gli organismi istituzionali (es. AgID, Agenzia per la Cyber Sicurezza Nazionale) in materia di Innovazione.

- **AQ HUB e CE SMART HUB -** Strutture aggiuntive composte da esperti di diversi ambiti, con il compito di stimolare e promuovere, rispettivamente a livello di AQ e di CE, l'innovazione e le competenze tecnologiche nell'erogazione dei servizi, rafforzare il livello di conoscenze nei vari domini di sicurezza e di awareness verso le PA anche rispetto alle opportunità offerte dal contratto, garantire la conformità a standard e best practice di settore.

Per quanto concerne invece i **Centri Servizi**, questi vengono coordinati da uno specifico Responsabile che opera a livello "Governo AQ" e in accordo ai seguenti criteri:

- struttura organizzativa unica che assume la responsabilità dell'erogazione del servizio per tutte le sedi operative;
- assegnazione di responsabilità specifiche centralizzate, a livello di CS e a diretto riporto del responsabile del CS, in merito alla gestione della sicurezza informatica e della continuità operativa;
- assegnazione di responsabilità specifiche distribuite, a livello di sede operativa, in merito alla sicurezza fisica e alla gestione ambientale ed energetica.

4.1 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività saranno svolte dalle aziende secondo la ripartizione seguente:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center	X			
L1.S5 – Threat Intelligence & Vulnerability Data Feed	X			
L1.S7 – Protezione degli endpoint		X		
L1.S15 – Servizi Specialistici	X	X	X	X
TOTALE (%)	51,15%	48,63 %	0,11 %	0,11%
TOTALE (€)	€ 442.212,00	€ 420.461,44	€ 976,00	€ 976,00

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

Nella tabella che segue sono riportate le principali figure di riferimento del Fornitore, cui ruoli e responsabilità sono stati illustrati nella parte introduttiva del Capitolo:

FIGURE DI RIFERIMENTO E REFERENTI DEL FORNITORE
RUAC AQ
GOVERNANCE AQ (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
RESPONSABILE CENTRO SERVIZI
RESPONSABILE DI SICUREZZA INFORMATICA E CONTINUITÀ OPERATIVA
RESPONSABILE DI SEDE OPERATIVA
RUAC CE
GOVERNANCE CE (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
REFERENTE TECNICO CE
RESPONSABILI DELL'EROGAZIONE DEI SERVIZI

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

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

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

5 AMBITI E SERVIZI

5.1 Ambiti di intervento

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti di **ARPAC** così come riportati nel Piano dei Fabbisogni:

- L1.S1 – Security Operation Center
- L1.S5 – Threat Intelligence & Vulnerability Data Feed
- L1.S7 – Protezione degli endpoint
- L1.S15 – Servizi Specialistici

5.2 Servizi richiesti

Con specifico riferimento ai Servizi L1.S15 Servizi Specialistici, dal momento che vengono richiesti nel Piano dei Fabbisogni, senza uno specifico riferimento al relativo dimensionamento, il RTI propone le quantità come di seguito riportate per l'esecuzione dei relativi servizi come descritti nei paragrafi seguenti:

SERVIZIO	FASCIA	IMPORTO I ANNO/Q.TA	IMPORTO II ANNO/Q.TA	IMPORTO III ANNO/Q.TA	IMPORTO IV ANNO/Q.TA
L1.S1 – Security Operation Center	Fascia 4- Fino a 6.000 Eps	€ 36.036,00 /165	€ 36.036,00 /165	€ 36.036,00 /165	€ 36.036,00 /165
L1.S5 – Threat Intelligence & Vulnerability Data Feed	Fascia 3- > 50 datafeed		€14.200,00/71	€14.200,00/71	€14.200,00/71
L1.S7 – Protezione degli endpoint	Fascia 2- fino a 1000 nodi	€11.907,36/720	€11.907,36/720	€11.907,36/720	€11.907,36/720
L1.S15 – Servizi Specialistici per L1.S1	gg/p Team ottimale	€ 22.936,00/94	€17.568,00/72	€17.568,00/72	€17.568,00/72
L1.S15 – Servizi Specialistici per L1.S5	gg/p Team ottimale		€67.588,00/277	€56.608,00/232	€56.608,00/232
L1.S15 – Servizi Specialistici per L1.S7	gg/p Team ottimale	€93.452,00/383	€93.452,00/383	€93.452,00/383	€93.452,00/383

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

Di seguito l'indicatore di progresso (IP) identificato in questa fase per l'erogazione della fornitura, 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		

Tabella 8 - Schema definizione Indicatore di Progresso

Tale indicatore sarà oggetto di revisione con l'Amministrazione a valle della fase di presa in carico. In particolare, sarà attivato uno specifico tavolo di lavoro mirato a:

- valutare il grado di maturità digitale dei servizi offerti e il grado di maturità atteso;
- consolidare l'indicatore;
- definire le misure iniziali dell'indicatore;
- stabilire i target e cioè le misure attese alla fine del contratto.

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi richiesti

Di seguito i servizi proposti in linea con le esigenze espresse da **ARPAC**

6.1.1 L1.S1 Security Operation Center

La ventennale esperienza di Accenture, unitamente a quella di Fastweb nell'ambito della pubblica amministrazione, ha permesso di consolidare e far evolvere un modello di servizio ponendo a fattor comune esperienze analoghe nella realizzazione ed erogazione di servizi di Security Operation Center per istituzioni governative nazionali ed internazionali. Si è giunti alla definizione ed ingegnerizzazione di un modello di "Next Generation Security Operation Center (NG-SOC)" basato su tecnologia Splunk per la parte di "Security Information & Event Management (SIEM)" e Palo Alto Cortex XSOAR per la parte di "Security Orchestration, Automation & Response (SOAR)", entrambi leader di mercato secondo fonti affermate di analisti di settore quali Gartner e Forrester e partner decennali a livello globale delle aziende del RTI.

Il servizio proposto di SOC ha l'obiettivo di individuare nel minor tempo possibile potenziali incidenti di sicurezza, supportato dalle informazioni di dettaglio fornite dalle sorgenti di eventi di sicurezza dell'Amministrazione.

Il servizio SOC è erogato da un unico gruppo di lavoro (Accenture Cyber Fusion Center Napoli) che risponde a un Responsabile del Servizio SOC (RSOC, vale a dire il Service Manager) il quale rappresenterà il punto di contatto con il Referente tecnico dell'Amministrazione.

Team di servizio

Data la sua criticità, il servizio utilizza un framework di comunicazione che prevede allineamenti a differenti livelli, da quello operativo fino a quello Direzionale/Leadership.

Il team per il SOC del RTI è composto da:

- **un RSOC** in qualità di referente tecnico del RTI SOC;
- **un SOC team** con SME (Subject Matter Expert) esperti verticali nelle varie aree di Cyber Security.

Il **RSOC** rappresenta il punto di contatto tra il Referente Tecnico dell'Amministrazione e il SOC Team ed ha le seguenti responsabilità:

- stilare e condividere il Questionario di Preinstallazione (QPI) adattato al contesto e perimetro dell' Amministrazione contenente le informazioni necessarie al processo di onboarding, i contatti dei referenti operativi dell' Amministrazione e i processi di escalation;
- valutare e convalidare il perimetro di monitoraggio, inteso come l'insieme di sorgenti di log (eventi di sicurezza) dell'Amministrazione, identificati come fondamentali per la valutazione e la copertura del monitoraggio e, quindi, potenziali incidenti di sicurezza;
- valutare e convalidare la configurazione delle varie sorgenti di log di cui il punto precedente e, quindi, i collector/agent da utilizzare, aree geografiche coinvolte, canale di comunicazione protetto per il trasferimento di tali eventi di sicurezza dall'IT dell'Amministrazione verso il Centro Servizi, informazioni sugli use case e modello di automatizzazione e quanto altro al fine di definire al meglio il perimetro di lavoro;
- condividere e confermare le aspettative dell' Amministrazione ed evidenziare/indirizzare potenziali disallineamenti;
- creare i collegamenti tra i vari referenti dei team coinvolti;
- raccogliere le procedure di escalation e di incident management per individuare i punti di aggiornamento;
- lavorare a contatto con i referenti dell'Amministrazione per recepire i riscontri operativi e tradurli in attività di miglioramento continuo;
- mantenere contatti regolari con eventuali altri team, esterni all'ambito sicurezza, per condividere informazioni rilevanti che possano aiutare/migliorare l'integrazione e la collaborazione;
- identificare i processi di automazione che facilitino la condivisione delle informazioni e la risposta alle minacce per guidare una reazione più rapida e accurata.

Il SOC Team è composto da SME (Subject Matter Expert) esperti verticali nelle varie aree di Cyber Security e, si presenta suddiviso in tre gruppi di analisti incaricati dell'analisi e gestione degli incidenti a complessità crescente: L1, L2 ed L3.

Gli SME sono esperti di sicurezza certificati che operano all'interno di gruppi di lavoro ben definiti con chiara responsabilità e interagiscono tra loro e con l'Amministrazione attraverso canali di comunicazione con massimi livelli di confidenzialità in base alla natura delle informazioni scambiate. Di seguito si riporta una vista sintetica delle figure che compongono il 'SOC Team' adattato secondo le esigenze dell'Amministrazione:

FUNZIONE-TEAM	RUOLO / PROFILO	COMPITI E RESPONSABILITÀ
Responsabile del servizio	RSOC / SP	Punto di contatto tra l'Amministrazione e il SOC team con le responsabilità riportate precedentemente. Possiede certificazioni quali: ISO 27001, CISSP, ITIL, CISM.
Supporto di sicurezza Livello 1	Team L1 / Jr-ISC	Effettua il monitoraggio 24x7 degli allarmi di sicurezza, verifica la priorità degli allarmi, effettua l'analisi degli eventi e la verifica degli stessi, notifica gli eventi attraverso la piattaforma di ITSM del Centro Servizi ed attraverso mail o chiamate al reperibile dell'Amministrazione. Possiede certificazioni quali: SSCP, CEH.
Supporto di sicurezza Livello 2	Team L2 / Sr-ISC	Fornisce report SIEM predefiniti, revisiona e analizza i report, effettua l'analisi degli allarmi e la verifica dei falsi positivi, fornisce supporto per la prima investigazione di breve periodo, effettua la qualifica di un evento in incidente di sicurezza, crea e traccia gli incidenti, monitora le performance, identifica le azioni di contenimento di breve periodo. Inoltre, interagisce con il team operativo dell'Amministrazione a supporto dell'attività di risoluzione e successivamente di chiusura del caso, che è comunque a carico dell' Amministrazione ed in particolare del suo team operativo di competenza.
Supporto di sicurezza Livello 3	Team L3 / Sr-ISC	Supporta la risoluzione in caso di interruzione della raccolta dei log, supporta il tuning delle regole (casi d'uso), raccoglie e trasmette evidenze, valuta il post incidente per miglioramento continuo.
Legenda: SP Security Principal, Sr-ISC Senior Information Sec. Consultant, Jr-ISC Junior Information Sec.		

Tabella 9 - Figure del SOC team

Di seguito si elencano quelli che sono i prerequisiti al servizio in carico all'Amministrazione:

- Configurazione delle sorgenti di log (eventi di sicurezza) e di rete, per la lettura e/o invio degli eventi utili al completamento del servizio;
- Procedure di security incident management, escalation, Crisis Management.

Modello operativo

Il modello operativo del servizio SOC proposto prevede il monitoraggio continuo delle informazioni prodotte dalle sorgenti di log (eventi di sicurezza) identificati come perimetro di monitoraggio dall'Amministrazione.

In sintesi, il servizio consentirà di:

- Controllare in maniera attiva il perimetro infrastrutturale soggetto al servizio di monitoraggio, attraverso attività di "monitoring real-time" così da anticipare per quanto possibile eventuali incidenti di sicurezza;
- Produrre specifici allarmi e reportistica sugli eventi raccolti;
- Identificazione e comunicazione verso l'Amministrazione, delle possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione;
- Acquisizione di eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente. Le evidenze digitali raccolte sono poi trasmesse al referente tecnico dell'Amministrazione ed archiviate;
- Valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza dell'Amministrazione aumentando l'efficacia del SOC team.

Modalità di erogazione

Il modello di erogazione del servizio SOC si basa sulla logica che prevede la raccolta degli allarmi generati dal sistema di monitoraggio del Centro Servizi che, in seguito ad incidenti di sicurezza, apre il ticket verso il team "L1 SOC" sul sistema ITSM. Il

team “L1 SOC” controllerà le informazioni evidenziate dall’allarme, ed eseguirà le prime verifiche per una eventuale escalation verso il team “L2 SOC” o/e il reperibile dell’Amministrazione, nel caso di un fuori orario di servizio.

Successivamente alla conferma di un possibile incidente, il SOC Team procederà con le necessarie azioni, elencate di seguito solo a scopo esemplificativo:

- drill down sugli eventi aggregati che hanno generato l’evidenza/alert;
- verifica dei falsi positivi;
- investigazione/deep analysis del caso;
- escalation verso team di sicurezza ed il team operativo di pertinenza dell’Amministrazione per segnalare/supportare azioni di remediation;

verifica di chiusura del caso segnalato, da parte del team operativo dell’Amministrazione

6.1.2 L1.S5 Threat Intelligence & Vulnerability Data Feed

Il servizio in oggetto è erogato dal Centro Servizi avvalendosi della piattaforma di Threat Intelligence ATIP, sviluppata e gestita da Accenture che prevede l’accesso tramite interfaccia e API alle informazioni di intelligence che coprono le vulnerabilità di oltre 1.000 vendor, strumenti e tecniche malware, Indicatori di Compromissione, organizzazioni target, threat actor e loro motivazioni, campagne di phishing e minacce pertinenti l’organizzazione aziendale.
Per ulteriori dettagli sui servizi L1.S5 e l’utilizzo della piattaforma ATIP di Accenture si rimanda all’”Annex A” in fondo al presente documento.

Funzioni offerte
Il servizio TI&VDF consente di elaborare ed estrarre le informazioni necessarie attraverso le funzionalità offerte, articolate nei livelli riportati nella seguente figura:

Figura 3-Livelli Funzionalità

Tali livelli comprendono tutte le funzionalità previste nel capitolato dell’AQ Sicurezza e ne aggiungono alcune migliorative, come di seguito descritto:

- **Accesso web** - la piattaforma integra l'interfaccia che si basa su un modello di rappresentazione dei dati che consente agli analisti di mettere in relazione nodi di informazioni su threat actor, malware, vulnerabilità, campagne, target, domini, e-mail di phishing, ecc. Tale struttura di dati consente un accesso più rapido ai dati rilevanti e la capacità di visualizzare le relazioni tra i diversi dati;
- **Personalizzazione delle informazioni** - la piattaforma consente di personalizzare le informazioni richieste dalla Amministrazione in funzione dei sistemi adottati. Tramite l'interfaccia è possibile consultare i bollettini predisposti dal team di Threat Intelligence (TI) e generare report personalizzati; nello specifico saranno predisposti report contenenti:
  - IOCs, specifici per i sistemi gestiti dall’ Amministrazione;
  - notizie di interesse per l’Amministrazione e con lo scopo di mantenere l’Amministrazione allineata su possibili eventi di interesse, fintanto che questi non si traducano in una minaccia fattuale;

- sintesi delle segnalazioni effettuate nel periodo di riferimento e la loro classificazione sia per tipologia che per serverity (mensile).

- **Intelligence -** la piattaforma è gestita da un team specialistico di intelligence che ha l'obiettivo di arricchire le informazioni e contestualizzarle rispetto al contesto operativo della Amministrazione;

- Analisi / Prioritizzazione - la piattaforma dispone di funzionalità atte a filtrare le informazioni in funzione delle necessità dell' Amministrazione secondo meccanismi dinamici e continuativi che consentono di focalizzare l'attenzione sui fenomeni più rilevanti.

Feed di Threat Intelligence

I feed utilizzati per l'erogazione del servizio TI&VDF saranno gli outcome:

- di prodotti di Vendor di riferimento;
- di analisi effettuate da ricercatori di sicurezza;
- del network Accenture costituito da tutti Centri di Competenza a livello Globale progressivamente acquisiti negli anni.

Tali Feed, contengono informazioni affidabili, aggiornate e dettagliate sulle vulnerabilità di sicurezza. Ove possibile, i feed provengono dalle fonti primarie dei dati di intelligence in modo da ridurre la ridondanza delle informazioni raccolte e ottimizzarne l'utilizzo.

Di seguito vengono rappresentate le caratteristiche, in termini di descrizione e informazioni fornite, dei feed utilizzati raggruppati per Tipologia.

TIPOLOGIA - Vulnerability data feed	NUMEROSITÀ - 2 feed
Descrizione	Feed costituiti da informazioni sulle vulnerabilità che impattano i prodotti di interesse, provenienti dal National Vulnerability Database (NVD) e dal database di vulnerabilità CVE Details
Informazioni	Descrizione della vulnerabilità, CPE impattate, score CVSS, classificazione CWE, data pubblicazione e ultimo aggiornamento, link ai bollettini di sicurezza rilasciati dal vendor, sfruttamento della vulnerabilità in campagne di attacco.

Tabella 10- Vulnerability data feed

TIPOLOGIA - Vulnerability Intelligence Data Feed	NUMEROSITÀ - 6 feed
Descrizione	Feed costituiti da informazioni sulle vulnerabilità provenienti da diverse fonti tra cui la piattaforma proprietaria Accenture ATIP e i database di exploit per lo sfruttamento delle vulnerabilità disponibili in rete.
Informazioni	Descrizione della vulnerabilità, CPE impattate, score CVSS, classificazione CWE, data pubblicazione e ultimo aggiornamento, link ai bollettini di sicurezza rilasciati dal vendor, sfruttamento della vulnerabilità in campagne di attacco.

Tabella 11-Vulnerability Intelligence data feed

TIPOLOGIA - Threat Advisory Data Feed	NUMEROSITÀ - 2 feed
Descrizione	Bollettini riguardanti le minacce che impattano il contesto italiano e il settore dei Servizi Pubblici, redatti dal team di Cyber Threat Intelligence (CTI) del RTI
Informazioni	Descrizione di minacce, informazioni di contesto approfondite con un focus sulla PA, IoC aggiornati, azioni di mitigazione consigliate.

Tabella 12-Threat Advisory data feed

TIPOLOGIA - Threat Intelligence Data Feed	NUMEROSITÀ - 19 feed
Descrizione	Feed riguardanti il panorama globale delle minacce, inviati automaticamente dai vendor e dai provider di Intelligence.
Informazioni	Informazioni sulle minacce esistenti a livello globale, eventuali informazioni di contesto disponibili, IoC.

Tabella 13- Threat Intelligence data feed

TIPOLOGIA - Threat Indicators Data Feed	NUMEROSITÀ - 42 feed
Descrizione	Feed costituiti da Indicatori di Compromissione (IoC) relativi alle minacce che impattano il settore dei Servizi Pubblici in Italia.
Informazioni	IoC aggiornati relativi alle minacce di interesse per la PA contraente relativi a: domini sospetti, URL dannosi, elenchi di hash malware noti, indirizzi IP associati ad attività dannose.

Tabella 14-Threat Indicators data feed

6.1.3 L1.S7 Protezione degli End Point

La soluzione tecnologica di Endpoint Protection proposta è basata su tecnologia TrendMicro ApexOne, che fornisce un'ampia e consolidata copertura dei requisiti di tecnico-funzionali e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi. Accenture, Fastweb, utilizzano la tecnologia TrendMicro ApexOne, nell'esecuzione di numerose progettualità a livello globale su clienti di diversi settori e congiuntamente nello sviluppo delle soluzioni presso i propri clienti unendo

le competenze di prodotto e di system integration e gestione che, congiuntamente, consentono di adeguare il prodotto alle effettive necessità dei clienti. All'interno di tale collaborazione si procederà anche a indirizzare uno sviluppo/integrazione di prodotto dedicata alle PA. La soluzione proposta consente di:

- effettuare l'ispezione del traffico generato dalla postazione di lavoro;
- controllare lo scambio di dati in maniera tale che le informazioni sensibili non possano essere trasferite ad attori non autorizzati;
- controllare lo stato di compliance dei dispositivi rispetto a policy di sicurezza ben definite;
- inviare log al SIEM integrandosi nel Servizio di Security Operation Center e abilitando il monitoraggio 24x7.

La soluzione sfrutta tecniche di rilevamento delle anomalie avanzate ed è supportata da un team che svolge le seguenti attività:

- consulenza per configurazione della soluzione in caso di problematiche specifiche e/o nella gestione di eventi/incidenti che non possono essere gestiti con le azioni di analisi e rimedio ordinarie. Viene inoltre coinvolto per l'ottimizzazione della soluzione nel suo complesso;
- supporta e integra le attività del L1 e si attiva per incident di priorità elevata e change complesse. Attiva il supporto dei vendor e gestisce l'andamento della richiesta sino alla chiusura;
- esegue procedure per la risoluzione delle richieste relative a installazioni, configurazioni e incidenti, attivando eventualmente procedure di escalation verso L2 in caso di necessità.

Si riporta a seguire una rappresentazione di sintesi del modello operativo:

Figura 4-Modello operativo del Servizio End Point Protection

Di seguito viene presentata la descrizione delle attività delle fasi di configurazione ed erogazione specifiche per il servizio in oggetto:

CONFIGURAZIONE	
Setup e supporto alla distribuzione degli agenti	**Deliverable**: "Report distribuzione degli agenti" contenente la definizione delle funzionalità incluse nel pacchetto di installazione e del report finale di distribuzione degli agenti. **Descrizione**: Si procederà a ✓definizione del pacchetto di installazione dell'agente al fine di soddisfare le esigenze di sicurezza definite nell'analisi dei fabbisogni, ✓supporto per la strategia di distribuzione degli agenti (compatibilità con i sistemi, wave pilota, modalità di deployment), ✓verifica della copertura dei sistemi in perimetro.
Configurazione e messa in produzione	**Deliverable**: "Configurazione del servizio Protezione degli EndPoint", contenente il dettaglio delle policy implementate e i test eseguiti per validazione del deployment. **Descrizione**: Si procederà a: ✓ implementazione delle policy di sicurezza per garantire la protezione degli endpoint, ✓esecuzione di test per verificare che le policy implementate siano efficaci dal punto di vista funzionale di sicurezza e che non blocchino l'operatività della PA.

EROGAZIONE	
Gestione ciclo di vita policy	Deliverable: Aggiornamento delle policy di sicurezza
	Si procederà alla manutenzione continua delle policy di sicurezza in funzione delle esigenze espresse dalla PA e/o da evidenze provenienti dal Servizio SOC e/o di Threat Intelligence e Vulnerability Feed
Operation	Deliverable: Report attività manutenzione
	Si procederà alla gestione di anomalie mediante: ✓l'applicazione di soluzioni permanenti, ove già disponibili, utili a risolvere la casistica ✓l'applicazione di workaround e analisi successiva della root cause in assenza di soluzioni disponibili. Nel continuo si procederà alla verifica dello stato della soluzione e dei relativi processi di controllo
Reporting	Deliverable: Report di servizio
	Si procederà alla generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in xls o pdf

Figura 5-Fasi di configurazione ed erogazione del servizio EPP

6.1.4 L1.S15 Servizi Specialistici per L1.S1

I servizi specialistici a supporto del servizio SOC, prevedono l'utilizzo di personale specializzato in logica di progetto e sono finalizzati a supportare nell'evoluzione del processo di monitoraggio e gestione degli incidenti di sicurezza. Gli obiettivi in-dicati per tale servizio specialistico sono i seguenti e saranno oggetto di puntale pianificazione durante il periodo contrattuale:

- Supporto nell'integrazione con le log source identificate
- Supporto all'identificazione e realizzazione di nuovi Use Case a supporto del processo di detection al fine di migliorare continuamente la libreria di casi dedicati
- Supporto nell'integrazione di playbook per l'ottimizzazione dei processi di risposta ad eventi di sicurezza
- Supporto alla investigazione di possibili attacchi informatici.

6.1.5 L1.S15 Servizi Specialistici per L1.S5

I servizi specialistici saranno quindi erogati al fine di integrare il servizio standard con ulteriori moduli che consentiranno all'Amministrazione di avere un quadro più dettagliato delle minacce che possono impattare il proprio dominio.
Di seguito una descrizione dei moduli che saranno integrati:

- Il modulo **Domain and Phishing Monitoring** monitora la registrazione di nuovi domini e permette di identificare quelli che contengono riferimenti a siti web, brand o termini di ricerca legittimi del perimetro del Cliente. Il modulo consente, attraverso la raccolta di feed di phishing, di verificare la presenza di eventi di phishing relativi al marchio del Cliente, segnalando proattivamente potenziali abusi. Il modulo permette inoltre di valutare il takedown delle risorse. Per il presente modulo è previsto un limite di volume di 10 domini Web e di 1 brand.

- Il modulo **Data and Credential Leakage** è progettato per identificare e segnalare tempestivamente l'**esposizione non autorizzata** o la **fuga di dati** aziendali sensibili, inclusi documenti riservati, violazioni delle credenziali dei clienti, a seguito di attacchi informatici che potrebbero portare a modifica, perdita, distruzione, divulgazione impropria o accesso non autorizzato ai dati. Il rilevamento di dati e credenziali trapelati si basa sull'uso di diversi feed OSINT e privati, raccolti e analizzati per mitigare il **potenziale abuso** da parte di attori criminali. Per il presente modulo è previsto un limite di volume di 10 domini web e 1 brand.

- Il modulo **Dark Web Monitoring** è specializzato nel monitoraggio di vari **forum e marketplace del cybercrime** accessibili ad Accenture su fonti del Deep e Dark Web, per comprendere le intenzioni dei threat actor, come ad esempio le discussioni tra threat actor e insider malintenzionati, le vulnerabilità e i punti deboli nei processi aziendali. Il modulo monitora i siti di "Malware as a Service", i marketplace e i forum sulla Darknet e le piattaforme di messaggistica per rilevare **fughe di notizie** o **menzioni al Cliente** e ai suoi fornitori, partner e peer. Per il presente modulo è previsto un limite di volume di 10 domini web e 1 brand.

- Il modulo **Vulnerability Advisory** fornisce notifiche di nuove vulnerabilità per individuare quelle che potrebbero avere un impatto sulle CPE* relative agli asset monitorati. Il servizio monitora la pubblicazione di **nuove vulnerabilità** o **aggiornamenti** del National Vulnerability Database (NVD), le **vulnerabilità precedentemente sconosciute (zero-day)** pubblicate da fonti CLOSINT e HUMINT e la pubblicazione di **exploit code (Proof Of Concept)** relativi a vulnerabilità che hanno un impatto sull'ambiente del Cliente. Per il presente modulo è previsto un limite di volume di 50 Tecnologie.

6.1.6 L1.S15 Servizi Specialistici per L1.S7

Sono previste in totale 1.532 giornate di servizi specialistici a supporto del servizio L1.S7. Verranno erogate 383 giornate/anno. Tali giornate saranno usate per il mantenimento del livello e delle policy di sicurezza stabilite, per il supporto all' individuazione e pianificazione delle attività rispetto alle evoluzioni del panorama delle minacce informatiche e per la produzione della reportistica necessaria alla gestione della protezione degli endpoint.

6.2 Utenza interessata / coinvolta

Personale di **ARPAC**

6.3 Eventuali riferimenti / vincoli normativi

N/A

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 48 mesi per i servizi L1.S1, L1.S7, L1.S15 per L1.S1 e L1.S15 per L1.S7, 36 mesi per i servizi L1.S5 e L1.S15 per L1.S5, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

Tabella 15 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo dispiegherà i suoi effetti dalla data di stipula e avrà una durata di 48 mesi, decorrenti dalla data di conclusione delle attività di presa in carico.

7.3 Gruppo di Lavoro

L'approccio organizzativo individuato e descritto all'interno del Capitolo 4 consente di predisporre team e organizzazioni del lavoro secondo condizioni ad hoc per ogni progetto, secondo i carichi di lavoro previsti nella progettualità condivisa ma facilmente scalabili, qualora in corso d'opera maturassero condizioni tali da richiedere una modifica al numero dei team, delle risorse o del perimetro d'intervento. Una volta individuate le peculiarità dell'Amministrazione contraente, la selezione del gruppo di lavoro avviene analizzando il contesto della stessa sia dal punto di vista tecnologico, individuando il personale maggiormente qualificato sulle tecnologie e sui prodotti già in uso o attese, che tematico, andando ad identificare le figure professionali con esperienze e competenze nel settore pubblico.

7.4 Modalità di esecuzione dei Servizi

Per la modalità di esecuzione dei servizi è possibile far riferimento al Capitolo 8 del Capitolato Tecnico Speciale. In generale, a partire dal Piano di Lavoro Generale, l'Amministrazione richiederà la stima ed il Piano di Lavoro del singolo stream progettuale (obiettivo), fornendo la documentazione di supporto ed i macro-requisiti per poter effettuare una stima dell'obiettivo.
Di seguito si riporta una tabella di sintesi con le principali milestone per ogni servizio:

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	**Amministrazione**
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	**RTI**

MILESTONE	DESCRIZIONE	ATTORE
Collaudo	Esecuzione del collaudo dei servizi per cui è stato richiesto	**RTI**
Attivazione	Individuazione del ciclo di vita ed avvio del fornitore a procedere con le attività sul servizio. Al momento dell'attivazione saranno noti elementi caratteristici ai quali si associa una valutazione di complessità	**Amministrazione**
Consegna	Rilascio degli artefatti previsti dal piano di lavoro, sia intermedi che finali	**RTI**
Approvazione e Verifica di Conformità	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto	**Amministrazione**
Accettazione e Verifica di Conformità	Verifica e validazione dei prodotti intermedi di servizio, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione	**Amministrazione**
Valutazione difettosità all'avvio e Verifica di Conformità	Verifica della piena fruizione delle funzionalità e dei servizi da parte dell'utente (cittadino/ impresa/ operatore amministrativo/ decisore/ fruitore) tramite l'esame della quantità e della tipologia di malfunzionamenti e non conformità rilevati durante il periodo di avvio in esercizio. Certificazione della corretta esecuzione del servizio	**Amministrazione**

Tabella 16 - Descrizione milestone per obiettivo

Per il Governo della Fornitura, si propone l'adozione delle pratiche di seguito descritte:

- **Stato avanzamenti lavori – tecnico.** Con cadenza mensile (o su richiesta dell'Amministrazione) per le attività progettuali e mensile (o su richiesta dell'Amministrazione) per quelle continuative, verrà prodotto un report di sintesi che sarà discusso nel corso di un meeting ad hoc con l'Amministrazione. Il report riporterà, a livello di progetto e a livello di obiettivo: i) avanzamento e scostamenti rispetto al piano di lavoro; ii) attività svolte e attività previste; iii) rischi e problematiche operative; iv) punti aperti; v) azioni da intraprendere per il corretto svolgimento delle attività.

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

La quota massima di attività subappaltabile – o concedibile in cottimo – da parte del RTI è pari al 50% dell'importo complessivo previsto dal contratto. Di seguito è riportato l'elenco delle attività / prestazioni per parti delle quali il RTI intende ricorrere al subappalto:

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S1 – Security Operation Center, L1.S5 Threat Intelligence & Vulnerability Data Feed; L1.S15 – Servizi Specialistici	**Accenture**	**50%**
L1.S7 – Protezione degli endpoint; L1.S15 – Servizi Specialistici	**Fastweb**	**50%**
L1.S15 – Servizi Specialistici	**Fincantieri**	**50%**
L1.S15 – Servizi Specialistici	**Deas**	**50%**

Tabella 17 - Modalità di ricorso al Subappalto da parte del Fornitore

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

Di seguito è riportato per ogni servizio le metriche di misura e le modalità di erogazione e consuntivazione.

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ	VALORE ECONOMICO
L1.S1	Device equivalenti /anno	Da remoto	Canone	Mensile	€ 218,40	660	€ 144.144,00
L1.S5	Data-Feed/anno	Da remoto	Canone	Mensile	€ 200,00	213	€ 42.600,00
L1.S7	Numero nodi/anno	Da remoto	Canone	Mensile	€ 16,538	2880	€ 47.629,44
L1.S15 per L1.S1	GG/P – Team Ottimale	Da remoto/on-site	Progettuale - A corpo	Mensile	€ 244,00	310	€ 75.640,00
L1.S15 per L1.S5	GG/P – Team Ottimale	Da remoto/on-site	Progettuale - A corpo	Mensile	€ 244,00	741	€ 180.804,00
L1.S15 per L1.S7	GG/P – Team Ottimale	Da remoto/on-site	Progettuale - A corpo	Mensile	€ 244,00	1.532	€ 373.808,00

Tabella 18 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **€ 864.625,44 (iva esclusa).**

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

La fatturazione sarà eseguita in accordo con quanto previsto nello Schema di Contratto Esecutivo. Per quanto concerne i termini di pagamento si fa riferimento a quanto previsto nell'Accordo Quadro.

9 ALLEGATI

9.1 Piano di Lavoro Generale

Per il piano di lavoro generale si rimanda all'allegato Piano di Lavoro Generale.

9.2 Piano di Presa in Carico

Come riportato nel Piano dei Fabbisogni, una prima pianificazione di queste attività, è riportato nell'allegato Piano di Presa in Carico. Il RTI si impegna a garantire l'esecuzione dei collaudi nelle modalità e con riferimento ai servizi per i quali è richiesto come sarà concordato con l'Amministrazione durante il periodo di Presa in Carico.

9.3 Piano della Qualità Specifico

Per il piano di qualità specifico si rimanda al documento denominato Piano della Qualità Specifico.

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Referente Tecnico di CE, il relativo nominativo sarà fornito per la stipula del CE ed il relativo CV sarà fornito entro 5 giorni dalla stipula.

9.5 Misure di Sicurezza poste in essere

Per le misure di sicurezza poste in essere si rimanda al Piano di Sicurezza del Centro Servizi.

9.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH)

Si allega la documentazione trasmessa a Consip tramite pec in data 11/11/2022, relativa al principio "Do No Significant Harm" (DNSH).

SERVIZI

1.1 Accenture, come dettagliato nel presente Piano Operativo, fornirà i servizi di **L.1S.5 Threat Intelligence & Vulnerability Data Feed** (nel seguito del presente documento il "Servizio" o i "Servizi"), tramite la piattaforma ATIP (la "Piattaforma ATIP" o la "Piattaforma").

1.2 **Piattaforma ATIP.** La Piattaforma ATIP raccoglie, normalizza ed organizza le informazioni raccolte nell'ambito dei Servizi. La Piattaforma ha tre componenti operative principali:

• *Acquisizione di informazioni:* la Piattaforma acquisisce informazioni per eseguire i Servizi. Le fonti di queste informazioni includono feed "OSINT" di intelligence open source.

• *Analisi dell'intelligence:* Accenture utilizza una combinazione di metodi automatizzati e manuali per analizzare le informazioni all'interno della Piattaforma.

• *Reporting delle informazioni:* la Piattaforma produce degli alert. Tali alert includono dettagli sugli eventi, correlazione con eventi noti, cause degli attacchi, metodi utilizzati e soluzioni consigliate per la risoluzione o la prevenzione della minaccia. Gli alert, accessibili in modalità di sola lettura, informano tempestivamente l'Amministrazione sugli eventi individuati dal Servizio. La Piattaforma può essere configurata per inviare gli alert sotto forma di feed di posta elettronica ad una mailing list personalizzata, che tenga conto di flussi diversi per livello di intelligence (strategico, operativo e tattico). Una volta avvisata tramite e-mail, l'Amministrazione può accedere ad una sezione dedicata della Piattaforma contenente un bollettino dettagliato sulle minacce ("Bollettino delle Minacce"), archivio dei risultati contestualizzati per l'Amministrazione stessa.

1.3 **Data Feed.** Il Servizio prevede l'abilitazione dei feed di dati sulle minacce e sulle vulnerabilità sulla Piattaforma allo scopo di migliorare il flusso di dati relativi alle minacce di sicurezza e alle vulnerabilità. In linea con il Piano Operativo di cui al Contratto, il Cliente richiede 71 Data Feed di seguito elencati:

Feed	Tipologia
abuse.ch	Indicator
Alienvault	Indicator
Alienvault	Report
Blocklist	Indicator
Greensnow	Indicator
Emerging Threats	Indicator
CERT-FR	Indicator
CERT-FR	Report
ci-badguys	Indicator
CIRCL OSINT Feed	Indicator
CIRCL OSINT Feed	Report
CyberCrime	Indicator
CyberCure	Indicator
DiamondFox	Indicator
DigitalSide	Indicator
DigitalSide	Report
DataPlane DNS	Indicator

Feed	Tipologia
sipregistration	Indicator
SMTP data	Indicator
sshpwauth	Indicator
Honeynet Telnet Bruteforce Ips	Indicator
DataPlane TELNET login	Indicator
The Botvrij.eu Data	Indicator
The Botvrij.eu Data	Report
ZeroDot1	Indicator
Threatfox	Indicator
Threatfox	Report
dan.me.uk TOR	Indicator
Honeynet honeypots urls	Indicator
URLHaus	Indicator
URLHaus	Report
VNC RFB	Indicator
VXvault	Indicator
Accenture Cyber Threat Intelligence - Actively exploited vulnerabilities	Indicator

Feodo IP Blocklist	Indicator
firehol_level1	Indicator
IP protocol 41	Indicator
IP Blocklist SNORT	Indicator
ipspamlist	Indicator
IPsum	Indicator
malshare	Indicator
malsilo	Indicator
Malware Bazaar	Indicator
MalwareBazaar	Report
Metasploit	Vulnerability
mirai.security.gives	Indicator
OpenPhish	Indicator
Panels Tracker	Indicator
PhishScore	Indicator
Phishtank	Indicator
pop3gropers	Indicator
sipinvitation	Indicator
sipquery	Indicator

Accenture Cyber Threat Intelligence - Public sector-targeting	Indicator
Accenture Cyber Threat Intelligence - Italy-targeting	Indicator
Accenture Cyber Threat Intelligence - Actively exploited vulnerabilities	Report
Accenture Cyber Threat Intelligence - Public sector-targeting	Report
Accenture Cyber Threat Intelligence - Italy-targeting	Report
Accenture Cyber Threat Intelligence	Malware
Accenture Cyber Threat Intelligence	Threat Actor
CISA Cybersecurities Alert & Advisories	Report
CISA Blog & News	Report
ACTI Data Feed	Indicator
ACTI Data Feed	Vulnerability
CSIRT-ITA	Report
MITRE	Malware
MITRE	Attack Pattern
MITRE	Tool
MITRE	Intrusion Set
MITRE	Course of Action
NIST	Vulnerability

IMPEGNI

2.1 L'Amministrazione dovrà:

(a) Nominare gli utenti autorizzati ad accedere alla Piattaforma ATIP (ivi inclusi gli accessi tramite modalità API) I nonché a ricevere gli alert e garantire che detti utenti mantengano riservati nome utente, e password. Nel caso in cui uno o più utenti non necessitino più dei suddetti accessi e/o qualora lascino l'Amministrazione, la stessa dovrà informare tempestivamente Accenture per la relativa rimozione. Si precisa che per "utenti autorizzati" si intendono i dipendenti dell'Amministrazione e/o i dipendenti di fornitori terzi dell'Amministrazione che sono autorizzati ad accedere alla Piattaforma ATIP dall'Amministrazione stessa. Qualora gli utenti autorizzati siano dipendenti di fornitori terzi dell'Amministrazione, l'Amministrazione (con esclusione dei competitors) si impegna a far sottoscrivere anche al fornitore interessato le presenti condizioni e a darne evidenza ad Accenture.

(b) Assicurarsi che tutte le azioni degli utenti autorizzati siano in linea con il presente accordo ed il corretto uso delle proprie connessioni al sistema Accenture.

(c) Fornire tempestivamente ad Accenture tutte le informazioni necessarie per la fase di acquisizione delle informazioni;

(d) Determinare se i Servizi soddisfino i requisiti dell'Amministrazione e siano conformi alle leggi, regolamenti, policy o guide a cui l'Amministrazione è soggetta;

(e) Determinare se intraprendere azioni sulla base dei risultati dei Servizi, e/o se implementare eventuali modifiche alle politiche interne, ai sistemi o alle misure di sicurezza. Resta inteso che quanto fornito da Accenture durante l'erogazione dei Servizi non costituisce mai in alcun modo consulenza, opinione o raccomandazione legale;

(f) Garantire l'utilizzo del Contenuto (come sotto definito), qualsiasi azione o della mancata azione, in risposta al Contenuto.

(g) Al termine dei Servizi cessare immediatamente di utilizzare la Piattaforma ATIP; a tale data i diritti di utilizzo della stessa cesseranno immediatamente, fermo restando, tuttavia, che l'Amministrazione avrà il diritto di continuare ad utilizzare il Contenuto (come di seguito definito) in suo possesso anche dopo tale termine e sempre in conformità al presente Accordo.

2.2**. Proprietà intellettuale di Accenture**. Allo scopo di fornire i Servizi, Accenture utilizzerà contenuti di Threat Intelligence generati su misura per la Piattaforma ATIP ("**Contenuto**"), che sono e resteranno di sua proprietà e ne conserva tutti i diritti, i titoli e gli interessi relativi alle opere di Accenture, che consistono in: (a) informazioni sulle vulnerabilità zero day pubbliche e non pubbliche derivanti da molteplici fonti pubbliche e ricerche interne; (b) flussi di indicatori di minaccia atti a rilevare gli attacchi informatici; e (c) altre informazioni di cyber intelligence, avvisi, strumenti analitici e visualizzazioni interattive. L'Amministrazione è consapevole che il Contenuto costituisce knowhow di Accenture e che pertanto può utilizzare tale Contenuto solo così come gli viene fornito (secondo i principi di "*as is*", "*where is*" e "*as available*") e solo ed esclusivamente allo scopo di gestione e protezione della propria rete, sistemi e risorse. L'Amministrazione, consapevole che il Contenuto costituisce Informazioni Riservate di Accenture, non trasferirà nè distribuirà il Contenuto o qualsiasi parte di esso a terzi e non dovrà: (a) tentare di copiare la Piattaforma ATIP e il Contenuto nonchè creare un servizio o un prodotto sostitutivo attraverso l'uso della Piattaforma ATIP; (b) consentire l'uso diretto o indiretto del Servizio avente ad oggetto il Contenuto da parte di terzi, fatti salvi gli utenti autorizzati;(c) utilizzare il Contenuto per fornire servizi a terzi; (e) rimuovere qualsiasi riservatezza, diritto d'autore o altri segni distintivi dal Contenuto o da qualsiasi opera Accenture visualizzata o copiata in conformità al presente accordo; (f) creare opere derivate del Contenuto; o (g) modificare, disassemblare, decompilare, decodificare o effettuare qualsiasi altro tentativo di scoprire o ottenere la proprietà intellettuale che fornisce il Servizio relativo alla Piattaforma ATIP.

TERMINI E CONDIZIONI AGGIUNTIVE

3.1 L'Amministrazione riconosce che il Servizio si basa sulla disponibilità di intelligence open source e di informazioni disponibili al pubblico e accetta che Accenture non può garantire che i Servizi eseguiti:

- nè i report di Accenture o le raccomandazioni rese nel corso dei Servizi saranno prive di errori, complete o legalmente perseguibili;
- rileveranno o individueranno tutte le vulnerabilità, le minacce alla sicurezza, le intrusioni e i danni alla rete, alle strutture, agli asset e alle proprietà della stessa;
- Resta inteso inoltre che qualunque eventuale report fornito in seguito alla esecuzione dei Servizi non si intende realizzato per essere utilizzato (i) al fine di ottenere certificazioni, (ii) nell'ambito di procedimenti contenziosi o a fini di (iii) auditing.

Il Servizio, il Contenuto e i singoli componenti del Servizio, nonché le API per accedervi, costituiscono Informazioni riservate di Accenture o dei suoi concessori di licenza terzi e saranno trattati come tali in conformità al presente Accordo. L'Amministrazione è responsabile di mantenere riservato il Contenuto, di utilizzarlo solo internamente all'interno della propria attività allo scopo di proteggere le proprie reti e di proteggere il Contenuto dalla divulgazione a terzi. L'Amministrazione deve informare tempestivamente Accenture dopo essere venuta a conoscenza di qualsiasi accesso, acquisizione, divulgazione, perdita o utilizzo non autorizzato del Servizio e del Contenuto.

3.2 Se Accenture determina, che il report fornito contiene errori, o è, o potrebbe essere, soggetto a un reclamo secondo cui viola qualsiasi diritto di qualsiasi persona o entità, l'Amministrazione si impegna ad eliminare, correggere o rendere inaccessibili tale Contenuto su richiesta di Accenture. .

3.3 **Metadati.** L'Amministrazione autorizza Accenture a conservare per i propri scopi aziendali eventuali indicatori di compromissione, malware, vulnerabilità, anomalie o altri metadati rilevati come parte o correlati alla prestazione dei Servizi ("Metadati"). Accenture quindi potrà analizzare, copiare, archiviare e utilizzare tali metadati per scopi di miglioramento della sicurezza, compreso lo sviluppo di risorse di intelligence sulle minacce.

3.4 **Segnalazione**. L'Amministrazione resta responsabile della segnalazione di eventuali data breach. Qualora Accenture sia tenuta a segnalare qualsiasi informazione dell'Amministrazione alle forze dell'ordine o alle autorità di regolamentazione, Accenture farà tutto il possibile per avvisare l'Amministrazione stessa prima di rispondere e, se possibile, consentire alla stessa di sollevare

obiezioni presso tali autorità. Fatto salvo quanto sopra, l'Amministrazione consente ad Accenture di conformarsi ai requisiti delle autorità preposte all'applicazione della legge o delle autorità di regolamentazione in relazione ai Servizi.

3.5. **Trattamento Dati.** Il trattamento dei dati effettuato all'interno della Piattaforma ATIP, si intenderà regolato dall'atto di nomina che verrà sottoscritto tra le parti prima dell'avvio dei servizi. Si precisa che nelle categorie di interessati si intendono con il presente atto inclusi anche (i) i nomi e gli indirizzi e-mail aziendali degli utenti autorizzati ad accedere alla Piattaforma ATIP, come comunicati ad Accenture dall'Amministrazione, al fine di fornire le credenziali di accesso. (ii) qualsiasi dato personale con cui Accenture potrebbe, nel corso del Servizio, entrare in contatto e quindi condividere con l' Amministrazione, inclusi indirizzi e-mail aziendali, password o altri dati personali simili del personale, dei fornitori o dei clienti dell' Amministrazione, nonché di qualsiasi altro individuo i cui dati vengono restituiti a seguito di ricerche in base ai nomi/dati sulle parole chiave forniti dall'Amministrazione (dati personali ai sensi di (i) e (ii) collettivamente, nel contesto dei Servizi).