SERVIZIO SANITARIO NAZIONALE

REGIONE PIEMONTE

Azienda Sanitaria Locale "Città di Torino"

Costituita con D.P.G.R. 13/12/2016 n. 94
Cod. fiscale/P.I 11632570013
Sede legale: Via San Secondo, 29 – 10128 Torino
Tel. 011/5661566 e 011/4393111

Verbale di deliberazione del Direttore Generale,
Dott. Carlo Picco

*n. **1750**/01.03/2023 del 28 Dicembre 2023*

OGGETTO: **P.N.R.R. Missione 6 Salute, C2, Investimento 1.1. "AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO". Adesione ad Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi" - Lotto 2 (ID 2367) per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi NEXT GENERATION EU per la durata di 18 mesi, Unico Fornitore R.T.I. costituendo da TELECOM ITALIA S.p.A. P.I. 00488410010 (mandataria), MATICMIND S.p.A., DGS S.p.A., SCAI SOLUTION GROUP S.p.A. Importo 672.432,20 o.f.i. comprensivo di incentivo alle funzioni tecniche art. 45. CIG derivato A020E7A724.**

L'anno ***Duemilaventitre***, il giorno ***Ventotto*** del mese di ***Dicembre***, in Torino, presso l'Azienda Sanitaria Locale Città di Torino, in sede di via S. Secondo, 29

art.14

SERVIZIO SANITARIO NAZIONALE
REGIONE PIEMONTE
Azienda Sanitaria Locale "Città di Torino"
Costituita con D.P.G.R. 13/12/2016 n. 94
Cod. fiscale/P.I. 11632570013
Sede legale: Via San Secondo, 29 – 10128 Torino
☏ 011/5661566 ☏ 011/4393111

Deliberazione del Direttore Generale
S.C. Tecnologie

OGGETTO: P.N.R.R. Missione 6 Salute, C2, Investimento 1.1. "AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO". Adesione ad Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi" – Lotto 2 (ID 2367) per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi NEXT GENERATION EU per la durata di 18 mesi, Unico Fornitore R.T.I. costituendo da TELECOM ITALIA S.p.A. P.I. 00488410010 (mandataria), MATICMIND S.p.A., DGS S.p.A., SCAI SOLUTION GROUP S.p.A. Importo 672.432,20 o.f.i. comprensivo di incentivo alle funzioni tecniche art. 45. CIG derivato A020E7A724.

Su proposta del Direttore della Struttura Complessa Tecnologie, Ing. Francesco PENSALFINI, che di seguito si riporta:

- Visto il Piano Nazionale di Ripresa e Resilienza presentato dall'Italia alla Commissione europea in data 30 aprile 2021, ai sensi dell'articolo 18 del Regolamento (UE) n. 2021/241 sopra richiamato, ed approvato il 13 luglio 2021 con Decisione di esecuzione del Consiglio Europeo;

- Preso atto che tra le Missioni del PNRR è prevista la Missione 6 Salute, in cui investimenti e riforme sono finalizzati a rafforzare la prevenzione e i servizi sanitari sul territorio, modernizzare e digitalizzare il sistema sanitario, garantire equità di accesso alle cure, migliorare le dotazioni infrastrutturali e tecnologiche, promuovere la ricerca e l'innovazione e lo sviluppo di competenze tecnico-professionali, digitali e manageriali del personale sanitario; la suddetta Missione 6 Salute si articola in Componenti e aree di Investimento e sotto interventi;

- Dato atto che l'investimento [M6.C2_1.1.1.] mira alla digitalizzazione dei processi clinico-assistenziali delle strutture ospedaliere pubbliche del SSR sede di DEA di I e II livello. Secondo la programmazione del Piano, ogni ospedale digitalizzato dovrà disporre di un Centro Elaborazione Dati (DPC) necessario per realizzare l'informatizzazione dell'intera struttura ospedaliera e di sufficienti tecnologie informatiche hardware e/o software, tecnologie elettromedicali, nonché tecnologie aggiuntive necessarie per realizzare l'informatizzazione di ciascun reparto ospedaliero per assicurare un livello 4 di informatizzazione;

- Richiamati i provvedimenti di Giunta regionali relativi al Piano operativo regionale (POR), D.G.R. n.1-4892 del 20 aprile 2022, e del contratto istituzionale di sviluppo (CIS), D.G.R. n. 23-5124 del 27 maggio 2022;

- Dato atto della D.G.R. n. 25 – 5186 del 14 giugno 2022, PNRR Missione 6 Salute. Ripartizione, ai sensi dell'art.5, comma 1 del contratto istituzionale di sviluppo (CIS), delle attività per l'attuazione del PNRR e del Piano nazionale per gli investimenti complementari (PNC), alle Aziende sanitarie regionali, in qualità di soggetti attuatori esterni delegati. Riparto agli Enti del SSR delle risorse del PNRR e PNC per complessivi Euro 524.744.995,00;

- Vista la nota della Regione Piemonte prot. n. 7578 del 25.02.2022 avente ad oggetto: "PNRR Missione 6 Salute, investimento 1.1 Ammodernamento del parco tecnologico e digitale ospedaliero, componente 2 Innovazione ricerca e digitalizzazione del SSN (digitalizzazione delle strutture ospedaliere – DEA I e II)", in cui sono fornite le indicazioni operative per pubblicare le Schede d'intervento sul sito AGE.NA.S.;

- Preso atto che in data 01.03.2022 l'ing. Francesco Pensalfini, ha provveduto alla compilazione e al conseguente caricamento delle schede AGE.NA.S. finalizzate all'attuazione degli interventi M6.C2_1.1.1 del PNRR del Ministero della Salute, consultabili su sito https://pnrr.agenas.it, protocollo di riferimento n. 0173791 del 22.11.2022;

- Vista la deliberazione 410/02.00/2022 del 21.03.2022 avente ad oggetto la nomina a RUP del Direttore della S.C. Tecnologie, Ing. Francesco Pensalfini, per la gestione e il coordinamento del progetto riguardante l'ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione delle strutture Ospedaliere – DEA Dipartimenti di Emergenza e Accettazione di livello I e II);

- Considerato che il settore sanitario italiano ha subito un incremento degli attacchi informatici da parte dei cyber criminali in ragione della qualità e della quantità di dati sensibili che vi transitano e che generano un grande valore economico; tenuto conto dell'attacco informatico di tipo "ransomware" subito in data 19.08.2022 da questa amministrazione, che ha significativamente disagiato le regolari attività, impegnandola per mesi nel processo di ripristino degli applicativi e dei dati; rilevata la necessità di attuare degli interventi di miglioramento su alcuni moduli relativi al progetto "Cartella Clinica Elettronica Ospedaliera", in questo contesto l'ASL Città di Torino ha ritenuto opportuno affiancare alle misure di sicurezza attualmente in uso, ulteriori servizi specialistici per il raggiungimento di un livello di sicurezza maggiore, attraverso:
  - il rinnovo della fornitura delle licenze Cynet;
  - la raccolta e l'analisi dei dati di tutti i sistemi on-site, quali PDL dell'utenza, server fisici o virtuali e apparati di vario genere, da effettuare anche per i servizi che permettono di avere visibilità sugli eventi di sicurezza attivati interni all'ASL. Nella fattispecie: controllori di dominio e loro servizi (AD, DNS, DHCP), sistema di rilevazione antivirus, sistema di analisi EDR delle postazioni (Cynet), sistemi di analisi del traffico (Medigate), sistemi di autenticazione per apparati Wifi (Aruba Clearpass), sistemi di inventario

delle PDL (Lansweeper), sistemi di raccolta dati di navigazione (Firewall, FortyAnalyzer) nonché il sistema di piattaforma virtuale (VSphere);
- l'analisi esaustiva e predittiva, attraverso le verifiche dei log inviati dai sistemi, al fine di ottenere una valida risposta alle problematiche di sicurezza che vengono riscontrate.

- Dato atto che sul sito "acquistinretepa.it" risulta attivo l'Accordo Quadro "Cybersecurity 2 - prodotti e servizi connessi" – Lotto 2 (ID 2367), CIG 8898075BC5, il cui operatore economico aggiudicatario risulta essere il RTI costituendo da TELECOM ITALIA SPA - MATICMIND SPA - DGS SPA - SCAI SOLUTION GROUP SPA;

- Preso atto che risultano oggetto del suddetto AQ i prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi. In particolare sono previsti i seguenti beni:
  - Next Generation Firewall (NGFW)
  - Network Access Control (NAC)
  - Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR)
  - Server Protection Platform (SPP)
  - Protezione Anti-Advanced Persistent Threat (Anti-APT)

  e i seguenti servizi connessi alla fornitura:
  - installazione e configurazione
  - formazione e affiancamento
  - manutenzione
  - hardening su client
  - Contact Center ed help desk
  - supporto specialistico.

  La durata temporale dell'AQ è fissata in 18 mesi dalla data di sottoscrizione del contratto tra l'Asl e l'operatore economico. I singoli contratti di fornitura si perfezionano con l'accettazione da parte dell'Aggiudicatario degli Ordinativi di Fornitura e non potranno avere una durata superiore a 24 mesi;

- Dato atto che a supporto degli interventi sopra descritti si rende necessaria la seguente acquisizione:
  - Installazione e configurazione delle Licenze Cynet - 360 - EPP - EDR - C - Fascia 4 per 6.000 endpoint di tipo client;
  - Erogazione di servizi di supporto specialistico per l'esecuzione delle seguenti attività:
    a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Asl al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso;
    b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Asl;

c) il supporto operativo al personale dell'Asl nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Asl, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito

d) supporto alla reingegnerizzazione della rete dell'Amministrazione, incluse le necessarie attività di assessment, profilazione e documentazione dell'AS-IS e del TO-BE;

- Dato atto che in data 19.09.2023 il RUP, Ing. Francesco Pensalfini, ha provveduto ad inviare al RTI aggiudicatario del Lotto 2, tramite la piattaforma "acquistinretepa.it", l'ordine preliminare n. 7411144 con il relativo Piano dei Fabbisogni (prot. n. 135787 del 20.09.2023, allegati alla presente delibera), inerenti l'Accordo Quadro in oggetto;

- Preso atto che in data 10.10.2023 il RTI ha restituito il Piano Operativo definitivo (prot. n. 148197 del 10.10.2023, allegato alla presente delibera) per "l'affidamento di prodotti per la sicurezza perimentrale – protezione degli endpoint";

- Dato atto che in data 20.10.2023 il RUP con pec prot. n. 155153 ha richiesto alcune modifiche al piano operativo;

- Preso atto che in data 23.10.2023 è pervenuto il piano operativo modificato (prot. n. 155407);

- Considerato che in data 20.11.2023 l'ASL Città di Torino ha approvato il Piano Operativo, ritenuto congruo alle richieste del piano dei fabbisogni trasmesso, e che contestualmente in data 24.11.2023 codesta ASL ha provveduto al caricamento sulla piattaforma acquistinretepa.it dell'ordinativo di fornitura, RDO n. 7518448 (prot. n. 183047);

- Considerato che la tabella seguente riporta l'importo contrattuale (I.V.A. esclusa) con indicazioni di quantità e metrica:

Prodotti:

Prodotto	Tecnologia	Fascia	Modello	Codice articolo produttore	Quantità	Importo unitario	Importo totale
EPP	CYNET	4	Agent Cynet 360	Cynet 360 EPP EDR C F4	6.000	4,61 €	27.660 €

Servizi di supporto specialistico:

Prodotto / Fascia	Codice servizio	Codice fornitore	Quantità (gg/uomo)	Importo unitario	Importo totale
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	1.050	227,50 €	238.875 €
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	1.024	271,00 €	277.504 €

Nella tabella successiva si riporta il dimensionamento della fornitura, in termini economici per singolo presidio DEA:

CUP	Presidio	Accordo Quadro	CIG A.Q.	CIG Derivato	Importo O.F.I.
F17H22001230001	Osp. Maria Vittoria	Cybersecurity 2 - Prodotti e servizi connessi - Lotto 2	8898075BC5	A020E7A724	212.632,75 €
F17H22001240001	Osp. Martini	Cybersecurity 2 - Prodotti e servizi connessi - Lotto 2	8898075BC5	A020E7A724	195.194,31 €
F17H22001250001	Osp. S.G. Bosco	Cybersecurity 2 - Prodotti e servizi connessi - Lotto 2	8898075BC5	A020E7A724	255.900,52 €

- Dato atto che il costo complessivo di € 663.727,58 inclusa IVA derivante dal presente provvedimento è riconducibile nell'autorizzazione di spesa n. 700 del 2023, conto economico n. 1110302 – Software;

- Dato atto che sono state acquisite agli atti le dichiarazioni di assenza di conflitto di interessi firmate dal RUP, Ing. Francesco Pensalfini (prot. n. 171611 del 20.11.2023) e dal DEC, sig. Gianluca Lucarelli (prot. n. 171646 del 20.11.2023);

- Dato atto che è stato rispettato il divieto del doppio finanziamento e che risulta agli atti la dichiarazione del Responsabile della S.C. Economico Finanziario, prot. n. 179470 del 04.12.2023, e il principio di addizionalità del sostegno dell'Unione europea previsto dall'art. 9 del Regolamento (UE) 2021/241;

- Dato atto che relativamente alla "tutela del rispetto degli interessi finanziari dell'Unione Europea", sono state effettuate verifiche relative alle misure di contrasto al riciclaggio e finanziamento del terrorismo;

- Dato atto che i beni oggetto del presente provvedimento (licenze software e supporto specialistico) rispettano il principio del "non arrecare danno significativo all'ambiente" (DNSH) e il principio del contributo all'obiettivo climatico e digitale (cd. Tagging);

- Dato atto che rispetto al principio delle pari opportunità, il fornitore ha dichiarato:
  - di assicurare una quota pari ad almeno il 30% delle assunzioni necessarie per l'esecuzione del contratto o per la realizzazione di attività ad esso connesse o strumentali, destinata sia all'occupazione giovanile sia all'occupazione femminile, come previsto dall'art. 47 comma 4 del D.L. n. 77/2021 convertito con modifiche in l. n. 108/2021;
  - che nei dodici mesi antecedenti alla presentazione dell'offerta nell'ambito della presente procedura, non ha violato l'obbligo di cui all'art. 47, comma 3, del D.L. 77/2021, convertito con modificazioni dalla L. n. 108/2021;

- Dato atto che sono state rispettate le Clausole contenenti l'obbligo di conseguimento di milestone e garantita la realizzazione della misura prevista nel progetto coerente con il PNRR;

- Preso atto che la procedura, associata ai CUP F17H22001230001, F17H22001240001, e F17H22001250001, sono state registrate sul sito dell'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture:

Accordo Quadro	CIG Accordo Quadro	Numero gara	CIG Derivato	Ditta	RDO
Servizi di supporto in ambito "Sanità Digitale"	8898075BC5	9388466	A020E7A724	Telecom Italia S.p.A., Maticmind S.p.A., DGS S.p.A., Scai Solution Group S.p.A.	7518448

- Dato atto che tutta la documentazione sopra citata è custodita presso la S.C. Tecnologie dell'ASL Città di Torino;

- Tenuto conto che l'art. 45 del D.Lgs. 36/2023 e s.m.i. "Incentivi alle funzioni tecniche", al comma 1 prevede che "*Gli oneri relativi alle attività tecniche indicate nell'allegato I.10 sono a carico degli stanziamenti previsti per le singole procedure di affidamento di lavori, servizi e forniture negli stati di previsione della spesa o nei bilanci delle stazioni appaltanti e degli enti concedenti*" in misura non superiore al 2% dell'importo posto a base delle procedure di affidamento (comma 2), comprensivi anche degli oneri previdenziali ed assistenziali a carico dell'Amministrazione (comma 3);

- Considerato che ai sensi dello stesso articolo di cui sopra al comma 3 si stabilisce che *"L'80 per cento delle risorse di cui al comma 2, è ripartito, per ogni opera, lavoro, servizio e fornitura, tra il RUP e i soggetti che svolgono le funzioni tecniche indicate al comma 2, nonché tra i loro collaboratori"* e che il restante 20%, secondo il comma 5 art. 45, non è soggetto ad accantonamento al fondo innovazione nel caso di progetti finanziati;

- Tenuto conto che l'art. 8, comma 5, DL 13/2023 (convertito dalla L. 41/2023) per gli anni dal 2023 al 2026, gli enti locali e gli enti e le aziende del Servizio sanitario nazionale prevedono nei propri regolamenti e previa definizione dei criteri in sede di contrattazione decentrata, la possibilità di erogare, relativamente ai progetti del PNRR, l'incentivo di cui all'articolo 113 del codice dei contratti pubblici, di cui al decreto legislativo 18 aprile 2016, n. 50, anche al personale di qualifica dirigenziale coinvolto nei predetti progetti;

- Tenuto conto delle attività tecniche presenti nell'allegato I.10 "Attività tecniche a carico degli stanziamenti previsti per le singole procedure" del D.Lgs. 36/2023 e s.m.i. si è stabilito di individuare il fondo incentivante pari a € 8.704,62 basato su un importo pari a € 544.039,00 (o.f.e.) secondo il seguente quadro economico ed interamente a carico del finanziamento:

QUADRO ECONOMICO	IMPORTO
A) Importo per fornitura del servizio (o.f.e.)	*€ 544.039,00*
B) Quota incentivo per attività tecniche art. 45 comma 2 del D.Lgs. 36/2023	*€ 8.704,62*
C) IVA (22%): A)	*€ 119.688,58*
TOTALE GENERALE	**€ 672.432,20**

- dato atto che a seguito dell'approvazione aziendale del regolamento concernente le modalità operative per la corresponsione degli incentivi tecnici alle funzioni tecniche ai sensi dell'art. 45 del Dlgs 36/2023 la S.C. Tecnologie provvederà a verificare ed adeguare, se necessario, gli stanziamenti effettuati in coerenza alle modalità operative definite aziendalmente;

- considerato che la formulazione della proposta di un atto deliberativo impegna la responsabilità del soggetto proponente circa la regolarità amministrativa del contenuto della deliberazione nonché della legittimità della stessa;

Tutto ciò premesso,

Il Direttore Generale
Dr. Carlo PICCO
nominato con D.G.R. n. 9 - 2521 dell'11/12/2020

- Visto il D. Lgs. 30.12.1992, n. 502 e successive modificazioni e integrazioni;
- Vista la L.R. 6.8.2007, n. 18;
- Vista la L.R. 24.1.1995, n. 10;
- Esaminata e condivisa la succitata proposta del Direttore della Struttura Complessa Tecnologie, Ing. Francesco PENSALFINI;
- Considerato che la formulazione della proposta di un atto deliberativo impegna la responsabilità del soggetto proponente circa la regolarità amministrativa del contenuto della deliberazione nonché della legittimità della stessa;
- Acquisiti i pareri favorevoli espressi dal Direttore Amministrativo, Dott.ssa Elena Teresa TROPIANO, e dal Direttore Sanitario, Dr. Stefano TARAGLIO, a norma dell'art. 3 del D.lgs 30.12.1992 n. 502, e successive modificazioni e integrazioni;

D E L I B E R A

1. Per le motivazioni espresse in premessa, di aderire, nell'ambito del P.N.R.R. Missione 6 Salute, C2 Innovazione ricerca e digitalizzazione del SSN (digitalizzazione delle strutture ospedaliere – DEA I e II), Investimento 1.1. "Ammodernamento del parco tecnologico e digitale ospedaliero", all'Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi

connessi" – Lotto 2 (ID 2367) per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi occorrenti all'ASL Città di Torino per la durata di 18 mesi, con decorrenza dalla data di sottoscrizione del contratto, con unico fornitore il RTI costituendo da Telecom Italia S.p.A. (mandataria) P.I. 00488410010, Maticmind S.p.A., DGS S.p.A., Scai Solution Group S.p.A. Importo pari ad euro 672.432,20 o.f.i. finanziato con fondi dell'Unione Europea nell'ambito del progetto NextGenerationEU.

2. Di autorizzare la S.C. Tecnologie ad emettere l'ordinativo NSO alla Società Telecom Italia S.p.A., P.I 00488410010, con sede legale in Milano, Piazza degli Affari per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi.

3. Di approvare come parte integrante e sostanziale del presente atto:
   - Ordine n. 7411144 (prot. n. 135787 del 20.09.2023)
   - Piano dei Fabbisogni (prot. n. 135787 del 20.09.2023)
   - Piano Operativo (prot. n. 155407 del 23.10.2023)
   - Contratto esecutivo tra ASL e Fornitore, e relativi allegati (prot. n. 185241 del 14.12.2023).

4. Di dare atto che la spesa complessiva derivante dal presente provvedimento trova copertura nell'ambito del finanziamento di cui al PNRR - Missione 6 Salute, Componente 2 Innovazione ricerca e digitalizzazione del SSN (digitalizzazione delle strutture ospedaliere – DEA I e II), investimento 1.1. "Ammodernamento del parco tecnologico e digitale ospedaliero" dell'Unione Europea-NextGenerationEU, di cui alla D.G.R. 25-5186 del 14.06.2022, ed è riconducibile al Conto economico 1110302 – Sofware nell'autorizzazione di spesa n. 700 del 2023 per l'importo pari ad euro 663.727,58 oneri fiscali inclusi (euro 544.039,00 + IVA euro 119.688,58) e al Conto economico 3101684 – Acc. Incentivi funzioni tecniche per l'importo pari ad euro 8.704,62 e che sarà capitalizzato successivamente sul conto economico 1110302 – Software.

5. Di dare altresì atto che i finanziamenti, di cui al punto precedente, sono codificati nella contabilità dell'ASL Città di Torino, con i seguenti codici progetto, al fine di assicurare la tracciabilità dell'utilizzo delle risorse del PNRR.:
   - Maria Vittoria, DEA I, CUP n. F17H22001230001, sub autorizzazione 1, Cod. Progetto PNRR_TECNO_1_F7;
   - Martini, DEA I, CUP n. F17H22001240001, sub autorizzazione 2, Cod. Progetto PNRR_TECNO_2_F7;
   - San Giovanni Bosco, DEA II, CUP n. F17H22001250001, sub autorizzazione 3, Cod. Progetto PNRR_TECNO_3_F7

SEDE	LIVELLO DEA	CODICE CUP	ANNO 1	ANNO 2	INCENTIVO art. 45
MARIA VITTORIA	DEA I	F17H22001230001	111.721,71	100.911,05	2.788,63
MARTINI	DEA I	F17H22001240001	102.559,18	92.635,12	2.559,92
S.G. BOSCO	DEA II	F17H22001250001	134.455,50	121.445,02	3.356,07
		TOTALE (IVA INCLUSA)	***348.736,39***	***314.991,19***	***8.704,62***

6. Di dare atto che, in conformità a quanto previsto dal D.M. 7 marzo 2018, n. 49 la responsabilità dell'esecuzione del contratto, in ordine al controllo tecnico contabile e amministrativo, è affidato al Direttore della S.C. Tecnologie, Ing. Francesco Pensalfini;

7. Di nominare ai sensi dell'art. 114 comma 1 del D.Lgs 36/2023 il sig. Gianluca Lucarelli quale Direttore per l'esecuzione del Contratto, le cui attestazioni di assenza di conflitto di interessi sono conservate agli atti (prot. n. 171646 del 20.11.2023).

8. Di trasmettere la presente deliberazione al Collegio Sindacale, per gli adempimenti di competenza, ai sensi dell'articolo 14, comma 2 lettera b), della L.R. 25 gennaio 1995, n. 10.

9. Di dichiarare la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 28 della legge regionale 24.01.1995, n. 10, al fine di avviare la stipula del contratto d'esecuzione nel più breve tempo possibile.

Allegati:
1. Ordine n. 7411144
2. Piano dei Fabbisogni
3. Piano Operativo
4. Contratto esecutivo tra ASL e Fornitore, e relativi allegati

Firmatari:

Responsabile del Procedimento: Ing. Francesco Pensalfini
Proponente: Direttore S.C. Tecnologie, Ing. Francesco Pensalfini
Direttore S.C. Gestione economico finanziaria: Dott.ssa Stefania Marino
Direttore Amministrativo: **Dott.ssa Elena Teresa TROPIANO***
Direttore Sanitario: **Dr. Stefano TARAGLIO***
Direttore Generale: **Dr. Carlo PICCO**
Estensore dell'atto: Ing. Simona Iaropoli

**I pareri favorevoli dei Direttori Amministrativo e Sanitario sono confermati con la sottoscrizione digitale del presente atto ed il rinvio automatico ai motivi della proposta. I pareri sfavorevoli sono esplicitamente motivati ed indicati in un allegato, firmato digitalmente.

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

12-87-69-DA-6A-86-E3-82-91-78-4D-01-78-95-9C-22-5C-CE-CD-A9

CAdES 1 di 6 del 28/12/2023 17:22:25

Soggetto: Carlo Picco

S.N. Certificato: E16942

Validità certificato dal 28/12/2022 10:18:43 al 28/12/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 6 del 27/12/2023 17:49:32

Soggetto: Stefano Taraglio

S.N. Certificato: E5BBC7

Validità certificato dal 13/01/2023 11:01:07 al 13/01/2026 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 6 del 27/12/2023 16:20:06

Soggetto: Elena Teresa Tropiano

S.N. Certificato: 15F9887

Validità certificato dal 28/07/2021 10:38:02 al 28/07/2024 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 4 di 6 del 22/12/2023 15:35:27

Soggetto: Stefania Marino

S.N. Certificato: BDF488

Validità certificato dal 02/09/2022 12:48:30 al 16/09/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 5 di 6 del 21/12/2023 14:36:34

Soggetto: Francesco Pensalfini

S.N. Certificato: 16E5129

Validità certificato dal 30/03/2022 16:57:33 al 08/04/2025 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 6 di 6 del 21/12/2023 12:23:25

Soggetto: Simona Iaropoli

S.N. Certificato: B2B41D

Validità certificato dal 21/07/2022 09:52:51 al 21/07/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

DELIBERAZIONE n° **0001750/01.03/2023** del 28 DICEMBRE 2023

IMMEDIATAMENTE ESEGUIBILE

INVIO AL COLLEGIO SINDACALE

Prot. n. 2024/0000402 del 02/01/2024

INVIO AL CONTROLLO DELLA GIUNTA REGIONALE

Data spedizione

Prot. n.

Ricezione regione

Risposta della regione

D.G.R. n. del

Commento:

Atto decaduto per i seguenti motivi:

INVIO AL CONTROLLO DELLA CORTE DEI CONTI

Prot. n. del

CERTIFICATO DI PUBBLICAZIONE ALL' ALBO ON LINE

La verifica della corretta composizione del plico documentale pubblicato è stata effettuata da VENEZIANO CALOGERO GIUSEPPE, in data 08 GENNAIO 2024.

Si certifica che il presente provvedimento è stato pubblicato senza opposizioni all'Albo on-line sul sito www.aslcittaditorino.it per 15 giorni consecutivi, dal giorno 08 GENNAIO 2024

ESECUTIVITA' **18 GENNAIO 2024**

Torino, 09 febbraio 2024

ASL CITTA' DI TORINO
S.C. Legale e Affari Generali
Settore Deliberazioni e Determinazioni

sottoscritto con firma elettronica qualificata

Nota bene: Eventuali originali cartacei sono conservati presso gli archivi aziendali della struttura proponente/adottante il provvedimento.

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

B5-5F-0D-3D-88-2F-8B-0B-23-05-99-B1-6E-EA-4E-1D-24-23-71-58

CAdES 1 di 1 del 15/02/2024 10:36:23

Soggetto: Rosella Andriola

S.N. Certificato: FCB578

Validità certificato dal 16/03/2023 10:01:17 al 17/03/2026 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

---

acquistinretepa.it
Il Portale degli acquisti della Pubblica Amministrazione

ORDINE DIRETTO DI ACQUISTO	
Nr. Identificativo Ordine	7411144
Descrizione Ordine	Servizi di Sicurezza Informatica Cyber Security - PNRR digitalizzazione DEA
Strumento d'acquisto	Accordi Quadro
CIG	non sussiste l'obbligo di richiesta
CUP	F17H22001230001
Bando	Cybersecurity 2 - prodotti e servizi connessi
Categoria(Lotto)	Lotto 2 - Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi – Lotto PAL Nord
Data Creazione Ordine	19/09/2023
Validità Documento d'Ordine (gg solari)	nessuna scadenza / nessun limite
Data Limite invio Ordine firmato digitalmente	nessuna scadenza / nessun limite
AMMINISTRAZIONE CONTRAENTE	
Nome Ente	AZIENDA SANITARIA LOCALE - CITTA' DI TORINO
Codice Fiscale Ente	11632570013
Nome Ufficio	SC TECNOLOGIE
Indirizzo Ufficio	CORSO SVIZZERA 164 10149 TORINO, 10100 - TORINO (TO)
Telefono / FAX ufficio	0114393809/null
IPA - Codice univoco ufficio per Fatturazione elettronica	Z87MJV
Punto Ordinante	FRANCESCO PENSALFINI / CF: PNSFNC65D06G479K
Email Punto Ordinante	FRANCESCO.PENSALFINI@ASLCITTADITORINO.IT
Partita IVA Intestatario Fattura	11632570013
Ordine istruito da	FRANCESCO PENSALFINI
FORNITORE CONTRAENTE	
Ragione Sociale	TELECOM ITALIA SPA (in RTI)
Partita IVA Impresa	00488410010
Codice Fiscale Impresa	00488410010
Indirizzo Sede Legale	VIA GAETANO NEGRI, 1 - 20100 - MILANO(MI)
Telefono / Fax	800333666/800333669
PEC Registro Imprese	GESTIONE.CONVENZIONI@PEC.TELECOMITALIA.IT
Tipologia impresa	SOCIETÀ PER AZIONI
Numero di Iscrizione al Registro Imprese / Nome e Nr iscrizione Albo Professionale	00488410010
Data di iscrizione Registro Imprese / Albo Professionale	05/08/2003
Provincia sede Registro Imprese / Albo Professionale	MI
INAIL: Codice Ditta / Sede di Competenza	3441073
INPS: Matricola aziendale	7036858465
Posizioni Assicurative Territoriali - P.A.T. numero	08315476
PEC Ufficio Agenzia Entrate competente al rilascio attestazione regolarità pagamenti imposte e tasse:	DR.LOMBARDIA.GTPEC@PCE.AGENZIAENTRATE.IT
CCNL applicato / Settore	IMPRESE ESERCENTI SERVIZI DI

acquistinretepa.it
Il Portale degli acquisti della Pubblica Amministrazione

Oggetto dell'ordine (1 di 1) - Scheda tecnica: CS2L2 Richiesta Piano Operativo
Nome commerciale: Richiesta Piano Operativo - Descrizione tecnica: Richiesta Piano Operativo - Codice articolo accordo quadro: CS2L2-RPO - Unità di vendita: Servizio - Prezzo: 0,00 - Area di consegna: ITALIA - Tipo contratto: Acquisto - Condizioni di fornitura: PRELIMINARE

RIEPILOGO ECONOMICO

Oggetto	Nome Commerciale	Prezzo Unitario (€)	Qtà ordinata	Prezzo Complessivo (IVA esclusa)	Aliquota IVA (%)
1	Richiesta Piano Operativo	0,00	1 (Servizio)	0,00 €	22,00

Totale Ordine (IVA esclusa) €	0,00
IVA €	0,00
Totale Ordine (IVA inclusa) €	0,00

INFORMAZIONI DI CONSEGNA E FATTURAZIONE

Indirizzo di Consegna	CORSO SVIZZERA 164 10149 TORINO - 10100 - TORINO - (TO)
Indirizzo di Fatturazione	CORSO SVIZZERA 164 10149 TORINO - 10100 - TORINO - (TO)
Intestatario Fattura	AZIENDA SANITARIA LOCALE - CITTA' DI TORINO
Codice Fiscale Intestatario Fattura	11632570013
Partita IVA da Fatturare	11632570013
Modalità di Pagamento	Bonifico Bancario

NOTE ALL'ORDINE

ORDINE PER PIANO OPERATIVO RELATIVO A N. 3 CUP PROGETTO PNRR:
F17H22001230001
F17H22001240001
F17H22001250001

DOCUMENTI ALLEGATI ALL'ORDINE

Allegato 1.PIANO DEI FABBISOGNI PIANO DEI FABBISOGNI ASL CITTÀ DI TORINO V3 SIGNED.PDF - dim. 1204.81 Kb

DISCIPLINA ED ALTRI ELEMENTI APPLICABILI AL PRESENTE CONTRATTO

Visto l'Accordo Quadro per ogni lotto, avente ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni - ID 2367 - considerati i termini, le modalità e le condizioni in esso stabilite – DICHIARA: di aderire all'Accordo Quadro e di accettare tutte le condizioni normative ed economiche ivi previste.

QUESTO DOCUMENTO NON HA VALORE SE PRIVO DELLA SOTTOSCRIZIONE A MEZZO FIRMA DIGITALE

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

5F-06-59-54-51-71-F0-57-48-30-CA-8E-B8-63-B1-1E-FC-69-B0-72

CAdES 1 di 1 del 19/09/2023 16:45:16

Soggetto: Francesco Pensalfini PNSFNC65D06G479K

Validità certificato dal 18/07/2023 15:02:18 al 18/07/2026 02:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT con S.N. 012D ACE3

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

B2-85-2A-35-4B-FA-EE-EA-34-DA-39-E8-85-BC-A1-5B-1F-34-2A-2F

CAdES 1 di 6 del 28/12/2023 17:22:26

Soggetto: Carlo Picco

S.N. Certificato: E16942

Validità certificato dal 28/12/2022 10:18:43 al 28/12/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 6 del 27/12/2023 17:49:33

Soggetto: Stefano Taraglio

S.N. Certificato: E5BBC7

Validità certificato dal 13/01/2023 11:01:07 al 13/01/2026 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 6 del 27/12/2023 16:20:06

Soggetto: Elena Teresa Tropiano

S.N. Certificato: 15F9887

Validità certificato dal 28/07/2021 10:38:02 al 28/07/2024 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 4 di 6 del 22/12/2023 15:35:28

Soggetto: Stefania Marino

S.N. Certificato: BDF488

Validità certificato dal 02/09/2022 12:48:30 al 16/09/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 5 di 6 del 21/12/2023 14:36:34

Soggetto: Francesco Pensalfini

S.N. Certificato: 16E5129

Validità certificato dal 30/03/2022 16:57:33 al 08/04/2025 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 6 di 6 del 21/12/2023 12:23:26

Soggetto: Simona Iaropoli

S.N. Certificato: B2B41D

Validità certificato dal 21/07/2022 09:52:51 al 21/07/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

ACCORDO QUADRO PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI

ID 2367

PIANO DEI FABBISOGNI SERVIZI

Spett.le
TELECOM ITALIA S.p.A.

Lo scrivente __**ASL Città di Torino** _____ C.F. / P.IVA **11632570013**
Codice IPA ASLTO
con sede legale in **Torino** Prov. **TO** CAP **10128** Nazione **ITALIA**
Indirizzo: **Via San Secondo 29**

chiede che venga realizzato quanto di seguito indicato (barrare i servizi richiesti con il presente piano dei fabbisogni):

X EDP/EPR (compilare il Quadro **A**)	☐ **NAC** (compilare il Quadro **B**)
☐ **NGFW** (compilare il Quadro **C**)	☐ **ANTI - APT** (Compilare il Quadro **D**)
☐ **Server Protection** (compilare il Quadro **E**)	☐ **Servizio di Hardening** (compilare il Quadro **F**)
☐ **Servizio di Formazione** (compilare il Quadro **G**)	**X Servizio di Supporto Specialistico** (compilare il Quadro **H**)
☐ **Servizio di di Manutenzione** (compilare il Quadro **I**)	

Invio delle fatture

Codice Univoco Ufficio: **Z87MJV**
CIG (quando disponibile)**: ND**
NSO (quando disponibile)**: ND**
CUP: F17H22001230001, F17H22001240001, F17H22001250001

Domicilio fattura:

Località **Torino** Prov. **TO** CAP **10128** Nazione **ITALIA**
Indirizzo **Via San Secondo 29**

☐ Cliente esente IVA in base a _____ (allegare dichiarazione di intento)

Responsabile dell'Amministrazione per i rapporti con TELECOM ITALIA[1]

Nome **Francesco** Cognome **PENSALFINI**
Tel **011 566 2548** _____ Fax
E-mail**(obbligatoria)**tecnologie@aslcittaditorino.it **PEC** tecnologie@pec.aslcittaditorino.it

DATA _____ TIMBRO E FIRMA DEL CLIENTE

1 Tale nominativo sarà l'unico riconosciuto da TELECOM ITALIA per qualsiasi contatto inerente. a problematiche di tipo amministrativo/commerciale anche relative all'indicazione del/i luogo/ghi di esecuzione dei servizi. In caso di variazione il Cliente è tenuto a trasmettere a Telecom Italia, come indicato nella Richiesta di Adesione al Servizio, una comunicazione scritta.

Descrizione del Contesto di Riferimento in cui si riferisce la fornitura dell'Amministrazione
La fornitura è riferita al rinnovo delle licenze Cynet attualmente in uso per un totale di 6.000 end point.

Macro Requisiti ed Obiettivi che l'Amministrazione si propone con la fornitura

La necessità è quella di abbinare alla fornitura delle licenze sopra indicate le attività professionali in grado di erogare un servizio che prenda in carico le attività che riguardino in maniera specifica o generica le procedure di sicurezza informatica dell'ente.

Tali servizi devono includere la raccolta e l'analisi dei dati di tutti i sistemi on-site, quali PDL dell'utenza, server fisici o virtuali e apparati di vario genere. La raccolta dei dati verrà effettuata non solo per le postazioni precedentemente indicate ma anche da tutti quei servizi già attivi nel nostro perimetro che ci permettono di avere visibilità sugli eventi di sicurezza attivati al nostro interno. Questi sistemi sono nella fattispecie: controllori di dominio e loro servizi (AD, DNS, DHCP), sistema di rilevazione antivirus, sistema di analisi EDR delle postazioni (Cynet), sistemi di analisi del traffico (Medigate), sistemi di autenticazione per apparati Wifi (Aruba Clearpass), sistemi di inventario delle PDL (Lansweeper), sistemi di raccolta dati di navigazione (Firewall, FortyAnalyzer) nonché dal sistema di piattaforma virtuale (VSphere).

La necessità è quella di un'analisi esaustiva e predittiva, attraverso le verifiche dei log inviati dai sistemi oltre che quella di ottenere una valida risposta alle problematiche di sicurezza che vengono riscontrate.

La necessità dell'Ente è quella di esternalizzare il servizio relativo agli incidenti di sicurezza che avvengono all'interno delle reti Aziendali. Si chiede che la società affidataria del servizio preveda delle modalità di intervento risolutive delle problematiche che possano essere messe in atto in maniera tempestiva senza preoccuparsi della presenza in sede dei referenti interni all'ente. Ci saranno casi per i quali verrà previsto un confronto diretto tra le due parti (quale per esempio la presenza di incidenti su postazioni server) per ottenere la risposta più efficace e meno impattante sul lavoro quotidiano dell'utenza, ma la maggior parte delle attività dovrà essere svolta in "autonomia" fornendo all'ente le note informative delle attività intraprese per rispondere agli eventi riguardanti la sicurezza informatica.

Per poter operare in autonomia l'ente fornirà tutti gli strumenti per poter accedere ai propri sistemi di monitoraggio e analisi alla società offerente. Inoltre verranno forniti i recapiti delle persone incaricate dall'ente del servizio di reperibilità, al di fuori del normale orario di servizio, per un intervento celere verso PdL, server e apparati da effettuare in loco.

Al di là delle normali procedure operative già definite l'offerente dovrà garantire metodi per risolvere le problematiche di sicurezza e implementare procedure e percorsi condivisi e dedicati alle esigenze specifiche dell'Ente, nella normale evoluzione delle dinamiche di sicurezza dei sistemi.

Indicazione se il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché' dal PNC

Il Contratto è integralmente finanziato con fondi PNRR intervento M6.C2.1.1.1 Digitalizzazione dei DEA

Tempistiche richieste per la realizzazione della fornitura, con descrizione di eventuali vincoli e/o criticità

si chiede l'avvio dei servizi entro 30 giorni dall'ordine

Indicazione del/i luogo/ghi di interesse della fornitura

Corso Svizzera, n. 164, 10149 Torino TO

Durata del Contratto Esecutivo

24 mesi

Informazioni tecniche quali schemi di rete, piani di indirizzamento, apparati già in essere, utili a meglio comprendere il perimetro di interesse e indirizzare la migliore soluzione tecnologica, specificare:
Alloggiamento ed eventuale fissaggio sullo specifico supporto che sarà messo a disposizione dall'Amministrazione (rack, ripiano, …) in relazione alla tipologia apparato.
Indicazione del/i luogo/ghi di interesse della fornitura
N/A

Collegamento alla rete di alimentazione, presso il punto di presenza della rete indicato dall'Amministrazione.
Indicazione del/i luogo/ghi di interesse della fornitura

N/A_

Collegamento alla rete dati, presso il punto di presenza della rete indicato dall'Amministrazione.
N/A

Se prodotto hardware non è acquistato in sostituzione di un prodotto già presente l'amministrazione dovrà indicare i prerequisiti necessari all'installazione e configurazione :

1. **schemi logici dell'architettura**
2. **schemi di indirizzamento**
3. **requisiti delle policy di sicurezza stabiliti dall'Amministrazione**

N/A_____

Se il prodotto hardware è acquistato in sostituzione di un prodotto già presente presso l'Amministrazione oltre agli schemi logici e di indirizzamento indicare le impostazioni/policy/configurazioni attive e attualmente in esercizio
_N/A_____

Se il prodotto software è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare il tipo di prodotto attualmente utilizzato e se è un prodotto SaaS o On premise. La migrazione di un prodotto che sia SaaS oppure On premise nesessità di un supporto di servizi professionali.
N/A_____

Se il prodotto software non è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare la tipologia dei Client/Server sui quali dovrà essere installato il software.
N/A_

Le installazioni di prodotti software richiedono la configurazione del software di management sia per la componente Client (EPP) che Server (SPP)
L'amministrazione dovrà mettere a disposizione ambienti virtuali o fisici per gestire l'installazione di circa 5500 client EPP e circa 500 client SPP

Ulteriori informazioni che l'Amministrazione ritieni utili per lo svolgimento dell'attività del fornitore

N/A

QUADRO A - EDP/EPR

Descrizione del Servizio

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per l'EPP/EDR sono previste quattro fasce dimensionali:

- EPP_EDR_1 (fascia 1): fino a 500 client
- EPP_EDR_2 (fascia 2): fino a 1000 client
- EPP_EDR_3 (fascia 3): fino a 5000 client
- EPP_EDR_4 (fascia 4): oltre 5000 client

Endpoint Protection Platform & Endpoint Detection and Response				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
EPP & EDR - Fascia 1	EPP-F1-CYN	CYNET	Cynet-360-EPP-EDR-C-F1	
	EPP-F1-TM	TRENDMICRO	OS01141-EPP-C-F1	
	EPP-F1-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F1	
	EPP-F1-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F1	
EPP & EDR - Fascia 2	EPP-F2-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F2	
	EPP-F2-TM	TRENDMICRO	OS01141-EPP-C-F2	
	EPP-F2-CYN	CYNET	Cynet-360-EPP-EDR-C-F2	
	EPP-F2-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F2	
EPP & EDR - Fascia 3	EPP-F3-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F3	
	EPP-F3-TM	TRENDMICRO	OS01141-EPP-C-F3	
	EPP-F3-CYN	CYNET	Cynet-360-EPP-EDR-C-F3	
	EPP-F3-MCA	MCAFEE	MV6DEE-AA-DA+DLPECE-AT-DA-F3	
EPP & EDR - Fascia 4	EPP-F4-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F4	
	EPP-F4-TM	TRENDMICRO	OS01141-EPP-C-F4	
	EPP-F4-CYN	CYNET	Cynet-360-EPP-EDR-C-F4	**6.000**
	EPP-F4-MCA	MCAFEE	MV6DEE-AA-EA+DLPECE-AT-EA-F4	

QUADRO B - NAC

Descrizione del Servizio

Il NAC consente l'implementazione di regole per il controllo degli accessi all'infrastruttura aziendale da parte degli utenti, siano essi "umani" (attraverso personal computer, apparati mobili, …) oppure "cose" (elementi in ambito IoT). Le regole possono basarsi su più modalità quali l'autenticazione degli utenti, la configurazione degli apparati che accedono alla rete, il ruolo degli utenti. Per mezzo del NAC è inoltre possibile applicare regole successive alla connessione degli utenti, in base ad eventi che possono provenire da altri elementi di sicurezza.

Per i NAC sono previste sei fasce dimensionali/prestazionali:

- NAC_1 (fascia 1): fino a 100 Endpoint concorrenti
- NAC_2 (fascia 2): fino a 500 Endpoint concorrenti
- NAC_3 (fascia 3): fino a 1.000 Endpoint concorrenti
- NAC_4 (fascia 4): fino a 10.000 Endpoint concorrenti
- NAC_5 (fascia 5): fino a 25.000 Endpoint concorrenti
- NAC_6 (fascia 6): fino a 50.000 Endpoint concorrenti.

Network Access Control				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
NAC- Fascia 1	NAC-F1-HPE	HPE	JZ508AM-3Y-100C	
	NAC-F1-FN	FORTINET	FNC-CA-500C-BDL-C1	
NAC- Fascia 2	NAC-F2-HPE	HPE	JZ508AM-3Y-500C	
	NAC-F2-FN	FORTINET	FNC-CA-500C-BDL-C2	
NAC- Fascia 3	NAC-F3-HPE	HPE	JZ508AM-3Y-1000C	
	NAC-F3-FN	FORTINET	FNC-CA-500C-BDL-C3	
NAC- Fascia 4	NAC-F4-HPE	HPE	R1V81AM-3Y-10000C	
	NAC-F4-FN	FORTINET	FNC-CA-700C-BDL-C1	
NAC- Fascia 5	NAC-F5-HPE	HPE	R1V82AM-3Y-25000C	
	NAC-F5-FN	FORTINET	FNC-CA-700C-BDL-C2	
NAC- Fascia 6	NAC-F6-HPE	HPE	R1V82AM-3Y-50000C	
	NAC-F6-FN	FORTINET	FNC-CA-700C-BDL-C3	

QUADRO C - NGFW

Descrizione del Servizio

I NGFW sono apparati che consentono l'ispezione dei pacchetti di rete e si differenziano dai firewall "tradizionali" in quanto non si occupano solamente di analizzare e filtrare i pacchetti dati sulla base della porta e/o protocollo ma consentono di eseguire l'ispezione a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware e capacità di utilizzo di sorgenti esterne a supporto della propria attività di protezione.
Per i NGFW sono previste sei fasce dimensionali.

Next Generation Firewall				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
NGFW - Fascia 1	NGFW-F1-FN	FORTINET	FG-60F-BDL-C	
	NGFW-F1-CI	CISCO	CISCO-FPR1010-F1C	
	NGFW-F1-FP	FORCEPOINT	N120-C-F1	
	NGFW-F1-PA	PALO ALTO	PAN-PA-440-CONSIP-BUN-F1	
NGFW - Fascia 2	NGFW-F2-CI	CISCO	CISCO-FPR2110-F2C	

	NGFW-F2-FN	FORTINET	FG-200F-BDL-C	
	NGFW-F2-FP	FORCEPOINT	N2101-C-F2	
	NGFW-F2-PA	PALO ALTO	PAN-PA-3220-CONSIP-BUN-F2	
NGFW - Fascia 3	NGFW-F3-CI	CISCO	CISCO-FPR2130-F3C	
	NGFW-F3-FP	FORCEPOINT	N2101-C-F3	
	NGFW-F3-FN	FORTINET	FG-600E-BDL-C	
	NGFW-F3-PA	PALO ALTO	PAN-PA-3260-CONSIP-BUN-F3	
NGFW - Fascia 4	NGFW-F4-PA	PALO ALTO	PAN-PA-5220-CONSIP-BUN-F4	
	NGFW-F4-CI	CISCO	CISCO-FPR2140-F4C	
	NGFW-F4-FP	FORCEPOINT	N3401-C-F4	
	NGFW-F4-FN	FORTINET	FG-1100E-BDL-C	
NGFW - Fascia 5	NGFW-F5-PA	PALO ALTO	PAN-PA-5250-CONSIP-BUN-F5	
	NGFW-F5-CI	CISCO	CISCO-FPR4115-F5C	
	NGFW-F5-FP	FORCEPOINT	N3405-C-F5	
	NGFW-F5-FN	FORTINET	FG-2600F-BDL-C	
NGFW - Fascia 6	NGFW-F6-PA	PALO ALTO	PAN-PA-5260-CONSIP-BUN-F6	
	NGFW-F6-CI	CISCO	CISCO-FPR9300-F6C	
	NGFW-F6-FP	FORCEPOINT	N3410-C-F6	
	NGFW-F6-FN	FORTINET	FG-3400E-BDL-C	

QUADRO D - ANTI - APT

Descrizione del Servizio

La soluzione di Anti-APT consente l'analisi di file che possono essere inviati all'elemento da altri dispositivi di sicurezza o direttamente dal personale che si occupa di sicurezza. All'interno dell'ambiente protetto (sandbox) è quindi possibile, attraverso varie tecniche, esaminare i file e i loro comportamenti per determinare se questi siano o meno malevoli, assegnando loro un grado di severità.

Per l'Anti-APT sono previste due fasce dimensionali/prestazionali:

- Anti_APT_1 (fascia 1): fino a 450 file/ora
- Anti_APT_2 (fascia 2): fino a 1000 file/ora

Protezione anti-Advanced Persistent Threat				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
Anti-APT - Fascia 1	Anti-APT-F1-CP	CHECKPOINT	SandBlast TE Appliance TE100X-C	
	Anti-APT-F1-TM	TRENDMICRO	ADAXZZE5XL-C-F1	
Anti-APT - Fascia 2	Anti-APT-F2-CP	CHECKPOINT	SandBlast TE Appliance TE250X-C	
	Anti-APT-F2-TM	TRENDMICRO	ADAXZZE5XL-C-F2	

QUADRO E - Server Protection

Descrizione del Servizio

La soluzione SPP consente di proteggere gli endpoint di tipo server da minacce quali virus, trojan, worm, malware, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per la SPP sono previste quattro fasce dimensionali:

- SPP_1 (fascia 1): fino a 50 server
- SPP_2 (fascia 2): fino a 100 server
- SPP_3 (fascia 3): fino a 500 server
- SPP_4 (fascia 4): oltre 500 server

Server Protection Platform				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
SPP - Fascia 1	SPP-F1-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F1	
	SPP-F1-TM	TRENDMICRO	DX0099-SPP-C-F1	
SPP - Fascia 2	SPP-F2-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F2	
	SPP-F2-TM	TRENDMICRO	DX0099-SPP-C-F2	
SPP - Fascia 3	SPP-F3-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F3	
	SPP-F3-TM	TRENDMICRO	DX0099-SPP-C-F3	
SPP - Fascia 4	SPP-F4-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F4	
	SPP-F4-TM	TRENDMICRO	DX0099-SPP-C-F4	

QUADRO F - Servizio di Hardening

Descrizione del Servizio

Il servizio di hardening fornisce all'Amministrazione il supporto operativo necessario per rendere sicuri i client utilizzati. Le attività effettuate dovranno essere aderenti a quanto previsto dalle "*Linee guida per adeguare la sicurezza del software di base*" rilasciate da AgID.
Le specifiche attività che dovranno essere eseguite sono dipendenti dagli specifici software utilizzati sui client, ma in linea generale possono essere riassunte in:

- eliminazione di programmi non necessari dalle postazioni utente. Potenzialmente ogni programma è una porta di accesso per soggetti non legittimati e dunque la loro diminuzione consente di limitare i rischi di intrusioni. Tutti i programmi che non sono stati autorizzati e controllati e che non sono strettamente utili all'esecuzione delle attività lavorative dovrebbero essere rimossi;
- supporto ai sistemisti PA nelle fasi di monitoraggio e controllo che il sistema operativo e i programmi leciti siano aggiornati alle ultime versioni e agli ultimi "*service pack*" disponibili;
- controllo che sui client siano abilitati i servizi autorizzati, ossia che non vi siano "*demoni*" in ascolto sulle porte di rete se non quelli strettamente necessari;
- verifica che gli utenti abbiano i corretti privilegi in relazione al loro ruolo e che appartengono ai corretti gruppi utenti;
- verifica della consistenza delle password richieste e della periodicità di cambio password richiesta agli utenti;
- supporto ai sistemisti PA nella definizione di gruppi di policy che potranno essere applicati agli utenti sulla base dei loro ruoli;

- verifica che gli eventi di sicurezza siano correttamente storicizzati (logging) ai fini del controllo e dell'audit;
- supporto al personale dell'Amministrazione nella distribuzione delle azioni correttive individuate (ad es. installazione di eventuali *patch* mancanti, realizzazione e installazione di fix temporanee, etc..) siano esse relative al sistema operativo che ai programmi utilizzati.

Il servizio dovrà essere effettuato sulle postazioni di tipo client e dovrà includere almeno i seguenti software:

- Sistemi operativi Windows Client;
- Sistemi operativi macOS;
- Sistemi operativi UNIX/Linux di tipo Client;
- Principali Web Browser (Edge, Explorer, Firefox, Chrome);
- Principali applicativi software di produttività (Microsoft Office/OpenOffice, Pdf Readers, Outlook.

Servizio di Hardening			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Fase di assessment	ASS	HARD_ASSMNT	
Fase di distribuzione degli interventi -1001_5000	DISINT 1001-5000	HARD_DISTR_1001_5000	
Fase di distribuzione degli interventi - 2_1000	DISINT 2-1000	HARD_DISTR_2_1000	
Fase di distribuzione degli interventi - 5001_	DISINT>5000	HARD_DISTR_5001_	
Fase di progettazione degli interventi	PRINT	HARD_PROG	

QUADRO G - Servizio di Formazione

Descrizione del Servizio

Il servizio di formazione e affiancamento consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione Contraente che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'AQ, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software;
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti presso l'Amministrazione e le relative finalità;
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

È richiesto che tali attività formative siano erogate in moduli da massimo 16 ore e che per ogni modulo siano previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni indicativamente di 8 ore ciascuna:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste;

- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità *traning on the job*.

Formazione			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Modulo Formativo	FOR	FORMAZIONE	

QUADRO H - Servizio di Supporto Specialistico

Descrizione del Servizio

Il servizio supporto specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica.
Il servizio riguarderda le attività riportate nel seguito:
a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito.
Tale servizio potrà essere acquistato dalle Amministrazioni Contraenti unicamente in maniera contestuale ai prodotti e avere durata massima pari a 24 mesi.
Il servizio potrà essere prestato secondo le seguenti modalità:
i. in fase iniziale - lett. a) del precedente elenco;

ii. in modalità "*spot*" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco

iii. con periodicità definita - lett. c) (limitatamente alla modalità "presidio") e d) del precedente elenco.

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	**525**
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	

Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	**512**
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

QUADRO I - Servizio di Manutenzione

Descrizione del Servizio

Il servizio di manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità.
La manutenzione, in base alla qualità del servizio richiesto per i servizi erogati, prevede due profili *Low Profile* (*Business Day*) o *High Profile* (*H24*) e potrà essere offerta per annualità, quindi per 12 mesi o massimo 24 mesi.
Le attività di manutenzione sono associate ai soli elementi di fornitura acquistati nell'ambito del presente AQ e potranno essere acquistate solo contestualmente alla fornitura.
Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code;
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
  1. intervento presso la sede/luogo interessato;
  2. ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati;
  3. verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Servizio di manutenzione		
Fascia di acquisizione	Codice Servizio	Quantità (mesi)
Manutenzione LP	MANLP-EPP-F1	
	MANLP-EPP-F2	
	MANLP-EPP-F3	
	MANLP-EPP-F4	
	MANLP-NAC-F1	
	MANLP-NAC-F2	
	MANLP-NAC-F3	
	MANLP-NAC-F4	
	MANLP-NAC-F5	
	MANLP-NAC-F6	
	MANLP-NGFW-F1	
	MANLP-NGFW-F2	

	MANLP-NGFW-F3	
	MANLP-NGFW-F4	
	MANLP-NGFW-F5	
	MANLP-NGFW-F6	
	MANLP-Anti-APT-F1	
	MANLP-Anti-APT-F2	
	MANLP-SPP-F1	
	MANLP-SPP-F2	
	MANLP-SPP-F3	
	MANLP-SPP-F4	

Manutenzione HP	MANHP-EPP-F1	
	MANHP-EPP-F2	
	MANHP-EPP-F3	
	MANHP-EPP-F4	
	MANHP-NAC-F1	
	MANHP-NAC-F2	
	MANHP-NAC-F3	
	MANHP-NAC-F4	
	MANHP-NAC-F5	
	MANHP-NAC-F6	
	MANHP-NGFW-F1	
	MANHP-NGFW-F2	
	MANHP-NGFW-F3	
	MANHP-NGFW-F4	
	MANHP-NGFW-F5	
	MANHP-NGFW-F6	
	MANHP-Anti-APT-F1	
	MANHP-Anti-APT-F2	
	MANHP-SPP-F1	
	MANHP-SPP-F2	
	MANHP-SPP-F3	
	MANHP-SPP-F4	

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

6C-3D-47-30-B4-88-03-5B-FB-86-92-1B-19-03-73-E6-DE-AC-97-B2

PAdES 1 di 1 del 19/09/2023 16:40:31

Soggetto: Francesco Pensalfini TINIT-PNSFNC65D06G479K

Validità certificato dal 18/07/2023 13:02:18 al 18/07/2026 00:00:00

Rilasciato da InfoCert S.p.A. con S.N. 12DACE3

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

31-A3-E1-9A-FE-C7-4D-2A-85-6B-49-BE-D9-C6-3E-8C-50-3D-D0-7B

CAdES 1 di 6 del 28/12/2023 17:22:26

Soggetto: Carlo Picco

S.N. Certificato: E16942

Validità certificato dal 28/12/2022 10:18:43 al 28/12/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 6 del 27/12/2023 17:49:34

Soggetto: Stefano Taraglio

S.N. Certificato: E5BBC7

Validità certificato dal 13/01/2023 11:01:07 al 13/01/2026 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 6 del 27/12/2023 16:20:07

Soggetto: Elena Teresa Tropiano

S.N. Certificato: 15F9887

Validità certificato dal 28/07/2021 10:38:02 al 28/07/2024 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 4 di 6 del 22/12/2023 15:35:29

Soggetto: Stefania Marino

S.N. Certificato: BDF488

Validità certificato dal 02/09/2022 12:48:30 al 16/09/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 5 di 6 del 21/12/2023 14:36:35

Soggetto: Francesco Pensalfini

S.N. Certificato: 16E5129

Validità certificato dal 30/03/2022 16:57:33 al 08/04/2025 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 6 di 6 del 21/12/2023 12:23:27

Soggetto: Simona Iaropoli

S.N. Certificato: B2B41D

Validità certificato dal 21/07/2022 09:52:51 al 21/07/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE - PROTEZIONE DEGLI ENDPOINT

LOTTO 2

AQ CONSIP 2367

ASL Città di Torino

Indice

Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	05/10/2023

Introduzione

Premessa

Il presente documento descrive il Piano Operativo, relativamente alla richiesta di fornitura di prodotti e servizi per la sicurezza perimetrale per ASL Città di Torino in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (allegato all'ordine n. **7411144**).

Con questo progetto ASL Città di Torino intende acquisire una fornitura EPP/Cynet e utilizzare i servizi specialistici per raggiungere un adeguato livello di sicurezza in correlazione con i requisiti previsti dal PNRR.

Il progetto sarà finanziato con le risorse del PNRR (Piano Nazionale di Ripresa e Resilienza).

Scopo

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro ed in risposta al Piano dei Fabbisogni inviato dal cliente.

Riferimenti

Identificativo
Piano dei Fabbisogni - 7411144 Piano dei Fabbisogni ASL Città di Torino allegato all'ordine
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

Acronimi e Glossario

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa
SPC	Sistema Pubblico di Connettività

Organizzazione del contratto esecutivo

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- ✓ **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**

  Massimiliano Materazzi

  e-mail: ***massimiliano.materazzi@telecomitalia.it***

che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro.

- ✓ **Responsabile del Fornitore**
  Andrea Favaro

  telefono/cellulare: ***335 7837749***

  e-mail: ***andrea.favaro@telecomitalia.it***

che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo.

- ✓ **Referente Tecnico per l'erogazione dei servizi**

  Antonio Dell'Erba

  telefono/cellulare: ***331 6002172***

  e-mail: ***antonio.dellerba@telecomitalia.it***

che dovrà garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5).

Categorizzazione degli interventi

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

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

Progetto d'attuazione

La fornitura di cui al presente Piano Operativo ha per oggetto le tecnologie per la sicurezza perimetrale elencate nel paragrafo a seguire. Unitamente a tale fornitura, saranno erogati i seguenti servizi:

- installazione e configurazione delle tecnologie di nuova fornitura (Cynet);

Saranno inoltre erogati i seguenti servizi di Supporto Specialistico:

- supporto alla reingegnerizzazione della rete dell'Amministrazione, incluse le necessarie attività di assessment, profilazione e documentazione dell'AS-IS e del TO-BE;
- supporto al personale dell'Amministrazione nella gestione di tutti i servizi preesistenti e di nuova fornitura.

Modalità e tempistiche per l'esecuzione di ciascuna delle attività sopra riportate saranno oggetto di apposita pianificazione, da concordare fra le parti.

Prodotti richiesti

Prodotto	Tecnologia	Fascia	Modello	Codice articolo produttore	Quantità
EPP	Cynet	4	Agent Cynet 360	Cynet 360 EPP EDR C F4	6.000

Prodotti della fornitura

Nel seguente paragrafo è riportata una descrizione tecnica dei prodotti forniti.

Endpoint Protection Platform

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Nel seguente paragrafo è riportata una descrizione tecnica del servizio di EPP/EDR Cynet.

La piattaforma si distingue per la copertura della superficie d'attacco aziendale e per il modo in cui si occupa dell'intero ciclo di protezione dagli attacchi, rispondendo alle minacce e mitigando i rischi informatici.

Cynet supporta una ampia gamma di versioni su tre macro famiglie di sistemi operativi: Windows, Linux e Mac. Per quanto riguarda le versioni specifiche:

- Microsoft Windows (32b/64b), a partire dalla versione XP SP3, Vista, 7, 8, 8.1 fino a tutte le versioni 10 e la nuova versione Windows 11 (sono anche supportate le versioni Windows Server a partire dalla versione 2003 SP2 fino alla versione 2019 e alla nuova 2022);
- Linux, supporto per 8 diverse distribuzioni, a partire dalle versioni RedHat 6.9, CentOS 6.9, Fedora 23, SUSE 12, Debian 9.x, Ubuntu 16.04,Oracle Linux 7.6, Amazon Linux prima versione e v2;
- Apple macOS, a partire dalla versione 10.13 in avanti comprese le versioni con processori Apple M1;

Sono supportati anche ambienti VDI basati su Windows 10 e 11.

Di seguito si riporta una tabella riassuntiva delle funzionalità richieste dal capitolato tecnico supportate dai diversi sistemi operativi:

EPP/EDR - Tutte le fasce	Windows	Windows Legacy	MAC	MAC Legacy	Linux	Linux Legacy
Supporto degli endpoint con Sistema Operativo Windows (almeno Windows 8 e Windows 10) – EPP/EDR	□	✓ a partire da XP SP3	n.a	n.a	n.a	n.a
Funzionalità Antimalware signature based – EPP	□	□	□	□	□	□
Aggiornamento delle signature in maniera automatica – EPP	□	□	□	□	□	□
Possibilità di effettuare: Blocco azioni dannose; gestione della quarantena dei file; pulizia dell'endpoint – EPP	□	□	□	□	□	□
Protezione del traffico in entrata e in uscita dagli endpoint, comprensivo di controllo delle applicazioni, delle porte e dei protocolli utilizzati al fine di prevenire attacchi e intrusioni contro gli endpoint– EPP	□	□	✓ (1)	✓ (1)	✓ (1)	✓ (1)
Protezione dell'endpoint dai malware attraverso il monitoraggio degli eventi che accadono sull'endpoint e l'analisi comportamentale, controllando le principali modifiche (controllo/interruzione di programmi, modifica chiavi di registro, installazione impropria di device o driver, accesso anomalo alla memoria) apportate sull'endpoint. In caso di tentativo di modifica, è richiesto il blocco della modifica e l'avviso all'utente. – EPP	□	□	✓ (2)	✓ (2)	✓ (2)	✓ (2)
Protezione dai ransomware– EPP	□	□	□	□	□	□
Protezione anti-exploit– EPP	□	□	□	□	□	□
Possibilità di impostare regole per limitare o bloccare l'accesso a supporti removibili collegati all'endpoint. – EPP	□	✓ (3)				
Disponibilità di strumenti che consentano, durante la navigazione, di verificare se un sito web è considerato sicuro o meno con impostazione di eventuali policy di sicurezza associate (ad esempio blocco di siti considerati non sicuri). – EPP	□					
Possibilità di definire policy di sicurezza attraverso le quali sia consentita l'esecuzione dei soli programmi autorizzati. – EPP	□	□	□	□	□	□
Possibilità di effettuare delle scansioni in modalità: real time; manuale; programmata – EPP	□	✓ (3)	□	□	□	□
Funzionalità di reportistica e logging: monitoring in real time, template predefiniti ed esportazione – EPP/EDR	□	□	□	□	□	□
Supporto del protocollo IPv6– EPP	□	□	□	□	□	□
Possibilità di effettuare la Root Cause Analysis– EDR	□	□	□	□	□	□
Possibilità di effettuare detection di malware attraverso sorgenti IoC– EDR	□	□	□	□	□	□

(1) No protocolli; (2) No chiavi di registro; (3) Si dalla versione 7, No su XP; (4) No modifiche di registro

In generale la piattaforma Cynet 360 comprende le funzioni di: ☒NGAV, ☒EDR, ☒Network Analytics, ☒User/File/Host Deception (HoneyPots) User Behavior Analytics (UBA), Vulnerability Assessment, Log collection and retention, ☒Inventory Assessment, File Integrity Monitoring, Windows Event collection, Network Traffic Analysis e threat Hunting.

La piattaforma offre capacità di Pre-set Auto-Remediations (singolo switch per abilitazione complessiva delle Best Practice Protections), Custom Remediations e Automated Playbooks per automatizzare tutte le operazioni più frequenti e ripetitive effettuate in genere dagli operatori SOC. Infine, è disponibile anche un Incident Investigation Engine in grado di analizzare automaticamente quanto osservato, in grado di trovare in autonomia gli Indicatori di Compromissione disseminati nell'infrastruttura e, se impostato, consentendo la rimozione.

Si riporta un esempio di UBA. La Forensic di Cynet permette di andare a mostrare comportamenti degli utenti altamente sospetti correlando varie attività anomale.

Figura 1: Esempio di UBA

Si riporta, inoltre, un esempio di NTA – Rilevamento di una fase avanzata nella kill chain dell'attacco in cui l'attaccante ha ottenuto l'accesso ai dati di destinazione e tenta di esfiltrarli mascherando i dati compromessi come traffico DNS legittimo. Di lato si riporta un esempio di UBA. La Forensic di Cynet permette di andare a mostrare comportamenti degli utenti altamente sospetti correlando varie attività anomale.

Figura 2: Esempio di NTA

Caratteristiche del servizio

Il servizio di EPP dovrà essere erogato nella sede di Corso Svizzera, 164 – 10149 Torino – referente: Pensalfini Francesco mail francesco.pensalfini@aslcittaditorino.piemonte.it

Nella sede\i indicata\e verrà resa disponibile, la seguente suite di prodotto, come indicato in tabella, secondo quanto richiesto nel Piano dei fabbisogni:

Endpoint Protection Platform				
Prodotto / Fascia	**Codice servizio**	**Brand**	**Codice fornitore**	**Quantità**
CYNET/4	EPP-F4-CYN	Cynet	Cynet 360 EPP EDR C F4	6000

Caratteristiche hardware EPP

Il servizio EPP ha la finalità di proteggere gli strumenti di lavoro del personale del Cliente da possibili attacchi informatici che possano sfruttare l'endpoint quale vettore preferenziale verso il Sistema Informativo.

La soluzione proposta adotta la tecnologia Cynet, ideata per la protezione degli endpoint da molteplici virus quali ransomware, trojan e altri malware specifici, che consente anche di controllarne ed impedirne la diffusione all'interno della rete.

Servizio di supporto specialistico

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione.

Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Quantità (gg/uomo)**
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	1050
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	1024

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa

Per le competenze che ciascuna risorsa specialistica deve possedere si rimanda a quanto previsto nell'allegato 2 – Capitolato Tecnico – Parte Speciale (paragrafo 3.2.4), e come di seguito riportate:

Junior Security Analyst: in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst,

Senior Security Analyst: in possesso di almeno una delle seguenti certificazioni:

EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst

Le attività che l'Amministrazione intende svolgere attraverso il servizio di supporto specialistico consistono in:

Servizio di Security Assessment

Lo scopo delle attività descritte in questo paragrafo è quello di definire e concordare l'ambito stimato delle attività e delle tempistiche necessarie per assistere l'Amministrazione nel proteggere i suoi asset informativi attraverso la realizzazione dei servizi di sicurezza informatica.

Si eseguirà l'analisi del contesto operativo in cui opera l'Organizzazione mediante la raccolta di necessarie informazioni.

Tali attività consentono di iniziare il processo di analisi "AS-IS" finalizzato a comprendere lo stato attuale dei presidi di sicurezza posti in essere oltre all'esame dei punti di forza, delle debolezze, delle opportunità e delle minacce cyber rilevanti per l'Organizzazione.

Tale fase di analisi dell'attuale modello di "governance" della sicurezza dell'Organizzazione include l'analisi di processi riguardanti la gestione del rischio cyber, ovvero processi di:

- risposta ad attacchi ransomware, o incidenti di natura cyber
- modalità di supporto alla continuità operativa,
- modello di rilevazione e gestione delle vulnerabilità
- gestione delle identità digitali e degli accessi ai sistemi informativi,

Durante la fase di analisi si intende rilevare e analizzare il fabbisogno formativo del personale dell'Organizzazione nell'ambito del dominio "awareness".

Successivamente, l'Organizzazione verrà supportata nell'identificare i gap esistenti elaborando la roadmap strategica per definire il Modello Organizzativo di gestione della sicurezza cui orientarsi strategicamente.

Questa valutazione verrà condotta per valutare la situazione attuale della sicurezza e identificare le vulnerabilità dell'infrastruttura interna ed esterna esistente di ASL Città di Torino secondo l'ambito. Al termine dei servizi di sicurezza informatica proposti per ASL Città di Torino, sarà possibile avere una visione completa delle varie minacce insieme a indicazioni di rimedio e "best practice".

L'approccio suggerito è che ogni serie di valutazioni di sicurezza programmate inizierà dalla ricerca delle eventuali vulnerabilità e successivamente verranno effettuati test di resistenza dei sistemi, concentrato sugli elementi selezionati con rischio potenzialmente più alto.

Nel corso delle attività saranno rilasciati report di dettaglio che saranno condivisi con la PA contraente e di comune accordo verranno definite le strategie e le azioni da intraprendere al fine di raggiungere tutti gli obiettivi prefissati

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico in base alle esigenze del cliente e comunque in funzione della fornitura prodotti richiesta

tramite questo piano. Qualsiasi altra necessità sarà valutata di volta in volta in accordo con il cliente.

Si specifica che le attività di cui sopra contemplano esclusivamente il supporto al personale dell'Amministrazione in attività di assessment e di progetto, incluso il supporto alla produzione della necessaria documentazione tecnica.

Come indicato nel par.10 – TABELLA RIEPILOGATIVA, i gg/UU relativi ai servizi professionali saranno suddivisi tra i soci del RTI per erogare quanto richiesto dall'Amministrazione.

Piano di lavoro

Il processo di Start-up è incluso nel servizio e comprende le fasi propedeutiche all'attivazione del servizio ed è composto da diverse attività che devono essere implementate in collaborazione con il cliente ASL Città di Torino

Le fasi principali dello Start-Up sono:

- Incontro preliminare e pianificazione;
- Installazione componenti del servizio;
- Collaudo (User Acceptance Test)
- Kickoff
- Attivazione del Servizio

Il processo può in parte variare in base alla tipologia o TIER di servizio attivato, ma le principali fasi operative sono le medesime.

Incontro preliminare e pianificazione

- Condivisione del piano di attivazione del servizio che comprende la pianificazione dell'installazione dei suoi componenti e della VPN tra l'infrastruttura del cliente ASL Città di Torino e il cloud del partner TIM. A tal fine verrà consegnata e illustrata al cliente ASL Città di Torino una Checklist riepilogativa di tutte le informazioni tecniche necessarie per l'attivazione e l'installazione dei componenti del servizio.

- Definizione asset: il cliente ASL Città di Torino dovrà fornire l'elenco dei sistemi aziendali oggetti del servizio. Nell'elenco dovranno essere evidenziati i sistemi ritenuti critici o importanti per il business con il maggior numero di informazioni possibili (es. modello, ubicazione, IP address, note operative, etc.).

- Mappa infrastruttura di rete: il cliente ASL Città di Torino dovrà fornire una mappa dell'infrastruttura fisica e logica con riportati i link tra gli apparati di rete e quelli di sicurezza e di computing.

- Contatti: durante l'incontro il team di lavoro presenterà al cliente ASL Città di Torino le diverse modalità con prendere contatti per il servizio, Il cliente ASL Città di Torino dovrà altresì fornire i contatti aziendali che saranno i riferimenti per il team (Key User). Inoltre, nel caso in cui il con il cliente ASL Città di Torino affidi al team anche l'attività di escalation verso le terze parti (es. ISP), in questa occasione fornirà anche i riferimenti dei loro partner ed i relativi numeri di contratto.

- Definizione delle policy di sicurezza e distribuzione agent: saranno concordati i protocolli del collegamento VPN, i canali e i protocolli di comunicazione sicura per la raccolta dei log, l'invio degli

eventi e per le comunicazioni di servizio. Sarà messo a disposizione del cliente ASL Città di Torino il software (agent) con i parametri necessari per la distribuzione sui sistemi supportati.

- Discussione di eventuali criticità e definizione dei livelli di severità: il cliente ASL Città di Torino dovrà rendersi disponibile per valutare le eventuali criticità dei suoi asset e della sua infrastruttura, sia in termini strategici che operativi. Tali informazioni sono di massima importanza per dare la giusta rilevanza ai problemi che si dovessero presentare durante l'erogazione del servizio e consentono di definire i livelli di severità che, dopo essere stati concordati con il cliente ASL Città di Torino, saranno assegnati agli eventi di sicurezza rilevati durante il servizio.

- Definizione dell'Use Case: Una volta raccolte tutte le informazioni necessarie, gli esperti di sicurezza del team supporteranno il cliente ASL Città di Torino nella definizione e mappatura delle sorgenti log e eventi, delle Politiche di Sicurezza e delle regole di correlazione. Tutte le Politiche di Sicurezza decise dal cliente ASL Città di Torino verranno dallo stesso sottoscritte e costituiranno l'esatta analisi di quanto verrà implementato. Le eventuali variazioni alla struttura inizialmente implementata subiranno il medesimo iter.

- Definizione delle modalità di intervento in risposta alle minacce. Tutti gli aspetti legati alle modalità di intervento, incluse le regole d'ingaggio, verranno concordate e documentate. Eventuali asset di security con le rispettive credenziali e i rispettivi livelli di accesso, a cui il team potrà accedere saranno definiti in questa sezione.

Installazione componenti del servizio e implementazione Use Case

Dopo l'incontro preliminare verranno installati i componenti del servizio presso la sede del cliente ASL Città di Torino. Per poter eseguire tale attività, il cliente ASL Città di Torino dovrà aver compilato il documento di Checklist precedentemente condiviso. Verrà configurata la VPN tra l'infrastruttura del cliente ASL Città di Torino ed il Cloud del partner TIM e verrà avviata l'implementazione dell'Use Case.

User Acceptance - Collaudo

Completata l'installazione dei componenti e la configurazione secondo le specifiche concordate nell'ambito dell'Use Case, il team effettuerà il collaudo del servizio. Tutta la documentazione sulla configurazione del servizio, la Checklist, le policy e la configurazione dell'Use Case e i risultati del collaudo saranno verbalizzati in un unico documento con il titolo di User Acceptance Test (Verbale di Collaudo) che sarà consegnato al cliente ASL Città di Torino durante la riunione di Kick-Off.

Kick-Off del servizio

Non appena tutte le precedenti fasi verranno portate a termine, il Team di lavoro incontrerà il cliente ASL Città di Torino per ufficializzare il completamento delle attività di configurazione, la messa a regime dei servizi acquistati e il rilascio di User Acceptance Test che sarà sottoscritto da entrambe le parti.

Attivazione del servizio

Concluse le attività precedentemente illustrate, viene comunicata al cliente ASL Città di Torino l'attivazione del servizio.

Grace Period

Si definisce Grace Period, un periodo temporale di 3 mesi successivi alla messa a regime che prevede il "fine tuning" (sintonizzazione accurata) del servizio. L'obbiettivo principale di questo periodo

è di verificare e validare l'efficacia dell'Use Case, di tutte le procedure di presa in carico delle richieste di intervento e di eventuale escalation verso terze parti. In questo periodo il servizio viene erogato in modo completo.

Requisiti

Il cliente ASL Città di Torino dovrà mettere a disposizione le risorse computazionali e di spazio necessarie all'appliance che ha il ruolo di collector e processor degli eventi.

Requisiti dell'appliance che dovrà essere installata presso l'infrastruttura del cliente ASL Città di Torino

Descrizione	vCPU	vRAM	vSDD
EVENT PROCESSOR	16	24 GB	1TB

GANTT

Attività di delivery e attivazione del servizio

PIANO DELLE ATTIVITA'	settimana 1					settimana 2					settimana 3			
	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4
ATTIVITÀ	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4
•Incontrl preliminare e pianificazione;														
•Installazione componenti del servizio e implementazione Use Case														
•User Acceptance - Collaudo														
•Attivazione del servizio														t>0

In concomitanza della fase di attivazione del servizio si assume t>0 per dare avvio alla rendicontazione

Attività di "fine tuning"

PIANO DELLE ATTIVITA'	ANNO		
	MESE 1	MESE 2	MESE 3
•Grace Period			

Piano di presa in carico

L'attività di presa in carico del sistema consiste nell'acquisire tutte le informazioni che sono necessarie all'erogazione dei servizi e di quanto indicato nel sopra riportato piano di lavoro, con l'obiettivo di acquisire know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione oltre a standard, modalità operative, linee guida, ove presenti.

Come specificato da piano dei fabbisogni, l'amministrazione contraente fornirà la configurazione esistente degli apparati, il piano d'indirizzamento, gli accessi ai sistemi per la configurazione degli stessi, gli eventuali accessi fisici nei locali tecnici, le informazioni necessarie all'attivazione dei servizi nonché la disponibilità del personale referente affinché di comune accordo si possano definire le strategie implementative oggetto di fornitura. L'attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. schemi logici e di low level design dell'infrastruttura di rete, informative sulle connettività presenti, piani di indirizzamento etc) con assistenza di personale esperto e affiancamento condotta con eventuali ulteriori fornitori dell'amministrazione contraente.

Se previsto e/o richiesto dall'amministrazione contraente saranno altresì forniti i dettagli necessari (es. tools IT Management) alla corretta implementazione dei processi di Incident, Change e Deploy Management richiesta per l'espletamento dei servizi descritti nei successivi paragrafi.

Si noti che qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del piano di presa in carico.

Durante le attività di Presa in carico si dovrà garantire:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall'Amministrazione e che dovrà essere sottoscritto dal RTI e dall'Amministrazione.

Specifiche di collaudo

Per ciascun elemento che compone le macroaree di progetto, verranno effettuate prove di esercibilità e test funzionali secondo il piano di seguito riportato. Le date di collaudo potranno essere definite in accordo al piano riportato al paragrafo precedente.

Per il servizio di Endpoint Protection Platform (EPP) /Endpoint Detection & Response (EDR) saranno eseguite le seguenti attività di verifica e test da affinare in sede del cliente.

Tipologia	Descrizione
Test Funzionale	Verifica che i dispositivi funzionino come previste siano in grado di eseguire le funzionalità base come la prevenzione dell'intrusione, la verifica delle autorizzazioni agli accessi, delle politiche di sicurezza
Test di sicurezza	Verificare la capacità dei dispositivi di rilevare e prevenire possibili compromissioni e attacchi all'infrastruttura IT. Questi test possono includere simulazioni in ambiente controllato, test di identificazione e blocco di Virus e malware
Test di compatibilità	Questi tipi di test verificano la capacità dei dispositivi di funzionare correttamente con gli altri componenti dell'infrastruttura IT

Tabella riepilogativa dei servizi e relativi importi contrattuali

Forniture

Prodotto	Tecnologia	Fascia	Modello	Codice articolo produttore	Quantità
EPP	Cynet	4	Agent Cynet 360	Cynet 360 EPP EDR C F4	6.000

Servizi di supporto specialistico

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Quantità (gg/uomo)**
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	1.050
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	1.024

Valorizzazione economica

Codice articolo convenzione	Quantità	Durata (mesi)	Prezzo totale
CS2L2-EPP F4-CYN	6000		27.660,00€
CS2L2-JSAN-STA	1050		238.875,00€
CS2L2-SSSN-STA	1024		277.504,00€
		TOTALE	**544.039,00€**

Rendicontazione e SAL di avanzamento servizi professionali

SAL 1° t>0

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	260	70.460,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	261	59.377,50 €
		Totale	**129.837,50 €**

SAL 2° 3° 4°

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	84	22.764,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	88	20.020,00 €
		Totale	**42.784,00 €**

3 SAL trimestrali t>0 + 3 mesi con cadenza 3 mesi ciascuno

SAL 5° t>0 + 12 mesi

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	260	70.460,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	261	59.377,50 €
		Totale	**129.837,50 €**

SAL 6° 7° 8°

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	84	22.764,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	88	20.020,00 €
		Totale	**42.784,00 €**

3 SAL trimestrali t>0 + 15 mesi con cadenza 3 mesi ciascuno

Prestazioni subappalto

Nell'ambito dell'Accordo Quadro Cybersecurity 2 per le prestazioni erogate in subappalto è previsto quanto segue:

- Quota massima del subappalto: 50%
- Servizi per i quali è prevista la prestazione in subappalto:
- Formazione;
- Hardening;
- Supporto Specialistico.

Nella tabella sottostante è necessario riportare la quota, le prestazioni e il nome delle aziende che erogheranno i servizi in subappalto, nel rispetto di quanto indicato nel Piano dei fabbisogni:

Servizi	Quota subappalto	Azienda del RTI che eroga il servizio	Azienda che eroga la prestazione in subappalto
Supporto Specialistico	95%	TIM	Lantech Longwave
Formazione	n.a.	n.a.	n.a.

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

9D-52-4D-C5-66-8B-74-22-32-16-73-4B-D8-54-97-DA-F3-BA-10-7E

CAdES 1 di 2 del 10/10/2023 14:43:19

Soggetto: GIUSEPPE RUSSO RSSGPP67L29I480H

Validità certificato dal 28/04/2022 11:19:57 al 28/04/2025 11:19:56

Rilasciato da TI Trust Technologies QTSP CA 1, Telecom Italia Trust Technologies S.r.l., IT con S.N. 082

TimeStamp 2 di 2 del 10/10/2023 12:43:20

Soggetto: Time Stamp Server - 2, Telecom Italia Trust Technologies S.r.l., IT

Validità certificato dal 26/08/2023 00:00:00 al 25/08/2026 00:00:00

Rilasciato da TI Trust Technologies QTSP TSA CA, Telecom Italia Trust Technologies S.r.l., IT con S.

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

CA-16-AA-21-A9-72-B0-9E-D3-4D-C5-E8-F2-0A-90-5B-DA-C8-A4-33

CAdES 1 di 6 del 28/12/2023 17:22:28

Soggetto: Carlo Picco

S.N. Certificato: E16942

Validità certificato dal 28/12/2022 10:18:43 al 28/12/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 6 del 27/12/2023 17:49:35

Soggetto: Stefano Taraglio

S.N. Certificato: E5BBC7

Validità certificato dal 13/01/2023 11:01:07 al 13/01/2026 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 6 del 27/12/2023 16:20:08

Soggetto: Elena Teresa Tropiano

S.N. Certificato: 15F9887

Validità certificato dal 28/07/2021 10:38:02 al 28/07/2024 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 4 di 6 del 22/12/2023 15:35:30

Soggetto: Stefania Marino

S.N. Certificato: BDF488

Validità certificato dal 02/09/2022 12:48:30 al 16/09/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 5 di 6 del 21/12/2023 14:36:36

Soggetto: Francesco Pensalfini

S.N. Certificato: 16E5129

Validità certificato dal 30/03/2022 16:57:33 al 08/04/2025 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 6 di 6 del 21/12/2023 12:23:28

Soggetto: Simona Iaropoli

S.N. Certificato: B2B41D

Validità certificato dal 21/07/2022 09:52:51 al 21/07/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ID 2367

ACCORDO QUADRO AI SENSI DELL'ART. 54 COMMA 3 DEL D. LGS 50/2016 PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI – LOTTO 2 - ID 2367.

CONTRATTO ESECUTIVO

INDICE

CONTRATTO ESECUTIVO

TRA

L'Azienda Sanitaria Locale Città di Torino, con sede in Torino, Via San Secondo, n. 29, C.F. 11632570013, in persona del legale rappresentante pro tempore Dott. Carlo Picco nella sua qualità di Direttore Generale dell'Azienda, giusti poteri allo stesso conferiti mediante della Regione Piemonte n. 9-2521 dell'11 dicembre 2020

(nel seguito per brevità anche "**Amministrazione Contraente**")

E

Telecom Italia S.p.A., sede legale in Milano, Via Gaetano Negri n. 1, Direzione Generale e Sede Secondaria in Roma, Corso d'Italia n.41, capitale sociale Euro 11.677.002.855,10 i.v., iscritta al Registro delle Imprese di Milano – Monza – Brianza -Lodi al n. 00488410010, P. IVA 00488410010, domiciliata ai fini del presente atto in Milano, Via Gaetano Negri n. 1, in persona del Procuratore Roberto Cerutti, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo costituito oltre alla stessa, dai seguenti operatori economici mandanti:

Maticmind S.p.A. con sede legale in Milano, Via Roberto Bracco n.6, capitale sociale Euro 16.500.000,00 i.v., iscritta al Registro delle Imprese di Milano – Monza – Brianza -Lodi al n. 05032840968, P. IVA 05032840968, domiciliata ai fini del presente atto in Milano, Via Roberto Bracco n.6;

DGS S.p.A., con sede legale in Roma, Via Paolo Di Dono n. 73, capitale sociale Euro 3.900.000,00 i.v., iscritta al Registro delle Imprese di Roma al n. 03318271214, P. IVA 03318271214, domiciliata ai fini del presente atto in Roma, Via Paolo Di Dono n. 73;

SCAI Solution Group S.p.A., con sede legale in Milano, Viale Monte Nero n.73, capitale sociale Euro 400.000,00 i.v., iscritta al Registro delle Imprese di Roma al n. 05348521005, P. IVA 05348521005, domiciliata ai fini del presente atto in Milano, Viale Monte Nero n.73, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott.ssa Sandra De Franchis repertorio 17924, raccolta 8753;

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

PREMESSO CHE

(A) Consip, società interamente partecipata dal Ministero dell'economia e delle finanze, ai sensi dell'articolo 26, Legge 23 dicembre 1999, n. 488, dell'articolo 58, Legge 23 dicembre 2000, n. 388, nonché dei relativi decreti attuativi, DD.MM. del 24 febbraio 2000 e del 2 maggio 2001, ha, tra l'altro, il compito di attuare lo sviluppo e la gestione operativa del Programma di razionalizzazione della spesa di beni e servizi per la pubblica amministrazione.

(B) L'articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip 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 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 S.p.A. 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) Consip, nell'ambito del Programma di razionalizzazione degli acquisti può supportare le amministrazioni statali, centrali e periferiche nell'acquisizione di beni e servizi di particolare rilevanza strategica secondo quanto previsto dal Piano Triennale nonché può supportare i medesimi soggetti nell'individuazione di specifici interventi di semplificazione, innovazione e riduzione dei costi dei processi amministrativi.

(F) In virtù di quanto sopra, a seguito dell'approvazione del Piano triennale per l'informatica nella Pubblica Amministrazione 2019-2021 ed in accordo con Agid, è stato aggiornato il programma delle gare strategiche ICT.

(G) Ai fini del perseguimento degli obiettivi di cui al citato Piano triennale per l'informatica nella Pubblica Amministrazione, e in esecuzione di quanto precede, Consip, in qualità di stazione appaltante e centrale di committenza, ha indetto con Bando di gara per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni.

(H) Il Fornitore è risultato aggiudicatario del Lotto 2 - 8898075BC5 della predetta gara, ed ha stipulato il relativo Accordo Quadro.

(I) In applicazione di quanto stabilito nel predetto Accordo Quadro, ciascuna Amministrazione Contraente utilizza il medesimo mediante la stipula di Contratti Esecutivi, attuativi dell'Accordo Quadro stesso.

(J) L'Amministrazione Contraente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto Esecutivo, in conformità alla documentazione di gara.

(K) Il Fornitore è stato selezionato dall'Amministrazione Contraente con le modalità indicate nel Capitolato Tecnico Generale.

(L) 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 servizi 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;

(M) Il CIG del presente Contratto Esecutivo è il seguente: **A020E7A724**

(N) I CUP (Codice Unico Progetto) del presente Contratto Esecutivo sono i seguenti:
- **F17H22001230001**: Presidio Ospedaliero Maria Vittoria/Amedeo di Savoia
- **F17H22001240001**: Presidio Ospedaliero Martini
- **F17H22001250001**: Presidio Ospedaliero San Giovanni Bosco

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 Parte Generale e Speciale, salvo che il contesto delle singole clausole disponga diversamente.

1.3. Il presente Contratto Esecutivo è regolato:

- 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 Contraente relativamente alle attività e prestazioni contrattuali;
- dalle disposizioni dell'Accordo Quadro e dai suoi allegati;
- dalle disposizioni del D. Lgs. 50/2016 e s.m.i. e relative prassi e disposizioni attuative;
- dalle disposizioni di cui al D. Lgs. n. 82/2005;
- 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.
- Il Piano dei Fabbisogni.
- Il Piano Operativo con il documento allegato di specifiche tecniche.
- Il DUVRI.
- Il DNSH.
- Il Patto d'integrità tra ASL e O.E.

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.

2.5. In relazione alle procedure afferenti gli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10

febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC e dai programmi cofinanziati dai fondi strutturali dell'Unione Europea, il contratto diviene efficace con la stipula e non trova applicazione l'articolo 32, comma 12, del decreto legislativo 18 aprile 2016 n. 50.

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 Contraente da parte del Fornitore come riportati nel Piano Operativo approvato e nel Piano dei Fabbisogni.

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

3.3. 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.

3.4. Sono designati quale Responsabile unico del procedimento, ai sensi dell'art. 31 del D. Lgs. n. 50/2016 Ing. Francesco Pensalfini e Direttore dell'esecuzione ai sensi dell'art. 101 del D. Lgs. n. 50/2016 il sig. Gianluca Lucarelli.

4. EFFICACIA E DURATA

4.1. Il presente Contratto Esecutivo spiega i suoi effetti dalla data di avvio dell'attività di collaudo ed avrà termine allo spirare di 24 mesi previsti dall'Accordo Quadro.

5. GESTIONE DEL CONTRATTO ESECUTIVO

5.1. Ai fini dell'esecuzione del presente Contratto Esecutivo, il Fornitore ha nominato i seguenti Responsabili tecnici per l'esecuzione dei servizi: Lunetta Simona.

5.2. Le attività di supervisione e controllo della corretta esecuzione del presente Contratto Esecutivo, in relazione ai servizi/forniture richieste, sono svolte dall'Amministrazione Contraente, eventualmente d'intesa con il fornitore.

5.3. Ai sensi dell'art. 47 comma 3, D.L. 77/2021, convertito in l. 108/2021, il Fornitore è tenuto a consegnare all'Amministrazione, in relazione a ciascuna impresa e/o consorziata del RTI che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1 d.lgs. n. 198/2006, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta. La suddetta relazione dovrà essere trasmessa, altresì, alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità. La relazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della stessa

alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, dovrà essere consegnata all'Amministrazione, entro 6 mesi dalla stipula del presente contratto. La violazione del succitato obbligo determina, ai sensi dell'art. 47, D.L. n. 77/2021, convertito con modificazioni dalla L. n. 108/2021, l'applicazione della penale pari a 2.000,00 € per ogni giorno di ritardo, nonché l'impossibilità di partecipare per un periodo di dodici mesi ad ulteriori procedure di affidamento afferenti gli investimenti pubblici.

5.4. Ai sensi dell'art. 47 comma 3bis, del D.L. n. 77/2021, convertito con modificazioni dalla L. n. 108/2021, il Fornitore è tenuto a consegnare all'Amministrazione, in relazione a ciascuna impresa e/o consorziata che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1, del d.lgs. n. 198/2006, una relazione relativa all'assolvimento degli obblighi di cui alla medesima legge n. 68/1999 e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di scadenza di presentazione delle offerte. La relazione dovrà essere trasmessa anche alle rappresentanze sindacali aziendali. La documentazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della relazione alle rappresentanze sindacali aziendali, dovrà essere consegnata alla Amministrazione, entro 6 mesi dalla stipula del Contratto. La violazione di tale obbligo comporta l'applicazione della penale pari a 100,00 € per ogni giorno di ritardo.

5.5. Le relazioni di cui ai precedenti punti 5.4 e 5.5 verranno pubblicate sul profilo dell'Amministrazione contraente, nella sezione "Amministrazione trasparente", ai sensi dell'art. 29, comma 1 del Codice e dell'art. 47, comma 9, D.L. n. 77/2021, convertito in l. 108/2021. L'Amministrazione contraente procederà anche con gli ulteriori adempimenti di cui al citato articolo 47 comma 9, D.L. 77/2021, convertito in l. 108/2021. Inoltre, in riferimento al comma 4 di cui al citato articolo 47, il Fornitore deve assicurare una quota pari almeno al 30 per cento, delle assunzioni necessarie per l'esecuzione del contratto o per la realizzazione di attività ad esso connesse o strumentali, sia all'occupazione giovanile sia all'occupazione femminile.

6. ATTIVAZIONE E DISMISSIONE DEI SERVIZI/FORNITURE

6.1. Il Fornitore, a decorrere dalla data di stipula del presente Contratto Esecutivo, dovrà procedere alla presa in carico dei servizi/forniture con le modalità indicate nel Capitolato Tecnico Generale e Speciale dell'Accordo Quadro.

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

7. VERIFICHE DI CONFORMITA'

7.1. Nel periodo di efficacia del presente Contratto Esecutivo, l'Amministrazione Contraente procederà ad effettuare la verifica di conformità dei servizi/forniture oggetto del presente Contratto Esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali, con le modalità e le specifiche stabilite nell'AccordoQuadro e nel Capitolato Tecnico Generale e Speciale ad esso allegati.

8. PENALI

8.1. L'Amministrazione Contraente potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nell'Accordo Quadro al Capitolato Tecnico Speciale paragrafo 6, qui da intendersi integralmente trascritte, fatto comunque salvo il risarcimento del maggior danno.

8.2. L'Amministrazione potrà applicare altresì le seguenti penali: in relazione alle procedure afferenti gli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, inserire penali di cui all'art. 47 comma 6 D.L. 31 maggio 2021 n. 77, convertito con mod. in l. 108/2021, con riguardo al mancato rispetto dei requisiti necessari e ulteriori requisiti premiali dell'offerta come previsto dall'art. 47, comma 4 e 5, D.L. n. 77/2021. L'operatore economico, entro 6 (sei) mesi dalla conclusione del contratto, è tenuto a consegnare alla stazione appaltante una relazione relativa all'assolvimento degli obblighi volti a favorire la pari opportunità di genere e generazionali, nonché l'inclusione lavorativa delle persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, come da Decreto della Presidenza del Consiglio dei Ministri Dipartimento per le Pari Opportunità, pubblicato in data 30/12/2021, di cui al suddetto articolo: per ogni giorno lavorativo di ritardo sarà calcolata una penale di € 100,00.

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

9. CORRISPETTIVI

9.1. Il corrispettivo complessivo, calcolato sulla base del dimensionamento dei servizi/forniture indicato del Piano dei Fabbisogni, è pari a € 544.039,00 esclusa IVA.

9.2. I corrispettivi unitari, per singolo servizio, dovuti al Fornitore per i servizi/forniture prestati in esecuzione del presente Contratto Esecutivo sono determinati in ragione dei prezzi unitari stabiliti nell'Offerta Economica relativa all'Appalto Specifico.

9.3. Il corrispettivo contrattuale si riferisce all'esecuzione dei servizi/forniture a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.

9.4. 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.

9.5. 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 (data di collaudo).

10. FATTURAZIONE E PAGAMENTI

10.1. La fattura relativa ai corrispettivi maturati secondo quanto previsto al precedente art. 9 viene emessa ed inviata dal Fornitore a fronte di un verbale redatto congiuntamente al termine delle verifiche di conformità delle rendicontazioni emesse mensilmente come indicato nel Piano dei fabbisogni.

10.2. Resta inteso che il fornitore potrà emettere fattura posticipata solo al termine positivo della verifica di conformità corrispondente.

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

11. GARANZIA DELL'ESATTO ADEMPIMENTO

11.1. A garanzia dell'esatto e tempestivo adempimento degli obblighi contrattuali di cuial presente Contratto Esecutivo, il Fornitore ha costituito la garanzia di cui all'Accordo Quadro, cui si rinvia.

12. SUBAPPALTO

12.1. Il Fornitore, conformemente a quanto dichiarato in sede di Offerta, si è riservato, per ciascun lotto, di affidare in subappalto l'esecuzione di tutti i servizi/forniture offerti, per una quota pari al 85% dell'importo contrattuale dell'Accordo Quadro.

12.2. Il Fornitore si impegna a depositare presso l'Amministrazione Contraente, 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.

12.3. In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, l'Amministrazione Contraente 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 sub-appalto, che ricomincerà a decorrere dal completamento della documentazione.

12.4. 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 l'Amministrazione Contraente revocherà l'autorizzazione.

12.5. Il Fornitore 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.

12.6. 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 per lo specifico Lotto.

12.7. 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;

12.8. 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.

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

12.10. Il Fornitore è responsabile in solido con il subappaltatore nei confronti dell'Amministrazione Contraente dei danni che dovessero derivare alla Amministrazione contraente 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 l'Amministrazione Contraente 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 UE n. 2016/679.

12.11. 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.

12.12. 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.

12.13. 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.

12.14. Trova applicazione l'art. 105, comma 13, del d. lgs. n. 50/2016 e s.m.i. al ricorrere dei prescritti presupposti. Ove tale previsione non sia applicata, e salvo diversa indicazione del direttore dell'esecuzione, il Fornitore si obbliga a trasmettere all'Amministrazione Contraente entro 20 giorni dalla data di ciascun pagamento effettuato nei confronti del subappaltatore, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.

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

12.16. In caso di inadempimento da parte del fornitore agli obblighi di cui ai precedenti commi, l'Amministrazione Contraente può risolvere il Contratto Esecutivo, salvo il diritto al risarcimento del danno.

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

12.18. Il Fornitore si impegna a comunicare all'Amministrazione Contraente, 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.

12.19. 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 il Fornitore 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 Contraente prima o contestualmente alla sottoscrizione del Contratto.

12.20. 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.

12.21. L'Amministrazione Contraente 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.

13. RISOLUZIONE E RECESSO

13.1 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"

14. FORZA MAGGIORE

14.1 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.

14.2 Nel caso in cui un evento di forza maggiore impedisca la fornitura dei servizi da parte del Fornitore, l'Amministrazione Contraente, 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/forniture interessati fino a che tali servizi non siano ripristinati e, ove possibile, avrà diritto di affidare i servizi/forniture in questione ad altro fornitore assegnatario per una durata ragionevole secondo le circostanze.

14.3 L'Amministrazione Contraente 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 il servizio/fornitura.

15. RESPONSABILITA' CIVILE E POLIZZA ASSICURATIVA

15.1 Fermo restando quanto previsto dall'art. 16 dell'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 Contraente 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.

15.2 A fronte dell'obbligo di cui al precedente comma, il Fornitore è tenuto, entro e non oltre 10 giorni lavorativi dal perfezionamento del presente contratto a presentare polizza/e assicurativa/e conforme/i ai requisiti indicati nell'A.Q.

15.3 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.

15.4 Con specifico riguardo al mancato pagamento del premio, ai sensi dell'art. 1901 del c.c., l'Amministrazione Contraente 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 Contraente di procedere a compensare quanto versato con i corrispettivi maturati a fronte delle attività eseguite.

15.5 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 Contraente 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.

15.6 Resta fermo che il Fornitore si impegna a consegnare, annualmente e con tempestività, all'Amministrazione Contraente, 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.

16. TRASPARENZA DEI PREZZI

16.1 Il Fornitore 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.

16.2 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 contraente di incamerare la garanzia prestata.

17. TRACCIABILITÀ DEI FLUSSI FINANZIARI

17.1 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.

17.2 Ferme restando le ulteriori ipotesi di risoluzione previste dal presente contratto, si conviene che l'Amministrazione Contraente, 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 al Fornitore 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.

17.3 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.

17.4 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 Contraente e alla Prefettura – Ufficio Territoriale del Governo della provincia ove ha sede l'Amministrazione medesima.

17.5 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.

17.6 L'Amministrazione Contraente verificherà che nei contratti di subappalto sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale il subappaltatore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge. Con riferimento ai contratti di subfornitura, il Fornitore si obbliga a trasmettere alla Committente, oltre alle informazioni sui sub-contratti di cui all'art. 105, comma 2, anche apposita dichiarazione resa ai sensi del DPR 445/2000, attestante che nel relativo sub-contratto, sia stata inserita, a pena di nullità assoluta, un'apposita clausola con la quale il subcontraente assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge, restando inteso che l'Amministrazione Contraente, si riserva di procedere a verifiche a campione sulla presenza di quanto attestato, richiedendo all'uopo la produzione degli eventuali sub-contratti stipulati, e, di adottare, all'esito dell'espletata verifica ogni più opportuna determinazione, ai sensi di legge e di contratto.

17.7 Il Fornitore 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.

17.8 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.

18. ONERI FISCALI E SPESE CONTRATTUALI

18.1 Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto, come previsto all'art. 30 dell'Accordo Quadro.

19. FORO COMPETENTE

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

20. TRATTAMENTO DEI DATI PERSONALI

20.1 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/fornitura 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.

20.2 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.

20.3 Le finalità del trattamento sono: sicurezza informatica.

20.4 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 particolari (dati sanitari).

20.5 Le categorie di interessati sono: dipendenti e collaboratori, utenti dei servizi, ecc…

20.6 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

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, 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.

20.7 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:

- 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;
- il divieto di far fuoriuscire i dati presenti nelle basi dati di sviluppo, test e produzione, al di fuori della sede dell'ASL Città di Torino;
- l'obbligo, nel caso di accesso da remoto, di utilizzare strumenti idonei alla salvaguardia dei dati

l Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento.

20.8 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 Contraente 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 Contraente 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 Contraente applicherà al Fornitore/Responsabile Iniziale 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, la Committente 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.

20.9 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.

20.10 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.

20.11 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;

20.12 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, l'Amministrazione Contraente 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, la Committente potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

20.13 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.

20.14 Al termine della prestazione dei servizi/forniture 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.

20.15 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".

20.16 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.

20.17 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 Contraente potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

20.18 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.

20.19 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.

20.20 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 Contraente potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

20.21 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

Torino, 13.12.2023

Il Direttore Generale dell'ASL Città di Torino
Dott. Carlo Picco
(Documento sottoscritto con firma elettronica qualificata)

Il Procuratore della Società Telecom Italia S.p.A.
Dott. Giuseppe Russo
(Documento sottoscritto con firma elettronica qualificata)

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 Attivazione e dismissione dei servizi, Art. 7 Verifiche di conformità, Art. 8 Penali, Art. 9 Corrispettivi, Art. 10 Fatturazione e pagamenti, Art. 11 Garanzia dell'esatto adempimento, Art. 12 Subappalto, Art. 13 Risoluzione e Recesso, Art. 14 Forza Maggiore, Art. 15 Responsabilità civile, Art. 16 Trasparenza dei prezzi, Art. 17 Tracciabilità dei flussi finanziari, Art. 18 Oneri fiscali e spese contrattuali, Art. 19 Foro competente, Art. 20 Trattamento dei dati personali

Letto, approvato e sottoscritto

_____
(per il Fornitore)

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ACCORDO QUADRO PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI – LOTTI 1, 2, E 3, PER LE PUBBLICHE AMMINISTRAZIONI AI SENSI DELL'ART. 54, COMMA 3, DEL D. LGS. N. 50/2016

ID SIGEF 2367

ACCORDO QUADRO

PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI

TRA

Consip S.p.A., a socio unico, con sede legale in Roma, Via Isonzo n. 19/E, capitale sociale Euro 5.200.000,00= i.v., iscritta al Registro delle Imprese presso la Camera di Commercio di Roma al n. REA 878407 di Roma, CF e P. IVA 05359681003, in persona dell'Amministratore Delegato e legale rappresentante, Ing. Cristiano Cannarsa, domiciliato per la carica presso la sede sociale, giusta poteri allo stesso conferiti dalla deliberazione di aggiudicazione del Consiglio di Amministrazione del 15/03/2022 (nel seguito per brevità anche "**Consip S.p.A**.")

E

Telecom Italia S.p.A., sede legale in Milano, Via Gaetano Negri n. 1, Direzione Generale e Sede Secondaria in Roma, Corso d'Italia n.41, capitale sociale Euro 11.677.002.855,10 i.v., iscritta al Registro delle Imprese di Milano – Monza – Brianza - Lodi al n. 00488410010, P. IVA 00488410010, domiciliata ai fini del presente atto in Milano, Via Gaetano Negri n. 1, in persona del Procuratore Speciale Ing. Massimiliano Materazzi, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa la mandante **Maticmind S.p.A.** *con* sede legale in Milano, Via Roberto Bracco n.6, capitale sociale Euro 16.500.000,00 i.v., iscritta al Registro delle Imprese di Milano – Monza – Brianza -Lodi al n. 05032840968, P. IVA 05032840968, domiciliata ai fini del presente atto in Milano, Via Roberto Bracco n.6, la mandante **DGS S.p.A.**, con sede legale in Roma, Via Paolo Di Dono n. 73, capitale sociale Euro 3.900.000,00 i.v., iscritta al Registro delle Imprese di Roma al n. 03318271214, P. IVA 03318271214, domiciliata ai fini del presente atto in Roma, Via Paolo Di Dono n. 73 e la mandante **SCAI Solution Group S.p.A.**, con sede legale in Milano, Viale Monte Nero n.73, capitale sociale Euro 400.000,00 i.v., iscritta al Registro delle Imprese di Roma al n. 05348521005, P. IVA 05348521005, domiciliata ai fini del presente atto in Milano, Viale Monte Nero n.73, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott.ssa Sandra De Franchis repertorio 17924, raccolta 8753;
(nel seguito per brevità congiuntamente anche "***Fornitore***" o "**Impresa**")

PREMESSO

a) che Consip S.p.A., società interamente partecipata dal Ministero dell'economia e delle finanze, ai sensi dell'articolo 26, Legge 23 dicembre 1999, n. 488, dell'articolo 58, Legge 23 dicembre 2000, n. 388, nonché dei relativi decreti attuativi, DD.MM. del 24 febbraio 2000 e del 2 maggio 2001, ha, tra l'altro, il compito di attuare lo sviluppo e la gestione operativa del Programma di razionalizzazione della spesa di beni e servizi per la pubblica amministrazione;

b) che 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) che, 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) che, 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 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 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) che Consip, nell'ambito del Programma di razionalizzazione degli acquisti può supportare le amministrazioni statali, centrali e periferiche nell'acquisizione di beni e servizi di particolare rilevanza strategica secondo quanto previsto dal Piano Triennale nonché può supportare i medesimi soggetti nell'individuazione di specifici interventi di semplificazione, innovazione e riduzione dei costi dei processi amministrativi;

f) che, in virtù di quanto sopra, d'intesa con AgID, a seguito dell'approvazione del Piano triennale per l'informatica nella Pubblica Amministrazione 2019-2021 e del Piano 2020 -2022, è stato aggiornato il programma delle gare strategiche ICT;

g) che, ai fini del perseguimento degli obiettivi di cui al citato Piano triennale per l'informativa 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. 115 del 04/10/2021 e nella Gazzetta Ufficiale dell'Unione Europea n. S-191 del 01/10/2021, una procedura aperta per la stipula di un Accordo Quadro, ai sensi dell'art. 54, comma 3, del D. Lgs. n. 50/2016 con un unico operatore;

h) il Fornitore che sottoscrive il presente Accordo Quadro è risultato aggiudicatario della predetta procedura per i Lotti 1, 2 e 3 e, per l'effetto, ha manifestato la volontà di impegnarsi ad eseguire quanto stabilito nel presente Accordo Quadro e relativi Allegati alle condizioni, modalità e termini ivi stabiliti e nei successivi Contratti di Fornitura;

i) che la stipula del presente Accordo Quadro con i suoi Allegati non è fonte di alcuna obbligazione per la Consip S.p.A. e/o per le Amministrazioni nei confronti del Fornitore;

j) che i singoli Contratti di Fornitura verranno stipulati a tutti gli effetti tra le Amministrazioni ed il Fornitore affidatario del singolo ordinativo, in base alle modalità ed i termini indicati nel presente Accordo Quadro e relativi Allegati;

k) che il Fornitore dichiara che quanto risulta dal presente Accordo Quadro e dai suoi Allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico, nonché gli ulteriori atti della procedura, definiscono in modo adeguato e completo gli impegni assunti con la firma del presente atto, nonché l'oggetto delle prestazioni da fornire e, in ogni caso, ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica delle stesse e per la formulazione dell'offerta;

l) il Fornitore ha presentato la documentazione richiesta ai fini della stipula del presente Accordo Quadro che, anche se non materialmente allegata al presente atto, ne forma parte integrante e sostanziale, ivi incluse le seguenti garanzie definitive:

- Lotto 1: garanzie definitive nei confronti di Consip S.p.a. e delle Amministrazioni, rilasciata rispettivamente dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia ed avente n 2348037 per un importo di Euro 240.000,00 = (duecentoquarantamila/00) e dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia ed avente n 2348038 per un importo di Euro 42.560.000,00 = (quarantaduemilionicinquecentosessantamila/00), quest'ultimo è esteso fino al valore di Euro 63.840.000 = (sessantatremilioniottocentoquarantamila/00), come da appendice n.2 della suddetta garanzia, in considerazione dell'incremento del valore stimato del Lotto 1 di cui al comma 2 dell'art. 3;
- Lotto 2: garanzie definitive nei confronti di Consip S.p.a. e delle Amministrazioni, rilasciate rispettivamente

dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia ed avente n 2348044 per un importo di Euro 76.800,00 = (settantaseimilaottocento/00) e dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia ed avente n 2348042 per un importo di Euro 13.872.640,00 = (tredicimilioniottocentosettantaduemilaseicentoquaranta/00), quest'ultimo è esteso fino al valore di Euro 20.808.960,00 = (ventimilioniottocentoottomilanovecentosessanta/00), come da appendice n.3 della suddetta garanzia, in considerazione dell'incremento del valore stimato del Lotto 2 di cui al comma 2 dell'art. 3;

- Lotto 3: garanzie definitive nei confronti di Consip S.p.a. e delle Amministrazioni, rilasciata rispettivamente dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia ed avente n 2348045 per un importo di Euro 91.200,00 = (novantunomiladuecento/00) e dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia ed avente n 2348046 per un importo di Euro 16.102.880,00 = (sedicimilionicentoduemilaottocentoottanta/00), quest'ultimo è esteso fino al valore di Euro 24.154.320,00 = (ventiquattromilionicentocinquantaquattromilatrecentoventi/00), come da appendice n.3 della suddetta garanzia, in considerazione dell'incremento del valore stimato del Lotto 3 di cui al comma 2 dell'art. 3;

a garanzia dell'adempimento delle obbligazioni contrattuali nascenti dall'Accordo Quadro e degli ordinativi di fornitura.

m) che il Fornitore, con la seconda sottoscrizione, dichiara, ai sensi e per gli effetti di cui agli artt. 1341 e 1342 cod. civ., di accettare tutte le condizioni e patti contenuti nel presente Accordo Quadro e relativi Allegati, e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni riportate in calce al presente Accordo Quadro;

n) che il presente Accordo Quadro viene sottoscritto dalle parti con firma digitale rilasciata da ente certificatore autorizzato.

o) risulta allo stato pendente, innanzi al TAR Lazio Roma, sez II, il giudizio N.R.G.4763/2022 instaurato dalla FASTWEB s.p.a. in proprio e quale mandataria del costituendo RTI con le mandanti Fincantieri NexTech S.p.A., N&C S.r.l., Business Integration partners S.p.A. e Consorzio Reply Public Sector contro Consip S.p.A. e il RTI Telecom Italia S.p.A., Dgs S.p.a., Scai Solution Group S.p.a., Maticmind S.p.a, nonché ex art.49 cod. proc. amm., nei confronti del Ministero per l'innovazione tecnologica e la transizione digitale, Presidenza del Consiglio dei Ministri, Agenzia per l'Italia digitale, per l'annullamento dell'aggiudicazione definitiva non efficace (note del 15 marzo 2022, prott. 12724, 12727 e 12749 del 2022), relativamente al quale, senza concedere misure cautelari, all'udienza del 18 maggio 2022, il Tribunale ha fissato la trattazione del merito al 13 luglio 2022. Con ricorso con motivi aggiunti il RTI Fastweb ha impugnato l'aggiudicazione definitiva efficace facendo altresì richiesta di fissazione dell'udienza cautelare. In data 15 maggio 2022 il RTI TIM proponeva ricorso incidentale avverso gli atti della procedura selettiva chiedendo l'esclusione del RTI Fastweb. L'udienza cautelare veniva fissata al 13 luglio 2022. Con Ordinanza numero 4602/2022 del 15 luglio 2022, il TAR del Lazio Roma ha rigettato la richiesta di misure cautelari ed ha disposto: la fissazione dell'udienza di merito per il 7 dicembre 2022 nonché, ai sensi dell'art. 66 cod. proc. amm. una verificazione sulle censure proposte nel giudizio dalle parti.

Ciò premesso, tra le parti come in epigrafe rappresentate e domiciliate

SI CONVIENE E SI STIPULA QUANTO SEGUE

ARTICOLO 1 - DEFINIZIONI

1. Nell'ambito del presente Accordo Quadro, si intende per:

a) **Accordo Quadro:** il presente atto, comprensivo di tutti i suoi Allegati, nonché dei documenti ivi richiamati, quale accordo concluso da Consip S.p.A. anche per conto delle Amministrazioni, da una parte, ed il Fornitore, dall'altra parte, con lo scopo di stabilire le clausole relative agli Appalti Specifici da affidare per tutta la durata del medesimo Accordo Quadro;

b) **Amministrazione/i o Amministrazione/i Contraente/i:** le stazioni appaltanti, nonché gli altri soggetti che ai sensi della normativa vigente sono legittimati a affidare gli Ordinativi di Fornitura basati sul presente Accordo Quadro;

c) **Ministero:** Ministero dell'Economia e delle Finanze;

d) **Data di Attivazione**: la data a partire dalla quale le Amministrazioni Pubbliche possono utilizzare l'Accordo Quadro, ai sensi di quanto disposto nel successivo art. 4;

e) **Fornitore**: il singolo aggiudicatario (impresa, raggruppamento temporaneo o consorzio di imprese) della procedura aperta di cui in premessa, che, conseguentemente, sottoscrive l'Accordo Quadro impegnandosi a quanto nello stesso previsto e, in particolare, ad eseguire i singoli contratti derivanti dagli Appalti Specifici;

f) **Capitolato d'Oneri**: il documento che ha disciplinato la partecipazione alla procedura aperta di cui in premessa, e contenente, altresì, le condizioni e le modalità per l'affidamento degli Appalti Specifici;

g) **Appalto/i Specifico/i o Contratto di fornitura:** il Contratto che si perfeziona in seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione dell'Ordine di fornitura da parte dell'operatore economico aggiudicatario dell'Accordo Quadro, avente ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi, in base ai criteri, le modalità ed i termini indicati nel presente Accordo Quadro e nei relativi Allegati;

h) **Ordine di fornitura:** il documento inviato dall'Amministrazione al Fornitore, individuato sulla base di quanto previsto alla lettera precedente, con il quale l'Amministrazione medesima affida il singolo Appalto Specifico;

l) **Unità/Punto/i Ordinante/i**: gli uffici e, per essi, le persone fisiche delle Amministrazioni Contraenti abilitati ad effettuare gli Ordinativi di Fornitura e che verranno negli stessi indicate;

i) **Giorno lavorativo**: da lunedì a venerdì, esclusi sabato e festivi;

j) **Soggetti aggregatori:** le centrali di committenza iscritte nell'elenco istituito ai sensi dell'art. 9, comma 1, del decreto legge 24 aprile 2014, n. 66, convertito con modificazioni, dalla legge 23 giugno 2014, n. 89, come definiti all'art. 3, comma 1, lett. n) del D.Lgs. n. 50/2016.

2. Le espressioni riportate negli Allegati al presente Accordo Quadro hanno il significato, per ognuna di esse, specificato nei medesimi Allegati, tranne qualora il contesto delle singole clausole dell'Accordo Quadro disponga diversamente.

ARTICOLO 2 - VALORE DELLE PREMESSE, DEGLI ALLEGATI E NORME REGOLATRICI

1. Le premesse di cui sopra, gli atti ed i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ivi incluso il Bando di gara, il Capitolato d'Oneri, il Capitolato Tecnico parte Generale e parte Speciale,i chiarimenti resi in fase di garae le Regole del Sistema di e-Procurement della Pubblica Amministrazione – Parte I, , ancorché non materialmente allegati, costituiscono parte integrante e sostanziale e sono fonte delle obbligazioni del presente Accordo Quadro per effetto della sua sottoscrizione. Tali documenti sono disponibili al seguente link: **https://www.consip.it/bandi-di-gara/gare-e-avvisi/gara-sicurezza-on-premises-protezione-perimetrale-endpoint-e-anti-apt-per-le-pa**.

2. Costituiscono, altresì, parte integrante e sostanziale dell'Accordo Quadro: l'Allegato "A" (Offerta Tecnica del Fornitore), l'Allegato "B" (Offerta Economica del Fornitore), l'Allegato "C" (Corrispettivi e tariffe), l'Allegato "D" (Patto di integrità), l'Allegato "E" (Contratto di avvalimento), l'Allegato "F" (Nomina a responsabile del trattamento dei dati l'Allegato), l'Allegato "G" (Flusso dati per le Commissioni a carico del Fornitore), l'Allegato "H" (Disposizioni per la Governance) e l'Allegato "I" (Regolamento degli Organismi di coordinamento e controllo).

3. Il presente Accordo Quadro è regolato:
   a) dal contenuto dell'Accordo Quadro e dei suoi Allegati che costituiscono la manifestazione integrale di tutti gli accordi intervenuti con il Fornitore relativamente alle attività e prestazioni contrattuali che costituiscono parte integrante e sostanziale dell'Accordo Quadro;
   b) dalle disposizioni di cui al D.Lgs. n. 50/2016 e s.m.i.;
   c) dalle disposizioni di cui al d.P.R. 10 ottobre 2010, n. 207, nei limiti stabiliti dagli artt. 216 e 217 del D. Lgs. n. 50/2016;
   d) dalle disposizioni anche regolamentari in vigore per le Amministrazioni, di cui il Fornitore dichiara di avere esatta conoscenza e che, sebbene non siano materialmente allegati, formano parte integrante del presente atto;
   e) dalle norme in materia di Contabilità pubblica;
   f) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato;
   g) dal Codice Etico e dal Piano Triennale per la prevenzione della corruzione e della trasparenza della Consip S.p.A., consultabili sul sito internet della stessa Consip;
   h) dal patto di integrità.
4. I Contratti di Fornitura saranno regolati dalle disposizioni in essi previste, dal presente Accordo Quadro e dai suoi allegati, dalle disposizioni indicate al precedente comma nonché dalla disciplina speciale in materia di Perimetro nazionale di Sicurezza.
5. In caso di contrasto o difficoltà interpretativa tra quanto contenuto nel presente Accordo Quadro e relativi Allegati, da una parte, e quanto dichiarato nell'Offerta Tecnica, dall'altra parte, prevarrà quanto contenuto nei primi, fatto comunque salvo il caso in cui l'Offerta Tecnica contenga, a giudizio di Consip S.p.A. e/o delle Amministrazioni, previsioni migliorative rispetto a quelle contenute nel presente Accordo Quadro e relativi Allegati.
6. Le clausole dell'Accordo Quadro e dei Contratti di Fornitura sono sostituite, modificate od abrogate automaticamente per effetto di norme aventi carattere cogente contenute in leggi o regolamenti che entreranno in vigore successivamente, fermo restando che in ogni caso, anche ove intervengano modificazioni autoritative dei prezzi migliorativi per il Fornitore, quest'ultimo rinuncia a promuovere azioni o ad opporre eccezioni rivolte a sospendere o a risolvere il rapporto contrattuale in essere.
7. Nel caso in cui dovessero sopraggiungere provvedimenti di pubbliche autorità dai contenuti non suscettibili di inserimento di diritto nel presente Accordo Quadro e nei Contratti di Fornitura e che fossero parzialmente o totalmente incompatibili con l'Accordo Quadro e relativi Allegati e/o con i Contratti di Fornitura, Consip S.p.A. e/o le Amministrazioni, da un lato, e il Fornitore, dall'altro lato, potranno concordare le opportune modifiche ai surrichiamati documenti sul presupposto di un equo contemperamento dei rispettivi interessi e nel rispetto dei relativi criteri di aggiudicazione della procedura.
8. In virtù della stipula dell'Accordo Quadro in pendenza del/i ricorso/i giurisdizionale/i, e in conseguenza della relativa sentenza, nonché di ogni altro eventuale e futuro provvedimento giurisdizionale e/o amministrativo relativo a ulteriori e diversi giudizi o procedimenti di qualsivoglia natura che dovessero essere instaurati da chicchessia - dovesse essere imposto il riesame e/o l'annullamento, anche in autotutela, dell'aggiudicazione definitiva e/o della gara e da ciò scaturisse qualsiasi tipo di invalidità e/o perdita di efficacia dell'Accordo Quadro, il Fornitore con la sottoscrizione dell'Accordo Quadro espressamente rinuncia, ora per allora, irrevocabilmente ed a titolo definitivo, a proporre successive azioni e/o eccezioni volte ad ottenere un risarcimento del danno nei confronti di Consip S.p.A. e delle Amministrazioni eventualmente aderenti all'Accordo Quadro, fatto sempre salvo verso queste ultime il diritto al pagamento dei corrispettivi per le prestazioni eseguite a regola d'arte nelle more della pronuncia giurisdizionale resa in qualunque grado di giudizio. Restano salvi ed impregiudicati i diritti del Fornitore all'impugnativa dei provvedimenti giudiziali e/o amministrativi che lo vedessero soccombente nei procedimenti giudiziari di cui sopra.

ARTICOLO 3 - OGGETTO DELL'ACCORDO QUADRO

1. L'Accordo Quadro definisce la disciplina normativa e contrattuale relativa alle condizioni e alle modalità di affidamento da parte delle Amministrazioni dei singoli Appalti Specifici e, conseguentemente, di esecuzione delle prestazioni dei singoli Contratti di Fornitura aventi ad oggetto la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi alle condizioni tutte espressamente stabilite nel presente atto e relativi Allegati.
2. I valori indicativi stimati dei 3 lotti del presente Accordo Quadro, rappresentativo della sommatoria degli importi massimi presunti degli Appalti Specifici che verranno affidati in virtù dell'Accordo Quadro medesimo, sono i seguenti:
   - Lotto 1: Euro 100.000.000,00 = (centomilioni/00), IVA esclusa;
   - Lotto 2: Euro 32.000.000,00 = (trentaduemilioni/00), IVA esclusa;
   - Lotto 3: Euro 38.000.000,00 = (trentoottomilioni/00), IVA esclusa.

   Ai sensi dell'art. 49 comma 1 del D.L. 50/2022 che ha modificato l'articolo 16-bis, comma 7, del decreto-legge 21 ottobre 2021, n. 146, convertito, con modificazioni, dalla legge 17 dicembre 2021, n. 215, il valore indicativo stimato è incrementato in misura pari al 50%. Pertanto i valori finali stimati dei 3 lotti del presente Accordo Quadro sono pari a:
   - Lotto 1: Euro 150.000.000,00 = (centocinquantamilioni/00), IVA esclusa;
   - Lotto 2: Euro 48.000.000,00 = (quarantottomilioni/00), IVA esclusa;
   - Lotto 3: Euro 57.000.000,00 = (cinquantasettemilioni/00), IVA esclusa.
3. Qualora, anteriormente alla scadenza del termine di durata dell'Accordo Quadro di ogni Lotto, anche eventualmente prorogata, il valore relativo ad un Appalto Specifico raggiunga il valore stimato dell'Accordo Quadro medesimo oppure lo ecceda (comunque fino a una soglia massima del 20%), Consip considererà quest'ultimo come giunto a scadenza e di conseguenza non potranno essere emessi ulteriori ordini di fornitura.
4. Fermo quanto sopra, Consip S.p.A., in costanza del termine di durata summenzionato, effettuerà, periodicamente, una verifica sugli Appalti specifici già aggiudicati finalizzata ad accertare se l'importo offerto dal rispettivo aggiudicatario è inferiore a quello posto a base di gara provvedendo, in tale evenienza, a ricalcolare, in aumento, la quota di massimale ancora disponibile per nuovi e successivi Appalti specifici.
5. Il presente Accordo Quadro è concluso con il Fornitore aggiudicatario della procedura aperta di cui in premessa, che con la sottoscrizione del presente atto, si impegna a dare esecuzione ai Contratti di Fornitura che si perfezionano decorso il termine di 4 giorni solari dalla ricezione, dell'Ordine di fornitura inviato dalla singola Amministrazione, che vale quale affidamento dell'Appalto Specifico basato sulle condizioni stabilite nel presente Accordo Quadro e relativi Allegati.
6. L'affidamento dell'Appalto Specifico da parte della singola Amministrazione in favore del Fornitore avviene attraverso l'invio dell'Ordine di fornitura.
7. Il Fornitore, pertanto, si impegna ad eseguire in caso di affidamento dei singoli Appalti Specifici, in ragione di quanto negli stessi richiesto con Ordine di fornitura, le prestazioni meglio specificate nell'Accordo Quadro, nel Capitolato Tecnico e nell'Ordine di fornitura e segnatamente:
   a) fornitura dei seguenti prodotti:
      - Next Generation Firewall (NGFW);
      - Network Access Control (NAC);
      - Endpoint Protection Platform (EPP)/Endpoint Detection & Response (EDR);
      - Server Protection Platform (SPP);
      - Protezione Anti-Advanced Persistent Threat (Anti-APT);
   b) erogazione dei seguenti servizi connessi:
      - installazione e configurazione (inclusi nella fornitura);
      - formazione e affiancamento;

- manutenzione;
- Contact Center ed help desk (incluso nel complesso dei corrispettivi offerti);
- hardening su client;
- supporto specialistico;

secondo quanto stabilito ai paragrafi 3.1 e 3.2 del Capitolato Tecnico parte Speciale e nel rispetto delle caratteristiche e delle condizioni di erogazione migliorative eventualmente offerte in Accordo Quadro, dei livelli minimi di servizio e degli eventuali livelli migliorativi offerti.

8. Al fine di affidare un Appalto Specifico basato sul presente Accordo Quadro, le singole Amministrazioni procedono:
   a. alla definizione dell'oggetto del Singolo Appalto, del quantitativo e dell'importo contrattuale, nel rispetto di quanto stabilito ed alle condizioni di cui al presente Accordo Quadro e relativi Allegati;
   b. *<qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Appalto specifico sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019* alla comunicazione al CVCN o a uno dei CV secondo quanto previsto dall'art. 1 comma 6 lettera a), legge n. 133/2019 la cui efficacia è stata modificata dall'art 16 comma 9, lett. a) del D.L. n.82/2021 (convertito con modificazioni dalla L. n 109/2021);
   c. all'affidamento dell'Appalto Specifico in favore del Fornitore mediante invio dell'Ordine di fornitura al Fornitore nel rispetto delle condizioni previste nel presente Accordo Quadro e relativi Allegati, e al conseguente perfezionamento del Contratto di Fornitura.
9. Ai sensi di quanto stabilito all'art. 89, comma 9, del D. Lgs. n. 50/2016, le Amministrazioni contraenti eseguono in corso d'esecuzione del Contratto di fornitura le verifiche sostanziali circa l'effettivo possesso dei requisiti e delle risorse oggetto dell'avvalimento da parte dell'impresa ausiliaria, nonché l'effettivo impiego delle risorse medesime nell'esecuzione dell'appalto. A tal fine l'Amministrazione contraente accerta in corso d'opera che le prestazioni oggetto del Contratto di fornitura sono svolte direttamente dalle risorse umane e strumentali dell'impresa ausiliaria che il Fornitore utilizza in adempimento degli obblighi derivanti dal contratto di avvalimento.

ARTICOLO 4 - DURATA DELL'ACCORDO QUADRO E DEI CONTRATTI DERIVANTI DA APPALTI SPECIFICI

1. Il presente Accordo Quadro ha una durata di 24 mesi a decorrere dalla data di attivazione, ovvero la minore durata determinata dall'esaurimento del valore massimo stabilito nel precedente articolo.
2. Resta inteso che, per durata dell'Accordo Quadro, si intende il termine entro il quale le Amministrazioni potranno affidare i singoli Appalti Specifici mediante l'invio ai Fornitori dell'Ordine di fornitura.
3. Con riferimento a ciascun Appalto Specifico, il relativo Contratto di Fornitura ha una durata di massima di 24 mesi decorrenti dalla data di inizio dell'esecuzione della fornitura.
4. L'Amministrazione, in conformità a quanto disposto all'articolo 106, comma 11, del D. Lgs. n. 50/2016, si riserva la facoltà in corso di esecuzione di modificare la durata del contratto di fornitura, con comunicazione inviata a mezzo pec al Fornitore, prorogandolo per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione di un nuovo contraente, ivi inclusa la stipula del contratto. In tal caso il Fornitore è tenuto all'esecuzione delle prestazioni previste nel contratto agli stessi prezzi, patti e condizioni o più favorevoli per l'Amministrazione.

ARTICOLO 5 - PREZZI E VINCOLI DEGLI APPALTI SPECIFICI

1. I corrispettivi per ciascun Appalto Specifico verranno determinati sulla base dei prezzi stabiliti nell'Allegato D, "Corrispettivi e tariffe", i quali rappresentano quindi un vincolo per il Fornitore.
2. Il Fornitore, inoltre, nel dare seguito al singolo Ordine di fornitura dovrà, fermi i prezzi unitari offerti, fornire prodotti e/o servizi che dovranno necessariamente possedere tutte le caratteristiche (minime e migliorative offerte) per

l'aggiudicazione del presente Accordo Quadro.

3. Il pagamento dei corrispettivi dovrà essere effettuato mediante strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché ai sensi delle emanate Determinazioni dell'A.N.AC., e, fatte salve le eventuali ulteriori indicazioni sugli "strumenti idonei" che dovessero essere emanate dalla medesima Autorità.
4. I corrispettivi dovuti al Fornitore, a decorrere dal secondo anno di esecuzione, sono oggetto di revisione sulla base di un'istruttoria condotta in considerazione dei prezzi di riferimento pubblicati dall'ANAC ai sensi dell'art. 9, comma 7, del D.L. 66/2014 convertito nella legge n. 89/2014, in mancanza, in ragione dell'indice ISTAT dei prezzi al consumo. Restano ferme le disposizioni di cui all'art. 1, comma 511, della legge 28 dicembre 2015, n. 208.

ARTICOLO 6 - AFFIDAMENTO DEGLI APPALTI SPECIFICI

1. Ciascun Appalto Specifico verrà affidato dalla singola Amministrazione nel rispetto e alle condizioni stabilite al paragrafo 24 del Capitolato d'Oneri e agli artt. 3 e 4 del presente atto.
2. Fermo quanto stabilito in altre parti del presente Accordo Quadro e relativi Allegati, nell'Ordine di Fornitura che verrà inviato al Fornitore affidatario dell'Appalto Specifico, l'Amministrazione:
   - determinerà l'importo contrattuale ed il quantitativo della fornitura*;*
   - dovrà contenere l'indicazione del/i luogo/ghi di esecuzione della fornitura;
   - dovrà prevedere la durata del Contratto di fornitura;
   - dovrà, laddove necessario, predisporre/integrare il documento dei rischi da interferenze.

   Nel caso di Appalto Specifico affidato da un Soggetto Aggregatore, nell'Ordine di fornitura il Soggetto Aggregatore, inoltre:
   - dovrà indicare tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'affidamento;
   - dovrà indicare gli importi e i quantitativi relativi ad ogni singola Amministrazione;
   - potrà indicare le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni.
3. L'utilizzo dell'Accordo Quadro avviene esclusivamente attraverso il Sistema di e-Procurement della Pubblica Amministrazione. L'accesso e l'utilizzo del Sistema sono disciplinati dalle Regole del Sistema di e-Procurement della Pubblica Amministrazione, Parte I, Allegato 19 al Capitolato d'Oneri, che le Amministrazioni e il Fornitore dichiarano di ben conoscere ed accettare integralmente.
4. Sono legittimate ad utilizzare l'Accordo Quadro, ai sensi della normativa vigente, le Amministrazioni come definite nel precedente articolo 1.
5. Per potere acquistare attraverso l'Accordo Quadro ed emettere validi Ordini di Fornitura, il Punto Ordinante dell'Amministrazione deve preventivamente abilitarsi al Sistema di e-Procurement. Resta inteso che l'abilitazione del Punto Ordinante non comporta, in capo alla Consip S.p.A. e/o al Ministero, una verifica dei poteri di acquisto attribuiti a ciascuna Unità Ordinante.
6. Le predette Amministrazioni, previa effettuazione di apposita abilitazione al Sistema di e-Procurement della Pubblica Amministrazione tramite il proprio Punto Ordinante attraverso l'apposita procedura prevista dal Sistema, utilizzano l'Accordo Quadro mediante Ordini di Fornitura. L'Ordine di Fornitura consiste in un documento informatico identificato con un apposito numero e generato automaticamente dal Sistema sulla base dei dati forniti dal Punto Ordinante, con le modalità di seguito descritte.
7. Affinché l'Ordine di Fornitura possa produrre effetti, esso deve assumere la forma di un documento informatico generato dal Sistema, sottoscritto con firma digitale dal Punto Ordinante e trasmesso al Fornitore attraverso il Sistema. Non è consentito l'invio di Ordini di Fornitura con altre modalità. Il Fornitore prende atto e accetta che non dovrà in alcun modo dare seguito ad Ordini di Fornitura che non siano trasmessi nel rispetto delle modalità di cui sopra.

8. Ove il Fornitore ritenga di non poter dare esecuzione ad Ordini di Fornitura provenienti da un soggetto non legittimato, in base alla normativa vigente, ad utilizzare gli Accordi Quadro, dovrà, tempestivamente, e comunque entro quattro giorni solari dal ricevimento degli Ordini stessi, informare l'Amministrazione e Consip S.p.A., spiegando le ragioni del rifiuto.
9. Qualora l'Ordine di Fornitura non sia completo in ogni sua parte necessaria, l'Ordine di Fornitura medesimo non avrà validità ed il Fornitore non dovrà darvi esecuzione; quest'ultimo, tuttavia, dovrà darne tempestiva comunicazione alla Amministrazione, entro e non oltre quattro giorni solari dal ricevimento dell'Ordine stesso. In tal caso, l'Amministrazione potrà emettere un nuovo Ordine di Fornitura, secondo le indicazioni sopra riportate.
10. Per effetto dell'Ordine di Fornitura, il Fornitore sarà obbligato ad eseguire la fornitura richiesta, nell'ambito dell'oggetto contrattuale, restando inteso che in caso di mancata utilizzazione dell'Accordo Quadro da parte dei soggetti sopra indicati nulla potrà essere preteso a qualsiasi titolo dal medesimo Fornitore il quale, infatti, sarà tenuto a svolgere le attività, effettuare le forniture e prestare i servizi solo a seguito della ricezione degli Ordini di Fornitura, compilati ed inviati entro i termini ed in conformità alle condizioni sopra indicate.
11. I singoli Contratti di fornitura si concludono il quarto giorno lavorativo successivo alla ricezione da parte del Fornitore degli Ordini di Fornitura inviati dalle medesime Amministrazioni. Spirato il predetto termine, l'Ordine di Fornitura è irrevocabile per le Parti e, per l'effetto, il Fornitore è tenuto a dare esecuzione completa alla fornitura richiesta entro il termine indicato nell'Ordine di Fornitura. Il ritardo nell'avvio dell'esecuzione per causa imputabile al Fornitore costituisce causa di risoluzione di diritto dell'Ordinativo di Fornitura, ai sensi dell'art. 2, comma 1 della L. n. 120/2020 DL. 76/2020.

    Qualora il Fornitore non abbia autorizzato Consip S.p.A. alla pubblicazione delle generalità e del codice fiscale del/i delegato/i ad operare sul conto/i corrente/i dedicato/i, il Fornitore medesimo sarà tenuto a comunicare, entro e non oltre due giorni dalla conclusione del singolo Contratto di fornitura i surrichiamati dati alle Amministrazioni ordinanti.
12. Il Fornitore prende atto, rinunziando ora per allora a qualsiasi pretesa di risarcimento o di indennizzo, che l'Amministrazione ha la facoltà di revocare l'Ordine di Fornitura, avvalendosi esclusivamente del Sistema, da esercitarsi entro un giorno lavorativo dall'emissione dell'Ordine di Fornitura.
13. Qualora venga richiesto da Consip S.p.A., il Fornitore, entro un giorno lavorativo dalla richiesta, ha l'obbligo di dare riscontro alla medesima Consip S.p.A., anche per via telematica, di ciascun Ordine di Fornitura divenuto irrevocabile.
14. Le Amministrazioni provvederanno, al momento dell'emissione del singolo Ordine di Fornitura, tra le altre cose: i) alla nomina del Responsabile del Procedimento, ai sensi e per gli effetti dell'art. 31 del D.Lgs. n. 50/2016 ii) alla nomina del Direttore dell'esecuzione, laddove le relative funzioni non siano svolte dal Responsabile del procedimento nel rispetto degli artt. 101, 102 e 111 del D.Lgs. n. 50/2016; iii) ai sensi e per gli effetti dell'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i., degli artt. 6 e 7 del Decreto Legge 12 novembre 2010, n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora A.N.AC.) n. 8 del 18 novembre 2010, alla indicazione sul medesimo Ordine di Fornitura del CIG (Codice Identificativo Gara) "derivato" rispetto a quello dell'Accordo Quadro e da esse richiesto nonché del CUP (Codice Unico Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3.
15. Le Amministrazioni Contraenti procedono ad inviare a Consip S.p.A. il certificato di verifica di conformità di cui all'art. 102 del D.Lgs. n. 50/2016 e s.m.i. relativamente ai singoli contratti attuativi. Resta salva la facoltà per Consip S.p.A. di svolgere verifiche e controlli sull'esecuzione delle singole prestazioni.
16. 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 di Fornitura, 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.
17. Le Amministrazioni possono apportare modifiche al contratto di fornitura 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.

18. 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.
19. Così come chiarito dal **Comunicato Anac del 23 marzo 2021**, l'Amministrazione potrà imporre al fornitore affidatario dell'Appalto Specifico 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 dal presente Contratto, solo laddove ricorrano i presupposti di cui al **combinato disposto dei commi 1, lett. c) e 12 dell'art. 106, del Codice.** In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.
20. <*Qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Appalto specifico sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019*> atteso che prima di procedere all'emissione dell'Ordinativo di fornitura, il Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 (convertito con modificazioni dalla L. 109/2021) presso l'Agenzia per la cybersicurezza nazionale , o uno dei Centri di Valutazione (CV), istituiti presso il Ministero dell'interno e il Ministero della difesa, potrà aver riscontrato la comunicazione della medesima prevedendo la necessità di effettuare verifiche preliminari e/o imporre condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2 lett. b) legge 133/2019, l'Amministrazione contraente prevedrà nell'Ordinativo medesimo le clausole che condizioneranno, sospensivamente ovvero risolutivamente l'ordinativo al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN o da uno dei CV.

ARTICOLO 7 - OBBLIGAZIONI GENERALI DEL FORNITORE

1. Sono a carico del Fornitore tutti gli oneri e rischi relativi alla prestazione delle attività oggetto degli Appalti Specifici basati sul presente Accordo Quadro, nonché ad ogni attività che si rendesse necessaria per l'attivazione e la prestazione degli stessi o, comunque, opportuna per un corretto e completo adempimento delle obbligazioni previste, ivi compresi quelli relativi ad eventuali spese di trasporto, di viaggio e di missione per il personale addetto alla esecuzione contrattuale.
2. Il Fornitore si obbliga ad eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nell'Accordo Quadro, nel Capitolato d'Oneri, nel Capitolato Tecnico, nell'Ordine di fornitura, ivi inclusi i rispettivi Allegati.
3. Le prestazioni contrattuali dovranno necessariamente essere conformi alle caratteristiche tecniche e qualitative eventualmente migliorate in Offerta tecnica ed alle specifiche indicate nel Capitolato d'Oneri e nei relativi Allegati; in ogni caso, il Fornitore si obbliga ad osservare, nell'esecuzione delle prestazioni contrattuali, tutte le norme e le prescrizioni tecniche e di sicurezza in vigore, nonché quelle che dovessero essere successivamente emanate.
4. Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula dell'Accordo Quadro, resteranno ad esclusivo carico del Fornitore, intendendosi in ogni caso remunerati con il corrispettivo contrattuale indicato nell'Ordine di fornitura ed il Fornitore non potrà, pertanto, avanzare pretesa di compensi a tale titolo, nei confronti delle Amministrazioni e/o della Consip S.p.A., assumendosene ogni relativa alea.
5. Il Fornitore si impegna espressamente a:
   a) impiegare, a proprie cura e spese, tutte le strutture ed il personale necessario per l'esecuzione dei Contratti di Fornitura secondo quanto specificato nell'Accordo Quadro e nei rispettivi Allegati e negli atti di gara richiamati

nelle premesse;

b) rispettare, per quanto applicabili, le norme internazionali UNI EN ISO vigenti per la gestione e l'assicurazione della qualità delle proprie prestazioni;
c) predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a consentire alla Consip S.p.A. e alle singole Amministrazioni, per quanto di propria competenza, di monitorare la conformità dei servizi e delle forniture alle norme previste nell'Accordo Quadro e nei Contratti di Fornitura;
d) predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a garantire elevati livelli di servizi, ivi compresi quelli relativi alla sicurezza e riservatezza;
e) nell'adempimento delle proprie prestazioni ed obbligazioni, osservare tutte le indicazioni operative, di indirizzo e di controllo che a tale scopo saranno predisposte e comunicate dalle Amministrazioni o dalla Consip S.p.A., per quanto di rispettiva ragione;
f) comunicare tempestivamente a Consip S.p.A. e alle Amministrazioni, per quanto di rispettiva competenza, le eventuali variazioni della propria struttura organizzativa coinvolta nell'esecuzione dell'Accordo Quadro e nei singoli Appalti Specifici, indicando analiticamente le variazioni intervenute ed i nominativi dei nuovi responsabili;
g) non opporre a Consip S.p.A. e alle Amministrazioni qualsivoglia eccezione, contestazione e pretesa relative alla fornitura e/o alla prestazione dei servizi;
h) manlevare e tenere indenne Consip S.p.A. e le Amministrazioni da tutte le conseguenze derivanti dalla eventuale inosservanza delle norme e prescrizioni tecniche, di sicurezza, di igiene e sanitarie vigenti;
i) adottare, in fase di esecuzione contrattuale, le eventuali cautele rese necessarie dallo svolgimento delle prestazioni affidate in locali o ambienti in cui l'Amministrazione Contraente tratta informazioni classificate, con particolare riguardo alle specifiche misure previste dalla normativa in proposito vigente;
j) rispettare gli obblighi in materia ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali elencate nell'allegato X del D. Lgs. n. 50/2016.
k) a supportare le Amministrazioni nell'effettuazione delle verifiche preliminari richieste dal CVCN o dai CV nonché a rispettare le condizioni e i test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2 lett. b) legge 133/2019 eventualmente imposti dal CVCN o dai CV.

6. Le attività necessarie per la predisposizione dei mezzi e per l'attivazione dei servizi e/o delle forniture oggetto dell'Accordo Quadro e dei singoli Contratti di Fornitura, eventualmente da svolgersi presso gli uffici delle Amministrazioni, dovranno essere eseguite senza interferire nel normale lavoro degli uffici; modalità e tempi dovranno comunque essere concordati con le Amministrazioni stesse nel rispetto di quanto stabilito nel Capitolato Tecnico; peraltro, il Fornitore prende atto che, nel corso dell'esecuzione delle prestazioni contrattuali, gli uffici delle Amministrazioni continueranno ad essere utilizzati dal personale delle Amministrazioni stesse e/o da terzi autorizzati. Il Fornitore si impegna, pertanto, ad eseguire le predette prestazioni salvaguardando le esigenze delle Amministrazioni e/o di terzi autorizzati, senza recare intralci, disturbi o interruzioni alla attività lavorativa in atto.
7. Il Fornitore rinuncia espressamente, ora per allora, a qualsiasi pretesa o richiesta di compenso nel caso in cui l'esecuzione delle prestazioni contrattuali dovesse essere ostacolata o resa più onerosa dalle attività svolte dalle Amministrazioni e/o da terzi autorizzati.
8. Il Fornitore si impegna ad avvalersi di personale specializzato, in relazione alle diverse prestazioni contrattuali; detto personale potrà accedere agli uffici delle Amministrazioni nel rispetto di tutte le relative prescrizioni di accesso, fermo restando che sarà cura ed onere del Fornitore verificare preventivamente tali procedure.
9. Il Fornitore si obbliga a: *(a)* dare immediata comunicazione a Consip S.p.A. e alle singole Amministrazioni, di ogni circostanza che abbia influenza sull'esecuzione delle attività di cui all'Accordo Quadro e ai singoli Contratti di Fornitura; *(b)* prestare le forniture e/o i servizi nei luoghi che verranno indicati nei Contratti di Fornitura stessi.
10. Il Fornitore prende atto ed accetta che le forniture e/o i servizi oggetto dell'Accordo Quadro dovranno essere prestati

con continuità anche in caso di eventuali variazioni della consistenza e della dislocazione delle sedi e degli uffici delle Amministrazioni.

11. Nel rispetto della normativa vigente, le forniture e/o i servizi oggetto dell'Accordo Quadro e dei singoli Contratti di Fornitura non sono affidati al Fornitore in via esclusiva, pertanto le Amministrazioni possono affidare le stesse forniture, attività e servizi anche a soggetti terzi, diversi dal medesimo Fornitore.
12. Il Fornitore è tenuto a comunicare a Consip S.p.A. e alle altre Amministrazione ogni modificazione negli assetti proprietari, nella struttura di impresa e negli organismi tecnici e amministrativi. Tale comunicazione dovrà pervenire a Consip S.p.A. entro 15 (quindici) giorni dall'intervenuta modifica.
13. Ai sensi dell'art. 105, comma 2, D.Lgs. n. 50/2016, con riferimento a tutti i sub–contratti stipulati dal Fornitore per l'esecuzione del contratto, è fatto obbligo al Fornitore stesso di comunicare, a Consip S.p.A. e all'Amministrazione interessata, prima dell'inizio della prestazione, il nome del sub-contraente, l'importo del contratto, l'oggetto delle attività, delle forniture e dei servizi affidati. Eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto dovranno essere altresì comunicate a Consip S.p.A. e all'Amministrazione interessata.
14. Il monitoraggio di tutte le attività relative all'Accordo Quadro è effettuato dalla Consip mediante l'uso di nuove tecnologie e soluzioni organizzative, anche attraverso strumenti di "Information Technology", adottate in base alle esigenze di volta in volta individuate dalla/e Amministrazione/i e/o dalla Consip; a tal fine, il Fornitore si impegna a prestare piena collaborazione per rendere possibile dette attività di monitoraggio, per quanto di sua competenza. In particolare potrà essere richiesto al Fornitore l'invio periodico di informazioni, secondo le modalità innanzi specificate, per via telematica riguardanti tra l'altro: le Amministrazioni Contraenti; gli Ordini di Fornitura ricevuti con indicazione, a titolo esemplificativo e non esaustivo, della data di emissione e suddivisi per Amministrazione completi di: quantitativi, importo contrattuale, data di Consegna; gli importi fatturati suddivisi per Amministrazione.
15. La Consip si riserva il diritto di verificare in ogni momento l'esecuzione delle prestazioni contrattuali, ivi compreso l'andamento dei consumi della/e Amministrazione/i, e di richiedere al Fornitore l'elaborazione di report specifici, ivi inclusi quelli relativi alle penali eventualmente applicate dalle Amministrazioni contraenti che dovranno essere in ogni caso prodotti in sede di svincolo della garanzia di cui al successivo art. 13, anche in formato elettronico e/o in via telematica, da inviare a Consip entro 15 giorni dalla data di richiesta, pena l'applicazione delle penali di cui oltre. In particolare, con riferimento al report sulle penali, il Fornitore dovrà, preventivamente allo svincolo, inviare una dichiarazione resa ai sensi degli artt. 47 e 76 del d.P.R. n. 445/2000, contenente a titolo esemplificativo: numero identificativo dell'ordine, lotto di riferimento, data di ricezione da parte del Fornitore della comunicazione di applicazione della penale, importo della penale, motivazione e indicazione dell'articolo da cui sorge la sanzione. La suddetta dichiarazione dovrà essere inviata anche in assenza di applicazione di penali.
16. Il Fornitore si obbliga a comunicare all'indirizzo P.E.C. dprpaconsip@postacert.consip.it la data di cessazione degli effetti dell'ultimo contratto di fornitura stipulato, entro 15 giorni dall'evento, dichiarando contestualmente che non sussistono altri contratti di fornitura, a valere sull'Accordo Quadro, ancora vigenti e/o efficaci.
17. Il Fornitore si obbliga altresì a comunicare la data dell'ultima fattura emessa a carico delle Amministrazioni a valere sui contratti stipulati entro il termine di 15 giorni dall'emissione della stessa, fermo restando gli obblighi di invio, mensile e semestrali, relativi alle dichiarazioni di fatturato connesse all'obbligo del pagamento della fee di cui al successivo articolo sulla Commissione a carico del Fornitore.
18. Ai sensi dell'art. 47 comma 3, del D.L. n. 77/2021, convertito con modificazioni dalla L. n. 108/2021, il Fornitore è tenuto a consegnare alla Consip in relazione a ciascuna impresa e/o consorziata che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1, del d.lgs. n. 198/2006, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta. La

suddetta relazione dovrà essere tramessa, altresì, alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.

La relazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della stessa alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, dovrà essere consegnata alla Consip, **entro 6 mesi dalla stipula** dell'Accordo Quadro.

La violazione del succitato obbligo determina, ai sensi dell'art. 47, comma 6, del D.L. n. 77/2021, convertito con modificazioni dalla L. n. 108/2021, l'applicazione della penale di cui al successivo articolo "Penali", nonché l'impossibilità di partecipare per un periodo di dodici mesi ad ulteriori procedure di affidamento afferenti gli investimenti pubblici.

19. Ai sensi dell'art. 47 comma 3bis, del D.L. n. 77/2021, convertito con modificazioni dalla L. n. 108/2021, il Fornitore è tenuto a consegnare alla Consip Committente in relazione a ciascuna impresa e/o consorziata che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1, del d.lgs. n. 198/2006 una relazione relativa all'assolvimento degli obblighi di cui alla medesima legge n. 68/1999 e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di scadenza di presentazione delle offerte. La relazione dovrà essere trasmessa anche alle rappresentanze sindacali aziendali.
    La documentazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della relazione alle rappresentanze sindacali aziendali, dovrà essere consegnata alla Consip, **entro 6 mesi dalla stipula** dell'Accordo Quadro.
    La violazione anche di uno solo di tali obblighi comporta l'applicazione delle penali di cui al successivo articolo "Penali".
20. Le relazioni di cui ai precedenti commi 18 e 19, saranno pubblicate, sul profilo del Committente, nella sezione "Amministrazione trasparente", ai sensi dell'art. 29, comma 1 del Codice e dell'art. 47, comma 9, della L. n. 108/2021.
    La Committente procederà anche con gli ulteriori adempimenti di cui al citato articolo 47 comma 9, del D.L. n. 77/2021, convertito con modificazioni dalla L. n. 108/2021.
21. Il Fornitore si impegna a garantire il rispetto delle obbligazioni relative alla reportistica, di cui ai paragrafi 4.3.1 e 4.3.2 del Capitolato tecnico parte speciale, pena l'applicazione delle penali.
22. Le licenze d'uso dei prodotti software, nonché la proprietà della relativa documentazione, sono non esclusive e trasferibili ai sensi dell'articolo 6 della direttiva 19 dicembre 2003; le Amministrazioni Contraenti ne saranno titolari a partire dalla "Data di accettazione della fornitura"; prima di tale data tutti i rischi saranno a carico del Fornitore anche nell'ipotesi di detenzione dello stesso da parte dell'Amministrazione stessa; le licenze, pertanto, dovranno prevedere espressamente la facoltà di utilizzo dei prodotti software, nonché delle relative versioni correttive, da parte del personale delle Amministrazioni Contraenti e di terzi da queste autorizzati.
23. Si precisa che le attività di coordinamento del presente AQ verranno svolte con il supporto dell'Organismo di Coordinamento e Controllo di cui al Capitolato Tecnico parte generale.
24. Il Fornitore dell'Accordo Quadro in ottemperanza a quanto richiesto al par 2.4 Requisiti organizzativi del Capitolato tecnico Generale, ha l'obbligo di assicurare una quota pari ad almeno il 35,1 per cento delle assunzioni necessarie per l'esecuzione dell'Accordo Quadro o per la realizzazione di attività ad esso connesse o strumentali, destinata sia all'occupazione giovanile sia all'occupazione femminile, come previsto dall'art. 47, comma 4 del D.L. 77/2021, convertito con modifiche in l. 108/2021 e come meglio disciplinato dalle Linee Guida volte a favorire la pari opportunità di genere e generazionali, nonché l'inclusione lavorativa delle persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC, come da Decreto della Presidenza del Consiglio dei Ministri Dipartimento per le Pari Opportunità, pubblicato in data 30/12/2021. In caso di violazione del suddetto obbligo, verranno applicate le penali di cui al successivo articolo 12. A tal fine dovrà produrre quanto richiesto al par. 4.3 Reporting per le Amministrazioni del Capitolato Tecnico Speciale nei termini ivi indicati.

ARTICOLO 8 - OBBLIGAZIONI SPECIFICHE DEL FORNITORE

1. Il Fornitore dell'Accordo Quadro ha l'obbligo di tenere costantemente aggiornata, per tutta la durata del presente Accordo Quadro, la documentazione amministrativa richiesta e presentata a Consip S.p.A. per la stipula del presente Accordo Quadro. In particolare, pena l'applicazione delle penali di cui oltre, ciascun Fornitore ha l'obbligo di:
   a) comunicare, entro 15 (quindici) giorni dall'intervenuta modifica e/o integrazione, ogni modificazione e/o integrazione relativa al possesso dei requisiti di cui al paragrafo III.1.1 del Bando di gara;
   b) comunicare, entro 15 (quindici) giorni dalle intervenute modifiche, le modifiche soggettive di cui all'art. 80 del D.Lgs. n. 50/2016;
   c) comunicare alla Consip S.p.A. ogni modifica o il venir meno dei requisiti attestanti la capacità tecnica richiesta ai fini della partecipazione, entro il termine perentorio di 15 (quindici) giorni lavorativi decorrenti dall'evento modificativo.

L'affidatario si impegna a rispettare 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), per il quale il Fornitore ha provveduto a consegnare la documentazione a comprova nel rispetto dei suddetti requisiti.
Il Fornitore in adempimento di quanto previsto dall' articolo 22 del Regolamento UE/2021/241 del 12 febbraio 2021, in tema di tutela degli interessi finanziari dell'Unione Europea, ha dichiarato i dati identificativi dei titolari effettivi, anche eventualmente schermati da società fiduciarie**.**

ARTICOLO 9 - VERIFICA DI CONFORMITÀ

1. Con riferimento al singolo Contratto di Fornitura, ciascuna Amministrazione Contraente procederà ad effettuare la verifica di conformità delle forniture oggetto dell'Appalto Specifico per la verifica della corretta esecuzione delle prestazioni contrattuali; tale verifica, che potrà essere eseguita anche a campione, verrà effettuata, su richiesta di ciascuna Amministrazione secondo le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico. La verifica di conformità sarà svolta dalle Amministrazioni nel rispetto di quanto stabilito dagli artt. 101 e 102 del D. Lgs. n. 50/2016, nonché di quanto previsto nei provvedimenti di attuazione.
2. Le verifiche di conformità di cui ai precedenti commi si intendono positivamente superate solo se le verifiche abbiano dato esito positivo ed i beni/servizi siano risultati conformi alle prescrizioni dell'Accordo Quadro, del Capitolato Tecnico e dell'offerta tecnica, ove migliorativa; tutti gli oneri e le spese delle verifiche di conformità sono a carico del Fornitore.
3. Nel caso di esito positivo della verifica di conformità relativamente ai prodotti di cui all'art. 3 comma 8 lett. a), la data del relativo verbale verrà considerata quale "Data di accettazione della Fornitura", salvo diverso accordo tra l'Amministrazione contraente ed il Fornitore sulla data di inizio dell'erogazione.
4. Nel caso di esito positivo della verifica di conformità relativamente ai servizi di cui all'art. 3 comma 8 lett. b), n. 7, 8, 10 e 11**,** la data del relativo verbale verrà considerata quale "Data di accettazione del Servizio**".**
5. Nel caso di esito negativo della verifica di conformità e/o di esito negativo delle verifiche di funzionalità effettuate in corso d'opera a norma del successivo comma, il Fornitore dovrà sostituire i beni non perfettamente funzionanti e/o svolgere ogni attività necessaria affinché la verifica sia ripetuta e positivamente superata, salvo in ogni caso l'applicazione delle penali di cui oltre.
6. Conclusa positivamente la verifica di conformità, e comunque entro un termine non superiore a sette giorni dalla conclusione della stessa, l'Amministrazione Contraente rilascia il certificato di pagamento o altro documento equivalente ai fini dell'emissione della fattura da parte dell'appaltatore.
7. Le Amministrazioni Contraenti e la Consip S.p.A., per quanto di propria competenza, potranno effettuare unilaterali verifiche, anche in corso d'opera, per l'accertamento della conformità delle forniture e servizi resi disponibili.
8. Su richiesta del Fornitore, il Responsabile del Procedimento dell'Amministrazione contraente e/o di Consip S.p.A. emetterà/nno il certificato di esecuzione prestazioni delle forniture (CEF) e il certificato di esecuzione prestazioni dei

servizi (CES), coerentemente al modello predisposto dall'Autorità Nazionale Anticorruzione. Il certificato verrà emesso solo a seguito della verifica, da parte dell'Amministrazione contraente, dell'avvenuta consegna della fornitura dei beni oggetto dell'ordine di fornitura e della conseguente verifica di conformità della fornitura predetta, nel rispetto delle prescrizioni contrattuali e della normativa vigente.

9. In caso di mancata attestazione di regolare esecuzione, la singola Amministrazione potrà risolvere il contratto di fornitura e provvederà a dare comunicazione a Consip S.p.A. la quale potrà risolvere il presente Accordo Quadro.

ARTICOLO 10 - CORRISPETTIVI E FATTURAZIONE

1. I corrispettivi dovuti al Fornitore dalle singole Amministrazioni Contraenti per le prestazioni oggetto di ciascun Appalto Specifico sono indicati nell'Offerta Economica, di cui all'Allegato "B" e Corrispettivi e tariffe di cui all'Allegato "C" del presente Accordo Quadro.
2. I corrispettivi, indicati nell'Accordo Quadro, si riferiscono ai servizi e/o forniture prestati a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.
3. Tutti gli obblighi ed oneri derivanti al Fornitore dall'esecuzione dell'Accordo Quadro e dei singoli Appalti Specifici, dall'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti Autorità, sono compresi nel corrispettivo contrattuale.
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, ad eccezione di quanto previsto per i contratti ad esecuzione periodica e continuativa all'art. 5.
5. Tali corrispettivi sono dovuti dalle Amministrazioni Contraenti al Fornitore, successivamente all'esito positivo della verifica di conformità della prestazione, e secondo le seguenti tempistiche:
   a) con riferimento ai corrispettivi relativi alla fornitura dei beni oggetto del presente appalto, il Fornitore potrà emettere fattura a decorrere dalla "Data di accettazione della fornitura" di cui al precedente art. 9;
   b) con riferimento ai corrispettivi relativi ai servizi di "manutenzione" e "supporto specialistico", di cui ai paragrafi 3.2.3 e 3.2.4 del Capitolato Tecnico Speciale, il Fornitore potrà emettere fattura al termine del trimestre di riferimento a decorrere dalla "Data di accettazione del servizio". In particolare per il supporto specialistico la fattura dovrà tenere conto delle giornate effettivamente erogate nel trimestre di riferimento;
   c) con riferimento al corrispettivo relativo al servizio di "formazione e affiancamento" di cui al paragrafo 3.2.7 del Capitolato Tecnico Speciale, il Fornitore potrà emettere fattura – limitatamente alle giornate di addestramento effettuate – in seguito all'esito positivo della verifica e valutazione sull'andamento del corso sopra descritta, ossia dalla data riportata nel "Verbale di erogazione del Corso".
   d) con riferimento al corrispettivo relativo al servizio di "hardening su client" di cui al paragrafo 3.2.5 del Capitolato Tecnico Speciale, il Fornitore potrà emettere fattura – limitatamente alle attività erogate – in seguito all'esito positivo della verifica dei deliverable previsti nel Piano Operativo.
6. Ciascuna fattura dovrà contenere, oltre alle indicazioni che verranno fornite dall'Amministrazione, il riferimento all'Accordo Quadro, al singolo Ordine, cui si riferisce e dovrà essere intestata e trasmessa alla Amministrazione. Il CIG (Codice Identificativo Gara) "derivato" rispetto a quello dell'Accordo Quadro o il CUP (Codice Unico di Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003, comunicato dalle Amministrazioni sarà inserito, a cura del Fornitore, nelle fatture e dovrà essere indicato dalle Amministrazioni nei rispettivi pagamenti ai fini dell'ottemperanza agli obblighi scaturenti dalla normativa in tema di tracciabilità dei flussi finanziari.
7. Nel caso in cui l'aggiudicatario sia un R.T.I., gli obblighi di cui sopra dovranno essere tutti puntualmente assolti sia nelle fatture emesse dalla mandataria, sia dalle mandanti, nel rispetto delle condizioni e delle modalità tutte disciplinate dal presente articolo.

8. I predetti corrispettivi saranno fatturati con la cadenza riportata nel precedente comma 5 e saranno corrisposti dalle Amministrazioni secondo la normativa vigente in materia di Contabilità delle Amministrazioni Contraenti e previo accertamento della prestazione effettuate.
9. Ciascuna fattura dovrà essere inviata in forma elettronica in osservanza delle modalità previste dal D. Lgs. 20 febbraio 2004 n. 52, dal D. Lgs. 7 marzo 2005 n. 82 e dai successivi decreti attuativi. Il Fornitore si impegna, inoltre, ad inserire nelle fatture elettroniche i dati e le informazioni che la singola Amministrazione Contraente riterrà di richiedere, nei limiti delle disposizioni normative vigenti.
10. Ai fini del pagamento di corrispettivi di importo superiore ad euro 5.000,00, l'Amministrazione Contraente procederà in ottemperanza alle disposizioni previste dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973, con le modalità di cui al Decreto del Ministero dell'Economia e delle Finanze del 18 gennaio 2008 n. 40.
11. Rimane inteso che l'Amministrazione prima di procedere al pagamento del corrispettivo acquisirà di ufficio il documento unico di regolarità contributiva (D.U.R.C.) - attestante la regolarità del Fornitore in ordine al versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti.
12. A decorrere dal 1 Febbraio 2020, per gli acquisti di beni, e dal 1 Febbraio 2021, per gli acquisti di servizi, ai sensi dell'articolo 1, comma 412, della legge 31 dicembre 2009, n. 196 nonché dall'articolo 3 del Decreto del Ministro dell''Economia e delle Finanze 7 dicembre 2018, così come modificato dal Decreto del Ministero dell'Economia e delle Finanze 27 dicembre 2019, e in conformità alle "Linee Guida per l'emissione della trasmissione degli ordini elettronici adottate dal Ministero dell'Economia e delle Finanze" in data 29 dicembre 2020, l'Amministrazione Contraente rientrante nell'ambito applicativo della normativa sopra richiamata, dovrà, fatta eccezione per le esclusioni previste dal par. 3.1.2 delle richiamate Linee guida, trasmettere al Nodo di Smistamento degli Ordini di acquisto (NSO), il documento informatico attestante l'Ordinativo di Fornitura stesso (di seguito "Ordine NSO"). A tal fine, l'Amministrazione Contraente utilizza la funzione di trasmissione automatica al NSO, disponibile sul Sistema di e-procurement di Consip S.p.A., o, in alternativa, trasmette, l'Ordine NSO attraverso altre piattaforme.
13. Ciascuna fattura relativa agli acquisti, da e per conto degli enti del Servizio sanitario nazionale, di cui all'articolo 19, comma 2, lettere b) e c), del D. Lgs. 23 giugno 2011, n. 118, dovrà riportare gli estremi dei documenti informatici attestanti l'ordinazione e l'esecuzione dell'acquisto, trasmessi per mezzo del NSO. Qualora la fattura non indichi gli estremi dell'Ordine NSO da cui promana, a causa del mancato invio dell'Ordine NSO da parte dell'Ente, quest'ultimo è tenuto a provvedere al mancato invio con la trasmissione di un Ordine di convalida, secondo le modalità indicate nelle Linee Guida sopra richiamate. La mancanza dell'Ordine NSO non fa venir meno la validità della fattura regolarmente emessa dal Fornitore; conseguentemente, in caso di ritardato pagamento dovuto al tardivo invio dell'Ordine NSO, verranno riconosciuti al Fornitore gli interessi di cui al successivo comma 17, oltre a quanto previsto dai successivi commi in merito alla possibilità di sospensione delle prestazioni contrattuali.
14. Le Amministrazioni contraenti opereranno sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5 % che verrà liquidata dalle stesse solo al termine del Contratto di Fornitura; le ritenute possono essere svincolare solo in sede di liquidazione finale, in seguito all'approvazione del certificato di verifica di conformità e previa acquisizione del documento unico di regolarità contributiva.
15. I termini di pagamento delle predette fatture saranno definiti secondo le modalità di cui alla normativa vigente, e, in particolare, dell'art. 113 bis del Codice e del D.Lgs. n. 231/2002 s.m.i. I corrispettivi saranno accreditati, a spese dell'Amministrazione Contraente o del Fornitore ove sia previsto da norme di legge o regolamentari, sui conti correnti indicati nell'area "documentazione" relativa all'AQ in oggetto sul portale www.acquistinretepa.it.
    Il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e s.m.i..
16. Le generalità e il codice fiscale del/i soggetto/i delegato/i ad operare sul/sui predetto/i conto/i sono contenute in apposita e separata autorizzazione rilasciata alla Consip la quale ancorché non materialmente allegata, costituisce parte integrante e sostanziale dell'Accordo Quadro.

17. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto nell'art. 5 del D.Lgs. 9 ottobre 2002, n. 231.
18. Il Fornitore, sotto la propria esclusiva responsabilità, renderà tempestivamente noto alle Amministrazioni e alla Consip S.p.A., per quanto di propria competenza, le variazioni che si verificassero circa le modalità di accredito indicate nell'Accordo Quadro e nei singoli Appalti Specifici; in difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, il Fornitore non potrà sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.
19. Le singole imprese costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione Contraente, dovranno provvedere ciascuna alla fatturazione delle sole attività effettivamente svolte, corrispondenti alle attività dichiarate in fase di gara risultanti nell'atto costitutivo del Raggruppamento Temporaneo di Imprese, che il Fornitore si impegna a trasmettere in copia, ove espressamente richiesto dall'Amministrazione Contraente. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi e/o forniture cui si riferisce.
20. Il R.T.I. avrà facoltà di scegliere se: i) il pagamento da parte delle Amministrazioni Contraenti dovrà essere effettuato nei confronti della mandataria che provvederà poi alla redistribuzione dei corrispettivi a favore di ciascuna mandante in ragione di quanto di spettanza o ii) se, in alternativa, il pagamento dovrà essere effettuato dalle Amministrazioni Contraenti direttamente a favore di ciascun membro del RTI. La predetta scelta dovrà risultare dall'atto costitutivo del RTI medesimo. In ogni caso, la società mandataria del Raggruppamento medesimo è obbligata a trasmettere apposito prospetto riepilogativo delle attività e delle competenze maturate dalle singole imprese membri del RTI e, in maniera unitaria, le fatture di tutte le imprese raggruppate e prospetto riepilogativo delle attività e delle competenze maturate da ciascuna. Resta in ogni caso fermo quanto previsto dall'art. 48, comma 13, del D.Lgs. n. 50/2016.
21. Resta tuttavia espressamente inteso che in nessun caso il Fornitore potrà sospendere la fornitura e/o la prestazione dei servizi e, comunque, delle attività previste nell'Accordo Quadro e nei singoli Appalti Specifici, salvo quanto diversamente previsto nell'Accordo Quadro medesimo.
22. Qualora il Fornitore si rendesse inadempiente a tale obbligo, i singoli Contratti di Fornitura e/o l'Accordo Quadro si potranno risolvere di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi tramite pec o con lettera raccomandata A/R, rispettivamente dalle Amministrazioni Contraenti e dalla Consip S.p.A., ciascuno per quanto di propria competenza.
23. E' ammessa la cessione dei crediti maturati dal Fornitore nei confronti dell'Amministrazione a seguito della regolare e corretta esecuzione delle prestazioni oggetto del contratto di fornitura, nel rispetto dell'art. 106, comma 13, del D.Lgs. n. 50/2016. In ogni caso, è fatta salva ed impregiudicata la possibilità per l'Amministrazione Contraente di opporre al cessionario tutte le medesime eccezioni opponibili al Fornitore cedente. Le cessioni dei crediti devono essere stipulati mediante atto pubblico o scrittura privata autenticata e devono essere notificate alla Amministrazione Contraente. Si applicano le disposizioni di cui alla Legge n. 52/1991. Resta fermo quanto previsto in tema di tracciabilità dei flussi finanziari di cui al successivo articolo 28.
24. Ai fini del versamento dell'IVA per cessione di beni e prestazioni di servizi a favore delle Pubbliche Amministrazioni, si applica quanto previsto dall'art. 17-ter del d.P.R. n. 633 del 1972 ("split payment"), introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96, e le relative disposizioni di attuazione tra le quali il DM 23 gennaio 2015 come modificato dal DM 27 giugno 2017.
25. In caso di pericolo di insolvenza di Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, diversi dalle società pubbliche 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.

196, a totale partecipazione pubblica diretta o indiretta, è facoltà del Fornitore non inadempiente richiedere di prestare idonea garanzia per l'adempimento dell'obbligazione di pagamento relativa al contratto attuativo; tale garanzia dovrà essere rilasciata per un importo pari all'intero valore dell'Ordine di fornitura. La garanzia dovrà essere richiesta dal Fornitore entro il termine di 4 giorni lavorativi dalla ricezione dell'ordine e l'Amministrazione dovrà rilasciarla entro 30 giorni dalla ricezione della richiesta. Il Fornitore non inadempiente è legittimato a sospendere l'esecuzione della fornitura fino ad avvenuta ricezione della garanzia richiesta. Decorso inutilmente il termine per il rilascio della garanzia e ferma restando la facoltà di sospensione dell'esecuzione, è facoltà del Fornitore, ai sensi dell'art. 1454 c.c., diffidare per iscritto l'Amministrazione ad adempiere entro 15 giorni, decorsi inutilmente i quali il contratto s'intenderà risolto di diritto. Resta salva la facoltà dell'Amministrazione di recedere dal contratto di fornitura in caso di sospensione.

26. In caso di Ordinativi effettuati da Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, verso i quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato del presente AQ o in precedenti rapporti contrattuali, il Fornitore è legittimato a sospendere l'esecuzione del contratto di fornitura fino ad avvenuta ricezione della comprova del pagamento per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dei suddetti soggetti di recedere dal contratto attuativo in caso di sospensione.
27. Fermo restando quanto stabilito al precedente comma, in caso di ordinativi effettuati da Amministrazioni verso le quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato nel presente Accordo Quadro ovvero in precedenti rapporti contrattuali relativi alla fornitura di beni o servizi ricompresi nell'oggetto dell'Accordo Quadro, il Fornitore è legittimato a sospendere l'esecuzione del contratto di fornitura fino ad avvenuta ricezione della comprova del pagamento/stanziamento di fondi per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione all'Amministrazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dell'Amministrazione di recedere dal contratto attuativo in caso di sospensione.
28. Gli Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, nell'Ordinativo di fornitura, accettano preventivamente la cessione dei crediti ai sensi e per gli effetti di cui all'art. 106, comma 13 del D.Lgs. n. 50/2016.
29. Alle Amministrazioni Contraenti che effettueranno il pagamento dell'importo indicato in fattura in un termine inferiore rispetto a quello indicato al precedente comma 15 non verrà riconosciuto alcuno sconto.
30. Alle Amministrazioni Contraenti che all'atto dell'invio dell'Ordinativo di fornitura si impegnano a corrispondere l'importo indicato in fattura mediante addebito SEPA Direct Debit (SDD), non verrà riconosciuto alcuno sconto.
31. 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 del servizio di manutenzione un'anticipazione del prezzo di ciascun Ordine di Fornitura pari al 20 per cento del valore della suddetta prestazione. Tale percentuale può essere aumentata dall'Amministrazione Contraente fino ad un massimo del 30% al ricorrere dei presupposti di cui all'art. 207 del D.L. 34/2020.
    L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore dell'Amministrazione 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 che sarà indicato nel Piano Operativo/Piano di Lavoro Generale.
32. L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento della prestazione, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.
33. Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione della prestazione, 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 della anticipazione.

34. Laddove in relazione al singolo contratto attuativo ricorrano i presupposti soggettivi ed oggettivi, le Amministrazioni Contraenti e il Fornitore sono tenuti all'applicazione delle disposizioni di cui all'art. 17-bis del D.lgs. 241/1997 in materia di ritenute e compensazioni in appalti e subappalti.

ARTICOLO 11 - COSTI DELLA SICUREZZA

1. Le Amministrazioni, ai sensi dell'art. 26 del D. Lgs. 81/2008, provvederanno, prima dell'emissione dell'Ordine di Fornitura, ad integrare il "Documento di valutazione dei rischi standard da interferenze" allegato ai documenti di gara, riferendolo ai rischi specifici da interferenza presenti nei luoghi in cui verrà espletato l'appalto. In tale sede le Amministrazioni indicheranno i costi relativi alla sicurezza (anche nel caso in cui essi siano pari a zero).
2. Il Fornitore dovrà sottoscrivere per accettazione l'integrazione di cui al precedente comma. La predetta integrazione costituisce parte integrante e sostanziale dei documenti contrattuali.

ARTICOLO 12 - PENALI

1. Per ogni giorno di ritardo del Fornitore, non imputabile a Consip S.p.A. ovvero a forza maggiore o caso fortuito, nell'adempimento all'obbligo previsto al precedente articolo 8, comma 1, lettere a), b) e c), per la presentazione della documentazione ivi indicata, il Fornitore è tenuto a corrispondere a Consip S.p.A. una penale pari a euro 100,00 = (cento/00), fatto salvo il risarcimento del maggior danno.
2. In caso di invio della reportistica di cui al precedente articolo 7 comma 15, in ritardo, per cause non imputabili a Consip S.p.A. ovvero a forza maggiore o caso fortuito rispetto al termine ivi previsto, si procederà all'applicazione di una penale pari a 2000 euro, fatto salvo il risarcimento del maggior danno subito. Anche in caso di applicazione delle penali, resta fermo l'obbligo di adempiere all'invio delle informazioni richieste, entro l'ultimo giorno del mese successivo a quello di applicazione della sanzione, pena l'applicazione di ulteriori penali del medesimo importo, fino all'avvenuto adempimento.

   Solo con riferimento alla reportistica relativa alle penali eventualmente applicate dalle Amministrazioni contraenti, di cui al precedente articolo 7 comma 15, il ritardo, per cause non imputabili a Consip S.p.A. ovvero a forza maggiore o caso fortuito rispetto al termine ivi previsto, comporta l'applicazione di una penale pari a 2.000 euro, fatto salvo il risarcimento del maggior danno subito.
3. In caso di invio delle informazioni richieste al comma 2 del successivo articolo 31, oltre l'ultimo giorno del mese successivo a quello di pertinenza, il fornitore sarà tenuto a corrispondere a Consip S.p.A. una penale pari a 1.000 euro per ogni mese di ritardo, fatto salvo il risarcimento del maggior danno. Anche in caso di applicazione delle penali, resta fermo l'obbligo di adempiere all'invio delle informazioni richieste, entro l'ultimo giorno del mese successivo a quello di applicazione della sanzione, pena l'applicazione di ulteriori penali del medesimo importo, fino all'avvenuto adempimento.

   Resta inteso che, l'errata compilazione dei report previsti dal richiamato commi 2 del seguente articolo 31 deve intendersi, ai fini dell'applicazione delle penali di cui sopra, come mancato invio.

   In caso di invio delle informazioni richieste al comma 4 del successivo articolo 31, oltre l'ultimo giorno del mese successivo a quello di pertinenza, il fornitore sarà tenuto a corrispondere a Consip S.p.A. una penale pari a 1.000 euro, fatto salvo il risarcimento del maggior danno. Resta inteso che, l'errata compilazione dei report previsti dal richiamato comma 4 del seguente articolo 31 deve intendersi, ai fini dell'applicazione delle penali di cui sopra, come mancato invio.
4. In caso di mancato invio della documentazione richiesta al adempimento all'obbligazione di cui al precedente art. 7, comma 18 (ovvero la Relazione di genere ex art 47 comma 3) il Fornitore sarà tenuto a corrispondere, ai sensi dell'art. 47, comma 6, del DL 77/2021, convertito con modificazioni in L. 108/2021, una penale pari a 25.000 €. Il mancato adempimento dell'invio della documentazione richiesta entro 30 giorni dall'applicazione della penale comporta l'applicazione di una ulteriore penale del medesimo importo fino ad avvenuto adempimento e comunque, a parziale

deroga di quanto previsto dal successivo comma 12, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro.

5. In caso di mancato invio della documentazione richiesta di cui al precedente art. 7, comma 19, il Fornitore sarà tenuto a corrispondere, ai sensi dell'art. 47, comma 6 del DL 77/2021, convertito con modificazioni in L. 108/2021, una penale pari a 25.000 €. Il mancato adempimento dell'invio della documentazione richiesta entro 30 giorni dall'applicazione della penale comporta l'applicazione di una ulteriore penale del medesimo importo fino ad avvenuto adempimento e comunque, a parziale deroga di quanto previsto dal successivo comma 12, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro.
6. Si applicano le penali previste al paragrafo 6 del Capitolato Tecnico parte Speciale (che deve intendersi in questo articolo integralmente trascritto) nonché tutte quelle riportate nel presente articolo. E' sempre fatto salvo il risarcimento del maggior danno. In caso di penali da ritardo, deve considerarsi ritardo anche il caso in cui il Fornitore esegua il servizio in modo anche solo parzialmente difforme rispetto alle disposizioni di cui al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto Esecutivo, nonché alla propria Offerta Tecnica. In tal caso le Amministrazioni applicheranno al Fornitore la suddetta penale sino alla data in cui il servizio inizierà ad essere eseguito in modo effettivamente conforme al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto Esecutivo, all'Offerta Tecnica, fatto salvo il risarcimento del maggior danno.
7. Nel caso in cui, come previsto nell'atto di nomina a responsabile del Trattamento allegato all'Accordo Quadro, all'esito delle verifiche, ispezioni, audit e assessment compiuti dall'Amministrazioni o da terzi autorizzati le misure di sicurezza adottate dal Responsabile primario del trattamento dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione delle "Norme in materia di protezione dei dati personali", l'Amministrazione applicherà al Fornitore-Responsabile primario/Sub responsabile del trattamento una penale pari all'1 per mille del valore del contratto per ogni giorno necessario per il Fornitore per l'adozione di misure di sicurezza idonee ad assicurare l'applicazione della normativa sulla protezione dei dati
8. Nel caso in cui, come previsto nell'atto di nomina allegato all'Accordo Quadro, all'esito delle verifiche, ispezioni e audit e assessment compiute dall'Amministrazione o da terzi autorizzati, le misure di sicurezza adottate dal Sub-Responsabile/terzo autorizzato al trattamento dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione delle "Norme in materia di protezione dei dati personali", l'Amministrazione applicherà al Fornitore - Responsabile primario del trattamento una penale pari all'1 per mille del corrispettivo del singolo contratto esecutivo per ogni giorno necessario per l'adozione di misure di sicurezza idonee ad assicurare l'applicazione delle "Norme in materia di protezione dei dati personali", salvo il maggior danno.
9. Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali sopra stabilite, dovranno essere contestati al Fornitore per iscritto da Consip S.p.A. e/o dalla singola Amministrazione, per quanto di rispettiva competenza; in quest'ultimo caso, gli eventuali inadempimenti dovranno essere comunicati dalle Amministrazioni per conoscenza a Consip S.p.A.
10. In caso di contestazione dell'inadempimento da parte di Consip S.p.A. e/o della singola Amministrazione, per quanto di rispettiva competenza, il Fornitore dovrà comunicare, in ogni caso, per iscritto, le proprie deduzioni, supportate da una chiara ed esauriente documentazione, nel termine massimo di n. 5 (cinque) giorni lavorativi dalla ricezione della contestazione stessa. Qualora le predette deduzioni non pervengano a Consip S.p.A. e/o all'Amministrazione nel termine indicato, ovvero, pur essendo pervenute tempestivamente, non siano idonee, a giudizio di Consip S.p.A. e/o dall'Amministrazione, a giustificare l'inadempienza, potranno essere applicate al Fornitore le penali stabilite nell'Accordo Quadro a decorrere dall'inizio dell'inadempimento.
11. Consip S.p.A. potrà per l'applicazione delle penali dell'Accordo Quadro avvalersi della garanzia disciplinata nell'Accordo Quadro, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario. Le singole Amministrazioni potranno compensare i crediti derivanti dall'applicazione delle penali di cui all'Accordo Quadro con

quanto dovuto al Fornitore a qualsiasi titolo, quindi anche con i corrispettivi maturati, ovvero avvalersi della garanzia disciplinata nell'Accordo Quadro, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario.

12. Consip S.p.A., per le parti di sua competenza, potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) del valore dell'Accordo Quadro, fermo il risarcimento degli eventuali maggiori danni, nonché la risoluzione contrattuale per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima.
13. Le Amministrazioni, per le parti di loro competenza, potranno applicare al Fornitore penali sino a concorrenza della misura massima:
    - pari al 20% (venti per cento), per i contratti finanziati in tutto o in parte con i fondi del PNRR e del PNC,
    - ovvero
    - pari al 10% (dieci per cento), per i contratti non finanziati con i fondi del PNRR o del PNC;

    del Contratto di Fornitura, fermo il risarcimento degli eventuali maggiori danni, nonché la risoluzione contrattuale per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima.
14. La richiesta e/o il pagamento delle penali non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

ARTICOLO 13 - GARANZIE

1. A garanzia delle obbligazioni contrattuali assunte nei confronti della Consip S.p.A. dal Fornitore con la stipula della Accordo Quadro, il Fornitore medesimo ha prestato le seguenti garanzie definitive per ciascun lotto:
    - Lotto 1: garanzia definitiva rilasciata in data30/03/2022 dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia avente n. 2348037 di importo pari ad Euro 240.000,00 = (duecentoquarantamila/00);
    - Lotto 2: garanzia definitiva rilasciata in data 30/03/2022 dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia avente n. 2348044 di importo pari ad Euro 76.800,00 = (settantaseimilaottocento/00);
    - Lotto 3: garanzia definitiva rilasciata in data 30/03/2022 dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia avente n. 2348045 di importo pari ad Euro 91.200,00 = (novantunomiladuecento/00).
2. La garanzia rilasciata copre tutte le obbligazioni e gli impegni assunti dal Fornitore con l'Accordo Quadro ed i suoi allegati, ivi compreso il Patto di integrità, nei confronti della Consip, anche quelli a fronte dei quali è prevista l'applicazione di penali e, pertanto, resta espressamente inteso che la Consip S.p.A ha diritto di rivalersi direttamente sulla garanzia per l'applicazione delle penali. La garanzia copre altresì le obbligazioni assunte dal Fornitore nella fase preliminare alla stipula dei contratti attuativi di cui al paragrafo 2 del Capitolato Tecnico Parte Speciale e, in particolare, verrà escussa nel caso di mancata accettazione dell'ordinativo di fornitura per fatto del Fornitore.
3. La garanzia prestata in favore della Consip S.p.A. opera a far data dalla sottoscrizione dell'Accordo Quadro e per tutta la durata dell'Accordo Quadro e dei contratti di fornitura, e, comunque, sino alla completa ed esatta esecuzione delle obbligazioni nascenti dall'Accordo Quadro e dai predetti contratti di fornitura.
4. A garanzia delle obbligazioni contrattuali assunte dal Fornitore con la stipula dell'Accordo Quadro e dei relativi contratti di fornitura il Fornitore medesimo ha prestato le seguenti garanzie definitive per ciascun lotto:
    - Lotto 1: garanzia definitiva rilasciata in data 30/03/2022 dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia avente n. 2348038 di importo pari ad Euro 42.560.000,00 = (quarantaduemilionicinquecentosessantamila/00) in favore della delle Amministrazioni Contraenti, quest'ultimo è esteso fino al valore di Euro 63.840.000 = (sessantatremilioniottocentoquarantamila/00), come da appendice n.2 della suddetta garanzia, in considerazione dell'incremento del valore stimato del Lotto 1 di cui al comma 2 dell'art. 3;

- Lotto 2: garanzia definitiva rilasciata in data 30/03/2022 dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia avente n. 2348042 di importo pari ad Euro 13.872.640,00 = (tredicimilioniottocentosettantaduemilaseicentoquaranta/00) in favore della delle Amministrazioni Contraenti, quest'ultimo è esteso fino al valore di Euro 20.808.960,00 = (ventimilioniottocentoottomilanovecentosessanta/00), come da appendice n.3 della suddetta garanzia, in considerazione dell'incremento del valore stimato del Lotto 2 di cui al comma 2 dell'art. 3
- Lotto 3: garanzia definitiva rilasciata in data 30/03/2022 dalla Compagnie française d'assurance pour le commerce extérieur S.A.- Rappresentanza Generale per l'Italia avente n. 2348046 di importo pari ad Euro 16.102.880,00 = (sedicimilionicentoduemilaottocentoottanta/00) in favore della delle Amministrazioni Contraenti, quest'ultimo è esteso fino al valore di Euro 24.154.320,00 = (ventiquattromilionicentocinquantaquattromilatrecentoventi/00), come da appendice n.3 della suddetta garanzia, in considerazione dell'incremento del valore stimato del Lotto 3 di cui al comma 2 dell'art. 3.

5. La garanzia copre tutti gli obblighi specifici assunti dal Fornitore con i contratti di fornitura nei confronti delle Amministrazioni, anche quelli a fronte dei quali è prevista l'applicazione di penali da parte delle stesse e, pertanto, resta espressamente inteso che le Amministrazioni hanno diritto di rivalersi direttamente sulla garanzia per l'applicazione delle penali. La garanzia copre altresì il risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, 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 il rispetto degli impegni assunti con il Patto di integrità, l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione dei contratti attuativi disposta in danno dell'esecutore, il pagamento di quanto dovuto dall'esecutore 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.
6. La garanzia prestata in favore delle Amministrazioni decorre dalla data di stipula dell'Accordo Quadro e cessa alla data di emissione del certificato di verifica di conformità o dell'attestazione di regolare esecuzione delle prestazioni, emessi alla conclusione dell'esecuzione dell'ultimo contratto di fornitura e comunque decorsi 12 mesi dalla data di ultimazione delle prestazioni contrattuali risultante dal relativo certificato dell'ultimo contratto di fornitura, allorché si estingue automaticamente ad ogni effetto (art. 103, commi 1 e 5, del Codice). Resta fermo quanto previsto nello schema tipo del DM 31/2018 come derogato dal Capitolato d'Oneri.
7. Le garanzie di cui ai precedenti commi prevedono espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, comma 2, del codice civile, nonché l'operatività della garanzia medesima – anche per il recupero delle penali contrattuali - entro quindici giorni, a semplice richiesta scritta del rispettivo beneficiario.
8. E' onere della singola Amministrazione comunicare alla Consip S.p.a. l'importo delle somme percepite dal Garante.
9. Le garanzie di cui ai commi precedenti sono progressivamente svincolate in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80 per cento dell'iniziale importo garantito secondo quanto stabilito all'art. 103, comma 5, del D.Lgs. n. 50/2016. Lo svincolo avviene subordinatamente alla preventiva consegna al Garante ed alla Consip S.p.A. da parte del Fornitore, in relazione ai contratti stipulati nell'arco temporale di riferimento, di: *(i)* documenti delle Amministrazioni, in originale o in copia autentica, attestanti la corretta esecuzione delle prestazioni, ai sensi dell'articolo 102 del D.Lgs. n. 50/2016; e/o *(ii)* documentazione comprovante l'avvenuta ricezione del rimborso della ritenuta di legge dello 0,5%, di cui al precedente articolo 10, comma 14. Il Garante dovrà comunicare alla Consip il valore dello svincolo. La Consip S.p.a. si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.
10. In alternativa a quanto sopra, il Fornitore potrà consegnare alla Consip S.p.a. un prospetto contenente l'elenco delle Amministrazioni Contraenti con l'ammontare delle fatture emesse nel relativo arco temporale e regolarmente saldate, unitamente al dettaglio specifico della posizione di ciascuna singola Amministrazione Contraente (numero

fattura, numero contratto, mensilità di riferimento, data emissione, data pagamento, importo corrisposto), accompagnato da dichiarazione resa dal legale rappresentante del Fornitore o procuratore speciale munito dei necessari poteri, ai sensi del D.P.R. n. 445/2000, attestante la veridicità di tutte le informazioni contenute nel prospetto stesso e l'assenza di ogni contestazione sulle prestazioni eseguite e in esso consuntivate. La Consip S.p.a. procederà ad autorizzare lo svincolo comunicandolo al Garante e al Fornitore.

11. Ai fini dello svincolo dell'ammontare residuo delle garanzie (20%), il Fornitore dovrà produrre, in relazione ai rimanenti contratti attuativi: *(i)* i certificati di verifica di conformità o le attestazioni di regolare esecuzione delle prestazioni emessi alla conclusione dell'esecuzione dei contratti attuativi; e/o *(ii)* documentazione comprovante il rimborso della ritenuta di legge dello 0,5%, di cui al precedente articolo 10, comma 14.
12. In alternativa a quanto sopra, il Fornitore potrà produrre il prospetto e la dichiarazione, rilasciati nei modi e nelle forme di cui al precedente comma 10, accompagnati da copia dell'ultima fattura di ogni contratto attuativo vigente nel relativo arco temporale di riferimento, e dalla documentazione attestante l'avvenuto pagamento da parte delle Amministrazioni dell'ultima fattura di ogni contratto attuativo. In questo caso la garanzia sarà svincolata decorso il termine di 12 mesi dal pagamento dell'ultima fattura dell'ultimo contratto attuativo. Consip S.p.A. si riserva la possibilità di un controllo a campione sulla veridicità della dichiarazione di cui sopra.
13. Qualora l'ammontare delle garanzie prestate dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, il Fornitore dovrà provvedere al reintegro entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta effettuata dalla Consip S.p.A., pena la risoluzione dell'Accordo Quadro e/o dei singoli contratti di fornitura.
14. In caso di inadempimento alle obbligazioni previste nel presente articolo la Consip S.p.A. ha facoltà di dichiarare risolta l'Accordo Quadro e, del pari, le singole Amministrazioni Contraenti hanno facoltà di dichiarare risolto il contratto di fornitura, fermo restando il risarcimento del danno.
15. In ogni caso il garante sarà liberato dalle garanzie prestate di cui ai commi precedenti solo previo consenso espresso in forma scritta dalla Consip S.p.A..

ARTICOLO 13 BIS – GARANZIE SULLE APPARECCHIATURE E SUL SOFTWARE

1. Il Fornitore garantisce la piena proprietà delle apparecchiature, dei componenti materiali utilizzati per l'installazione, nonché la titolarità delle licenze d'uso dei programmi software forniti, e dichiara che tali suoi diritti sono liberi da vincoli o diritti a favore di terzi.
2. Il Fornitore garantisce espressamente che le apparecchiature, i materiali ed i supporti sui quali sono caricati i programmi sono esenti da vizi dovuti a progettazione o ad errata esecuzione o a deficienze dei materiali impiegati, che ne diminuiscano il valore e/o che li rendano inidonei, anche solo parzialmente, all'uso cui sono destinati.
3. Il Fornitore garantisce che i programmi sono esenti da vizi o difetti di funzionamento da essa conosciuti e/o conoscibili e che gli stessi sono conformi alle specifiche definite nel Capitolato Tecnico, "nell'Offerta Tecnica" e nei relativi manuali d'uso. Il Fornitore garantisce, altresì, che i programmi sono esenti da virus, essendo state adottate a tal fine tutte le opportune cautele.
4. Le suddette garanzie sono prestate in proprio dal Fornitore anche per il fatto del terzo, intendendo la Committente restare estranea ai rapporti tra l'Impresa e le ditte fornitrici dei vari materiali componenti la fornitura.
5. Le Parti convengono che i termini di cui agli articoli 1495, 1511 e 1667 c.c. decorreranno dalla "Data di accettazione della Fornitura" di cui all'articolo intitolato "Verifica di conformità".
6. Il termine per la denuncia dei vizi non riconoscibili viene convenuto in 6 (sei) mesi dalla scoperta.
7. In caso di inadempienza da parte del Fornitore alle obbligazioni di cui ai precedenti commi, la Committente, fermo restando il risarcimento di tutti i danni, avrà facoltà di dichiarare risolto di diritto il presente contratto ai sensi dell'articolo intitolato "Risoluzione", in seguito riportato, nonché dell'art. 1456 c.c..

ARTICOLO 14 - RISOLUZIONE

1. Consip e/o le Amministrazioni, per quanto di rispettiva competenza, senza bisogno di assegnare alcun termine per l'adempimento, potranno risolvere l'Accordo Quadro e il singolo Contratto di Fornitura ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art.1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
   a) il Fornitore si è trovato, al momento dell'aggiudicazione dell'Accordo Quadro in una delle situazioni di cui all'articolo 80, comma 1, del d. lgs. n. 50/2016 e s.m.i. e avrebbe dovuto pertanto essere escluso dalla gara;
   b) il Fornitore ha commesso, nella procedura di aggiudicazione del presente Accordo Quadro e/o dei successivi Appalti Specifici, un illecito antitrust accertato con provvedimento esecutivo dell'AGCM, ai sensi dell'articolo 80, comma 5, lett. c) del d. lgs. n. 50/2016 e s.m.i. e secondo le linee guida A.N.AC.;
   c) l'Accordo Quadro non avrebbe dovuto essere aggiudicato al Fornitore in considerazione di una grave violazione degli obblighi derivanti dai Trattati, come riconosciuto dalla Corte di giustizia dell'Unione europea in un procedimento ai sensi dell'articolo 258 TFUE;
   d) qualora fosse accertata la non sussistenza ovvero il venir meno di uno dei requisiti minimi richiesti per la partecipazione alla gara, nonché per la stipula dell'Accordo Quadro e per lo svolgimento delle attività ivi previste;
   e) qualora il Fornitore ponga in essere comportamenti tesi a eludere la modalità di affidamento degli Appalti Specifici;
   f) mancata copertura dei rischi durante tutta la vigenza dell'Accordo Quadro e dei contratti di fornitura;
   g) qualora il Fornitore, in esecuzione di un Appalto Specifico, offra o fornisca prodotti, ovvero la prestazione di servizi, che non abbiano i requisiti di conformità e/o le caratteristiche tecniche minime stabilite dalle normative vigenti, nonché nel Capitolato Tecnico, ovvero quelle migliorative eventualmente offerte in sede di aggiudicazione dell'Accordo Quadro;
   h) mancata reintegrazione della garanzia di cui all'art. 13 eventualmente escussa entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta da parte della Consip S.p.A.;
   i) azioni giudiziarie per violazioni di diritti di brevetto, di autore ed in genere di privativa altrui, intentate contro le Amministrazioni e/o la Consip S.p.A., ai sensi dell'articolo 21;
   j) nei casi di cui agli articoli 9 (Verifiche di conformità); 10 (Corrispettivi e Fatturazione), 17 (Trasparenza), 18 (Riservatezza), 20 (Divieto di cessione del contratto), 26 (Codice Etico - Modello di organizzazione e gestione ex D.Lgs. n. 231/2001 - Piano Triennale per la prevenzione della corruzione e della trasparenza) e 27 (Tracciabilità dei flussi finanziari), 28 (Subappalto), 29 (Danni, responsabilità civile);
   k) applicazione di penali oltre la misura massima stabilita all'articolo 12, commi 10 e 11*;*
   l) nell'ipotesi di non veridicità delle dichiarazioni rese dal Fornitore ai sensi del D.p.r. n. 445/00, fatto salvo quanto previsto dall'art. 71, del medesimo D.P.R. 445/2000;
   m) nell'ipotesi di irrogazione di sanzioni interdittive o misure cautelari di cui al D. Lgs. n. 231/01, che impediscano all'Impresa di contrattare con le Pubbliche Amministrazioni;
   n) in caso di avvalimento, ove a fronte delle segnalazioni delle Amministrazioni contraenti ed in ragione di quanto dichiarato dal Fornitore, risultasse la violazione dell'art. 89, comma 9 , del d. lgs. n. 50/2016 e s.m.i.;
   o) nei casi di cui all'articolo 3 e 5 del Patto di integrità.

   Nelle fattispecie di cui al presente comma non si applicano i termini previsti dall'articolo 21-nonies della legge 7 agosto 1990 n. 241.
2. Consip e/o le Amministrazioni Contraenti, per quanto di rispettiva competenza, devono risolvere l'Accordo Quadro e il singolo Contratto di fornitura senza bisogno di assegnare alcun termine per l'adempimento, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art.1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
   a) qualora nei confronti del Fornitore sia intervenuto un provvedimento definitivo che dispone l'applicazione di

una o più misure di prevenzione di cui al codice delle leggi antimafia e delle relative misure di prevenzione, fatto salvo quanto previsto dall'art. 95 del D. Lgs. n. 159/2011, o nel caso in cui gli accertamenti antimafia presso la Prefettura competente risultino positivi oppure sia intervenuta sentenza di condanna passata in giudicato per i reati di cui all'articolo 80 del D. Lgs. n. 50/2016 e s.m.i.;

b) qualora fosse accertato il venir meno dei requisiti richiesti dalla legge;

3. Inoltre, Consip S.p.a. si impegna ad avvalersi della clausola risolutiva espressa di cui all'art. 1456 c.c. ogni qualvolta nei confronti del Fornitore o dei componenti la propria compagine sociale, o dei dirigenti dell'impresa con funzioni specifiche relative all'affidamento alla stipula e all'esecuzione dell'Accordo Quadro sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317 cp 318 cp 319 cp 319 bis cp 319 ter cp 319 quater 320 cp 322 cp 322 bis cp 346 bis cp 353 cp 353 bis cp. La risoluzione di cui al periodo precedente è subordinata alla preventiva comunicazione all'ANAC, cui spetta la valutazione in merito all'eventuale prosecuzione del rapporto contrattuale, al ricorrere delle condizioni di cui all'art. 32 del dl. 90/2014 convertito in legge 114 del 2014.
4. Il Fornitore accetta le cause di risoluzione previste nell'atto di nomina a Responsabile/sub Responsabile del Trattamento allegato "L" al presente Accordo quadro, che devono intendersi integralmente trascritte.
5. Consip e/o le Amministrazioni Contraenti, quando accertino un grave inadempimento del Fornitore ad una delle obbligazioni assunte con l'Accordo Quadro e/o con i Contratti di fornitura tale da compromettere la buona riuscita delle prestazioni, formuleranno la contestazione degli addebiti al Fornitore e contestualmente assegneranno un termine, non inferiore a quindici giorni, entro i quali il Fornitore dovrà presentare le proprie controdeduzioni. Acquisite e valutate negativamente le controdeduzioni ovvero scaduto il termine senza che il Fornitore abbia risposto, Consip e/o le Amministrazioni Contraenti hanno la facoltà, per quanto di rispettiva competenza, di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei Contratti di Fornitura, di incamerare la garanzia ove essa non sia stata ancora restituita ovvero di applicare una penale equivalente, nonché di procedere all'esecuzione in danno dell'Impresa; resta salvo il diritto al risarcimento dell'eventuale maggior danno.
6. Qualora il Fornitore ritardi per negligenza l'esecuzione delle prestazioni rispetto alle previsioni dell'Accordo Quadro e dei Contratti di Fornitura, Consip e/o le Amministrazioni contraenti assegnano un termine che, salvo i casi d'urgenza, non può essere inferiore a 10 (dieci) giorni, entro i quali il Fornitore deve eseguire le prestazioni. Scaduto il termine assegnato, e redatto processo verbale in contraddittorio con il Fornitore, qualora l'inadempimento permanga, Consip e/o le Amministrazioni contraenti potranno risolvere l'Accordo Quadro e/o i Contratti di Fornitura, fermo restando il pagamento delle penali.
7. In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con la stipula dell'Accordo Quadro e dei Contratti di Fornitura che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato a mezzo di raccomandata A/R tramite pec dalla Consip e/o dall'Amministrazione Contraente, per quanto di propria competenza, per porre fine all'inadempimento, la Consip e/o l'Amministrazione Contraente hanno la facoltà di considerare, per quanto di rispettiva competenza, risolti di diritto l'Accordo Quadro e/o i Contratti di Fornitura e di ritenere definitivamente la garanzia ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.
8. In caso di risoluzione anche di uno solo dei Contratti di Fornitura, Consip S.p.A. si riserva di risolvere il presente Accordo Quadro. La risoluzione dell'Accordo Quadro legittima la risoluzione dei singoli Contratti di Fornitura a partire dalla data in cui si verifica la risoluzione dell'Accordo Quadro. La risoluzione dell'Accordo Quadro è, pertanto, causa ostativa all'affidamento di nuovi Appalti Specifici e può essere causa di risoluzione dei singoli Contratti di Fornitura, salvo che non sia diversamente stabilito nei medesimi e salvo, in ogni caso, il risarcimento del danno.
9. In tutti i casi di risoluzione dell'Accordo Quadro e dei Contratti di Fornitura, Consip S.p.A. e/o l'Amministrazione Contraente avranno diritto di escutere la garanzia prestata per l'intero importo della stessa o per la parte percentualmente proporzionale all'importo del/i Contratto/i di fornitura risolto/i. Ove l'escussione non sia possibile sarà applicata una penale di equivalente importo, che sarà comunicata al Fornitore con lettera raccomandata A/R o

via pec. In ogni caso, resta fermo il diritto della medesima Amministrazione Contraente e/o di Consip S.p.A. al risarcimento dell'ulteriore maggior danno.

10. La Consip S.p.A., fermo restando quanto previsto nel presente articolo e nei casi di cui all'art. 110 del D.Lgs. n. 50/2016, potrà interpellare progressivamente gli operatori economici che hanno partecipato all'originaria procedura di gara e risultanti dalla relativa graduatoria al fine di stipulare un nuovo Accordo Quadro per l'affidamento del completamento delle prestazioni contrattuali alle medesime condizioni già proposte dall'aggiudicatario in sede di offerta.

ARTICOLO 15 - RECESSO

1. La Consip S.p.A. e/o le Amministrazioni, per quanto di proprio interesse, hanno diritto di recedere unilateralmente dal presente Accordo Quadro e/o da ciascun singolo Contratto di Fornitura, in tutto o in parte, in qualsiasi momento, senza preavviso, nei casi di:
   a) giusta causa,
   b) reiterati inadempimenti del Fornitore, anche se non gravi.
   Si conviene che per giusta causa si intende, a titolo meramente esemplificativo e non esaustivo:
   - qualora sia stato depositato contro il Fornitore un ricorso ai sensi della legge fallimentare o di altra legge applicabile in materia di procedure concorsuali, che proponga lo scioglimento, la liquidazione, la composizione amichevole, la ristrutturazione dell'indebitamento o il concordato con i creditori, ovvero nel caso in cui venga designato un liquidatore, curatore, custode o soggetto avente simili funzioni, il quale entri in possesso dei beni o venga incaricato della gestione degli affari del Fornitore, resta salvo quanto previsto dall'art. 110, comma 3, del D.Lgs. n. 50/2016;
   - in qualsiasi altra fattispecie che faccia venire meno il rapporto di fiducia sottostante il presente Accordo Quadro o i contratti di fornitura.
2. In caso di mutamenti di carattere organizzativo interessanti l'Amministrazione che abbiano incidenza sull'esecuzione della fornitura o della prestazione dei servizi, la stessa Amministrazione potrà recedere in tutto o in parte unilateralmente da Contratto di Fornitura, con un preavviso almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore con lettera raccomandata a/r o tramite pec.
3. Fermo restando quanto previsto dagli artt. 88, comma 4-ter, e 92, comma 4, del D.Lgs. 159/2011, Consip S.p.A. e/o l'Amministrazione, ai sensi dell'art. 109, comma 1 del Codice, potrà recedere dall'Accordo Quadro e/o da ciascun singolo contratto di fornitura, in qualunque momento, con preavviso non inferiore a 20 (venti) giorni solari, previo il pagamento da parte delle Amministrazioni delle prestazioni oggetto di Appalto Specifico eseguite a regola d'arte, nonché del valore dei materiali utili esistenti in magazzino (ove esistenti), oltre al decimo dell'importo delle opere, dei servizi o delle forniture non eseguite, così come determinato ai sensi dell'art. 109 comma 2 del Codice, rinunciando espressamente il Fornitore, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso e/o indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ..
4. Qualora la Consip receda dall'Accordo Quadro, non potranno essere emessi nuovi ordini di fornitura da parte delle Amministrazioni e le singole Amministrazioni potranno a loro volta recedere dai singoli Contratti di fornitura, con un preavviso di almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore con lettera raccomandata A/R o tramite pec.

ARTICOLO 16 - OBBLIGHI DERIVANTI DAL RAPPORTO DI LAVORO

1. Il Fornitore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, in materia previdenziale e infortunistica, assumendo a proprio carico tutti i relativi oneri. In particolare, il Fornitore si impegna a rispettare nell'esecuzione delle obbligazioni derivanti dall'Accordo Quadro e dai singoli Appalti Specifici le disposizioni di cui al D.Lgs. 9 aprile 2008 n. 81.
2. Il Fornitore si obbliga altresì ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, le

condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi ed integrativi di lavoro applicabili alla data di stipula dell'Accordo Quadro alla categoria e nelle località di svolgimento delle attività, nonché le condizioni risultanti da successive modifiche ed integrazioni, anche tenuto conto di quanto previsto all'art. 95, comma 10 e all'art. 97 del D. Lgs. n. 50/2016.

3. Il Fornitore si obbliga, altresì, fatto in ogni caso salvo il trattamento di miglior favore per il dipendente, a continuare ad applicare i suindicati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione.
4. Gli obblighi relativi ai contratti collettivi nazionali di lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui questi non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità dell'Accordo Quadro e dei singoli Contratti di Fornitura.
5. Restano fermi gli oneri e le responsabilità in capo al Fornitore di cui all'art. 105, comma 9, del D. Lgs. n. 50/2016 in caso di subappalto.

ARTICOLO 17 - TRASPARENZA

1. Il Fornitore espressamente ed irrevocabilmente:
   a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione dell'Accordo Quadro;
   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 dell'Accordo Quadro 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 dell'Accordo Quadro rispetto agli obblighi con esso assunti, né a compiere azioni comunque volte agli stessi fini;
   d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.lgs. 50/2016 al fine di evitare situazioni di conflitto d'interesse.
2. Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse per tutta la durata dell'Accordo Quadro gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma, lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'articolo 1456 cod. civ., per fatto e colpa del Fornitore, con facoltà di Consip S.p.A. di incamerare la garanzia prestata.
3. Il Fornitore si impegna al rispetto di tutte le previsioni di cui al Patto di integrità.

ARTICOLO 18 - RISERVATEZZA

1. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi compresi quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione dell'Accordo Quadro e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
2. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione dell'Accordo Quadro e degli Appalti Specifici; tale obbligo non concerne i dati che siano o divengano di pubblico dominio.
3. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza anzidetti.
4. In caso di inosservanza degli obblighi di riservatezza, le Amministrazioni e/o Consip S.p.A. hanno la facoltà di dichiarare risolto di diritto, rispettivamente, il singolo Contratto di Fornitura ovvero l'Accordo Quadro, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare alle Amministrazioni e/o a Consip S.p.A..
5. Il Fornitore potrà citare i contenuti essenziali dell'Accordo Quadro e degli Appalti Specifici affidati in proprio favore nei casi in cui ciò fosse condizione necessaria per la partecipazione del Fornitore medesimo a gare e appalti.

6. Resta fermo quanto previsto nel successivo articolo 25.

ARTICOLO 19 - RESPONSABILE UNICO DELLE ATTIVITÁ CONTRATTUALI

1. Il Responsabile Unico delle Attività Contrattuali nominato dal Fornitore è l'Ing. Massimiliano Materazzi.
2. Il Responsabile Unico delle Attività Contrattuali è il referente responsabile nei confronti di Consip S.p.A. e/o delle Amministrazioni per l'esecuzione del presente Accordo Quadro e dei singoli Contratti di fornitura, e quindi, avrà la capacità di rappresentare ad ogni effetto il Fornitore, salvo quant'altro previsto nel Capitolato Tecnico Parte Generale.
3. Qualora il Fornitore dovesse trovarsi nella necessità di sostituire il Responsabile del Servizio, dovrà darne immediata comunicazione scritta a Consip S.p.A.

ARTICOLO 20 - DIVIETO DI CESSIONE DEL CONTRATTO

1. E' fatto assoluto divieto a ciascun Fornitore di cedere, a qualsiasi titolo, l'Accordo Quadro ed i Contratti di Fornitura, a pena di nullità della cessione medesima, fatto salvo quanto previsto dall'art. 106, comma 1, lett. d), del d. lgs. n. 50/2016 e s.m.i..
2. In caso di inadempimento da parte del Fornitore degli obblighi di cui al presente articolo, Consip S.p.A. e le Amministrazioni, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolto di diritto l'Accordo Quadro e i Contratti di fornitura.

ARTICOLO 21 - BREVETTI INDUSTRIALI, DIRITTI D'AUTORE E "LOGO"

1. Il Fornitore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui; il Fornitore, pertanto, si obbliga a manlevare l'Amministrazione e la Consip S.p.A., per quanto di propria competenza, dalle pretese che terzi dovessero avanzare in relazione a diritti di privativa vantati da terzi.
2. Qualora venga promossa nei confronti delle Amministrazioni e/o di Consip S.p.A. azione giudiziaria da parte di terzi che vantino diritti sulle prestazioni contrattuali, il Fornitore assume a proprio carico tutti gli oneri conseguenti, incluse le spese eventualmente sostenute per la difesa in giudizio. In questa ipotesi, l'Amministrazione e/o Consip S.p.A. sono tenute ad informare prontamente per iscritto il Fornitore in ordine alle suddette iniziative giudiziarie.
3. Nell'ipotesi di azione giudiziaria per le violazioni di cui al comma precedente tentata nei confronti di Consip S.p.A. e delle Amministrazioni e/o, le prime, fermo restando il diritto al risarcimento del danno nel caso in cui la pretesa azionata sia fondata, hanno facoltà di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei singoli Contratti di Fornitura, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per i servizi e/o le forniture erogati.
4. E' vietato qualsiasi uso da parte del Fornitore dei marchi e/o dei loghi e/o delle denominazioni "Ministero dell'Economia e Finanze" e/o "Consip S.p.A." o del testo o del materiale grafico contenuto nel Portale di "www.acquistinretepa.it" per esprimere in qualsiasi modo o rappresentare l'adesione, la sponsorizzazione, l'affiliazione o l'associazione dell'utente con il Ministero dell'Economia e Finanze e/o con la Consip S.p.A.

ARTICOLO 22 - FUORI PRODUZIONE

1. Nel corso di durata dell'Accordo Quadro, il Fornitore potrà non fornire l'apparecchiatura o il dispositivo opzionale come offerti nella procedura di gara, o nelle successive evoluzioni tecnologiche, e oggetto dell'Accordo Quadro medesimo, solo ed esclusivamente in caso di sopravvenuto "fuori produzione" accertato mediante la seguente documentazione da consegnare a Consip S.p.A.:
   a) dichiarazione in originale di "fuori produzione" resa, ai sensi e per gli effetti degli artt. 47 e 76 del d.P.R. n. 445/2000, dal Fornitore (ove coincidente con il produttore) ovvero dal produttore (ove diverso dal Fornitore);

b) dichiarazione resa, ai sensi e per gli effetti degli artt. 47 e 76 del d.P.R. n. 445/2000, dal Fornitore, con indicazione del prodotto offerto in sostituzione con specifica attestazione della sussistenza nel prodotto offerto in sostituzione delle funzionalità e caratteristiche (minime e migliorative) almeno pari a quelle del prodotto dichiarato "fuori produzione".

c) schede tecniche e/o dichiarazioni attestanti il possesso delle funzionalità e caratteristiche minime e migliorative dell'apparecchiatura o del dispositivo opzionale offerto in sostituzione, provenienti dal Fornitore (ove coincidente con il produttore) ovvero dal produttore (ove diverso dal Fornitore), in copia conforme all'originale, ai sensi del D.P.R. n.445/2000. A tal fine, potrà essere richiesta dalla Consip ogni più idonea documentazione tecnica del prodotto offerto in sostituzione.

Consip S.p.A. si riserva, altresì, di verificare l'effettiva sopravvenuta messa "fuori produzione" del bene.

Si precisa che, esclusivamente nel caso di "fuori produzione" è ammesso il mutamento della marca delle apparecchiature e/o componenti opzionali offerti, a condizione che nella dichiarazione di "fuori produzione" rilasciata dal produttore, il produttore medesimo dichiari di non disporre di nessuna apparecchiatura e/o componente opzionale avente funzionalità (minime e migliorative) almeno pari a quelle da sostituire.

2. Ricevuta la documentazione di cui al precedente comma, Consip S.p.A. procederà all'analisi della stessa in ordine alla sussistenza, sul prodotto offerto in sostituzione, di funzionalità e caratteristiche (minime e migliorative) almeno pari a quelle del prodotto dichiarato "fuori produzione". In particolare, al fine di procedere alla suddetta verifica, Consip S.p.A. potrà:
   a) procedere all'analisi delle schede tecniche e/o dichiarazioni di cui al precedente comma 1 lett. c). Ai fini della verifica potrà essere richiesta da Consip S.p.A. ogni ulteriore documentazione ritenuta idonea per comprovare le funzionalità e caratteristiche minime e migliorative del prodotto offerto in sostituzione. Successivamente all'analisi delle schede tecniche, in caso Consip S.p.A. lo ritenga necessario ai fini della verifica, potrà essere inoltre richiesta la messa a disposizione del prodotto come previsto nel successivo punto b);
   b) indipendentemente dalla presentazione delle schede tecniche e/o dichiarazioni di cui al comma 1 lett. c), chiedere al Fornitore di mettere a disposizione, presso la sede della medesima Consip S.p.A., il campione del prodotto offerto in sostituzione comprensivo degli eventuali dispositivi opzionali entro 10 (dieci) giorni lavorativi dalla relativa richiesta, per essere sottoposto a verifica di corrispondenza rispetto alle caratteristiche e funzionalità del prodotto dichiarato "fuori produzione". La verifica verrà effettuata alla data indicata in apposita comunicazione con la quale verrà altresì invitata a presenziare persona incaricata dal Fornitore; in ogni caso, la verifica avverrà a cura ed onere del Fornitore e sarà responsabilità del Fornitore medesimo predisporre le apparecchiature e tutte le procedure necessarie allo scopo.
3. Solo all'esito dell'analisi di cui al precedente comma 2 Consip S.p.A. ha la facoltà di:
   - in caso di esito negativo, recedere in tutto o in parte dalla presente Accordo quadro, ovvero
   - in caso di esito positivo, esonerare il Fornitore dalla fornitura dell'apparecchiatura o del dispositivo opzionale dichiarato "fuori produzione", sostituendolo con quello offerto in sostituzione.
4. Il Fornitore si impegna a recepire le indicazioni fornite dall'Organismo di Coordinamento e Controllo relative alla necessità di eliminare prodotti offerti ma ancora commercializzati, in accordo con quanto previsto nel paragrafo 5 del Capitolato Tecnico parte generale, ai sensi dell'art. 106 co. 1 lett. c).

ARTICOLO 23 - EVOLUZIONE TECNOLOGICA

1. Il Fornitore si impegna ad informare la Consip S.p.A. sulla evoluzione tecnologica dell'apparecchiatura o del materiale di consumo oggetto dell'Accordo Quadro e delle conseguenti possibili modifiche migliorative da apportare alle forniture medesime; le apparecchiature o il materiale di consumo "evoluti" dovranno possedere, ferma restando l'identità generale in particolare per quanto concerne la marca, funzionalità e caratteristiche (minime e migliorative) almeno pari a quelli da sostituire.
2. Il Fornitore potrà formulare la proposta in merito alle sopra citate modifiche migliorative producendo:
   a) una dichiarazione in originale resa, ai sensi e per gli effetti degli artt. 47 e 76 del d.P.R. n. 445/2000, dallo stesso

Fornitore (ove coincidente con il produttore) ovvero dal produttore (ove diverso dal Fornitore) in ordine: i) alla intervenuta evoluzione tecnologica; ii) alla sussistenza, sul prodotto "evoluto", di funzionalità (minime e migliorative) almeno pari a quelle del prodotto sostituito; iii) alla descrizione delle caratteristiche "evolutive".

b) schede tecniche e/o dichiarazioni, attestanti il possesso delle funzionalità e caratteristiche minime e migliorative del prodotto "evoluto", provenienti dal Fornitore (ove coincidente con il produttore) ovvero dal produttore (ove diverso dal Fornitore), in copia conforme all'originale, ai sensi del D.P.R. n.445/2000.

3. Ricevuta la documentazione di cui al precedente comma, Consip S.p.A. procederà con le modalità e la tempistica di cui ai commi 2 e 3 del precedente articolo 22 alla verifica in ordine alla sussistenza sul prodotto "evoluto" di funzionalità (minime e migliorative) almeno pari a quelle del prodotto sostituito.
4. Solo in caso di esito positivo dell'analisi di cui al precedente comma 3, Consip S.p.A. autorizzerà il Fornitore a sostituire il prodotto "evoluto" a quello precedentemente fornito.
5. Il Fornitore si impegna a recepire le indicazioni fornite dall'Organismo di Coordinamento e Controllo relative all'evoluzione delle tecnologie offerte, in accordo con quanto previsto nel paragrafo 5 del Capitolato Tecnico parte generale, ai sensi dell'art. 106 co. 1 lett. b) e c).

ARTICOLO 24 - FORO COMPETENTE

1. Per tutte le questioni relative ai rapporti tra il Fornitore e Consip S.p.A. inerenti il presente Accordo Quadro, sarà competente in via esclusiva il Foro di Roma.

ARTICOLO 25 - TRATTAMENTO DEI DATI PERSONALI

1. Il Fornitore dichiara di aver ricevuto prima della sottoscrizione del presente Accordo Quadro le informazioni di cui all'articolo 13 del "Regolamento UE", circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione dell'Accordo Quadro stesso e dei Contatti derivanti dagli Appalti specifici e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa. Tale informativa è contenuta nell'ambito del Capitolato d'Oneri al paragrafo25 che deve intendersi in quest'ambito integralmente trascritto.
2. Con la sottoscrizione dell'Accordo Quadro, il rappresentante legale del Fornitore acconsente espressamente al trattamento dei dati personali come sopra definito e si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione dell'Accordo Quadro e dei contratti Contatti derivanti dagli Appalti specifici, per le finalità descritte nell'informativa resa nel Capitolato d'oneri come sopra richiamata.
3. Le Amministrazioni Contraenti e qualsivoglia altro soggetto pubblico o privato aderendo all'Accordo Quadro, acconsentono espressamente al trattamento ed all'invio a Consip S.p.A. da parte del Fornitore e/o delle singole Amministrazioni, dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione dell'Accordo Quadro e Contatti derivanti dagli Appalti specifici.
4. In adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 1, comma 16, lett. b, e comma 32 L. 190/2012; art. 35 D. Lgs. n. 33/2013; nonché art. 29 D. Lgs. n. 50/2016), il concorrente/contraente prende atto ed acconsente a che i dati e la documentazione che la legge impone di pubblicare, siano pubblicati e diffusi, ricorrendone le condizioni, tramite il sito internet **www.consip.it**, sezione "Società Trasparente"; inoltre, il nominativo del concorrente aggiudicatario della gara ed il prezzo di aggiudicazione dell'appalto, saranno diffusi tramite i siti internet **www.acquistinretepa.it** e **www.mef.gov.it**.
5. Con la sottoscrizione dell'Accordo Quadro ed il perfezionamento dei Contatti derivanti dagli Appalti specifici, il Fornitore acconsente espressamente al trattamento dei dati personali e si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente (Regolamento UE 2016/679 D. Lgs. n. 196/2003 e s.m.i. e D. Lgs. n. 101/2018), ivi inclusi gli ulteriori provvedimenti, comunicati ufficiali,

autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la Protezione dei Dati Personali. In particolare, il Fornitore si impegna ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti.

6. Ove applicabile, in ragione dell'oggetto dell'Accordo Quadro, qualora il Fornitore sia chiamato ad eseguire attività di trattamento di dati personali, il medesimo potrà essere nominato "Responsabile/sub-Responsabile del trattamento" dei dati personali ai sensi dell'art. 28 del Regolamento UE sulla base dell'atto di nomina allegato al presente Accordo Quadro. In tal caso, il Fornitore si impegna ad accettare la designazione a Responsabile/sub-Responsabile del trattamento, da parte dell'Amministrazione, relativamente ai dati personali di cui la stessa è Titolare e che potranno essere trattati dal Fornitore nell'ambito dell'erogazione dei servizi contrattualmente previsti.
7. Nel caso in cui il Fornitore violi gli obblighi previsti dalla normativa in materia di protezione dei dati personali, o nel caso di nomina a Responsabile/sub-Responsabile, agisca in modo difforme o contrario alle legittime istruzioni impartitegli dal Titolare, oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento, risponderà integralmente del danno cagionato agli "interessati". In tal caso, l'Amministrazione potrà applicare le penali eventualmente previste nell'Accordo Quadro, e potrà risolvere il Contatto derivante dall'Appalto specifico ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno. L'Amministrazione dovrà segnalare la fattispecie alla Consip S.p.a. che potrà risolvere l'Accordo Quadro.
8. Il Fornitore si impegna ad osservare le vigenti disposizioni in materia di sicurezza e riservatezza dei dati personali e a farle osservare ai propri dipendenti e collaboratori, quali persone autorizzate al trattamento dei Dati personali.
9. In conformità a quanto previsto dal Regolamento UE/2016/679, il Fornitore dovrà garantire che i dati personali oggetto di trattamento, verranno gestiti nell'ambito dell'UE e che non sarà effettuato alcun trasferimento degli stessi verso un paese terzo o un'organizzazione internazionale al di fuori dell'UE o dello Spazio Economico Europeo, fatta eccezione dei paesi/territori/organizzazioni coperti da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 Regolamento UE/2016/679 o da altre garanzie adeguate di cui agli artt. 46 e ss. del Regolamento stesso (es. utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR), nonché l'adeguamento alle ulteriori eventuali misure supplementari di cui alle raccomandazioni dell'European Data Protection Board. Al di fuori delle predette eccezioni, il Fornitore dovrà garantire che le eventuali piattaforme/server su cui transitino i suddetti dati abbiano sede nell'UE e che qualunque replica dei dati non sia trasmessa al di fuori della UE o dello Spazio Economico Europeo.

   Nel caso di servizi di assistenza/manutenzione da remoto il cui espletamento implichi comunque il trasferimento al di fuori dell'UE di tracciati di dati connessi al servizio stesso, gli eventuali dati personali contenuti nel tracciato devono essere opportunamente anonimizzati a cura del Fornitore.
10. Nel caso in cui all'esito di eventuali verifiche, ispezioni e audit effettuati dalla Amministrazione Contraente in qualità di Titolare del trattamento, dovessero risultare trasferimenti di dati extra-UE in assenza delle adeguate garanzie e delle eventuali misure supplementari di cui sopra, l'Amministrazione diffiderà il Responsabile del trattamento all'immediata interruzione del trasferimento di dati non autorizzato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione ne darà comunicazione al Garante della Privacy e potrà, in ragione della gravità della condotta del Fornitore e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto attuativo ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

ARTICOLO 26 - CODICE ETICO – MODELLO DI ORGANIZZAZIONE E GESTIONE EX D.LGS. N. 231/2001 - PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA

1. Il Fornitore dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A.
2. Il Fornitore, per effetto della sottoscrizione del presente Accordo Quadro, promettendo anche il fatto dei propri dipendenti e/o collaboratori, si impegna: (i) ad operare nel rispetto dei principi e delle previsioni di cui al D. Lgs. n. 231/2001; (ii) ad uniformarsi alle previsioni contenute nel Modello di organizzazione, gestione e controllo adottato dalla Consip S.p.A. ai sensi della D.Lgs. n. 231/2001 per le parti di pertinenza del Fornitore medesimo nonché del Codice etico e del Piano triennale per la prevenzione della corruzione e della trasparenza per le parti di pertinenza del Fornitore medesimo.
3. In caso di inadempimento da parte del Fornitore agli obblighi di cui ai precedenti commi, la Consip S.p.A., fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolta di diritto il presente Accordo Quadro.

ARTICOLO 27 - TRACCIABILITÀ DEI FLUSSI FINANZIARI

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 rispetto ai Contratti di Fornitura.
2. Ferme restando le ulteriori ipotesi di risoluzione previste nel presente atto, si conviene che, in ogni caso, le Amministrazioni, 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, risolveranno di diritto, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., i Contratti di Fornitura nell'ipotesi in cui le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri documenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora A.N.AC.) n. 8 del 18 novembre 2010.
3. In ogni caso, si conviene che Consip S.p.A., senza bisogno di assegnare previamente alcun termine per l'adempimento, si riserva di risolvere di diritto il presente Accordo Quadro, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., nell'ipotesi di reiterati inadempimenti agli obblighi di cui al precedente comma.
4. Il Fornitore è tenuto 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.
5. Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, ad inserire nei contratti eventualmente sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, una 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.
6. Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui all'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i è tenuto a darne immediata comunicazione a Consip S.p.A., all'Amministrazione e alla Prefettura – Ufficio Territoriale del Governo della Provincia ove ha sede la stazione appaltante.
7. 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.

8. Consip S.p.A. verificherà che nei contratti di subappalto sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale il subappaltatore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge. Con riferimento ai contratti di subfornitura, il Fornitore si obbliga a trasmettere alla Consip e all'Amministrazione, oltre alle informazioni di cui all'art. 105, comma 2, quinto periodo, del D. Lgs. n. 50/2016, anche apposita dichiarazione resa ai sensi del d.P.R. n. 445/2000, attestante che nel relativo sub-contratto, ove predisposto, sia stata inserita, a pena di nullità assoluta, un'apposita clausola con la quale il subcontraente assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge, restando inteso che la Consip e/o le Amministrazioni, si riserva di procedere a verifiche a campione sulla presenza di quanto attestato, richiedendo all'uopo la produzione degli eventuali sub-contratti stipulati, e, di adottare, all'esito dell'espletata verifica ogni più opportuna determinazione, ai sensi di legge e di contratto.
9. Ai sensi della Determinazione dell'Autorità per la Vigilanza sui contratti pubblici (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.

ARTICOLO 28 - SUBAPPALTO

1. Il Fornitore, conformemente a quanto dichiarato in sede di Offerta si è riservato di affidare in subappalto l'esecuzione delle seguenti prestazioni: 51611100-9; 72212730-5; 72254100-1; 79511000-9; 72250000-2; 72267000-4; 72267100-0; 72253000-3; 72000000-5; 80500000-9 per una quota pari al 50 (%) dell'importo contrattuale.
2. Il subappalto è regolato da quanto previsto dall'art. 105 del Codice nonché dai successivi commi.
3. L'Impresa si impegna a depositare presso la Consip, 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 dal Bando 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) la 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; iv) se del caso, certificazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione prescritti dal D. Lgs. n. 50/2016 per l'esecuzione delle attività affidate.
   Resta inteso che l'Impresa si impegna ad inserire, nel contratto di subappalto e negli altri subcontratti, una clausola che preveda il rispetto degli obblighi di cui al Patto di Integrità da parte dei subappaltatori/subcontraenti, e la risoluzione, ai sensi dell'art. 1456 c.c., del contratto di subappalto e/o degli altri subcontratti, nel caso di violazione di tali obblighi da parte di questi ultimi; l'Impresa dovrà dare tempestiva comunicazione a Consip dell'intervenuta risoluzione.
4. In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, la 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 sub-appalto, che ricomincerà a decorrere dal completamento della documentazione.
5. 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 la Consip revocherà l'autorizzazione.
6. 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.

7. Per le prestazioni affidate in subappalto:
   A) 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;
   B) devono essere corrisposti i costi della sicurezza e della manodopera, relativi alle prestazioni affidate in subappalto, alle imprese subappaltatrici senza alcun ribasso.
   L'Amministrazione contraente, sentito il direttore dell'esecuzione, provvede alla verifica dell'effettiva applicazione degli obblighi di cui al presente comma. Il Fornitore è responsabile in solido con il subappaltatore degli adempimenti, da parte di questo ultimo, degli obblighi di sicurezza previsti dalla normativa vigente.
8. Il Fornitore e il subappaltatore sono responsabili in solido, nei confronti della Consip S.p.A. e/o delle Amministrazioni Contraenti, in relazione alle prestazioni oggetto del contratto di subappalto.
9. Il Fornitore è responsabile in solido con il subappaltatore nei confronti della Consip e delle Amministrazioni Contraenti dei danni che dovessero derivare, alla Consip e alle Amministrazioni contraenti 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 S.p.A. e/o le Amministrazioni Contraenti 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 UE n. 2016/679.
10. 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 alla Consip e 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, l'amministrazione contraente acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.
11. 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.
12. 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. 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 ai subappaltatori, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.
14. Nelle ipotesi di inadempimenti da parte dell'impresa subappaltatrice, ferma restando la possibilità di revoca dell'autorizzazione al subappalto, è onere del Fornitore affidatario svolgere in proprio le attività ovvero porre in essere, nei confronti del subappaltatore ogni rimedio contrattuale, ivi inclusa la risoluzione.
15. L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.

16. In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti comma, la Consip e l'Amministrazione contraente possono risolvere l'Accordo Quadro e il Contratto di Fornitura, salvo il diritto al risarcimento del danno.
17. Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016, con riferimento a tutti i sub–contratti che non sono subappalti stipulati dal Fornitore per l'esecuzione del contratto, è fatto obbligo al Fornitore stesso di comunicare, a Consip S.p.A. e all'Amministrazione Contraente interessata, il nome del sub-contraente, l'importo del contratto, l'oggetto delle attività, delle forniture e dei servizi affidati. Eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto dovranno essere altresì comunicate a Consip S.p.A. e all'Amministrazione Contraente interessata. Nel caso in cui il Fornitore ricorra a tali sub-contratti Consip si riserva di chiedere al medesimo Fornitore di produrre documentazione atta a dimostrare la sussistenza dei presupposti indicati dall'art. 105 comma 2.
18. 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.
    La Consip S.p.A., 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.

ARTICOLO 29 - DANNI E RESPONSABILITÀ CIVILE

1. Il Fornitore assume in proprio ogni responsabilità per qualsiasi danno causato a persone o beni, tanto del Fornitore stesso quanto delle Amministrazioni Contraenti e/o della Consip S.p.A. e/o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze relative all'esecuzione delle prestazioni che discendono dall'Accordo Quadro e ad esso riferibili, anche se eseguite da parte di terzi.

ARTICOLO 30 - ONERI FISCALI E SPESE CONTRATTUALI

1. Sono a carico del Fornitore tutti gli oneri tributari e le spese contrattuali ivi comprese quelle previste dalla normativa vigente relative all'imposta di bollo.
2. Laddove la registrazione sia operata dalla Consip S.p.A. e/o dalle Amministrazioni Contraenti, le stesse comunicano al Fornitore l'importo anticipato e il conto corrente sul quale il Fornitore si impegna a versare, entro dieci giorni, l'importo anticipato. L'attestazione del versamento deve essere prodotta a Consip S.p.A. e/o alle Amministrazioni Contraenti entro venti giorni dalla data in cui è effettuato. In caso di ritardo l'importo è aumentato degli interessi legali a decorrere dalla data di scadenza del suddetto termine fino alla data di effettivo versamento.
3. Il Fornitore dichiara che le prestazioni di cui trattasi sono effettuate nell'esercizio di impresa e che trattasi di operazioni soggette all'Imposta sul Valore Aggiunto, che il Fornitore – salvo il caso di applicazione dell'art. 17-ter del d.P.R. n. 633 del 1972 introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96 ("split payment") - è tenuto a versare, con diritto di rivalsa, ai sensi del D.P.R. n. 633/72; conseguentemente, all'Accordo Quadro dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'articolo 40 del D.P.R. n. 131/86, con ogni relativo onere a carico del Fornitore.

ARTICOLO 31 - COMMISSIONE A CARICO DEL FORNITORE AI SENSI DEL DECRETO MINISTERO DELL'ECONOMIA E DELLE FINANZE DEL 23 NOVEMBRE 2012

1. Ai sensi del Decreto del Ministero dell'Economia e delle Finanze del 23 novembre 2012 attuativo di quanto disposto dall'articolo 1, comma 453 della legge 27 dicembre 2006 n. 296, il Fornitore è tenuto a versare alla Consip S.p.A. una commissione pari allo 0,5% da calcolarsi sul valore, al netto dell'IVA, del fatturato realizzato, con riferimento agli acquisti effettuati tramite il presente Accordo Quadro dalle pubbliche amministrazioni e dagli altri soggetti legittimati ai sensi della normativa vigente.
    La previsione della commissione nonché l'entità della stessa sono state definite sulla base delle indicazioni del Dipartimento dell'amministrazione generale, del personale e dei servizi

2. Ai fini del calcolo dell'entità della commissione, il Fornitore a decorrere dalla data di stipula del primo contratto attuativo è tenuto a trasmettere alla Consip S.p.A., per via telematica ai sensi dell'art. 65 del D.Lgs. 7 marzo 2005, n. 82, e dell'art. 38 del D. L. 31 maggio 2010, n. 78, convertito dalla legge 30 luglio 2010, n. 122, entro 30 giorni solari dal termine di ciascuno dei due semestri dell'anno solare e ferma l'applicazione delle penali di cui al precedente articolo 12 in caso di ritardo, una dichiarazione sostitutiva, rilasciata ai sensi dell'art. 47 del D.P.R. 28 dicembre 2000, n. 445 e sottoscritta digitalmente da parte del legale rappresentante del Fornitore, con l'indicazione del fatturato, al netto dell'IVA, conseguito nel semestre di riferimento, al netto degli eventuali interessi di mora applicati alle Amministrazioni Contraenti. Il Fornitore è altresì tenuto a trasmettere, unitamente alla predetta dichiarazione e quale parte integrante della medesima, reports specifici, nel formato elettronico richiesto dalla Consip S.p.A. o in via telematica secondo tracciato e modalità fissati da Consip S.p.A. (di cui all'Allegato G"FLUSSO DATI PER LE COMMISSIONI A CARICO DEL FORNITORE alla presente Convenzione), contenenti per ciascuna fattura emessa nel semestre di riferimento gli elementi di rendicontazione di cui al suddetto Allegato G"FLUSSO DATI PER LE COMMISSIONI A CARICO DEL FORNITORE.
3. Tale dichiarazione, in presenza di importi sopravvenuti ma imputabili al semestre precedente, potrà essere rettificata o integrata nei seguenti termini:
    - entro 12 mesi dal termine di trasmissione della dichiarazione semestrale oggetto di integrazione, in caso di riduzione degli importi inizialmente dichiarati;
    - entro 12 mesi dal termine degli effetti dell'ultimo contratto attuativo stipulato dal fornitore, in caso di aumento degli importi inizialmente dichiarati.

    In entrambi i casi, al fine di poter trasmettere la dichiarazione rettificativa o integrativa, il Fornitore dovrà inviare una richiesta motivata a Consip che ne valuterà l'ammissibilità o meno.

    I controlli sulla veridicità delle dichiarazioni trasmesse e delle eventuali rettifiche e integrazioni alle stesse, saranno effettuati da Consip trascorsi 12 mesi dal termine per la trasmissione della dichiarazione semestrale di cui al precedente comma 2. All'esito dei suddetti controlli, in caso di difformità, verrà avviato un procedimento di contestazione. In caso di accertamento di dichiarazione mendace si procederà alla segnalazione alla Procura della Repubblica.
4. Il Fornitore si impegna, altresì, a trasmettere alla Consip S.p.A., , entro 15 giorni solari dal termine del mese in cui sono state emesse le fatture, e ferma l'applicazione delle penali di cui al precedente articolo 12, una dichiarazione sottoscritta digitalmente da parte del legale rappresentante del Fornitore medesimo, attestante l'importo delle fatture emesse nel mese di riferimento al netto degli eventuali interessi di mora applicati alle Amministrazioni. Si evidenzia che esclusivamente per la dichiarazione riferita alle fatture emesse nel mese di luglio il suddetto termine è fissato in 35 giorni solari dal termine del mese.

    Il Fornitore è, altresì, tenuto a trasmettere, unitamente alla predetta dichiarazione e quale parte integrante della medesima, *report* specifici, nel formato elettronico richiesto dalla Consip S.p.A. o in via telematica secondo tracciato e modalità fissati da Consip S.p.A. (di cui all'Allegato al presente Accordo Quadro "G" FLUSSO DATI PER LE COMMISSIONI A CARICO DEL FORNITORE), contenenti per ciascuna fattura emessa nel mese di riferimento gli elementi di rendicontazione di cui al suddetto Allegato "G" FLUSSO DATI PER LE COMMISSIONI A CARICO DEL FORNITORE.

    Si evidenzia che le dichiarazioni attestanti gli importi di fatturato, unitamente ai report specifici relativi sia al semestre che al mese di riferimento dovranno pervenire anche in caso di fatturato pari a zero o assenza di fatturato.
5. Il Fornitore si obbliga altresì a comunicare, all'indirizzo P.E.C. **dprpaconsip@postacert.consip.it** la data dell'ultima fattura emessa all' Amministrazione a valere sull'AQ stipulato con Consip e sui contratti stipulati, entro il termine di 15 giorni dall'emissione della stessa. Restano fermi restando gli obblighi di invio, mensile e semestrali, relativi alle dichiarazioni di fatturato connesse all'obbligo del pagamento della fee di cui ai precedenti commi.

6. L’obbligo di invio dei flussi mensili termina con l’invio dei valori relativi all’ultima fattura comunicata ai sensi di quanto previsto al precedente comma. L’obbligo di invio dei flussi semestrali termina con l’invio delle fatture relative al semestre in cui è stata trasmessa la comunicazione di cui al precedente comma.
7. La Consip S.p.A., decorsi novanta giorni solari dal ricevimento della dichiarazione sostitutiva di cui al precedente comma 2, procederà all'emissione della fattura relativa alla commissione. Eventuali importi risultanti dalle dichiarazioni rettificative o integrative di un semestre, saranno compensati nella fattura del semestre successivo. In caso di mancato rispetto del termine per la presentazione della dichiarazione medesima, la Consip S.p.A., unitamente all’applicazione delle penali di cui oltre, emetterà la fattura in un termine inferiore rispetto ai predetti 90 giorni solari.
8. Il Fornitore è tenuto a versare la commissione entro 60 giorni solari dalla data di ricevimento della fattura emessa dalla Consip S.p.A. mediante accredito, con bonifico bancario, sul conto corrente dedicato avente IBAN n. IT 27 X 03069 05036 100000004389 Bic BCITITMM intestato alla Consip S.p.A..
9. In caso di ritardo del pagamento da parte del Fornitore della commissione relativa alle fatture emesse dalle Amministrazioni, decorreranno gli interessi moratori il cui tasso viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell’Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto all’art. 5 del D.Lgs. 9 ottobre 2002, n. 231 s.m.i..
10. Il mancato o inesatto pagamento della commissione secondo le modalità ed i termini di cui ai precedenti commi del presente articolo comporterà, comunque, l'avvio delle procedure esecutive previste dal codice di procedura civile.
11. La Consip S.p.A. procederà ad informare rispettivamente il Dipartimento dell'amministrazione generale, del personale e dei servizi dell'eventuale avvio di procedure esecutive e dell'ammontare delle somme oggetto di riscossione.
12. Gli interessi di mora e le somme oggetto di riscossione coattiva dovranno essere versati sul conto corrente dedicato di cui al precedente comma 5.
13. La Consip S.p.A., ai sensi della normativa vigente, effettuerà - anche avvalendosi di organismi di ispezione accreditati – controlli a campione al fine di verificare la veridicità delle dichiarazioni sostitutive di cui al precedente comma 2 coinvolgendo, se del caso, le Amministrazioni Contraenti.

    La Consip S.p.A. si riserva di richiedere al Fornitore, a comprova di quanto dichiarato, di produrre, entro il termine di 30 giorni solari, un’autodichiarazione resa ai sensi del D.P.R. 445/2000 sul fatturato realizzato nell’ambito del semestre di riferimento, rilasciata dal soggetto o organo preposto al controllo contabile della società ove presente (sia esso il Collegio sindacale, il revisore contabile o la società di revisione). Nel caso in cui tale autodichiarazione non confermasse quanto presente nella dichiarazione sostitutiva di cui al precedente comma 2, si procederà alla valutazione ai sensi dell'art. 80, comma 5, lett. c), del D. Lgs. n. 50/2016. La Consip S.p.A. avrà comunque la facoltà di eseguire ulteriori verifiche e di chiedere al Fornitore ogni necessaria ulteriore documentazione relativa al suddetto fatturato.

    Ferma restando l'applicazione dell'art. 76 del D.P.R. n. 445/2000:

    - in caso di inadempimento dell’obbligo di pagamento della commissione di cui al precedente comma 5 del presente articolo, che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato a mezzo di raccomandata A/R. dalla Consip S.p.A., per porre fine all’inadempimento, la Consip S.p.A. ha la facoltà di considerare risolto di diritto l’Accordo Quadro e di ritenere definitivamente la garanzia, ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno;

    - la mancata trasmissione della dichiarazione di cui al precedente comma 2 o la riscontrata falsità della dichiarazione di cui al precedente comma 2 potrà comportare la risoluzione dell’Accordo Quadro e la conseguente valutazione ai sensi dell'art. 80, comma 5, lett. c), del D. Lgs. n. 50/2016 informando tempestivamente il Dipartimento dell'amministrazione generale, del personale e dei servizi sulla risultanza dei controlli a campione effettuati.

ARTICOLO 32 - CLAUSOLA FINALE

1. Il presente Accordo Quadro ed i suoi Allegati costituiscono manifestazione integrale della volontà negoziale delle parti che hanno altresì preso piena conoscenza di tutte le relative clausole, avendone negoziato il contenuto, che dichiarano quindi di approvare specificamente singolarmente nonché nel loro insieme e, comunque, qualunque modifica al presente atto ed ai suoi Allegati non potrà aver luogo e non potrà essere provata che mediante atto scritto; inoltre, l'eventuale invalidità o inefficacia di una delle clausole dell'Accordo Quadro e/o dei singoli Contratti Esecutivi non comporta l'invalidità o inefficacia dei medesimi atti nel loro complesso.
2. Qualsiasi omissione o ritardo nella richiesta di adempimento dell'Accordo Quadro o dei singoli Contratti Esecutivi (o di parte di essi) da parte di Consip S.p.A. e/o delle Amministrazioni non costituisce in nessun caso rinuncia ai diritti loro spettanti che le medesime si riservano comunque di far valere nei limiti della prescrizione.
3. Con il presente Accordo Quadro si intendono regolati tutti i termini generali del rapporto tra le Parti; in conseguenza esso non verrà sostituito o superato dai Contratti di Fornitura attuativi o integrativi dell'Accordo Quadro che sopravvivrà ai detti Contratti di Fornitura continuando, con essi, a regolare la materia tra le Parti.

Roma, lì ___ ___

CONSIP S.p.A.	**IL FORNITORE**
F.to digitalmente	F.to digitalmente

Il sottoscritto, nella qualità di legale rappresentante del Fornitore, dichiara di avere particolareggiata e perfetta conoscenza di tutte le clausole contrattuali e dei documenti ed atti ivi richiamati; ai sensi e per gli effetti di cui agli artt. 1341 e 1342 cod. civ., il Fornitore dichiara di accettare tutte le condizioni e patti ivi contenuti e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni di seguito elencate:
Articolo 3 (Oggetto dell'Accordo Quadro), Articolo 4 (Durata dell'Accordo Quadro e dei contratti derivanti da Appalti Specifici), Articolo 5 (Prezzi e vincoli degli appalti specifici), Articolo 6 (Affidamento degli Appalti Specifici), Articolo 7 (Obbligazioni generali del Fornitore), Articolo 8 (Obbligazioni specifiche del Fornitore), Articolo 9 (Verifica di conformità), Articolo 10 (Corrispettivi e fatturazione), Articolo 11 (Costi della sicurezza); Articolo 12 (Penali); Articolo 13 (Garanzie); Articolo 13 bis (Garanzie sulle apparecchiature e sul software); Articolo 14 (Risoluzione); Articolo 15 (Recesso); Articolo 16 (Obblighi derivanti dal rapporto di lavoro), Articolo 17 (Trasparenza), Articolo 18 (Riservatezza), Articolo19 (Responsabile unico delle attività contrattuali), Articolo 20 (Divieto di cessione del contratto), Articolo 21 (Brevetti industriali, diritti d'autore e "LOGO"); Articolo 23 (Evoluzione tecnologica), Articolo 24 (Foro competente); Articolo 25 (Trattamento dei dati personali); Articolo 26 (Codice Etico – Modello di organizzazione e gestione ex D.Lgs. n. 231/2001 – Piano Triennale per la prevenzione della corruzione e della trasparenza), Articolo 27 (Tracciabilità dei flussi finanziari), Articolo 28 (Subappalto), Articolo 29 (Danni e responsabilità civile), Articolo 30 (Oneri fiscali e spese contrattuali), Articolo 31 (Commissione a carico del Fornitore ai sensi del Decreto del Ministero dell'Economia e delle Finanze del 23 novembre 2012), Art. 32 (Clausola finale).
Roma, lì ___ ___

IL FORNITORE
F.to digitalmente

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO D – PATTO DI INTEGRITA'

ACCORDO QUADRO AI SENSI DELL'ART. 54 COMMA 3 DEL D. LGS 50/2016 PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI – LOTTI 1, 2, 3 – ID 2367

SOMMARIO

PREMESSA

L'art. 1, comma 17 della L. 6 novembre 2012, n. 190 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione") dispone che "*le stazioni appaltanti possono prevedere negli avvisi, bandi di gara o lettere di invito che il mancato rispetto delle clausole contenute nei protocolli di legalità o nei patti di integrità costituisce causa di esclusione dalla gara*".

Il Piano Nazionale Anticorruzione, approvato con delibera n. 72/2013 dall'Autorità Nazionale Anticorruzione e successivamente aggiornato, prevede che le pubbliche amministrazioni e le stazioni appaltanti, in attuazione del citato art. 1, comma 17 della L. 190/2012, predispongono e utilizzano protocolli di legalità o patti di integrità per l'affidamento di appalti pubblici. A tal fine, i predetti soggetti inseriscono negli avvisi, nei bandi di gara e nelle lettere di invito la clausola di salvaguardia che il mancato rispetto del protocollo di legalità o del patto di integrità dà luogo all'esclusione dalla gara e alla risoluzione del contratto.

L'ANAC, inoltre, con il parere 11/2014, si è espressa favorevolmente riguardo alla previsione del bando che richiede l'accettazione dei protocolli di legalità e dei patti di integrità quale possibile causa di esclusione, "*in quanto tali mezzi sono posti a tutela di interessi di rango sovraordinato e gli obblighi in tal modo assunti discendono dall'applicazione di norme imperative di ordine pubblico, con particolare riguardo alla legislazione in materia di prevenzione e contrasto della criminalità organizzata nel settore degli appalti.".*

Infine il presente patto recepisce le raccomandazioni fornite dall'ANAC con le Linee Guida n. 15 del 12 luglio 2019.

In attuazione di quanto sopra,

SI CONVIENE QUANTO SEGUE

ART. 1 OGGETTO

1. Il presente patto di integrità (di seguito, il "**Patto di Integrità**") stabilisce la reciproca e formale obbligazione – tra

- la Consip S.p.A. a socio unico in qualità di stazione appaltante (di seguito, anche "**Consip**"),
- i soggetti legittimati, sulla base della normativa vigente, ad utilizzare l'Accordo Quadro (di seguito, anche le "**Amministrazioni**" o la "**singola Amministrazione contraente**")
- l'operatore economico partecipante alla procedura di gara (di seguito anche **il "Concorrente");**
- l'aggiudicatario della procedura di gara (di seguito, anche il "**Fornitore)** relativa alla stipula dell'Accordo Quadro ovvero dei Contratti di Fornitura a valere sull'Accordo Quadro per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi

a conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, impegnandosi ciascuno, per quanto di rispettiva competenza, a contrastare fenomeni di corruzione e illegalità e comunque a non compiere alcun atto volto a distorcere o influenzare indebitamente il corretto svolgimento di tutte le fasi dell'appalto, dalla partecipazione alla procedura alla esecuzione dell'Accordo Quadro e dei singoli Contratti di Fornitura successivamente affidati.

2. Il Fornitore, la Consip e le Amministrazioni si impegnano a rispettare nonché a far rispettare al rispettivo personale, ai collaboratori e, per quanto riguarda il Fornitore, anche ai subappaltatori/subcontraenti/imprese ausiliarie, il presente Patto di Integrità, il cui spirito e contenuto condividono pienamente, informando gli stessi prontamente e puntualmente e vigilando scrupolosamente sulla loro osservanza.

ART. 2 AMBITO DI APPLICAZIONE

1. Il presente Patto di Integrità regola i comportamenti di tutti i soggetti individuati nel precedente art. 1, ed è vincolante:
   - **per Consip S.p.A.** nella fase di espletamento della procedura di gara dell'Accordo Quadro;
   - **per le Amministrazioni:** nella fase di esecuzione dei Contratti di Fornitura dell'Accordo Quadro;
   - **per l'Operatore Economico,** nella fase di svolgimento della procedura di gara per la stipula di Accordi Quadro e dei relativi Contratti di Fornitura;
   - **per il Fornitore**, nella fase di esecuzione dell'Accordo Quadro e dei Contratti di Fornitura.
2. Il Patto di Integrità costituisce parte integrante e sostanziale dell'Accordo Quadro e dei singoli Contratti di Fornitura successivamente affidati.

ART. 3 OBBLIGHI DEL CONCORRENTE E DEL FORNITORE

1. Obblighi del Concorrente:
   a1) il Concorrente s'impegna a non corrispondere né promettere di corrispondere ad alcuno – direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati - somme di denaro o altra utilità ai fini dell'aggiudicazione della gara o di distorcere il corretto svolgimento della stessa;
   b1) il Concorrente dichiara di astenersi dal compiere qualsiasi tentativo di turbativa, irregolarità o, comunque, violazione delle regole della concorrenza ovvero a segnalare tempestivamente a Consip e alla Pubblica Autorità qualsiasi tentativo di turbativa, irregolarità e violazioni delle regole di concorrenza di cui dovesse venire a conoscenza durante tutte le fasi della procedura, fornendo elementi dimostrabili a sostegno delle suddette segnalazioni;
   c1) il Concorrente si impegna a segnalare eventuali situazioni di conflitti di interesse, di cui sia o venga a conoscenza al momento della partecipazione e durante l'espletamento dell'intera procedura rispetto ai soggetti (sia di Consip che delle Amministrazioni) di cui al par. 4 delle Linee Guida Anac sopra richiamate, che siano coinvolti in una qualsiasi fase della procedura (programmazione, progettazione, preparazione documenti di gara, selezione dei concorrenti, aggiudicazione) o che possano influenzarne in qualsiasi modo l'esito in ragione del ruolo ricoperto all'interno dell'ente;
   d1) il Concorrente si impegna a far rilasciare all'impresa ausiliaria, ai fini della partecipazione alla procedura di gara, una dichiarazione di presa visione e accettazione delle clausole del presente Patto di integrità;
   e1) il Concorrente si impegna ad inserire nei contratti di avvalimento una clausola che prevede l'impegno dell'ausiliaria a rispettare gli obblighi di cui al Patto di integrità, pena la risoluzione del contratto di avvalimento e il conseguente obbligo per il Concorrente medesimo di sostituire l'impresa ausiliaria nel caso di violazione degli impegni assunti nel medesimo Patto di integrità;
   f1) il Concorrente dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A.;
2. Obblighi del Fornitore:
   a2) Il Fornitore si impegna a segnalare eventuali situazioni di conflitti di interesse, anche riferite alla fase di partecipazione alla procedura di gara, di cui sia o venga a conoscenza durante l'intera fase esecutiva del Contratto rispetto ai soggetti (sia di Consip che della Amministrazioni) di cui al par. 4 delle Linee Guida Anac sopra richiamate, che siano coinvolti in una qualsiasi fase della procedura (sottoscrizione del contratto,

esecuzione, collaudo, pagamenti) o che possano influenzarne in qualsiasi modo l'esito in ragione del ruolo ricoperto all'interno dell'ente;

b2) il Fornitore dichiara di non avere influenzato il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente e di non aver corrisposto né promesso di corrispondere ad alcuno direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati - somme di denaro o altra utilità al fine di agevolare o distorcere la corretta e regolare esecuzione dell'Accordo Quadro e dei singoli Contratti di Fornitura successivamente affidati;

c2) Il Fornitore dichiara di non aver concluso con altri operatori economici alcun tipo di accordo volto ad alterare o limitare la concorrenza, ovvero a determinare un unico centro decisionale ai fini della partecipazione alla procedura di gara e della formulazione dell'offerta, risultata poi essere la migliore;

d2) Il Fornitore dichiara di astenersi dal compiere qualsiasi tentativo di turbativa, irregolarità o, comunque, violazione delle regole della concorrenza ovvero a segnalare tempestivamente a Consip, alla Pubblica Autorità e alla singola Amministrazione contraente, qualsiasi tentativo di turbativa, irregolarità e violazioni delle regole di concorrenza di cui dovesse venire a conoscenza durante la fase di esecuzione dell'Accordo Quadro e dei singoli Contratti di Fornitura successivamente affidati, fornendo elementi dimostrabili a sostegno delle suddette segnalazioni;

e2) il Fornitore si impegna a segnalare a Consip e alla singola Amministrazione contraente, nonché alla Pubblica Autorità competente e alla Prefettura, qualunque tentativo di concussione e qualsiasi illecita richiesta o pretesa da parte dei dipendenti di Consip e/-della singola Amministrazione contraente o di chiunque possa influenzare le decisioni relative all'esecuzione dell'Accordo Quadro e dei singoli Contratti di Fornitura successivamente affidati;

f2) il Fornitore si impegna ad inserire nei contratti di subappalto e negli altri subcontratti una clausola che preveda il rispetto degli obblighi di cui al presente Patto di Integrità da parte dei subappaltatori/subcontraenti, e la risoluzione, ai sensi dell'art. 1456 c.c., del contratto di subappalto, nel caso di violazione di tali obblighi da parte di questi ultimi, con conseguente comunicazione a Consip dell'avvenuta risoluzione del predetto contratto;

g2) il Fornitore di impegna a rendere noti, su richiesta dell'Amministrazione contraente, tutti i pagamenti eseguiti e riguardanti i Contratti di Fornitura;

h2) il Fornitore dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A. in relazione degli obblighi assunti dal Fornitore nei confronti di quest'ultima.

3. Il Concorrente e il Fornitore dichiarano, inoltre, di essersi già impegnati nei confronti di Consip al rispetto degli obblighi di cui al presente patto di integrità, mediante apposita dichiarazione resa in sede di partecipazione alla procedura di gara.
4. Il Concorrente e il Fornitore prendono atto ed accettano che la violazione, comunque accertata da Consip e/o dalle Amministrazioni di uno o più impegni assunti con il presente Patto di Integrità può comportare l'applicazione delle sanzioni di cui al successivo art. 5.

ART. 4 OBBLIGHI DI CONSIP E DELLE AMMINISTRAZIONI

1. Nel rispetto del presente Patto di Integrità, Consip e le Amministrazioni si impegnano, per quanto di rispettiva competenza, a rispettare i principi di lealtà, trasparenza e correttezza di cui alla L. n. 190/2012, nonché, nel caso

in cui venga riscontrata una violazione di detti principi o di prescrizioni analoghe, a valutare l'eventuale attivazione di procedimenti disciplinari nei confronti del rispettivo personale a vario titolo intervenuto nella procedura di affidamento e nell'esecuzione dell'Accordo Quadro e dei singoli Contratti di Fornitura successivamente affidati, secondo quanto previsto dai rispettivi piani di prevenzione della corruzione.

ART. 5 SANZIONI

1. Il Concorrente e il Fornitore prendono atto ed accettano che la violazione degli obblighi assunti con il presente Patto di Integrità, nonché la non veridicità delle dichiarazioni rese, comunque accertati da Consip e/o dalle Amministrazioni, può comportare l'applicazione di una o più delle seguenti sanzioni:
   a. se la violazione è accertata nella fase precedente all'aggiudicazione dell'Accordo Quadro, esclusione dalla procedura di affidamento anche ai sensi dell'art. 80, comma 5, lettera c-bis del D.lgs. 50/2016, ed eventuale escussione della garanzia provvisoria prestata in favore della Consip, nei casi e nei modi previsti dalla lex specialis di gara;
   b. se la violazione è accertata nella fase successiva all'aggiudicazione ma precedentemente alla stipula dell'Accordo quadro, revoca dell'aggiudicazione ed escussione della garanzia provvisoria;
   c. se la violazione è accertata nella fase di esecuzione:

      risoluzione *ex* art. 1456 c.c. dell'Accordo Quadro, nonché incameramento della garanzia definitiva e risarcimento dell'eventuale danno ulteriore, nel caso in cui la violazione degli impegni di cui al precedente art. 3 sia accertata in relazione agli obblighi contrattuali assunti dal Fornitore nei confronti di Consip in forza dell'Accordo Quadro. La risoluzione può essere altresì esercitata ai sensi dell'art. 1456 c.c. i) ogni qualvolta nei confronti del Fornitore, dei suoi dirigenti e/o dei componenti della compagine sociale, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319bis, 319ter, 319quater, 320, 322, 322bis, 346bis, 353, 353bis, 355 e 356 c.p. ii) nel caso in cui, violato l'obbligo di segnalazione di cui all'art. 3, lett. e2) che precede, sia stata disposta nei confronti dei "pubblici amministratori"[1] che hanno esercitato funzioni relative alla stipula ed esecuzione del contratto, misura cautelare o sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 del c.p.. Nei casi sopra indicati sub i) e ii), Consip eserciterà la potestà risolutoria previa intesa con l'Autorità Nazionale Anticorruzione che potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto Contrattuale alle condizioni di cui all'art. 32 del D.L. 90/2014 convertito nella legge n. 114/2014.
      Resta fermo che dell'intervenuta risoluzione dell'Accordo Quadro, Consip potrà tenere conto ai fini delle valutazioni di cui all'articolo 80, comma 5, lett. c-ter), del D.Lgs. 50/2016.
      La risoluzione dell'Accordo Quadro prevista nel presente Patto di Integrità può costituire condizione risolutiva del singolo Contratto di Fornitura;
      risoluzione *ex* art. 1456 c.c. del singolo Contratto di Fornitura, nel caso in cui la violazione degli impegni di cui al precedente art. 3 sia accertata in relazione agli obblighi contrattuali assunti dal Fornitore nei confronti della singola Amministrazione contraente nell'ambito dell'Appalto Specifico. La risoluzione potrà essere altresì esercitata ai sensi dell'art. 1456 c.c. i) ogni qualvolta nei confronti del Fornitore, dei suoi dirigenti e/o dei componenti della compagine sociale, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319bis, 319ter, 319quater, 320, 322, 322bis, 346bis, 353, 353bis, 355 e 356 c.p.; ii) nel caso in cui, violato l'obbligo di segnalazione di cui all'art. 3, lett. e2) che precede, sia stata disposta nei confronti dei "pubblici amministratori" che hanno esercitato funzioni

[1] Per "pubblici amministratori" si intendono i soggetti che hanno esercitato attività di pubblico interesse.

relative alla stipula ed esecuzione del contratto, misura cautelare o sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 del c.p.. Nei casi sopra indicati sub i) e ii) l'Amministrazione eserciterà la potestà risolutoria previa intesa con l'Autorità Nazionale Anticorruzione che potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto contrattuale alle condizioni di all'art. 32 del D.L. 90/2014 convertito nella legge n. 114/2014.

La risoluzione del singolo Contratto di Fornitura comporterà altresì l'escussione della garanzia definitiva per un importo proporzionalmente corrispondente al valore del Contratto di Fornitura risolto e il risarcimento dell'eventuale danno ulteriore.

In caso di intervenuta risoluzione del Contratto di Fornitura su iniziativa della singola Amministrazione contraente, quest'ultima è tenuta a darne tempestiva notizia a Consip, motivandone le ragioni; Consip, a sua volta, ha la facoltà di procedere, ai sensi dell'art. 1456 c.c., alla risoluzione di diritto dell'Accordo Quadro. Resta fermo che dell'intervenuta risoluzione del Contratto di Fornitura Consip potrà tenere conto ai fini delle valutazioni di cui all'articolo 80, comma 5, lett. c-ter), del D.Lgs. 50/2016;

In ogni caso Consip procederà alla segnalazione del fatto all'ANAC ed alle competenti Autorità giurisdizionali.

ART. 6 AUTORITÀ COMPETENTE IN CASO DI CONTROVERSIE

Ogni eventuale controversia relativa all'interpretazione e all'esecuzione del presente Patto di Integrità sarà risolta dall'Autorità Giudiziaria competente, secondo quanto nell'Accordo Quadro.

Roma, lì ___ ___

Il presente Patto di integrità viene allegato quale parte integrante dell'Accordo Quadro.

ACCORDO QUADRO PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI

ID 2367

PIANO DEI FABBISOGNI SERVIZI

Spett.le
TELECOM ITALIA S.p.A.

Lo scrivente __**ASL Città di Torino** _____C.F. / P.IVA **11632570013**
Codice IPA ASLTO
con sede legale in **Torino** Prov. **TO** CAP **10128** Nazione **ITALIA**
Indirizzo: **Via San Secondo 29**

chiede che venga realizzato quanto di seguito indicato (barrare i servizi richiesti con il presente piano dei fabbisogni):

X EDP/EPR (compilare il Quadro **A**)	☐ **NAC** (compilare il Quadro **B**)
☐ **NGFW** (compilare il Quadro **C**)	☐ **ANTI - APT** (Compilare il Quadro **D**)
☐ **Server Protection** (compilare il Quadro **E**)	☐ **Servizio di Hardening** (compilare il Quadro **F**)
☐ **Servizio di Formazione** (compilare il Quadro **G**)	**X Servizio di Supporto Specialistico** (compilare il Quadro **H**)
☐ **Servizio di di Manutenzione** (compilare il Quadro **I**)	

Invio delle fatture

Codice Univoco Ufficio: **Z87MJV**
CIG (quando disponibile)**: ND**
NSO (quando disponibile)**: ND**
CUP: F17H22001230001, F17H22001240001, F17H22001250001

Domicilio fattura:

Località **Torino** Prov. **TO** CAP **10128** Nazione **ITALIA**
Indirizzo **Via San Secondo 29**
☐ Cliente esente IVA in base a _____ (allegare dichiarazione di intento)

Responsabile dell'Amministrazione per i rapporti con TELECOM ITALIA[1]

Nome **Francesco** Cognome **PENSALFINI**
Tel **011 566 2548** _____Fax
E-mail**(obbligatoria)**tecnologie@aslcittaditorino.it **PEC** tecnologie@pec.aslcittaditorino.it

DATA _____ TIMBRO E FIRMA DEL CLIENTE

1 Tale nominativo sarà l'unico riconosciuto da TELECOM ITALIA per qualsiasi contatto inerente. a problematiche di tipo amministrativo/commerciale anche relative all'indicazione del/i luogo/ghi di esecuzione dei servizi. In caso di variazione il Cliente è tenuto a trasmettere a Telecom Italia, come indicato nella Richiesta di Adesione al Servizio, una comunicazione scritta.

Descrizione del Contesto di Riferimento in cui si riferisce la fornitura dell'Amministrazione
La fornitura è riferita al rinnovo delle licenze Cynet attualmente in uso per un totale di 6.000 end point.

Macro Requisiti ed Obiettivi che l'Amministrazione si propone con la fornitura

La necessità è quella di abbinare alla fornitura delle licenze sopra indicate le attività professionali in grado di erogare un servizio che prenda in carico le attività che riguardino in maniera specifica o generica le procedure di sicurezza informatica dell'ente.

Tali servizi devono includere la raccolta e l'analisi dei dati di tutti i sistemi on-site, quali PDL dell'utenza, server fisici o virtuali e apparati di vario genere. La raccolta dei dati verrà effettuata non solo per le postazioni precedentemente indicate ma anche da tutti quei servizi già attivi nel nostro perimetro che ci permettono di avere visibilità sugli eventi di sicurezza attivati al nostro interno. Questi sistemi sono nella fattispecie: controllori di dominio e loro servizi (AD, DNS, DHCP), sistema di rilevazione antivirus, sistema di analisi EDR delle postazioni (Cynet), sistemi di analisi del traffico (Medigate), sistemi di autenticazione per apparati Wifi (Aruba Clearpass), sistemi di inventario delle PDL (Lansweeper), sistemi di raccolta dati di navigazione (Firewall, FortyAnalyzer) nonché dal sistema di piattaforma virtuale (VSphere).

La necessità è quella di un'analisi esaustiva e predittiva, attraverso le verifiche dei log inviati dai sistemi oltre che quella di ottenere una valida risposta alle problematiche di sicurezza che vengono riscontrate.

La necessità dell'Ente è quella di esternalizzare il servizio relativo agli incidenti di sicurezza che avvengono all'interno delle reti Aziendali. Si chiede che la società affidataria del servizio preveda delle modalità di intervento risolutive delle problematiche che possano essere messe in atto in maniera tempestiva senza preoccuparsi della presenza in sede dei referenti interni all'ente. Ci saranno casi per i quali verrà previsto un confronto diretto tra le due parti (quale per esempio la presenza di incidenti su postazioni server) per ottenere la risposta più efficace e meno impattante sul lavoro quotidiano dell'utenza, ma la maggior parte delle attività dovrà essere svolta in "autonomia" fornendo all'ente le note informative delle attività intraprese per rispondere agli eventi riguardanti la sicurezza informatica.

Per poter operare in autonomia l'ente fornirà tutti gli strumenti per poter accedere ai propri sistemi di monitoraggio e analisi alla società offerente. Inoltre verranno forniti i recapiti delle persone incaricate dall'ente del servizio di reperibilità, al di fuori del normale orario di servizio, per un intervento celere verso PdL, server e apparati da effettuare in loco.

Al di là delle normali procedure operative già definite l'offerente dovrà garantire metodi per risolvere le problematiche di sicurezza e implementare procedure e percorsi condivisi e dedicati alle esigenze specifiche dell'Ente, nella normale evoluzione delle dinamiche di sicurezza dei sistemi.

Indicazione se il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché' dal PNC

Il Contratto è integralmente finanziato con fondi PNRR intervento M6.C2.1.1.1 Digitalizzazione dei DEA

Tempistiche richieste per la realizzazione della fornitura, con descrizione di eventuali vincoli e/o criticità

si chiede l'avvio dei servizi entro 30 giorni dall'ordine

Indicazione del/i luogo/ghi di interesse della fornitura

Corso Svizzera, n. 164, 10149 Torino TO

Durata del Contratto Esecutivo

24 mesi

Informazioni tecniche quali schemi di rete, piani di indirizzamento, apparati già in essere, utili a meglio comprendere il perimetro di interesse e indirizzare la migliore soluzione tecnologica, specificare:
Alloggiamento ed eventuale fissaggio sullo specifico supporto che sarà messo a disposizione dall'Amministrazione (rack, ripiano, …) in relazione alla tipologia apparato.
Indicazione del/i luogo/ghi di interesse della fornitura
N/A

Collegamento alla rete di alimentazione, presso il punto di presenza della rete indicato dall'Amministrazione.
Indicazione del/i luogo/ghi di interesse della fornitura

N/A_

Collegamento alla rete dati, presso il punto di presenza della rete indicato dall'Amministrazione.
N/A

Se prodotto hardware non è acquistato in sostituzione di un prodotto già presente l'amministrazione dovrà indicare i prerequisiti necessari all'installazione e configurazione :

1. **schemi logici dell'architettura**
2. **schemi di indirizzamento**
3. **requisiti delle policy di sicurezza stabiliti dall'Amministrazione**

N/A_____

Se il prodotto hardware è acquistato in sostituzione di un prodotto già presente presso l'Amministrazione oltre agli schemi logici e di indirizzamento indicare le impostazioni/policy/configurazioni attive e attualmente in esercizio
_N/A_____

Se il prodotto software è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare il tipo di prodotto attualmente utilizzato e se è un prodotto SaaS o On premise. La migrazione di un prodotto che sia SaaS oppure On premise nesessità di un supporto di servizi professionali.
N/A_____

Se il prodotto software non è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare la tipologia dei Client/Server sui quali dovrà essere installato il software.
N/A_

Le installazioni di prodotti software richiedono la configurazione del software di management sia per la componente Client (EPP) che Server (SPP)
L'amministrazione dovrà mettere a disposizione ambienti virtuali o fisici per gestire l'installazione di circa 5500 client EPP e circa 500 client SPP

Ulteriori informazioni che l'Amministrazione ritieni utili per lo svolgimento dell'attività del fornitore
N/A

QUADRO A - EDP/EPR

Descrizione del Servizio

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per l'EPP/EDR sono previste quattro fasce dimensionali:

- EPP_EDR_1 (fascia 1): fino a 500 client
- EPP_EDR_2 (fascia 2): fino a 1000 client
- EPP_EDR_3 (fascia 3): fino a 5000 client
- EPP_EDR_4 (fascia 4): oltre 5000 client

Endpoint Protection Platform & Endpoint Detection and Response				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
EPP & EDR - Fascia 1	EPP-F1-CYN	CYNET	Cynet-360-EPP-EDR-C-F1	
	EPP-F1-TM	TRENDMICRO	OS01141-EPP-C-F1	
	EPP-F1-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F1	
	EPP-F1-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F1	
EPP & EDR - Fascia 2	EPP-F2-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F2	
	EPP-F2-TM	TRENDMICRO	OS01141-EPP-C-F2	
	EPP-F2-CYN	CYNET	Cynet-360-EPP-EDR-C-F2	
	EPP-F2-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F2	
EPP & EDR - Fascia 3	EPP-F3-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F3	
	EPP-F3-TM	TRENDMICRO	OS01141-EPP-C-F3	
	EPP-F3-CYN	CYNET	Cynet-360-EPP-EDR-C-F3	
	EPP-F3-MCA	MCAFEE	MV6DEE-AA-DA+DLPECE-AT-DA-F3	
EPP & EDR - Fascia 4	EPP-F4-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F4	
	EPP-F4-TM	TRENDMICRO	OS01141-EPP-C-F4	
	EPP-F4-CYN	CYNET	Cynet-360-EPP-EDR-C-F4	**6.000**
	EPP-F4-MCA	MCAFEE	MV6DEE-AA-EA+DLPECE-AT-EA-F4	

QUADRO B - NAC

Descrizione del Servizio

Il NAC consente l'implementazione di regole per il controllo degli accessi all'infrastruttura aziendale da parte degli utenti, siano essi "umani" (attraverso personal computer, apparati mobili, …) oppure "cose" (elementi in ambito IoT). Le regole possono basarsi su più modalità quali l'autenticazione degli utenti, la configurazione degli apparati che accedono alla rete, il ruolo degli utenti. Per mezzo del NAC è inoltre possibile applicare regole successive alla connessione degli utenti, in base ad eventi che possono provenire da altri elementi di sicurezza.

Per i NAC sono previste sei fasce dimensionali/prestazionali:

- NAC_1 (fascia 1): fino a 100 Endpoint concorrenti
- NAC_2 (fascia 2): fino a 500 Endpoint concorrenti
- NAC_3 (fascia 3): fino a 1.000 Endpoint concorrenti
- NAC_4 (fascia 4): fino a 10.000 Endpoint concorrenti
- NAC_5 (fascia 5): fino a 25.000 Endpoint concorrenti
- NAC_6 (fascia 6): fino a 50.000 Endpoint concorrenti.

Network Access Control				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
NAC- Fascia 1	NAC-F1-HPE	HPE	JZ508AM-3Y-100C	
	NAC-F1-FN	FORTINET	FNC-CA-500C-BDL-C1	
NAC- Fascia 2	NAC-F2-HPE	HPE	JZ508AM-3Y-500C	
	NAC-F2-FN	FORTINET	FNC-CA-500C-BDL-C2	
NAC- Fascia 3	NAC-F3-HPE	HPE	JZ508AM-3Y-1000C	
	NAC-F3-FN	FORTINET	FNC-CA-500C-BDL-C3	
NAC- Fascia 4	NAC-F4-HPE	HPE	R1V81AM-3Y-10000C	
	NAC-F4-FN	FORTINET	FNC-CA-700C-BDL-C1	
NAC- Fascia 5	NAC-F5-HPE	HPE	R1V82AM-3Y-25000C	
	NAC-F5-FN	FORTINET	FNC-CA-700C-BDL-C2	
NAC- Fascia 6	NAC-F6-HPE	HPE	R1V82AM-3Y-50000C	
	NAC-F6-FN	FORTINET	FNC-CA-700C-BDL-C3	

QUADRO C - NGFW

Descrizione del Servizio

I NGFW sono apparati che consentono l'ispezione dei pacchetti di rete e si differenziano dai firewall "tradizionali" in quanto non si occupano solamente di analizzare e filtrare i pacchetti dati sulla base della porta e/o protocollo ma consentono di eseguire l'ispezione a livello applicativo, fornendo inoltre funzionalità di prevenzione dalle intrusioni, analisi e rilevamento dei malware e capacità di utilizzo di sorgenti esterne a supporto della propria attività di protezione.
Per i NGFW sono previste sei fasce dimensionali.

Next Generation Firewall				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
NGFW - Fascia 1	NGFW-F1-FN	FORTINET	FG-60F-BDL-C	
	NGFW-F1-CI	CISCO	CISCO-FPR1010-F1C	
	NGFW-F1-FP	FORCEPOINT	N120-C-F1	
	NGFW-F1-PA	PALO ALTO	PAN-PA-440-CONSIP-BUN-F1	
NGFW - Fascia 2	NGFW-F2-CI	CISCO	CISCO-FPR2110-F2C	

	NGFW-F2-FN	FORTINET	FG-200F-BDL-C	
	NGFW-F2-FP	FORCEPOINT	N2101-C-F2	
	NGFW-F2-PA	PALO ALTO	PAN-PA-3220-CONSIP-BUN-F2	
NGFW - Fascia 3	NGFW-F3-CI	CISCO	CISCO-FPR2130-F3C	
	NGFW-F3-FP	FORCEPOINT	N2101-C-F3	
	NGFW-F3-FN	FORTINET	FG-600E-BDL-C	
	NGFW-F3-PA	PALO ALTO	PAN-PA-3260-CONSIP-BUN-F3	
NGFW - Fascia 4	NGFW-F4-PA	PALO ALTO	PAN-PA-5220-CONSIP-BUN-F4	
	NGFW-F4-CI	CISCO	CISCO-FPR2140-F4C	
	NGFW-F4-FP	FORCEPOINT	N3401-C-F4	
	NGFW-F4-FN	FORTINET	FG-1100E-BDL-C	
NGFW - Fascia 5	NGFW-F5-PA	PALO ALTO	PAN-PA-5250-CONSIP-BUN-F5	
	NGFW-F5-CI	CISCO	CISCO-FPR4115-F5C	
	NGFW-F5-FP	FORCEPOINT	N3405-C-F5	
	NGFW-F5-FN	FORTINET	FG-2600F-BDL-C	
NGFW - Fascia 6	NGFW-F6-PA	PALO ALTO	PAN-PA-5260-CONSIP-BUN-F6	
	NGFW-F6-CI	CISCO	CISCO-FPR9300-F6C	
	NGFW-F6-FP	FORCEPOINT	N3410-C-F6	
	NGFW-F6-FN	FORTINET	FG-3400E-BDL-C	

QUADRO D - ANTI - APT

Descrizione del Servizio

La soluzione di Anti-APT consente l'analisi di file che possono essere inviati all'elemento da altri dispositivi di sicurezza o direttamente dal personale che si occupa di sicurezza. All'interno dell'ambiente protetto (sandbox) è quindi possibile, attraverso varie tecniche, esaminare i file e i loro comportamenti per determinare se questi siano o meno malevoli, assegnando loro un grado di severità.

Per l'Anti-APT sono previste due fasce dimensionali/prestazionali:

- Anti_APT_1 (fascia 1): fino a 450 file/ora
- Anti_APT_2 (fascia 2): fino a 1000 file/ora

Protezione anti-Advanced Persistent Threat				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
Anti-APT - Fascia 1	Anti-APT-F1-CP	CHECKPOINT	SandBlast TE Appliance TE100X-C	
	Anti-APT-F1-TM	TRENDMICRO	ADAXZZE5XL-C-F1	
Anti-APT - Fascia 2	Anti-APT-F2-CP	CHECKPOINT	SandBlast TE Appliance TE250X-C	
	Anti-APT-F2-TM	TRENDMICRO	ADAXZZE5XL-C-F2	

QUADRO E - Server Protection

Descrizione del Servizio

La soluzione SPP consente di proteggere gli endpoint di tipo server da minacce quali virus, trojan, worm, malware, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Per la SPP sono previste quattro fasce dimensionali:

- SPP_1 (fascia 1): fino a 50 server
- SPP_2 (fascia 2): fino a 100 server
- SPP_3 (fascia 3): fino a 500 server
- SPP_4 (fascia 4): oltre 500 server

Server Protection Platform				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
SPP - Fascia 1	SPP-F1-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F1	
	SPP-F1-TM	TRENDMICRO	DX0099-SPP-C-F1	
SPP - Fascia 2	SPP-F2-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F2	
	SPP-F2-TM	TRENDMICRO	DX0099-SPP-C-F2	
SPP - Fascia 3	SPP-F3-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F3	
	SPP-F3-TM	TRENDMICRO	DX0099-SPP-C-F3	
SPP - Fascia 4	SPP-F4-CP	CHECKPOINT	CP-HAR-EP-COMPLETE-SPP-C-F4	
	SPP-F4-TM	TRENDMICRO	DX0099-SPP-C-F4	

QUADRO F - Servizio di Hardening

Descrizione del Servizio

Il servizio di hardening fornisce all'Amministrazione il supporto operativo necessario per rendere sicuri i client utilizzati. Le attività effettuate dovranno essere aderenti a quanto previsto dalle "*Linee guida per adeguare la sicurezza del software di base*" rilasciate da AgID.
Le specifiche attività che dovranno essere eseguite sono dipendenti dagli specifici software utilizzati sui client, ma in linea generale possono essere riassunte in:

- eliminazione di programmi non necessari dalle postazioni utente. Potenzialmente ogni programma è una porta di accesso per soggetti non legittimati e dunque la loro diminuzione consente di limitare i rischi di intrusioni. Tutti i programmi che non sono stati autorizzati e controllati e che non sono strettamente utili all'esecuzione delle attività lavorative dovrebbero essere rimossi;
- supporto ai sistemisti PA nelle fasi di monitoraggio e controllo che il sistema operativo e i programmi leciti siano aggiornati alle ultime versioni e agli ultimi "*service pack*" disponibili;
- controllo che sui client siano abilitati i servizi autorizzati, ossia che non vi siano "*demoni*" in ascolto sulle porte di rete se non quelli strettamente necessari;
- verifica che gli utenti abbiano i corretti privilegi in relazione al loro ruolo e che appartengono ai corretti gruppi utenti;
- verifica della consistenza delle password richieste e della periodicità di cambio password richiesta agli utenti;
- supporto ai sistemisti PA nella definizione di gruppi di policy che potranno essere applicati agli utenti sulla base dei loro ruoli;

- verifica che gli eventi di sicurezza siano correttamente storicizzati (logging) ai fini del controllo e dell'audit;
- supporto al personale dell'Amministrazione nella distribuzione delle azioni correttive individuate (ad es. installazione di eventuali *patch* mancanti, realizzazione e installazione di fix temporanee, etc..) siano esse relative al sistema operativo che ai programmi utilizzati.

Il servizio dovrà essere effettuato sulle postazioni di tipo client e dovrà includere almeno i seguenti software:

- Sistemi operativi Windows Client;
- Sistemi operativi macOS;
- Sistemi operativi UNIX/Linux di tipo Client;
- Principali Web Browser (Edge, Explorer, Firefox, Chrome);
- Principali applicativi software di produttività (Microsoft Office/OpenOffice, Pdf Readers, Outlook.

Servizio di Hardening			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Fase di assessment	ASS	HARD_ASSMNT	
Fase di distribuzione degli interventi -1001_5000	DISINT 1001-5000	HARD_DISTR_1001_5000	
Fase di distribuzione degli interventi - 2_1000	DISINT 2-1000	HARD_DISTR_2_1000	
Fase di distribuzione degli interventi - 5001_	DISINT>5000	HARD_DISTR_5001_	
Fase di progettazione degli interventi	PRINT	HARD_PROG	

QUADRO G - Servizio di Formazione

Descrizione del Servizio

Il servizio di formazione e affiancamento consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione Contraente che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'AQ, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software;
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti presso l'Amministrazione e le relative finalità;
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

È richiesto che tali attività formative siano erogate in moduli da massimo 16 ore e che per ogni modulo siano previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni indicativamente di 8 ore ciascuna:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste;

- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità *traning on the job*.

Formazione			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Modulo Formativo	FOR	FORMAZIONE	

QUADRO H - Servizio di Supporto Specialistico

Descrizione del Servizio

Il servizio supporto specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica.
Il servizio riguarderda le attività riportate nel seguito:
a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito.
Tale servizio potrà essere acquistato dalle Amministrazioni Contraenti unicamente in maniera contestuale ai prodotti e avere durata massima pari a 24 mesi.
Il servizio potrà essere prestato secondo le seguenti modalità:
i. in fase iniziale - lett. a) del precedente elenco;

ii. in modalità "*spot*" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco

iii. con periodicità definita - lett. c) (limitatamente alla modalità "presidio") e d) del precedente elenco.

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	**525**
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	

Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	**512**
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

QUADRO I - Servizio di Manutenzione

Descrizione del Servizio

Il servizio di manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità.
La manutenzione, in base alla qualità del servizio richiesto per i servizi erogati, prevede due profili *Low Profile* (*Business Day*) o *High Profile* (*H24*) e potrà essere offerta per annualità, quindi per 12 mesi o massimo 24 mesi.
Le attività di manutenzione sono associate ai soli elementi di fornitura acquistati nell'ambito del presente AQ e potranno essere acquistate solo contestualmente alla fornitura.
Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code;
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
  1. intervento presso la sede/luogo interessato;
  2. ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati;
  3. verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Servizio di manutenzione		
Fascia di acquisizione	Codice Servizio	Quantità (mesi)
Manutenzione LP	MANLP-EPP-F1	
	MANLP-EPP-F2	
	MANLP-EPP-F3	
	MANLP-EPP-F4	
	MANLP-NAC-F1	
	MANLP-NAC-F2	
	MANLP-NAC-F3	
	MANLP-NAC-F4	
	MANLP-NAC-F5	
	MANLP-NAC-F6	
	MANLP-NGFW-F1	
	MANLP-NGFW-F2	

	MANLP-NGFW-F3	
	MANLP-NGFW-F4	
	MANLP-NGFW-F5	
	MANLP-NGFW-F6	
	MANLP-Anti-APT-F1	
	MANLP-Anti-APT-F2	
	MANLP-SPP-F1	
	MANLP-SPP-F2	
	MANLP-SPP-F3	
	MANLP-SPP-F4	

Manutenzione HP	MANHP-EPP-F1	
	MANHP-EPP-F2	
	MANHP-EPP-F3	
	MANHP-EPP-F4	
	MANHP-NAC-F1	
	MANHP-NAC-F2	
	MANHP-NAC-F3	
	MANHP-NAC-F4	
	MANHP-NAC-F5	
	MANHP-NAC-F6	
	MANHP-NGFW-F1	
	MANHP-NGFW-F2	
	MANHP-NGFW-F3	
	MANHP-NGFW-F4	
	MANHP-NGFW-F5	
	MANHP-NGFW-F6	
	MANHP-Anti-APT-F1	
	MANHP-Anti-APT-F2	
	MANHP-SPP-F1	
	MANHP-SPP-F2	
	MANHP-SPP-F3	
	MANHP-SPP-F4	

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

6C-3D-47-30-B4-88-03-5B-FB-86-92-1B-19-03-73-E6-DE-AC-97-B2

PAdES 1 di 1 del 19/09/2023 16:40:31

Soggetto: Francesco Pensalfini TINIT-PNSFNC65D06G479K

Validità certificato dal 18/07/2023 13:02:18 al 18/07/2026 00:00:00

Rilasciato da InfoCert S.p.A. con S.N. 12DACE3

PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE - PROTEZIONE DEGLI ENDPOINT

LOTTO 2

AQ CONSIP 2367

ASL Città di Torino

Indice

Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	05/10/2023

Introduzione

Premessa

Il presente documento descrive il Piano Operativo, relativamente alla richiesta di fornitura di prodotti e servizi per la sicurezza perimetrale per ASL Città di Torino in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (allegato all'ordine n. **7411144**).

Con questo progetto ASL Città di Torino intende acquisire una fornitura EPP/Cynet e utilizzare i servizi specialistici per raggiungere un adeguato livello di sicurezza in correlazione con i requisiti previsti dal PNRR.

Il progetto sarà finanziato con le risorse del PNRR (Piano Nazionale di Ripresa e Resilienza).

Scopo

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro ed in risposta al Piano dei Fabbisogni inviato dal cliente.

Riferimenti

Identificativo
Piano dei Fabbisogni - 7411144 Piano dei Fabbisogni ASL Città di Torino allegato all'ordine
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

Acronimi e Glossario

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa
SPC	Sistema Pubblico di Connettività

Organizzazione del contratto esecutivo

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- ✓ **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**

  Massimiliano Materazzi

  e-mail: ***massimiliano.materazzi@telecomitalia.it***

che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro.

- ✓ **Responsabile del Fornitore**

  Andrea Favaro

  telefono/cellulare: ***335 7837749***

  e-mail: ***andrea.favaro@telecomitalia.it***

che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo.

- ✓ **Referente Tecnico per l'erogazione dei servizi**

  Antonio Dell'Erba

  telefono/cellulare: ***331 6002172***

  e-mail: ***antonio.dellerba@telecomitalia.it***

che dovrà garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5).

Categorizzazione degli interventi

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

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

Progetto d'attuazione

La fornitura di cui al presente Piano Operativo ha per oggetto le tecnologie per la sicurezza perimetrale elencate nel paragrafo a seguire. Unitamente a tale fornitura, saranno erogati i seguenti servizi:

- installazione e configurazione delle tecnologie di nuova fornitura (Cynet);

Saranno inoltre erogati i seguenti servizi di Supporto Specialistico:

- supporto alla reingegnerizzazione della rete dell'Amministrazione, incluse le necessarie attività di assessment, profilazione e documentazione dell'AS-IS e del TO-BE;
- supporto al personale dell'Amministrazione nella gestione di tutti i servizi preesistenti e di nuova fornitura.

Modalità e tempistiche per l'esecuzione di ciascuna delle attività sopra riportate saranno oggetto di apposita pianificazione, da concordare fra le parti.

Prodotti richiesti

Prodotto	Tecnologia	Fascia	Modello	Codice articolo produttore	Quantità
EPP	Cynet	4	Agent Cynet 360	Cynet 360 EPP EDR C F4	6.000

Prodotti della fornitura

Nel seguente paragrafo è riportata una descrizione tecnica dei prodotti forniti.

Endpoint Protection Platform

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza.

Nel seguente paragrafo è riportata una descrizione tecnica del servizio di EPP/EDR Cynet.

La piattaforma si distingue per la copertura della superficie d'attacco aziendale e per il modo in cui si occupa dell'intero ciclo di protezione dagli attacchi, rispondendo alle minacce e mitigando i rischi informatici.

Cynet supporta una ampia gamma di versioni su tre macro famiglie di sistemi operativi: Windows, Linux e Mac. Per quanto riguarda le versioni specifiche:

- Microsoft Windows (32b/64b), a partire dalla versione XP SP3, Vista, 7, 8, 8.1 fino a tutte le versioni 10 e la nuova versione Windows 11 (sono anche supportate le versioni Windows Server a partire dalla versione 2003 SP2 fino alla versione 2019 e alla nuova 2022);
- Linux, supporto per 8 diverse distribuzioni, a partire dalle versioni RedHat 6.9, CentOS 6.9, Fedora 23, SUSE 12, Debian 9.x, Ubuntu 16.04,Oracle Linux 7.6, Amazon Linux prima versione e v2;
- Apple macOS, a partire dalla versione 10.13 in avanti comprese le versioni con processori Apple M1;

Sono supportati anche ambienti VDI basati su Windows 10 e 11.

Di seguito si riporta una tabella riassuntiva delle funzionalità richieste dal capitolato tecnico supportate dai diversi sistemi operativi:

EPP/EDR - Tutte le fasce	Windows	Windows Legacy	MAC	MAC Legacy	Linux	Linux Legacy
Supporto degli endpoint con Sistema Operativo Windows (almeno Windows 8 e Windows 10) – EPP/EDR	□	✓ a partire da XP SP3	n.a	n.a	n.a	n.a
Funzionalità Antimalware signature based – EPP	□	□	□	□	□	□
Aggiornamento delle signature in maniera automatica – EPP	□	□	□	□	□	□
Possibilità di effettuare: Blocco azioni dannose; gestione della quarantena dei file; pulizia dell'endpoint – EPP	□	□	□	□	□	□
Protezione del traffico in entrata e in uscita dagli endpoint, comprensivo di controllo delle applicazioni, delle porte e dei protocolli utilizzati al fine di prevenire attacchi e intrusioni contro gli endpoint– EPP	□	□	✓ (1)	✓ (1)	✓ (1)	✓ (1)
Protezione dell'endpoint dai malware attraverso il monitoraggio degli eventi che accadono sull'endpoint e l'analisi comportamentale, controllando le principali modifiche (controllo/interruzione di programmi, modifica chiavi di registro, installazione impropria di device o driver, accesso anomalo alla memoria) apportate sull'endpoint. In caso di tentativo di modifica, è richiesto il blocco della modifica e l'avviso all'utente. – EPP	□	□	✓ (2)	✓ (2)	✓ (2)	✓ (2)
Protezione dai ransomware– EPP	□	□	□	□	□	□
Protezione anti-exploit– EPP	□	□	□	□	□	□
Possibilità di impostare regole per limitare o bloccare l'accesso a supporti removibili collegati all'endpoint. – EPP	□	✓ (3)				
Disponibilità di strumenti che consentano, durante la navigazione, di verificare se un sito web è considerato sicuro o meno con impostazione di eventuali policy di sicurezza associate (ad esempio blocco di siti considerati non sicuri). – EPP	□					
Possibilità di definire policy di sicurezza attraverso le quali sia consentita l'esecuzione dei soli programmi autorizzati. – EPP	□	□	□	□	□	□
Possibilità di effettuare delle scansioni in modalità: real time; manuale; programmata – EPP	□	✓ (3)	□	□	□	□
Funzionalità di reportistica e logging: monitoring in real time, template predefiniti ed esportazione – EPP/EDR	□	□	□	□	□	□
Supporto del protocollo IPv6– EPP	□	□	□	□	□	□
Possibilità di effettuare la Root Cause Analysis– EDR	□	□	□	□	□	□
Possibilità di effettuare detection di malware attraverso sorgenti IoC– EDR	□	□	□	□	□	□

(1) No protocolli; (2) No chiavi di registro; (3) Si dalla versione 7, No su XP; (4) No modifiche di registro

In generale la piattaforma Cynet 360 comprende le funzioni di: ☒NGAV, ☒EDR, ☒Network Analytics, ☒User/File/Host Deception (HoneyPots) User Behavior Analytics (UBA), Vulnerability Assessment, Log collection and retention, ☒Inventory Assessment, File Integrity Monitoring, Windows Event collection, Network Traffic Analysis e threat Hunting.

La piattaforma offre capacità di Pre-set Auto-Remediations (singolo switch per abilitazione complessiva delle Best Practice Protections), Custom Remediations e Automated Playbooks per automatizzare tutte le operazioni più frequenti e ripetitive effettuate in genere dagli operatori SOC. Infine, è disponibile anche un Incident Investigation Engine in grado di analizzare automaticamente quanto osservato, in grado di trovare in autonomia gli Indicatori di Compromissione disseminati nell'infrastruttura e, se impostato, consentendo la rimozione.

Si riporta un esempio di UBA. La Forensic di Cynet permette di andare a mostrare comportamenti degli utenti altamente sospetti correlando varie attività anomale.

Figura 1: Esempio di UBA

Si riporta, inoltre, un esempio di NTA – Rilevamento di una fase avanzata nella kill chain dell'attacco in cui l'attaccante ha ottenuto l'accesso ai dati di destinazione e tenta di esfiltrarli mascherando i dati compromessi come traffico DNS legittimo. Di lato si riporta un esempio di UBA. La Forensic di Cynet permette di andare a mostrare comportamenti degli utenti altamente sospetti correlando varie attività anomale.

Figura 2: Esempio di NTA

Caratteristiche del servizio

Il servizio di EPP dovrà essere erogato nella sede di Corso Svizzera, 164 – 10149 Torino – referente: Pensalfini Francesco mail francesco.pensalfini@aslcittaditorino.piemonte.it

Nella sede\i indicata\e verrà resa disponibile, la seguente suite di prodotto, come indicato in tabella, secondo quanto richiesto nel Piano dei fabbisogni:

Endpoint Protection Platform				
Prodotto / Fascia	**Codice servizio**	**Brand**	**Codice fornitore**	**Quantità**
CYNET/4	EPP-F4-CYN	Cynet	Cynet 360 EPP EDR C F4	6000

Caratteristiche hardware EPP

Il servizio EPP ha la finalità di proteggere gli strumenti di lavoro del personale del Cliente da possibili attacchi informatici che possano sfruttare l'endpoint quale vettore preferenziale verso il Sistema Informativo.

La soluzione proposta adotta la tecnologia Cynet, ideata per la protezione degli endpoint da molteplici virus quali ransomware, trojan e altri malware specifici, che consente anche di controllarne ed impedirne la diffusione all'interno della rete.

Servizio di supporto specialistico

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione.

Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Quantità (gg/uomo)**
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	1050
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	1024

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa

Per le competenze che ciascuna risorsa specialistica deve possedere si rimanda a quanto previsto nell'allegato 2 – Capitolato Tecnico – Parte Speciale (paragrafo 3.2.4), e come di seguito riportate:

Junior Security Analyst: in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst,

Senior Security Analyst: in possesso di almeno una delle seguenti certificazioni:

EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst

Le attività che l'Amministrazione intende svolgere attraverso il servizio di supporto specialistico consistono in:

Servizio di Security Assessment

Lo scopo delle attività descritte in questo paragrafo è quello di definire e concordare l'ambito stimato delle attività e delle tempistiche necessarie per assistere l'Amministrazione nel proteggere i suoi asset informativi attraverso la realizzazione dei servizi di sicurezza informatica.

Si eseguirà l'analisi del contesto operativo in cui opera l'Organizzazione mediante la raccolta di necessarie informazioni.

Tali attività consentono di iniziare il processo di analisi "AS-IS" finalizzato a comprendere lo stato attuale dei presidi di sicurezza posti in essere oltre all'esame dei punti di forza, delle debolezze, delle opportunità e delle minacce cyber rilevanti per l'Organizzazione.

Tale fase di analisi dell'attuale modello di "governance" della sicurezza dell'Organizzazione include l'analisi di processi riguardanti la gestione del rischio cyber, ovvero processi di:

- risposta ad attacchi ransomware, o incidenti di natura cyber
- modalità di supporto alla continuità operativa,
- modello di rilevazione e gestione delle vulnerabilità
- gestione delle identità digitali e degli accessi ai sistemi informativi,

Durante la fase di analisi si intende rilevare e analizzare il fabbisogno formativo del personale dell'Organizzazione nell'ambito del dominio "awareness".

Successivamente, l'Organizzazione verrà supportata nell'identificare i gap esistenti elaborando la roadmap strategica per definire il Modello Organizzativo di gestione della sicurezza cui orientarsi strategicamente.

Questa valutazione verrà condotta per valutare la situazione attuale della sicurezza e identificare le vulnerabilità dell'infrastruttura interna ed esterna esistente di ASL Città di Torino secondo l'ambito. Al termine dei servizi di sicurezza informatica proposti per ASL Città di Torino, sarà possibile avere una visione completa delle varie minacce insieme a indicazioni di rimedio e "best practice".

L'approccio suggerito è che ogni serie di valutazioni di sicurezza programmate inizierà dalla ricerca delle eventuali vulnerabilità e successivamente verranno effettuati test di resistenza dei sistemi, concentrato sugli elementi selezionati con rischio potenzialmente più alto.

Nel corso delle attività saranno rilasciati report di dettaglio che saranno condivisi con la PA contraente e di comune accordo verranno definite le strategie e le azioni da intraprendere al fine di raggiungere tutti gli obiettivi prefissati

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico in base alle esigenze del cliente e comunque in funzione della fornitura prodotti richiesta

tramite questo piano. Qualsiasi altra necessità sarà valutata di volta in volta in accordo con il cliente.

Si specifica che le attività di cui sopra contemplano esclusivamente il supporto al personale dell'Amministrazione in attività di assessment e di progetto, incluso il supporto alla produzione della necessaria documentazione tecnica.

Come indicato nel par.10 – TABELLA RIEPILOGATIVA, i gg/UU relativi ai servizi professionali saranno suddivisi tra i soci del RTI per erogare quanto richiesto dall'Amministrazione.

Piano di lavoro

Il processo di Start-up è incluso nel servizio e comprende le fasi propedeutiche all'attivazione del servizio ed è composto da diverse attività che devono essere implementate in collaborazione con il cliente ASL Città di Torino

Le fasi principali dello Start-Up sono:

- Incontro preliminare e pianificazione;
- Installazione componenti del servizio;
- Collaudo (User Acceptance Test)
- Kickoff
- Attivazione del Servizio

Il processo può in parte variare in base alla tipologia o TIER di servizio attivato, ma le principali fasi operative sono le medesime.

Incontro preliminare e pianificazione

- Condivisione del piano di attivazione del servizio che comprende la pianificazione dell'installazione dei suoi componenti e della VPN tra l'infrastruttura del cliente ASL Città di Torino e il cloud del partner TIM. A tal fine verrà consegnata e illustrata al cliente ASL Città di Torino una Checklist riepilogativa di tutte le informazioni tecniche necessarie per l'attivazione e l'installazione dei componenti del servizio.

- Definizione asset: il cliente ASL Città di Torino dovrà fornire l'elenco dei sistemi aziendali oggetti del servizio. Nell'elenco dovranno essere evidenziati i sistemi ritenuti critici o importanti per il business con il maggior numero di informazioni possibili (es. modello, ubicazione, IP address, note operative, etc.).

- Mappa infrastruttura di rete: il cliente ASL Città di Torino dovrà fornire una mappa dell'infrastruttura fisica e logica con riportati i link tra gli apparati di rete e quelli di sicurezza e di computing.

- Contatti: durante l'incontro il team di lavoro presenterà al cliente ASL Città di Torino le diverse modalità con prendere contatti per il servizio, Il cliente ASL Città di Torino dovrà altresì fornire i contatti aziendali che saranno i riferimenti per il team (Key User). Inoltre, nel caso in cui il con il cliente ASL Città di Torino affidi al team anche l'attività di escalation verso le terze parti (es. ISP), in questa occasione fornirà anche i riferimenti dei loro partner ed i relativi numeri di contratto.

- Definizione delle policy di sicurezza e distribuzione agent: saranno concordati i protocolli del collegamento VPN, i canali e i protocolli di comunicazione sicura per la raccolta dei log, l'invio degli

eventi e per le comunicazioni di servizio. Sarà messo a disposizione del cliente ASL Città di Torino il software (agent) con i parametri necessari per la distribuzione sui sistemi supportati.

- Discussione di eventuali criticità e definizione dei livelli di severità: il cliente ASL Città di Torino dovrà rendersi disponibile per valutare le eventuali criticità dei suoi asset e della sua infrastruttura, sia in termini strategici che operativi. Tali informazioni sono di massima importanza per dare la giusta rilevanza ai problemi che si dovessero presentare durante l'erogazione del servizio e consentono di definire i livelli di severità che, dopo essere stati concordati con il cliente ASL Città di Torino, saranno assegnati agli eventi di sicurezza rilevati durante il servizio.

- Definizione dell'Use Case: Una volta raccolte tutte le informazioni necessarie, gli esperti di sicurezza del team supporteranno il cliente ASL Città di Torino nella definizione e mappatura delle sorgenti log e eventi, delle Politiche di Sicurezza e delle regole di correlazione. Tutte le Politiche di Sicurezza decise dal cliente ASL Città di Torino verranno dallo stesso sottoscritte e costituiranno l'esatta analisi di quanto verrà implementato. Le eventuali variazioni alla struttura inizialmente implementata subiranno il medesimo iter.

- Definizione delle modalità di intervento in risposta alle minacce. Tutti gli aspetti legati alle modalità di intervento, incluse le regole d'ingaggio, verranno concordate e documentate. Eventuali asset di security con le rispettive credenziali e i rispettivi livelli di accesso, a cui il team potrà accedere saranno definiti in questa sezione.

Installazione componenti del servizio e implementazione Use Case

Dopo l'incontro preliminare verranno installati i componenti del servizio presso la sede del cliente ASL Città di Torino. Per poter eseguire tale attività, il cliente ASL Città di Torino dovrà aver compilato il documento di Checklist precedentemente condiviso. Verrà configurata la VPN tra l'infrastruttura del cliente ASL Città di Torino ed il Cloud del partner TIM e verrà avviata l'implementazione dell'Use Case.

User Acceptance - Collaudo

Completata l'installazione dei componenti e la configurazione secondo le specifiche concordate nell'ambito dell'Use Case, il team effettuerà il collaudo del servizio. Tutta la documentazione sulla configurazione del servizio, la Checklist, le policy e la configurazione dell'Use Case e i risultati del collaudo saranno verbalizzati in un unico documento con il titolo di User Acceptance Test (Verbale di Collaudo) che sarà consegnato al cliente ASL Città di Torino durante la riunione di Kick-Off.

Kick-Off del servizio

Non appena tutte le precedenti fasi verranno portate a termine, il Team di lavoro incontrerà il cliente ASL Città di Torino per ufficializzare il completamento delle attività di configurazione, la messa a regime dei servizi acquistati e il rilascio di User Acceptance Test che sarà sottoscritto da entrambe le parti.

Attivazione del servizio

Concluse le attività precedentemente illustrate, viene comunicata al cliente ASL Città di Torino l'attivazione del servizio.

Grace Period

Si definisce Grace Period, un periodo temporale di 3 mesi successivi alla messa a regime che prevede il "fine tuning" (sintonizzazione accurata) del servizio. L'obbiettivo principale di questo periodo

è di verificare e validare l'efficacia dell'Use Case, di tutte le procedure di presa in carico delle richieste di intervento e di eventuale escalation verso terze parti. In questo periodo il servizio viene erogato in modo completo.

Requisiti

Il cliente ASL Città di Torino dovrà mettere a disposizione le risorse computazionali e di spazio necessarie all'appliance che ha il ruolo di collector e processor degli eventi.

Requisiti dell'appliance che dovrà essere installata presso l'infrastruttura del cliente ASL Città di Torino

Descrizione	vCPU	vRAM	vSDD
EVENT PROCESSOR	16	24 GB	1TB

GANTT

Attività di delivery e attivazione del servizio

PIANO DELLE ATTIVITA'	settimana 1					settimana 2					settimana 3			
	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4
ATTIVITÀ	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4	GIORNO 5	GIORNO 1	GIORNO 2	GIORNO 3	GIORNO 4
•Incontrl preliminare e pianificazione;														
•Installazione componenti del servizio e implementazione Use Case														
•User Acceptance - Collaudo														
•Attivazione del servizio														t>0

In concomitanza della fase di attivazione del servizio si assume t>0 per dare avvio alla rendicontazione

Attività di "fine tuning"

PIANO DELLE ATTIVITA'	ANNO		
	MESE 1	MESE 2	MESE 3
•Grace Period			

Piano di presa in carico

L'attività di presa in carico del sistema consiste nell'acquisire tutte le informazioni che sono necessarie all'erogazione dei servizi e di quanto indicato nel sopra riportato piano di lavoro, con l'obiettivo di acquisire know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione oltre a standard, modalità operative, linee guida, ove presenti.

Come specificato da piano dei fabbisogni, l'amministrazione contraente fornirà la configurazione esistente degli apparati, il piano d'indirizzamento, gli accessi ai sistemi per la configurazione degli stessi, gli eventuali accessi fisici nei locali tecnici, le informazioni necessarie all'attivazione dei servizi nonché la disponibilità del personale referente affinché di comune accordo si possano definire le strategie implementative oggetto di fornitura. L'attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. schemi logici e di low level design dell'infrastruttura di rete, informative sulle connettività presenti, piani di indirizzamento etc) con assistenza di personale esperto e affiancamento condotta con eventuali ulteriori fornitori dell'amministrazione contraente.

Se previsto e/o richiesto dall'amministrazione contraente saranno altresì forniti i dettagli necessari (es. tools IT Management) alla corretta implementazione dei processi di Incident, Change e Deploy Management richiesta per l'espletamento dei servizi descritti nei successivi paragrafi.

Si noti che qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del piano di presa in carico.

Durante le attività di Presa in carico si dovrà garantire:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall'Amministrazione e che dovrà essere sottoscritto dal RTI e dall'Amministrazione.

Specifiche di collaudo

Per ciascun elemento che compone le macroaree di progetto, verranno effettuate prove di esercibilità e test funzionali secondo il piano di seguito riportato. Le date di collaudo potranno essere definite in accordo al piano riportato al paragrafo precedente.

Per il servizio di Endpoint Protection Platform (EPP) /Endpoint Detection & Response (EDR) saranno eseguite le seguenti attività di verifica e test da affinare in sede del cliente.

Tipologia	Descrizione
Test Funzionale	Verifica che i dispositivi funzionino come previste siano in grado di eseguire le funzionalità base come la prevenzione dell'intrusione, la verifica delle autorizzazioni agli accessi, delle politiche di sicurezza
Test di sicurezza	Verificare la capacità dei dispositivi di rilevare e prevenire possibili compromissioni e attacchi all'infrastruttura IT. Questi test possono includere simulazioni in ambiente controllato, test di identificazione e blocco di Virus e malware
Test di compatibilità	Questi tipi di test verificano la capacità dei dispositivi di funzionare correttamente con gli altri componenti dell'infrastruttura IT

Tabella riepilogativa dei servizi e relativi importi contrattuali

Forniture

Prodotto	Tecnologia	Fascia	Modello	Codice articolo produttore	Quantità
EPP	Cynet	4	Agent Cynet 360	Cynet 360 EPP EDR C F4	6.000

Servizi di supporto specialistico

Servizio di Supporto Specialistico			
Prodotto / Fascia	**Codice servizio**	**Codice fornitore**	**Quantità (gg/uomo)**
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	1.050
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	1.024

Valorizzazione economica

Codice articolo convenzione	Quantità	Durata (mesi)	Prezzo totale
CS2L2-EPP F4-CYN	6000		27.660,00€
CS2L2-JSAN-STA	1050		238.875,00€
CS2L2-SSSN-STA	1024		277.504,00€
		TOTALE	**544.039,00€**

Rendicontazione e SAL di avanzamento servizi professionali

SAL 1° t>0

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	260	70.460,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	261	59.377,50 €
		Totale	**129.837,50 €**

SAL 2° 3° 4°

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	84	22.764,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	88	20.020,00 €
		Totale	**42.784,00 €**

3 SAL trimestrali t>0 + 3 mesi con cadenza 3 mesi ciascuno

SAL 5° t>0 + 12 mesi

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	260	70.460,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	261	59.377,50 €
		Totale	**129.837,50 €**

SAL 6° 7° 8°

Descrizione Articolo Convenzione AQ Cybersecurity - 2367	Prezzo unitario	Q.TA GIORNATE	Totale
Servizio di supporto specialistico - Senior Security Analyst - fascia standard	271,00 €	84	22.764,00 €
Servizio di supporto specialistico - Junior Security Analyst - fascia standard	227,50 €	88	20.020,00 €
		Totale	**42.784,00 €**

3 SAL trimestrali t>0 + 15 mesi con cadenza 3 mesi ciascuno

Prestazioni subappalto

Nell'ambito dell'Accordo Quadro Cybersecurity 2 per le prestazioni erogate in subappalto è previsto quanto segue:

- Quota massima del subappalto: 50%
- Servizi per i quali è prevista la prestazione in subappalto:
- Formazione;
- Hardening;
- Supporto Specialistico.

Nella tabella sottostante è necessario riportare la quota, le prestazioni e il nome delle aziende che erogheranno i servizi in subappalto, nel rispetto di quanto indicato nel Piano dei fabbisogni:

Servizi	Quota subappalto	Azienda del RTI che eroga il servizio	Azienda che eroga la prestazione in subappalto
Supporto Specialistico	95%	TIM	Lantech Longwave
Formazione	n.a.	n.a.	n.a.

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

9D-52-4D-C5-66-8B-74-22-32-16-73-4B-D8-54-97-DA-F3-BA-10-7E

CAdES 1 di 2 del 10/10/2023 14:43:19

Soggetto: GIUSEPPE RUSSO RSSGPP67L29I480H

Validità certificato dal 28/04/2022 11:19:57 al 28/04/2025 11:19:56

Rilasciato da TI Trust Technologies QTSP CA 1, Telecom Italia Trust Technologies S.r.l., IT con S.N. 082

TimeStamp 2 di 2 del 10/10/2023 12:43:20

Soggetto: Time Stamp Server - 2, Telecom Italia Trust Technologies S.r.l., IT

Validità certificato dal 26/08/2023 00:00:00 al 25/08/2026 00:00:00

Rilasciato da TI Trust Technologies QTSP TSA CA, Telecom Italia Trust Technologies S.r.l., IT con S.

ASL CITTA' DI TORINO

SICUREZZA AZIENDALE GESTITA
LION SOC CYBERSECURITY
SIEM – MDR

Documento di specifiche tecniche

Il presente documento è stato redatto in coerenza con il Codice Etico e i Principi Generali del Controllo Interno

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

INDICE

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	REVISIONE	DATA
Prima emissione	0	04/10/2023

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

1 INTRODUZIONE

A seguito della Vostra gentile richiesta, TIM con questo documento vuole presentare a ASL CITTA' DI TORINO l'offerta inerente il servizio LION® Cybersecurity.

TIM si propone come un partner esperto e flessibile, in grado di valutare le necessità di ASL CITTA' DI TORINO, di consigliarlo nei passaggi evolutivi e di fornirgli le soluzioni più appropriate affiancandolo nella delicata fase di implementazione e gestione delle nuove tecnologie.

La presente proposta è rivolta a tutte le aziende che hanno l'esigenza di realizzare un efficace sistema di difesa, potendo disporre delle migliori tecnologie e competenze tecniche con tutti i benefici derivanti dalla gestione in outsourcing dell'attività.

Nei capitoli seguenti vengono illustrati l'offerta, la descrizione di dettaglio della proposta dal punto di vista tecnico ed operativo, infine i corrispettivi economici e le condizioni generali del servizio.

Nei capitoli seguenti verranno illustrati:

- l'offerta,
- la descrizione di dettaglio della proposta dal punto di vista tecnico ed operativo,
- le condizioni generali del servizio.

2 ESIGENZE DEL CLIENTE

L'esigenza espressa da **ASL CITTA' DI TORINO** è di dotarsi di una soluzione in grado di:

- raccogliere eventi e log da tecnologie eterogenee
- correlare ed analizzare i dati raccolti
- individuare tempestivamente potenziali minacce che possono pregiudicare:
  - la continuità operativa,
  - l'infrastruttura IT
  - gli asset intellettuali (dati, informazioni, software)
- rispondere in maniera efficace per contrastare le minacce.

Sintetizzando, gli obiettivi di ASL CITTA' DI TORINO possono essere raggiunti attraverso una soluzione che possa garantire:

- Cyber Intelligence, raccolta di log ed eventi da endpoint e loro correlazione.
- Anomaly Detection, analisi volta a rilevare potenziali minacce alla sicurezza.
- Response Automation - Risposta Automatica agli incidenti in grado di bloccare in tempi molto rapidi attacchi sofisticati.
- Remote Incident Response - il supporto remoto da parte di un team di specialisti security per il contrasto delle minacce.

3 I VANTAGGI DELLA SOLUZIONE PROPOSTA

TIM vuole supportare i suoi Clienti nel creare una strategia di security completa, trovando assieme la soluzione migliore in ogni contesto, perché la sicurezza può e deve diventare un fattore abilitante al business.

Il servizio garantisce importanti vantaggi:

- Un **team di specialisti** qualificati a disposizione di ASL CITTA' DI TORINO
- Disponibilità **H24, 7/7** con supporto specialistico in tempo reale fornito da presidio remoto
- Supporto in lingua italiana e **inglese**
- Condivisione dei dati analizzati attraverso un **portale dedicato**
- La piattaforma di sicurezza proposta è costantemente **controllata dal SOC**, che ne garantiscono la disponibilità, l'integrità e la riservatezza.
- **Nessun investimento** in hardware o in software è richiesto al ASL CITTA' DI TORINO. Tutti i dispositivi e le licenze necessarie saranno inclusi nel servizio.
- Assoluta **scalabilità** del servizio in termini di soluzioni tecnologiche che lo costituiscono.
- Tempestività degli **aggiornamenti**. Tutti gli upgrade e le patch software vengono installate ed attivate a cura del SOC che, una volta verificate, le distribuisce a tutti i componenti del servizio. In tal modo è garantito il constante aggiornamento e il massimo livello di protezione offerto dalla soluzione.
- **Unico referente**. L'implementazione, la gestione e il controllo del sistema di sicurezza da parte di un unico fornitore semplificano di molto il supporto e l'individuazione dei problemi e costituiscono un requisito essenziale per garantire un'assistenza tempestiva ed efficace.
- **Reportistica**. Da concordare fra le parti in fase di attivazione, disponibile con tutte le versioni del servizio.

4 DESCRIZIONE DELLA SOLUZIONE

Il servizio proposto:

- ha come obiettivo la raccolta centralizzata degli eventi e dei log, generati da applicazioni e sistemi in rete, per consentire la gestione efficace ed efficiente dei rischi aziendali di sicurezza informatica ma soprattutto intelligente in quanto va personalizzata attraverso regole di correlazione e sistemi di aggiornamento real-time.
- prevede il costante monitoraggio H 24 7/7. La gestione dei log è indispensabile per poter raggiungere gli obbiettivi di conformità con le principali normative di sicurezza (GDPR, PCI DSS, ecc).
- è il punto di raccolta e archiviazione centralizzato dei Log dell'infrastruttura IT, deve assicurare l'integrità, la riservatezza e la disponibilità.
- include:
    - la messa a disposizione dei sistemi di raccolta degli eventi. La proposta **LION® CYBERSECURITY** offre una soluzione completa "chiavi in mano"; tutti gli elementi necessari quali hardware, software, Start-Up, upgrade, backup della configurazione, policy e log, assistenza hardware/software e accesso ai servizi sono inclusi nel contratto.
    - l'attività necessaria alla loro gestione, offrendo vantaggi in termini economici è di performance. La gestione ed il controllo dei sistemi vengono infatti assicurati dal Security Operations Center del Partner di TIM (di seguito SOC). Il SOC controlla e gestisce tutti i sistemi della soluzione, interviene tempestivamente per risolvere eventuali malfunzionamenti delle apparecchiature e garantisce la sicurezza del sistema.

5 IL SERVIZIO LION® CYBERSECURITY (SIEM QRADAR)

LION® Cybersecurity è un servizio specifico per l'analisi degli eventi di sicurezza, che può essere applicato in un contesto multivendor e su ambienti eterogenei (ad esempio: Firewall, Web proxy, Antivirus, Domain Controller, Server Linux, Applicazioni, Database, ecc)

Il servizio viene erogato attraverso il SOC del Partner di TIM composto da specialisti con competenze tecniche qualificate supportati da infrastrutture hardware/software e da processi collaudati (UNI CEI ISO/IEC 20000-1:2012, UNI CEI ISO 27001:2017 e UNI EN ISO 9001:2015) in grado di erogare H24, 7/7 servizi real-time di monitoraggio e analisi degli eventi nel rispetto dei livelli di servizio definiti.

L' interazione fra ASL CITTA' DI TORINO ed il SOC avviene tramite:

- Telefono. Come canale da privilegiare in situazioni di emergenza.
- E-mail. È il canale di gestione del servizio. Da non usare in situazioni di urgenza.
- Sistemi di web collaboration (ticketing). Tutte le attività sono tracciate all'interno del sistema.

Per ovvi motivi di sicurezza, l'interazione con il SOC è disponibile solo a personale identificato di ASL CITTA DI TORINO, che ha funzione di interfaccia fra l'utenza di ASL CITTA DI TORINO e il SOC. Le figure aziendali di ASL CITTA DI TORINO saranno identificate durante la stipula del contratto e prendono il nome di Key User.

All'atto dell'attivazione del Servizio da parte di ASL CITTA' DI TORINO saranno concordati:

- l'Use Case di ASL CITTA' DI TORINO costituito dalla definizione:
  - del dimensionamento e del perimetro della soluzione e
  - delle Politiche di Sicurezza,
- le modalità di intervento in caso di necessità.

- I report di servizio. È inclusa nel servizio la realizzazione di report periodici, generati dall'analisi e tracciamento dei log e dalla correlazione delle informazioni raccolte. Ciò permette di avere a disposizione una chiara e immediata immagine del livello di sicurezza e di poter individuare le aree più vulnerabili.

- Il periodo di archiviazione dei log. Il servizio garantisce l'archiviazione dei dati raccolti per un periodo di tempo concordato; tali dati sono utilizzabili sia per conformità aziendale che per fini legali in caso di audit.

Se richiesto, il ASL CITTA DI TORINO potrà avere a disposizione un'interfaccia per interagire con il sistema centrale di gestione. L'accesso avverrà attraverso una sessione codificata ed autenticata e consentirà di accedere ad una serie di procedure di consultazione del sistema di sicurezza.

Gli specialisti di sicurezza TIM sono in grado di fornire consulenza e supporto sugli specifici eventi di sicurezza rilevati. L'analisi della sicurezza può mettere in correlazione tutte le informazioni provenienti da:

- sistemi infrastrutturali (apparati di rete e/o di sicurezza)
- ambienti sistemistici (data center, ambienti cloud, ecc.)
- end point (tramite soluzioni antivirus o di end point management di ASL CITTA' DI TORINO)
- flussi di traffico (netflow, sflow, ecc.)
- risultati di Vulnerability Assessment
- threat data feeds (informazioni sulle minacce esistenti in Internet)

6 CARATTERISTICHE E FUNZIONALITA'

La principale caratteristica del servizio è di rilevare tempestivamente, e con il massimo delle informazioni disponibili, tutte le minacce che possono avere un impatto sui sistemi e sul business di ASL CITTA' DI TORINO.

Il servizio è composto dall'insieme di tecnologie, processi e persone, organizzati in maniera strutturata al fine di prevenire, rilevare e rispondere rapidamente agli incidenti di sicurezza con le attività di remediation.

In termini di risposta agli incidenti di sicurezza informatica, la "remediation" rappresenta l'insieme delle azioni di contrasto alle minacce o alle violazioni per rispondere nel modo più efficace possibile e limitare la quantità di danni che potrebbero essere potenzialmente arrecati all'organizzazione che si trova sotto attacco.

Le azioni per contrastare le minacce rilevate vengono definite assieme ai Key Users di ASL CITTA DI TORINO.

6.1 TIER

Per rispondere in modo efficiente e aumentare il valore dell'infrastruttura IT dei Clienti, massimizzando gli investimenti di sicurezza già presenti, il servizio è organizzato a tre livelli denominati TIER.

Il ASL CITTA' DI TORINO può scegliere di acquistare i TIER in base alle proprie esigenze e capacità organizzative e di gestione della sicurezza. I TIER di livello superiore richiedono l'acquisto e la configurazione dei TIER di livello inferiore, che sono un prerequisito.

TIER	Caratteristiche	Modello	Dimensionamento
I DETECT	• Raccolta centralizzata • Monitoraggio • Individuazione automatica situazioni anomale	SaaS	EPS + FPM + Data Retention
II ANALYSIS & NOTIFY	• Analisi eventi anomali • Classificazione delle minacce • Notifica al Cliente le attività di remediation	SOC Security Analyst	In base al TIER I
III INCIDENT RESPONSE	• Analisi approfondita • Supporto per la remediation • Incident Response	SOC Security Expert	Prepagato o Servizi Accessori (Managed XDR)

Figura 1 - TIER

6.1.1 TIER I – DETECT - MONITORAGGIO E INDIVIDUAZIONE

Il **TIER I** è basato sulla tecnologia SIEM (Security Information and Event Management). La piattaforma SIEM ha come obiettivo la raccolta centralizzata degli eventi e dei log, generati da applicazioni e sistemi in rete, per consentire agli analisti di sicurezza di ridurrei i tempi necessari per le risoluzioni e le indagini su allarmi e incidenti di sicurezza.
Il **TIER I** svolge le seguenti funzionalità:

- **Raccolta** centralizzata delle informazioni e normalizzazione degli eventi e dei log
- **Monitoraggio,** aggregazione e correlazione degli eventi di sicurezza;
- **Individuazione** automatica di eventuali situazioni anomale; questa fase può includere tecnologie basate su *machine learning* (apprendimento automatico) e intelligenza artificiale per analisi di tipo

comportamentale. Tale analisi usa una baseline dinamicamente costruita per evidenziare possibili anomalie rispetto:
- al comportamento usuale degli utenti (**UBA**, User Behaviour Analytics) o
- al funzionamento usuale dell'infrastruttura di rete (**NBA**, Network Behaviour Analytics).

La soluzione SIEM proposta consente l'implementazione in un ambiente distribuito e completamente scalabile.

In una singola piattaforma il **TIER I** fornisce:
- **Threat Management:** rilevamento delle minacce. Realizzato attraverso la correlazione dei dati di sicurezza di rete e dei sistemi.
- **Log Management:** raccolta, analisi e archiviazione dei log. Viene usato per generare report degli eventi di sicurezza e consentire alle organizzazioni di proteggersi da minacce, attacchi e violazioni.
- **Conformità:** reportistica completa degli eventi per la conformità con diversi standard (GDPR, ISO27001, SOX, PCI, ecc).

Per garantire il servizio e la sua continuità operativa, all'interno **TIER I**, sono inclusi i seguenti componenti:
- **La messa a disposizione** dei componenti software e hardware (se previsti)**.** I componenti saranno messi a disposizione di ASL CITTA DI TORINO per tutta la durata del contratto.
- **Start-Up – Attivazione dell'infrastruttura.** Lo Startup del TIER I comprende le fasi propedeutiche all'attivazione dei servizi LION® Cybersecurity ed è composto da diverse attività che devono essere implementate in collaborazione con il ASL CITTA DI TORINO. Per la descrizione dettagliata delle attività si rimanda al capitolo 8, Start-Up del Servizio
- **Monitoraggio Proattivo.** Il servizio prevede la gestione da remoto dei suoi componenti e degli asset collegati per monitorare e tenerne sotto controllo il corretto funzionamento. La componente prevede: controllo remoto, gestione asset e inventario, monitoraggio, sicurezza, gestione delle policy. Il servizio viene erogato garantendo massima sicurezza dei dati in quanto è gestito attraverso canali cifrati, protetti e utilizza connessioni sicure.
- **Manutenzione software.** Il servizio include l'aggiornamento periodico dei suoi componenti in termini di nuovi release, patch e fix.
- **Supporto tecnico** remoto per la gestione di:
  - **Incident Management**. L'obiettivo del processo di Incident Management è quello di ripristinare il funzionamento del servizio nel più breve tempo possibile, riducendo al minimo gli impatti sui processi correlati. Ai fini del presente documento si intende per "incident IT" un evento, o una sequenza di eventi, che coinvolge i componenti del servizio LION in modo tale da causare un'interruzione non pianificata o una riduzione della qualità del servizio (definizione di IT Incident prevista dall'ITIL).
  - **Service Request**. L'obiettivo del processo di Service Request è quello di soddisfare le esigenze di ASL CITTA DI TORINO nel perimetro del Servizio Lion. Ai fini del presente documento il termine "Service Request" (SR o Richiesta di Servizio) è utilizzato come generica descrizione per differenti tipi di richieste. Si tratta in generale di richieste legate a piccoli cambiamenti che sono a basso rischio e basso impatto, di richieste di servizi standard (esempio: nuove funzionalità) o di richieste di informazioni.
  - **Change Management**. Una Change è la modifica (creazione, aggiornamento, eliminazione) di qualsiasi componente del servizio LION che potrebbe avere un effetto, diretto o indiretto, su servizio stesso o altri servizi IT di ASL CITTA DI TORINO. L'obiettivo del processo di Change Management è di assicurarsi che attraverso l'utilizzino di procedure e metodi standardizzati, una gestione efficiente ed efficace di tutti i cambiamenti del servizio LION, sia minimizzato l'impatto delle Change sul servizio stesso e/o sui servizi IT di ASL CITTA DI TORINO.

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

Le attività di gestione del **TIER I** saranno svolte da remoto.

Tutte le attività di gestione del **TIER I** saranno erogate durante Normale Orario di Lavoro. Eventuali necessità da parte di ASL CITTA' DI TORINO di conduzione attività fuori Normale Orario di Lavoro verranno concordate preventivamente

Se non diversamente indicato nel presente documento per Normale Orario di Lavoro si intende la giornata lavorativa feriale dalle 8.30 alle 18.30

I componenti del **TIER I** sono forniti in modalità **"as a Service"** e possono essere attivati in due diverse modalità:

- **Modalità Cloud:** la soluzione SIEM è installata nel Datacenter . Presso la sede di ASL CITTA DI TORINO viene installata un'applicane (virtuale o fisica) che raccoglie gli eventi e/o i flussi di rete e invia le informazioni tramite una VPN alla console SIEM nel Datacenter. L'ambiente permette la raccolta completamente separata dei dati dei singoli Clienti.

In termini di affidabilità e sicurezza vengono garantite al ASL CITTA' DI TORINO:

- ✓ **Alta affidabilità:** il sistema dispone di più nodi hardware con la sincronizzazione automatica dei dati, garantendo così la ripartenza automatica in caso di fail di uno dei nodi.
- ✓ **Backup completo a più livelli:** Tutte le Politiche di Sicurezza implementate nel sistema SIEM centralizzato sono scrupolosamente salvate attraverso il backup periodico. Le policy di backup includono il salvataggio giornaliero della configurazione della console e del tenant ASL CITTA' DI TORINO, di tutte le appliance del servizio e dei dati di log raccolti.
- ✓ **Continuità operativa:** il Datacenter è distribuito su due siti primari geografici; le sale sono provviste di sistemi anti incendio e alimentazione ridondata.
- ✓ **Disaster recovery:** più copie di backup dell'infrastruttura dedicata al servizio sono spostate ogni giorno in un sito secondario attrezzato con l'hardware necessario alla ripartenza nel caso in cui un evento disastroso accada nei siti primari.
- ✓ **Massima sicurezza dei dati:** i locali del Datacenter sono sorvegliati **H24, 7/7**; l'accesso è monitorato, tracciato e consentito solo al personale autorizzato. Tutti i log di accesso sono archiviati nel rispetto della normativa sulla protezione dei Dati Personali (Garante).
- ✓ **Sale operative ridondate:** il SOC è distribuito su due siti, a Noventa Padovana e Besana in Brianza, entrambe le sedi sono operative **H24, 7/7** e previste di connettività ridondata.
- ✓ **Scalabilità elevata:** la piattaforma SIEM è configurata in modalità distribuita in ambiente virtuale; ogni componente è:
  - installato su un'appliance dedicato alla sua funzione: console (gestione), event e flow processor (normalizzazione e correlazione), app node (machine learning) e
  - collegato ad un sistema ridondato per l'archiviazione dei dati offline.

- **Modalità On Premise:** la soluzione SIEM, completa di tutte le sue componenti, è installata presso il Datacenter di ASL CITTA DI TORINO. Il Team SOC del Partner di TIM deve avere accesso **H24, 7/7** alla console di gestione della piattaforma per eseguire le attività di gestione, manutenzione e supporto.

6.1.2 TIER II – ANALYSIS & NOTIFY - ANALISI E NOTIFICA

Il servizio LION Cyber Security prevede non solo la componente infrastrutturale di raccolta degli eventi e dei log, descritta in precedenza come **TIER I**, ma anche la struttura operativa che analizza ogni singolo alert segnalato dal **TIER I** o da altre fonti con cui può essere correlato.

In questo caso si riferisce alla struttura operativa come **TIER II** e il suo obbiettivo principale è quello di **gestire gli eventi di sicurezza** rilevati. Il **TIER II** consente al ASL CITTA' DI TORINO di avere a disposizione un team di esperti di sicurezza che effettua attività di analisi e reportistica degli eventi di sicurezza con copertura **H24, 7/7**.

Il **TIER II** include le seguenti funzionalità:

•**Analisi** da parte del Team SOC degli eventi anomali per individuare le minacce e definire le remediation.

•**Classificazione** delle minacce in base a un livello di severità, preventivamente concordato con il ASL CITTA' DI TORINO.

•**Segnalazione** ai Key User di ASL CITTA' DI TORINO delle minacce rilevate con le indicazioni per la remediation.

Gli analisti del SOC **TIER II** rilevano tempestivamente gli eventi anomali, li analizzano e forniscono al ASL CITTA' DI TORINO le indicazioni precise per poter:

- rispondere in maniera mirata,
- contenere eventuali attacchi e
- minimizzare l'impatto sul business.

1.

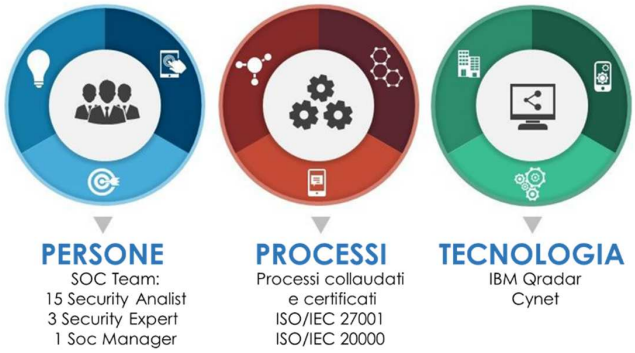

Figura 2 - Servizio Cyber Security e i suoi componenti

I componenti del **TIER II**: il TEAM SOC e il SOC Manager, i processi e la matrice di responsabilità sono descritti nella presente offerta più avanti.

Le attività incluse nel **TIER II** sono erogate con un canone opportunamente dimensionato rispetto ai sistemi oggetto del servizio e alle esigenze di ASL CITTA' DI TORINO. Il canone include tutte le attività necessarie per svolgere le funzionalità descritte.

6.1.3 TIER III – Incident Response - Risposta agli incidenti

Il **TIER III** ha come obbiettivo **il supporto al ASL CITTA DI TORINO, con l'intervento** remoto per il **contrasto** alle minacce. Le modalità di intervento dovranno essere preventivamente concordate.

Gli esperti del SOC potranno intervenire in varie modalità:

•**In affiancamento** al team di ASL CITTA' DI TORINO, in costante comunicazione durante gli incidenti di sicurezza, verranno elaborate, concordate e attivate le remediation.

•**Con intervento remoto** da parte del team SOC nei sistemi di security di ASL CITTA' DI TORINO, come firewall, web application firewall, proxy, web filter, intrusion prevention o simili per ulteriori analisi approfondite e applicare le remediation concordate nel più breve tempo possibile.

•Con il supporto di **uno o più servizi accessori**, come ad esempio **il Managed Endpoint Detection & Response** (non incluso nella presente offerta) è possibile sviluppare ulteriori attività, come:

- il Threat Hunting (ricerca proattiva e iterativa per rilevare e isolare minacce avanzate che possono sfuggire alle soluzioni di sicurezza esistenti) e
- l'intervento tempestivo del Team SOC nelle attività di remediation nei sistemi server e/o workstation.

Le modalità di intervento del **TIER III** potranno essere multiple, combinate o includere ulteriori servizi accessori.

Le attività dal **TIER III** "In affiancamento" e/o "Con intervento remoto" potranno essere erogate attraverso un monte ore prepagato di validità annuale, opportunamente dimensionato rispetto ai sistemi oggetto del servizio e alle esigenze di ASL CITTA DI TORINO.

Per eventuali servizi accessori a supporto del **TIER III** si rimanda all'offerta del rispettivo servizio e al canone afferente.

6.2 Il Team SOC

Il Team SOC è composto da esperti e analisti di sicurezza informatica, con competenze tecniche qualificate, organizzati in turni per erogare il servizio in **H24, 7/7**. I professionisti, dotati di certificazioni nell'ambito Cyber Security e con il supporto di tecnologie specifiche del servizio sono in grado di rilevare gli eventi anomali e indicare al ASL CITTA DI TORINO o avviare congiuntamente le azioni necessarie per minimizzare l'impatto negativo di tali eventi con l'obbiettivo di restaurare la normale operatività di ASL CITTA DI TORINO nel più breve tempo possibile. Il team SOC è organizzato in 3 livelli che svolgono le loro attività come illustrato nella seguente tabella:

TIER	Livello Team SOC	Attività del Team	Report* in carico al Team SOC
I	1°	• **Monitoraggio e gestione** delle piattaforme del servizio.	• Configuration Report • Change Management Report
II	1°	• **Monitoraggio proattivo** degli eventi di sicurezza e **identificazione** delle anomalie. • **Classificazione** degli eventi di sicurezza • Implementazione **Use Case.**	• Configuration Report review • Change Management Report • Supporto per implementazione dell'**Audit & Compliance Report**
	2°	• **Analisi** degli eventi di sicurezza. • **Gestione** iniziale degli eventi di sicurezza	• Security Report

		• L'elaborazione della **remediation e comunicazione** al ASL CITTA DI TORINO. • Supporto al ASL CITTA DI TORINO per la definizione iniziale e il review periodico dell'**Use Case**	• Supporto per la stesura dell'**Executive Report**
III	3°	• **Analisi approfondita** degli eventi di sicurezza. • Coordinamento e/o **gestione** remota delle attività di **remediation**.	• Incident Report • Supporto per la stesura dell'**Executive Report**

Tabella 1- Team SOC- Attività e Report

*il contenuto dei Report è descritto più avanti nella presente offerta, cap. 6.6 Report di Servizio.

6.3 Matrice attività e assegnazione responsabilità.

Nella seguente tabella sono messe in relazione le attività da svolgere del servizio con le relative entità coinvolte usando la matrice RACI, dove:

R – Responsible: è colui che esegue ed assegna l'attività

A - Accountable: è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato.

C - Consulted: è la persona che aiuta e collabora con il Responsible per l'esecuzione dell'attività

I - Informed: è colui che deve essere informato al momento dell'esecuzione dell'attività

Attività	TIM	ASL CITTA' DI TORINO
Definizione contatti e modalità di comunicazione	R	R/A
Definizione policy di sicurezza e attivazione VPN tra DTC del Partner di TIM e DTC ASL CITTA DI TORINO	R	R/A
Installazione e configurazione event collector e/o flow collector (virtuale o fisico)	R/A	R
Configurazione sistemi e account con i permessi necessari per l'invio eventi/flussi all'event/flow collector, installazione agent nei sistemi ASL CITTA DI TORINO	C/I	R/A
Integrazione sorgenti ASL CITTA DI TORINO con il SIEM	R/A	C/I
Definizione Use Case ASL CITTA DI TORINO (l'insieme delle politiche di sicurezza, analisi eventi, regole di correlazione e classificazione severità e incidenti)	R	R/A
Definizione regole di escalation tra SOC e le strutture di ASL CITTA DI TORINO	R	R/A
Definizione destinatari report	C	R/A
TIER I, Gestione infrastruttura di monitoraggio*	R/A	I
TIER II, Rilevazione anomalie, analisi e notifica*	R/A	I/C
TIER III, Gestione incidenti*	R	R/A

Tabella 2- Attività di Servizio e Responsabilità

*vedi paragrafo successivo, 6.4 Processi.

6.4 Processi

I processi del servizio sono strutturati in base all'input, al TIER di appartenenza e alla responsabilità di ciascuna delle parti coinvolte nel processo.

Il processo del **TIER I** si attiva per la gestione dell'infrastruttura SIEM e dei suoi componenti, segue le normali procedure di gestione di tipo infrastrutturale ed è organizzato su base ITIL come descritto nel paragrafo TIER I.

I processi dei **TIER II** e **TIER III** hanno come obbiettivo la gestione degli eventi di sicurezza, si possono attivare in base agli input, che costituiscono regole di ingaggio e sono descritti di seguito:

a. **Input: da SOC del Partner TIM.**

Il processo si attiva ogni qualvolta il SOC riceve dai sistemi in sua gestione un allarme oggetto del contratto.

b. **Input: da ASL CITTA' DI TORINO**

Il processo si attiva ogni qualvolta il SOC riceve l'apertura di un Ticket di sicurezza da parte di ASL CITTA' DI TORINO a fronte di un problema rilevato dal ASL CITTA' DI TORINO stesso.

Il flusso di lavoro del processo è il indicato nella seguente tabella con riportata la Matrice di Responsabilità del Processo (solo per i TIER II e TIER III)

Step	Descrizione Attività	INPUT	GESTIONE	TIER	SOC Partner TIM	ASL CITTA' DI TORINO
1	Apertura Ticket	a) SOC	**SOC**	**II**	R	I/C
		b) ASL CITTA DI TORINO		**II**	I/C	R
2	Presa in carico Ticket dal SOC, identificazione e classificazione	Ticket	**SOC**	**II**	R	I
3	Analisi e Notifica	Escalation Interna	**SOC**	**II**	R/A	I/C
4	Remediation	a) ASL CITTA DI TORINO	**ASL CITTA DI TORINO**	**II**	I/C	R/A
		b) SOC	**SOC**	**II/III**	R	R/A
5	Chiusura Ticket	ASL CITTA DI TORINO	**SOC**	**II**	R	I/C

Tabella 3- Processo e responsabilità TIER II e III

Il dettaglio delle attività incluse nel processo è descritto di seguito:

- **Step 1 e 2: Apertura del ticket e classificazione**
  a) da parte del SOC per segnalare la presa in carico dell'allarme ricevuto dai sistemi in gestione al SOC, informando il ASL CITTA' DI TORINO della severità definita.

b) da parte di ASL CITTA' DI TORINO a fronte di un problema rilevato dal ASL CITTA' DI TORINO stesso, informando il SOC anche della severità definita. Il SOC procede alla verifica e identificazione del problema.

- **Step 3:** Il SOC del Partner di TIM esegue **l'analisi della minaccia**, individua e **comunicata** al ASL CITTA' DI TORINO la **strategia di remediation**
- **Step 4:** Attuazione della remediation:
  a) Da parte di **ASL CITTA' DI TORINO**: nel caso di sistemi in gestione di ASL CITTA' DI TORINO.
  b) Da parte del **team SOC**:
    i. **TIER II**: Nel caso di sistemi in **gestione o servizi erogati dal Partner di TIM** (es. sistemi di security come firewall), il SOC **informa** il ASL CITTA' DI TORINO della remediation e dopo aver concordato l'attività con il ASL CITTA' DI TORINO, procede all'implementazione.
    ii. **TIER III**: qualora **il ASL CITTA' DI TORINO ha acquistato il TIER III** e sono state concordate preventivamente la modalità di intervento e di accesso ai rispettivi sistemi.
- **Step 5:** Confermato l'esito dell'azione di Remediation da parte di ASL CITTA' DI TORINO, il SOC procede alla **chiusura del ticket.**

Il workflow del Processo è illustrato nella seguente figura:

Figura 3 – Processi

7 START-UP DEL SERVIZIO

Il processo di Start-up è incluso nel servizio e comprende le fasi propedeutiche all'attivazione del servizio ed è composto da diverse attività che devono essere implementate in collaborazione col ASL CITTA' DI TORINO.

A tal fine, il ASL CITTA' DI TORINO si impegna sin d'ora a garantire la disponibilità del proprio personale (ivi incluso quello degli eventuali fornitori) in misura idonea ed adeguata per poter procedere, in modo puntuale e nei tempi a questo necessari, al trasferimento al personale Partner di TIM delle competenze e del know-how necessario alla corretta implementazione ed erogazione del servizio.

Le fasi principali dello Start-Up sono:

- Incontro preliminare e pianificazione;
- Installazione componenti del servizio;
- Collaudo (User Acceptance Test)
- Kickoff
- Attivazione del Servizio

Il processo può in parte variare in base alla tipologia o TIER di servizio attivato, ma le principali fasi operative sono le medesime.

Incontro preliminare e pianificazione

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

Al ricevimento dell'ordine, il team SOC del Partner di TIM contatterà il ASL CITTA' DI TORINO per pianificare l'avvio del processo di Start-Up. Gli argomenti trattati comprenderanno i seguenti task inseriti in un documento di piano lavori che riguarderà l'intero processo di Start-Up:

- Condivisione del piano di attivazione del servizio che comprende la pianificazione dell'installazione dei suoi componenti e della VPN tra l'infrastruttura di ASL CITTA' DI TORINO e il Datacenter. A tal fine verrà consegnata e illustrata al ASL CITTA' DI TORINO una Checklist riepilogativa di tutte le informazioni tecniche necessarie per l'attivazione e l'installazione dei componenti del servizio.
- Definizione asset: il ASL CITTA' DI TORINO dovrà fornire l'elenco dei sistemi aziendali oggetti del servizio. Nell'elenco dovranno essere evidenziati i sistemi ritenuti critici o importanti per il business con il maggior numero di informazioni possibili (es. modello, ubicazione, IP address, note operative, etc.).
- Mappa infrastruttura di rete: il ASL CITTA' DI TORINO dovrà fornire una mappa dell'infrastruttura fisica e logica con riportati i link tra gli apparati di rete e quelli di sicurezza e di computing. Nel caso in cui questa non fosse presente, il ASL CITTA' DI TORINO dovrà rendersi disponibile nel supportare il SOC nella costruzione della stessa.
- Contatti: durante l'incontro il team SOC presenterà al ASL CITTA' DI TORINO le diverse modalità con cui contattare il SOC. Il ASL CITTA' DI TORINO dovrà altresì fornire i contatti aziendali che saranno i riferimenti per il SOC (Key User). Inoltre, nel caso in cui il ASL CITTA' DI TORINO affidi al SOC anche l'attività di escalation verso le terze parti (es. ISP), in questa occasione fornirà anche i riferimenti dei loro partner ed i relativi numeri di contratto.
- Definizione delle policy di sicurezza e distribuzione agent: saranno concordati i protocolli del collegamento VPN, i canali e i protocolli di comunicazione sicura per la raccolta dei log, l'invio degli eventi e per le comunicazioni di servizio. Sarà messo a disposizione di ASL CITTA' DI TORINO il software (agent) con i parametri necessari per la distribuzione sui sistemi supportati.
- Discussione di eventuali criticità e definizione dei livelli di severità: il ASL CITTA' DI TORINO dovrà rendersi disponibile per valutare le eventuali criticità dei suoi asset e della sua infrastruttura, sia in termini strategici che operativi. Tali informazioni sono di massima importanza per dare la giusta rilevanza ai problemi che si dovessero presentare durante l'erogazione del servizio e consentono di definire i livelli di severità che, dopo essere stati concordati con il ASL CITTA' DI TORINO, saranno assegnati agli eventi di sicurezza rilevati durante il servizio.
- Definizione dell' Use Case: Una volta raccolte tutte le informazioni necessarie, gli esperti di sicurezza del team SOC supporteranno il ASL CITTA' DI TORINO nella definizione e mappatura delle sorgenti log e eventi, delle Politiche di Sicurezza e delle regole di correlazione. Tutte le Politiche di Sicurezza decise dal ASL CITTA' DI TORINO verranno dallo stesso sottoscritte e costituiranno l'esatta analisi di quanto verrà implementato. Le eventuali variazioni alla struttura inizialmente implementata subiranno il medesimo iter.
- Definizione delle modalità di intervento in risposta alle minacce. Tutti gli aspetti legati alle modalità di intervento, incluse le regole d'ingaggio, verranno concordate e documentate. Eventuali asset di security con le rispettive credenziali e i rispettivi livelli di accesso, a cui il team SOC potrà accedere saranno definiti in questa sezione.

Installazione componenti del servizio e implementazione Use Case

Dopo l'incontro preliminare verranno installati i componenti del servizio presso la sede di ASL CITTA' DI TORINO. Per poter eseguire tale attività, il ASL CITTA' DI TORINO dovrà aver compilato il documento di Checklist precedentemente condiviso. Verrà configurata la VPN tra l'infrastruttura di ASL CITTA' DI TORINO ed il Cloud e verrà avviata l'implementazione dell'Use Case.

User Acceptance - Collaudo

Completata l'installazione dei componenti e la configurazione secondo le specifiche concordate nell'ambito dell'Use Case, il team SOC effettuerà il collaudo del servizio. Tutta documentazione sulla configurazione del servizio, la Checklist, le policy e la configurazione dell'Use Case e i risultati del collaudo saranno verbalizzati

in un unico documento con il titolo di User Acceptance Test (Verbale di Collaudo) che sarà consegnato al ASL CITTA' DI TORINO durante la riunione di Kick-Off.

Kick-Off del servizio

Non appena tutte le precedenti fasi verranno portate a termine, il Team SOC del Partner di TIM incontrerà il ASL CITTA' DI TORINO per ufficializzare il completamento delle attività di configurazione, la messa a regime dei servizi acquistati e il rilascio di User Acceptance Test che sarà sottoscritto da entrambe le parti.

Attivazione del servizio

Concluse le attività precedentemente illustrate, viene comunicata al ASL CITTA' DI TORINO l'attivazione del servizio.

Da questo momento, il servizio entra nel cosiddetto periodo di tuning (vedi sotto la voce "Grace Period"), durante il quale viene completata l'eventuale messa a punto dei servizi attivati.

Grace Period

Si definisce Grace Period, un periodo temporale di **3 mesi successivi alla messa a regime** che prevede il "fine tuning" (sintonizzazione accurata) del servizio. L'obbiettivo principale di questo periodo è di verificare e validare l'efficacia dell'Use Case, di tutte le procedure di presa in carico delle richieste di intervento e di eventuale escalation verso terze parti. In questo periodo il servizio viene erogato in modo completo, i SLA vengono monitorati, ma un eventuale non raggiungimento dei livelli di servizio contrattualizzati non determinerà inadempimento o penali nei confronti di TIM.

8 REQUISITI DELL'APPLIANCE

Il ASL CITTA' DI TORINO dovrà mettere a disposizione le risorse computazionali e di spazio necessarie all'appliance che ha il ruolo di collector e processor degli eventi.

Requisiti dell'appliance che dovrà essere installata presso l'infrastruttura di ASL CITTA' DI TORINO:

Descrizione	vCPU	vRAM	vSDD
EVENT PROCESSOR	16	24 GB	1TB

L' SDD Data Transfer Rate minimo.: 500 MB/s, raccomandato 1000 MB/s

9 PERIODO DI CONSERVAZIONE DEI LOG

Gli eventi di sicurezza raccolti dalla soluzione SIEM e salvati nel Cloud vengono mantenuti in due modalità:

On-line: i dati si trovano all'interno della piattaforma SIEM e direttamente accessibili dalla console; questa modalità consente al sistema la correlazione e l'analisi degli eventi in tempo reale con l'obbiettivo di individuare tempestivamente eventi anomali.

Off-line: i dati sono archiviati in modalità sicura su un supporto esterno alla piattaforma SIEM. I dati sono accessibili per un'eventuale analisi, audit o report di conformità solo dopo un ripristino degli stessi nella console. I tempi di ripristino possono variare in base alla quantità di giorni (dati) richiesti e saranno messi a disposizione con il rispetto del livello di servizio concordati.

Gli eventi di sicurezza sono mantenuti per un periodo temporale come da Tabella 9:

Modalità di conservazione dei Log	Periodo Temporale
On-line	1 mese
Off-line	12 mesi

Tabella 4 -Periodo Temporale di conservazione

10 IL SERVIZIO TIER III - MANAGED XDR E THREAT HUNTING (CYNET)

Il panorama della Sicurezza nell'ambito Information Technology è profondamente mutato negli ultimi anni, acquisendo una maggiore consapevolezza del rischio e della necessità di adeguate misure di sicurezza.

Un approccio tradizionale non è più ritenuto sufficiente.

Le piattaforme di protezione dei sistemi (End Point Prevention - EPP), tradizionalmente chiamate anche Antivirus e normalmente presenti all'interno delle infrastrutture aziendali, monitorano le minacce conosciute come i malware tradizionali.

Tali piattaforme contrastano anche i virus sconosciuti, i quali possono utilizzare, ad esempio, una nuova forma di un virus/malware già conosciuto in precedenza. Si tratta di sistemi che proteggono in maniera eccellente da minacce conosciute e solo in parte da quelle sconosciute.

In ogni caso, le tecniche del cybercrimine si sono evolute negli ultimi anni ed i cybercriminali sono diventati sempre più sofisticati nelle loro procedure di attacco.

La combinazione di minacce comuni, caratteristiche particolari di certi malware e attività basate su tecniche di infiltrazione complesse da parte dei cybercriminali, fanno sì che minacce generiche possono mutare in attacchi mirati diventando così estremamente pericolose per un'azienda che si affida unicamente alle tecniche tradizionali di Sicurezza IT.

Il servizio è rivolto a tutte le aziende che hanno l'esigenza di realizzare un efficace sistema di difesa, potendo disporre delle migliori tecnologie e competenze tecniche con tutti i benefici derivanti dalla gestione in outsourcing dell'attività.

L'obiettivo della presente proposta è di mettere a disposizione di ASL CITTA' DI TORINO l'esperienza in ambito Cyber Security del Partner di TIM e fornire una soluzione gestita di Extended Detection and Response (Managed XDR o MDR) ad integrazione delle soluzioni di protezione tradizionale, per il monitoraggio in tempo reale delle minacce, focalizzata sull'analisi dei dati e sulla risposta agli incident, per offrire una visibilità end-to-end dell'attività di ogni endpoint dell'infrastruttura aziendale.

10.1 I vantaggi del Servizio

La piattaforma di XDR gestita del Partner di TIM utilizza Cynet 360 per offrire funzionalità di monitoraggio e controllo del perimetro, prevenzione e rilevamento delle minacce e orchestrazione della risposta come illustrato nella seguente figura.

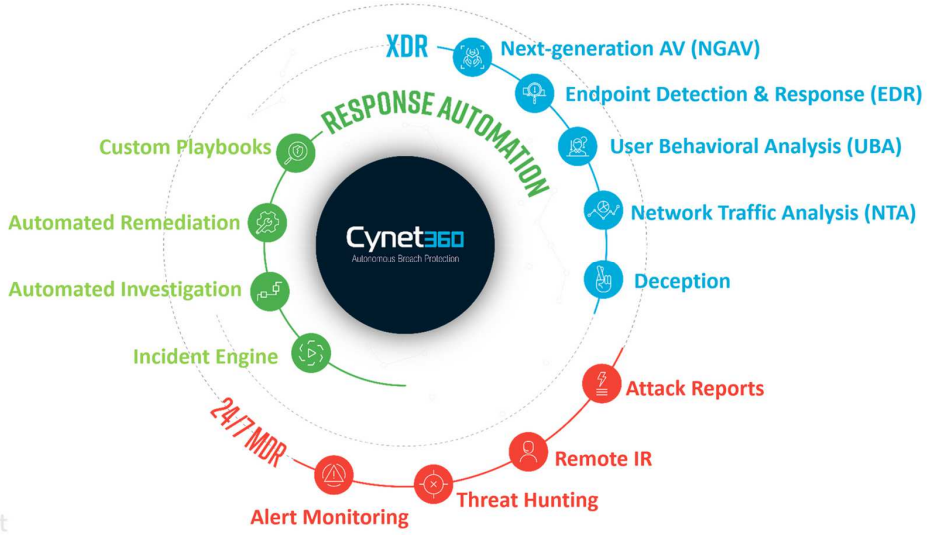

Figura 4 - Cynet 360

La piattaforma di prevenzione e rilevamento raccoglie, combina e analizza costantemente le attività di endpoint, rete e utenti, raggiungendo un livello di prevenzione e rilevamento che, altrimenti, solo varie tecnologie di sicurezza unite riescono a fornire.

Il servizio ha come obiettivo la gestione centralizzata della sicurezza degli endpoint, per consentire la gestione dei rischi aziendali legati alla sicurezza informatica in maniera efficace ed efficiente, ma soprattutto intelligente e sistemi di aggiornamento real-time. Il servizio prevede il costante monitoraggio H 24 7/7.

Sono incluse nel servizio la fornitura della piattaforma e l'attività necessaria alla sua gestione, offrendo vantaggi sia in termini economici che di performance. La gestione ed il controllo dei sistemi vengono infatti assicurati dal Security Operations Center del Partner di TIM (di seguito SOC). Il SOC controlla e gestisce tutti i sistemi della soluzione, interviene tempestivamente per risolvere eventuali malfunzionamenti e garantisce la sicurezza del sistema.

La proposta **LION® CYBERSECURITY – Manager XDR** offre una soluzione completa "chiavi in mano"; tutti gli elementi necessari quali software, Start-Up, management, upgrade, backup della configurazione, policy e log, assistenza software e accesso ai servizi sono inclusi nel contratto.

Sono incluse nel servizio:

- Messa a disposizione della tecnologia per tutta la durata del servizio
- Un **team di specialisti** qualificati a disposizione di ASL CITTA' DI TORINO
- Gestione della piattaforma dedicata al ASL CITTA' DI TORINO (Tenant)
- Disponibilità **H24, 7/7** con supporto remoto specialistico in tempo reale.
- il controllo costante della piattaforma e relativi eventi critici da parte del SOC.
- Supporto in lingua italiana ed **inglese**

- un **portale dedicato** alla condivisione dei dati analizzati.
- **Nessun investimento iniziale**! I dispositivi e le licenze sono inclusi nel servizio.
- **Scalabilità:** il servizio segue le esigenze di crescita o modifiche della vostra Azienda.
- **Aggiornamenti**: il SOC si occuperà di installare gli upgrade e le patch software che verranno distribuite a tutti gli componenti del servizio.
- **Unico referente**: il SOC avrà la gestione e il controllo del sistema di sicurezza facendo risparmiare tempo al Vostro IT.
- **Reportistica**: concorderemo assieme un livello personalizzato di reportistica.

11 IL SERVIZIO LION CYBERSECURITY - MANAGED XDR (CYNET)

LION® Cybersecurity Managed XDR è un servizio specifico per la gestione degli eventi di sicurezza degli endpoint.

Il servizio viene erogato attraverso il SOC del Partner di TIM composto da specialisti con competenze tecniche qualificate supportati da infrastrutture hardware/software e da processi collaudati (UNI CEI ISO/IEC 20000-1:2012, UNI CEI ISO 27001:2017 e UNI EN ISO 9001:2015) in grado di erogare **H24, 7/7** servizi real-time di monitoraggio e analisi degli eventi nel rispetto dei livelli di servizio definiti.

L' interazione fra il ASL CITTA' DI TORINO ed il SOC avviene tramite:

- Telefono. Come canale da privilegiare in situazioni di emergenza.
- E-mail. È il canale di gestione del servizio. Da non usare in situazioni di urgenza.
- Sistemi di web collaboration (ticketing). Tutte le attività sono tracciate all'interno del sistema.

L'accesso diretto al servizio SOC è disponibile solo a personale identificato di ASL CITTA' DI TORINO, che ha funzione di interfaccia fra l'utenza di ASL CITTA' DI TORINO e il SOC. Le figure aziendali di ASL CITTA' DI TORINO saranno identificate durante la stipula del contratto e prendono il nome di Key User.

Il servizio eroga non solo la componente infrastrutturale gestione della sicurezza degli endpoint, ma anche la struttura operativa (Security Operation Center) che analizza ogni singolo alert segnalato dalla piattaforma.

Brevemente, sono incluse nel servizio:

- la messa a disposizione dei componenti software per tutta la durata del contratto.
- il monitoraggio dei sistemi oggetto del contratto
- il supporto tecnico e
- l'attività necessaria alla sua gestione,

offrendo vantaggi sia in termini economici che di performance.

Nella seguente tabella abbiamo riepilogato i componenti del servizio:

Descrizione	Servizio
Messa a disposizione dei componenti software e delle licenze necessarie per tutta la durata del servizio	Sì
Accesso al SOC per supporto tecnico e gestione ticket	Sì
Servizio di Startup Base (attivazione, configurazione e installazione delle componenti software e dell'agent)	Sì
Startup Advanced*	OPZIONALE
Monitoraggio proattivo dell'infrastruttura	Sì

Manutenzione software: Aggiornamento del software, dell'agent e del tenant (Console)	Sì
Supporto tecnico remoto per la gestione di Service Request e Change Management.	Sì
Supporto per la gestione degli incidenti (Incident Management)	Sì

Tabella 5 - Managed XDR

*Es: rimozione del precedente EDR, Antivirus, ecc.

11.1 Funzionalità

La piattaforma gestita XDR in proposizione si avvale delle seguenti caratteristiche:

XDR – Extended Detection & Response e integra le seguenti funzionalità:

- ✓ **Endpoint Protection**: Protezione multilivello contro malware, ransomware, exploits e attacchi fileless (Next Generation Antivirus). Funzionalità che consente la coesistenza e la compatibilità con soluzioni Antivirus tradizionali, es. Symantec, Sophos, McAfee, ecc.
- ✓ **Network Protection:** Protezione contro gli scan, attacchi MitM, movimenti laterali e data exflitration (Network Traffic Analysis)
- ✓ **User Protection:** Regole di comportamento preimpostate (o User Beahavioral Analytics) insieme alla profilazione dinamica del comportamento per rilevare anomalie dannose
- ✓ **Deception:** Trappole di tipo file, sistemi, account utente e connessioni di rete per attirare e rilevare aggressori sofisticati

Response Automation - risposta automatica agli incident e integra le seguenti funzionalità:

- ✓ **Investigation:** Analisi automatizzata delle cause e dell'impatto
- ✓ **Remediation:** Elimina le attività malevoli e gli attacchi contro utenti, rete o end point
- ✓ **Playbooks:** Automatizza le risposte attraverso l'intera infrastruttura per qualsiasi scenario di attacco.
- ✓ **Incident View:** Layout grafico intuitivo per comprendere lo stato dell'attacco e delle azioni di risposta automatizzate

Management – Gestione della piattaforma XD e integra le seguenti funzionalità:

- ✓ **Alert Monitoring:** Notifica tempestiva degli eventi critici

- ✓ **Proactive Threat Hunting:** Ricerca di artefatti dannosi e IoC nell'ambiente di ASL CITTA' DI TORINO.
- ✓ **Incident Response:** Assistenza remota per bloccare e rimuovere le attività malevoli
- ✓ **Attacks Investigation:** Report dettagliato con l'analisi dell'attacco subito dal ASL CITTA' DI TORINO

La piattaforma si integra con eventuali soluzioni di sicurezza già presenti nell'infrastruttura di ASL CITTA' DI TORINO, come i sistemi di monitoraggio della sicurezza di tipo Security Information and Event Management (SIEM) a cui possono essere inviate le informazioni e gli eventi rilevati dagli endpoint.

11.2 Schema architetturale della soluzione

Il funzionamento della componente tecnologica è illustrato nella seguente figura:

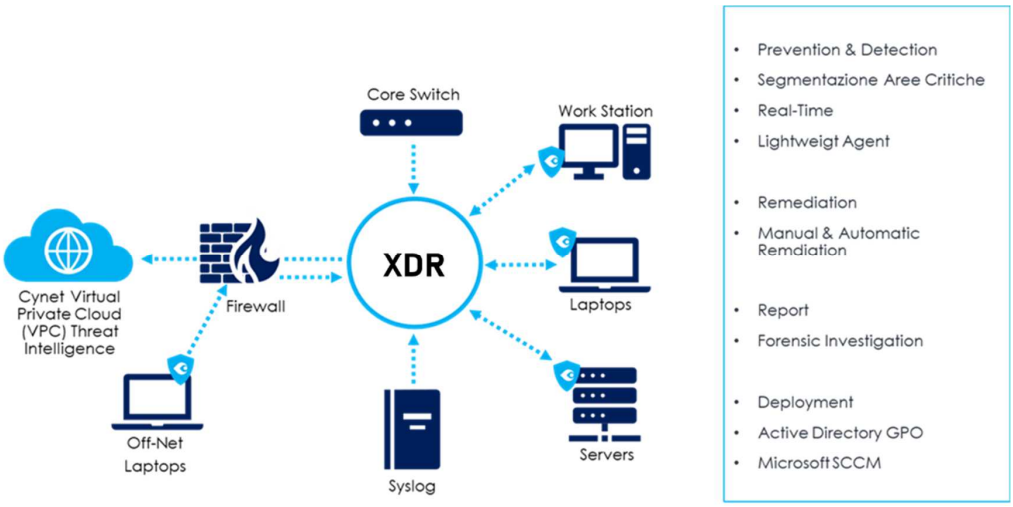

Figura 5 - Architettura Soluzione

La soluzione proposta è completamente cloud-based, così da permettere l'archiviazione di grandi quantità di dati che vengono aggregati, elaborati e analizzati in tempi molto rapidi e senza interruzioni, mentre, sui dispositivi endpoint (laptop, workstation e server) è prevista l'installazione di un agent.

La componente tecnologica viene erogata dal datacenter Private Cloud Cynet con sede nell'Unione Europea che garantisce il rispetto della normativa GDPR ed è certificato nell'ambito sicurezza CEI ISO 27001:2017 e CEI ISO 27032. La documentazione comprovante potrà essere fornita previa opportuna richiesta.

Opzionale, la console di gestione e raccolta delle informazioni può essere installata **on premise**. Con questa opzione si renderà necessaria l'installazione di alcuni sistemi di controllo e gestione presso il datacenter di ASL CITTA' DI TORINO. Il Team SOC del Partner di TIM deve avere accesso H24, 7/7 alla console di gestione della piattaforma per eseguire le attività di gestione, manutenzione e supporto. I requisiti tecnici della soluzione in modalità on premise sono illustrati nell'allegato tecnico.

SERVIZI LION® CYBER SECURITY	
COD	DESCRIZIONE
A	START-UP. Attivazione, configurazione, installazione (Una Tantum)

SERVIZI LION® CYBER SECURITY	
COD	DESCRIZIONE
TIER I	SIEM AS A SERVICE: 750 EPS - Include licenze IBM Qradar + 1 Event Collector (in modalità MSP)
	LION Cybersecurity - Servizio Gestito 1 Livello SIEM as a Service
TIER II	LION Cybersecurity - Servizio Gestito 2° Livello: Analisi, Detect and Notify, Remediation & Reporting- Servizio H24, 7/7
TIER III	SOC Monitoraggio Proattivo con: • Alert Monitoring: Notifica tempestiva degli eventi critici • Proactive Threat Hunting: Ricerca di artefatti dannosi e IoC nell'ambiente di ASL CITTA' DI TORINO. e Supporto Cyber Security per le seguenti attività di supporto Cyber Security: • Incident Response: Assistenza remota per bloccare e rimuovere le attività malevoli • Attacks Investigation: Report dettagliato con l'analisi dell'attacco subito dal ASL CITTA' DI TORINO Perimetro: 6000 End Point

11.3 Durata del servizio

Il presente servizio proposto a ASL CITTA' DI TORINO ha una durata di mesi:

- **X 24 (VENTIQUATTRO)**

12 ALLEGATO A. DETTAGLI TECNICI CYNET

Sistemi operativi supportati dalla soluzione

Versione minima di Windows:

Endpoints:	Servers:
o Windows XP Service Pack 3	o Windows 2003 R2
o Windows Vista Service Pack 1	o Windows 2008
o Windows 7 Service Pack 1	o Windows 2008 R2
o Windows 8	o Windows 2012
o Windows 8.1	o Windows 2012 R2
o Windows 10	o Windows 2016
o Windows 11	o Windows 2019

Versioni minime di UNIX\LINUX\MAC

Ubuntu 16

RedHat 6.7

Centos 6.7

Fedora 21

Debian 8.4

Suse 12

Oracle Enterprise Linux 7.6

MAC (El Capitan 10.11 64 bit)

E' richiesto l'accesso degli endpoint con il protocollo TCP porta 443 senza servizio proxy al Cloud Cynet, rappresentato dai seguenti due sottodomini internet: **slb.cynet.com** e **sav.cynet.com**

Nel caso il ASL CITTA' DI TORINO per politica interna non consente l'accesso diretto degli singoli endpoint al Cloud Cynet, dovrà essere installato un servizio di Traffic Router su un server dedicato con i seguenti requisiti:

CPU: 8 Core

RAM: 16 GB

HD: 0.25 TB(SSD)

Sistema Operativo: Windows Server 2012R2+

In questo caso, il Traffic Router sarà l'unico sistema che dovrà essere autorizzato all'accesso dei due indirizzi indicati precedentemente. Il software Traffic Router sarà messo a disposizione da TIM.

ASL CITTA' DI TORINO
SICUREZZA AZIENDALE GESTITA

Nella modalità on premise il ASL CITTA' DI TORINO dovrà mettere a disposizione, un sistema, compressivo di licenza del sistema operativo, con i requisiti indicati nella seguente tabella in base al numero degli endpoint gestiti:

250-1,000 endpoints (Windows Server 2012R2+)	1,000-5,000 endpoints (Windows Server 2012 R2+)	5,000-10,000 endpoints (Windows Server 2012 R2+)	10,000-20,000 endpoints (Windows 2012 R2+)	20,000-50,000 endpoints (Windows 2012 R2+)	50,000-100,000 endpoints (Windows 2012 R2+)
• Quad core processors – Physical cores (Intel compatible)	• Quad core processors – physical cores (Intel compatible)	•8 core processors – physical cores (Intel compatible)	• 16 core processors - physical cores (Intel compatible)	• 24 core processors - physical cores (Intel compatible)	• 32 core processors - physical cores (Intel compatible)
• 24 GB RAM	• 32 GB RAM	• 48 GB RAM	• 64GB RAM	• 96 GB RAM	• 128 GB RAM
• 300 GB HD (SSD Physical non shared Disk)	• 500 GB HD (SSD Physical non shared Disk)	•1.5 TB HD (SSD Physical non shared Disk)	• 2 TB HD (SSD Physical non shared Disk)	• 3 TB HD (SSD Physical non shared Disk)	• 4 TB HD (SSD Physical non shared Disk)

13 ALLEGATO B. LIVELLI DI SERVIZIO

Il servizio proposto nella presente offerta è erogato in modalità remota secondo le specifiche di qualità e performance indicate nelle seguenti tabelle.
La definizione puntuale dei livelli di servizio (SLA) presuppone la classificazione delle seguenti tipologie di informazioni:

- **Indicatori di Performance - KPI (Key Performance Indicator)**: rappresenta la definizione degli indicatori di performance chiave per i quali sono effettuate le rilevazioni di qualità:
  - **Up Time - Disponibilità del servizio:** rappresenta gli orari ed i periodi di disponibilità delle strutture operative coinvolte nel servizio.
  - **Qualification Time - Tempo di presa in carico:** rappresenta il tempo trascorso tra l'apertura del Ticket e la sua assegnazione alle strutture specialistiche di supporto
  - **Intervention Time -Tempo di Intervento:** il tempo trascorso tra l'assegnazione del Ticket e ed il tempo di intervento delle strutture specialistiche.
- **Livelli di severità**: rappresenta la classificazione delle severità
- **Matrice di qualità**: definizione dei valori del servizio da assegnare ai KPI in base ai livelli di priorità ed alla disponibilità del servizio

13.1 Indicatori di Performance – KPI (Key Performance Indicator)

Rappresentano la definizione degli indicatori di performance, chiave per i quali sono effettuate le rilevazioni di qualità. Di seguito sono descritti gli indicatori di performance previsti:

Up Time - Disponibilità del servizio.

Per disponibilità del servizio si intende la disponibilità delle strutture operative del Partner di TIM dedicate all'erogazione del servizio descritto nella presente offerta. Per l'utilizzo del servizio, il ASL CITTA' DI TORINO dovrà assicurarsi che le sonde e/o gli apparati installati presso le sue sedi siano accesi, connessi alla rete ed in generale verificare che ci siano tutti i presupposti tecnici per consentire la comunicazione con i sistemi del Datacenter. Qualora tali presupposti non siano verificati, il presente accordo di servizio (Service Level Agreement o SLA) non potrà essere applicato ed il ASL CITTA' DI TORINO non potrà dichiararne il mancato rispetto. La Disponibilità del Servizio verrà misurata, a livello di singolo componente della struttura, con una percentuale trimestrale e sarà calcolata come segue:

$$DISPONIBILITA'\ DEL\ SERVIZIO = \frac{N\_ORE\_DI\_DISPONIBILITA'\_DEL\_SERVIZIO}{N\_ORE\_DI\_FINESTRA\_DI\_SERVIZIO}\ x\ 100$$

Per N_ORE_DI_DISPONIBILITA'_DEL_SERVIZIO si intende il numero totale di ore del mese, durante le quali, all'interno della Finestra di Servizio, il Servizio stesso è effettivamente disponibile per il ASL CITTA' DI TORINO.

Per N_ORE_DI_FINESTRA_DI_SERVIZIO si intende il numero di ore totale della finestra di servizio illustrata nella Tabella 5, Disponibilità delle strutture operative.

Pertanto il N_ORE_DI_DISPONIBILITA'_DEL_SERVIZIO è determinato dal N_ORE_DI_FINESTRA_DI_SERVIZIO (totale mensile del numero di ore della finestra di servizio) a cui vengono detratte il numero di ore in cui il Servizio non sia stato disponibile per il ASL CITTA' DI TORINO a causa di un malfunzionamento di una qualsiasi componente (Hardware, Sistema Operativo, DBMS, Server Applicativo) affidata in gestione a del Partner di TIM nell'ambito del presente contratto e per cause imputabili a TIM;

La disponibilità delle strutture operative del servizio è rappresentata nella seguente tabella:

Struttura	SLA	Finestra
TIER I	24x7	Infrastruttura: Dal lunedì alla domenica, 24 ore su 24, comprese festività
	8x5	Gestione Service Request e Change: Dal lunedì al venerdì, dalle 8.30 alle 18.30, escluse festività nazionali
TIER II, TIER III	24x7*	Dal lunedì alla domenica, 24 ore su 24, comprese festività
	8x5*	Dal lunedì al venerdì, dalle 8.30 alle 18.30, escluse festività nazionali
Service Manager	8X5	Dal lunedì al venerdì, dalle 8.30 alle 18.30, escluse festività nazionali

Tabella 6- Disponibilità delle strutture operative

*In base alla tipologia di disponibilità di servizio scelta dal ASL CITTA' DI TORINO. I livelli di servizio sopra indicati possono essere adeguati, personalizzati e configurati nel corso del contratto secondo necessità specifiche di ASL CITTA' DI TORINO. Nel caso di disponibilità del servizio 8X5, i minuti/le ore si intendono lavorativi/e.

Qualification Time - Tempo di presa in carico

Misura il tempo trascorso tra l'apertura del Ticket e la sua assegnazione alle strutture specialistiche di supporto di TIM, di ASL CITTA' DI TORINO o di altri fornitori di ASL CITTA' DI TORINO competenti per la risoluzione del problema. La KPI per il Tempo di presa in carico verrà misurata con una percentuale trimestrale e sarà calcolata come segue

$$INDICATORE = \frac{Numero\_di\_ticket\_assegnati\_entro\_il\_target}{Numero\_totale\_di\_ticket\_assegnati}\ x\ 100$$

Response Time - Tempo di intervento

Misura il tempo trascorso tra l'assegnazione del Ticket ed il tempo di intervento delle strutture specialistiche di supporto di TIM. Sono escluse dal calcolo i tempi di intervento di ASL CITTA' DI TORINO o di altri fornitori di ASL CITTA' DI TORINO competenti per la risoluzione del problema. La KPI per il Tempo di intervento in carico verrà misurata con una percentuale trimestrale e sarà calcolata come segue:

$$INDICATORE = \frac{Numero\_di\_ticket\_di\_intervento\_entro\_il\_target}{Numero\_di\_ticket\_di\_intervento}\ x\ 100$$

Il Response Time è indicato con due valori:

RESPONSE TIME AGREEMENT (Tempo Massimo di **Intervento**). Il valore RTA ha valore contrattuale di tipo SLA (Service Level Agreement) è rappresenta l'impegno contrattuale di TIM nei confronti di ASL CITTA' DI TORINO

RESPONSE TIME TARGET (Tempo Massimo **Obbiettivo** di Intervento). Il valore RTT è basato sulle misurazioni degli ultimi 24 mesi del servizio è rappresenta l'obbiettivo del livello di servizio o SLO (Service Level Objective). Il valore rappresenta l'effort del team SOC nell'ambito del processo CSI (Continous Service Improvement, continuo miglioramento del servizio) e non ha valore contrattuale.

13.2 Livelli di Severità.

Gli eventi rilevati vengono classificati in base ad una scala di Severità e concordati con il ASL CITTA' DI TORINO in base alle criticità dei suoi asset, della sua infrastruttura IT e delle sue esigenze di Business. A titolo esemplificativo abbiamo inserito nella Tabella 6 una descrizione di quello che può rappresentare l'impatto sulle infrastrutture di ASL CITTA' DI TORINO. La descrizione dell'impatto corrispondente ad ogni livello di severità viene definita durante lo Start-Up del servizio. La rivisitazione periodica dei livelli di severità è inclusa nel processo di miglioramento del servizio.

LIVELLI DI SEVERITÀ	DESCRIZIONE
CRITICO	▪ La funzione/processo/asset in oggetto è indispensabile per lo svolgimento delle operazioni critiche del business di ASL CITTA' DI TORINO. ▪ Problemi o minace che stanno causando o potrebbero causare a breve termine impatti sulle infrastrutture di ASL CITTA' DI TORINO ad un livello tale da **impedire o mettere a rischio lo svolgimento dei processi di business supportati.** ▪ Il servizio o le strutture operative TIM non sono disponibili.
IMPORTANTE	▪ La funzione/processo/asset in oggetto è considerata importante per lo svolgimento delle operazioni di ASL CITTA' DI TORINO**.** ▪ Problemi o minacce che degradano o potrebbero portare a breve termine a un degrado delle performance delle risorse, in maniera tale da determinare **una difficoltà o una parziale/locale inutilizzabilità delle stesse**. ▪ Il servizio e le strutture operative TIM sono disponibili.
NORMALE	▪ La funzione/processo/asset è accessoria allo svolgimento delle operazioni di ASL CITTA' DI TORINO. ▪ **Vengono richieste attività che non impattano sulla normale esecuzione del servizio**. Service Request, Change Request, information service, estrazione log, analisi log, ecc. ▪ Il servizio e le strutture operative del Partner di TIM sono disponibili.

Tabella 7 - Livelli di Severità

13.3 Matrice di Qualità Servizio (SLA)

Il valore delle KPI di Servizio è indicato nella seguente tabella[1]:

LIVELLO DI SEVERITÀ	INDICATORE (KPI):		
	QUALIFICATION TIME	RESPONSE TIME TARGET	RESPONSE TIME AGREEMENT
	Tempo massimo di presa in carico[2]	Tempo massimo target di intervento[3]	Tempo massimo di intervento[4]

[1] Nel caso di disponibilità del servizio 8X5, i minuti/le ore si intendono lavorativi/e.

2 dall'apertura del ticket.

3 all'atto della presa in carico.

4 all'atto della presa in carico.

CRITICO	≤ 15 minuti	≤ 2 ore	≤ 4 ore
IMPORTANTE	≤ 30 minuti	≤ 4 ore	≤ 8 ore.
NORMALE	≤ 60 minuti	≤ 12 ore	≤ 24 ore

Tabella 8- Matrice di Qualità

In base ai valori KPI descritti in precedenza, la performance del Servizio (Service Level Agreement, SLA) è illustrata nella seguente tabella:

INDICATORE	PERFORMANCE (SLA)
UPTIME (Disponibilità del servizio e delle sue strutture operative)	≥ 99% del tempo
QUALIFICATION TIME (Tempo Massimo di Presa in Carico del Ticket)	≥ 95% dei casi
RESPONSE TIME AGREEMENT (Tempo Massimo di Intervento)	≥ 95% dei casi
RESPONSE TIME TARGET (Tempo Massimo Obbiettivo di Intervento)	≥ 90% dei casi

Tabella 9- Performance degli Indicatori

ASL
CITTÀ Dl TORINO

REGIONE PIEMONTE
Azienda Sanitaria Locale "Città di Torino"
Costituita con D.P.G.R. 13/12/2016 n. 94

Cod. fiscale/P.1 11632570013

SERVIZIO SANITARIO
NAZIONALE

Sede legale: Via San Secondo, 29 — 10128
Torino ☎ 011/5661566 011/4393111

DOCUMENTO UNICO
Dl VALUTAZIONE DEI RISCHI DA INTERFERENZA

OGGETTO DELL'APPALTO

AFFIDANIENTO Dl PRODOTTI PER LA SICUREZZA PER ŒNTRALE - PROTEZIONE DEGLI ENDPOINT

LOTTO 2

AQ CONSIP 2367

PREMESSA

Il presente documento è redatto dal Committente in ottemperanza all'art. 26 del D. Lgs. n. 81/08 ed, in particolare, al 3 ^{0} comma che prevede "l'elaborazione da parte del datore di lavoro committente di un unico documento di valutazione dei rischi che indichi le misure adottate per eliminare o, ove ciò non è possibile, ridurre al minimo i rischi da interferenze".

La verifica, con le modalità previste dal decreto, dell'idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare in appalto o mediante contratto d'opera o di somministrazione, viene effettuata a carico della Stazione Appaltante prima dell ' aggiudicazione.

Pertanto, il presente documento stabilisce unicamente le modalità di gestione della sicurezza negli appalti di servizi e costituisce una specifica tecnica della gara in quanto promuove la cooperazione ed il coordinamento tra il committente ed appaltatore all'attuazione delle misure di tutela della salute e sicurezza nei luoghi di lavoro.

Al fine di poter procedere alla valutazione degli eventuali rischi interferenti è necessario che ci sia, tra le parti, lo scambio delle informazioni sui rischi dovuti all'ambiente, alle attività e sulle relative misure di prevenzione e di emergenza adottate.

Il presente documento è articolato in sezioni delle quali alcune sono redatte in fase progettuale di gara d'appalto, mentre altre saranno completate successivamente in collaborazione con la ditta aggiudicataria dell'appalto.

Il presente documento, essendo un documento dinamico, prima dell'effettivo inizio dell'appalto e/o durante l'esecuzione potrà essere integrato e/o modificato a cura del committente coordinandosi e cooperando con l'appaltatore.

Si richiamano i contenuti dell'art. 26 del D.lgs 81/08 e s.m.i. di seguito integralmente riportato.

Art.26. "Obblighi connessi ai contratti d'appalto o d'opera o di somministrazione"

l. Il datore di lavoro, in caso di affidamento di lavori servizi e forniture all'impresa appaltatrice o a lavoratori autonomi all'interno della propria azienda, o di una singola unità produttiva della stessa, nonchè nell'ambito dell'intero ciclo produttivo dell'azienda medesima, sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo:

a) verifica, con le modalità previste dal decreto di cui all'articolo 6, comma 8, lettera g), l'idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somminisfrazione.

Fino alla data di entrata in vigore del decreto di cui al periodo che precede, la verifica è eseguita attraverso le seguenti modalità: 1) acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato;

2) acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale, ai sensi dell'articolo 47 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica del 28 dicembre 2000, n° 445;

b) fornisce agli stessi soggetti dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività. 2. Nell'ipotesi di cui al comma 1, i datori di lavoro, ivi compresi i subappaltatori:

a) cooperano all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;

b) coordinano gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva. 3. Il datore di lavoro committente promuove la cooperazione ed il coordinamento di cui al comma 2, elaborando un unico documento di valutazione dei rischi che indichi le misure adottate per eliminare o, ove ciò non è possibile, ridurre al minimo i rischi da interferenze. Tale documento è allegato al contratto di appalto o di opera e va adeguato in funzione dell'evoluzione dei lavori, servizi e forniture. Ai contratti stipulati anteriormente al 25 agosto 2007 ed ancora in corso alla data del 31 dicembre 2008, il documento di cui al precedente periodo deve essere allegato entro tale ultima data. Le disposizioni del presente comma non si applicano ai rischi specifici propri dell'attività delle imprese appaltatrici o dei singoli lavoratori autonomi. Nel campo di applicazione del decreto legislativo 12 aprile 2006

n. 163 e successive modifiche, tale documento è redatto, ai fini dell'affidamento del contratto dal soggetto titolare del potere decisionale e di spesa relativo alla gestione dello specifico appalto.

3 bis. Ferme restando le disposizioni di cui ai commi 1 e 2, l'obbligo di cui al comma3 non si applica ai servizi di natura intellettuale, alle mere forniture di materiali o attrezzature, nonché ai lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza di agenti cancerogeni, biologici, atmosfere esplosive o dalla presenza dei rischi particolari di cui all'allegato XI.

3 ter. Nel caso in cui il contratto sia affidato dai soggetti di cui all'articolo 3, comma 34, del decreto legislativo 12 aprile 2006 n. 163, o in tutti i casi in cui il datore di lavoro non coincide con il committente, il soggetto che affida il contratto redige il documento di valutazione dei rischi da interferenze recante una valutazione ricognitiva dei rischi standard relativi alla tipologia della prestazione che potrebbero potenzialmente derivare dall'esecuzione del contratto. Il soggetto presso il quale deve essere eseguito il contratto, prima dell'inizio dell'esecuzione, integra il predetto confratto riferendolo ai rischi specifici da interferenza presenti nei luoghi in cui verrà espletato l'appalto; l'integrazione, sottoscritta per accettazione dall'esecutore, integra gli atti contrattuali.

4. Ferme restando le disposizioni di legge vigenti in materia di responsabilità solidale per il mancato pagamento delle refribuzioni e dei contributi previdenziali e assicurativi, l'imprenditore committente risponde in solido con l'appaltatore, nonchè con ciascuno degli eventuali subappaltatori, per tutti i danni per i quali il lavoratore, dipendente dall'appaltatore o dal subappaltatore, non risulti indennizzato ad opera dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro OIAIL) o dell'Istituto di previdenza per il settore marittimo (IPSEMA). Le disposizioni del presente comma non si applicano ai danni conseguenza dei rischi specifici propri dell'attività delle imprese appaltatrici o subappaltatrici.

5. Nei singoli contratti di subappalto, di appalto e di somministrazione, anche qualora in essere al momento della data di entrata in vigore del presente decreto, di cui agli articoli 1559, ad esclusione dei contratti di somministrazione di beni e servizi essenziali, 1655, 1656 e 1677 del codice civile, devono essere specificamente indicati a pena di nullità ai sensi dell'articolo 1418 del codice civile i costi delle misure adottate per eliminare o, ove ciò non sia possibile , ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni. I costi di cui al primo periodo non sono soggetti a ribasso. Con riferimento ai contratti di cui al precedente periodo stipulati i prima del 25 agosto 2007 i costi della sicurezza del lavoro devono essere indicati entro il 31 dicembre 2008, qualora gli stessi confratti siano ancora in corso a tale data. A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori per la sicurezza e gli organismi locali delle organizzazioni sindacali dei lavoratori comparativamente più rappresentative a livello nazionale.

6. Nella predisposizione delle gare di appalto e nella valutazione dell'anomalia delle offerte nelle procedure di affidamento di appalti di lavori pubblici, di servizi e di forniture, gli enti aggiudicatori sono tenuti a valutare che il valore economico sia adeguato e sufficiente rispetto al costo del lavoro e al costo relativo alla sicurezza, il quale deve essere specificamente indicato e risultare congruo rispetto all'entità e alle caratteristiche dei lavori, dei servizi o delle forniture. Ai fini del presente comma il costo del lavoro è determinato periodicamente, in apposite tabelle, dal Ministro del lavoro e della previdenza sociale, sulla base dei valori economici previsti dalla contrattazione collettiva stipulata dai sindacati comparativamente più rappresentativi, delle norme in materia previdenziale ed assistenziale, dei diversi settori merceologici e delle differenti aree territoriali. In mancanza di contratto collettivo applicabile, il costo del lavoro è determinato in relazione al confratto collettivo del settore merceologico più vicino a quello preso in considerazione.

7. Per quanto non diversamente disposto dal decreto legislativo 12 aprile 2006, nº 163, come da ultimo modificate dall'articolo 8, comma 1, della legge 3 agosto 2007, nº 123, trovano applicazione in materia di appalti pubblici le disposizioni del presente decreto.
8. Nell'ambito dello svolgimento di attività in regime di appalto o subappalto, il personale occupato dall'impresa appaltatrice o subappaltatrice deve essere munito di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l' indicazione del datore di lavoro.

COMMITTENTE: AZIENDA SANITARIA LOCALE "Città di Torino"	
CODICE FISCALE: 11632570013	
PARTITA IVA: 11632570013	
DATORE Dl LAVORO: Dr. Carlo PICCO	
SEDE LEGALE: Via San Secondo 29 - 10128 Torino	
RESPONSABILE S.P.P.: ln . Cristina PRANDI	
COORDINATORE IVEDICO CONPETENTE: Dr.ssa Teresa EMANUELE	
RAPPRESENTANTI DEI LAVORATORI PER LA SICUREZZA (RLS)	Amabile Teodoro Armanda Fiorella Barba Luca Bozzetto Angelo Buda Igor Caiazzo Antonio Crosa Roberta De Candia Nunzia Di Bari Michele Evaristo Maria Cinzia Gasparri Robertino Guion Luca Italiano Rocco Lucia Stefano Maida Piera Mancin Danilo Mancuso Antonio Martella Giovanna Miccichè Salvatore Miglietta Alessandro Midiri Maria Morena Stefano Pascuzzi Pasquale Penza Antonio Rondinelli Cinzia Russo Pietro Scaramuzza Roberto Sorrentino Danilo Vernassa Dario Virzì Simone Zumbo Antonino
DESCRIZIONE DELL'ATTIVITÀ	

L'appalto prevede fornitura di prodotti e servizi per la sicurezza perimetrale.

Con questo progetto ASL Citta di Torino intende acquisire una fornitura EPP/Cynet e utilizzare i servizi specialistici per raggiungere un adeguato livello di sicurezza in correlazione con i requisiti previsti dal PNRR.
Il progetto sarà finanziato con le risorse del PNRR (Piano Nazionale di Ripresa e Resilienza).

Unitamente a tale fornitura, saranno erogati i seguenti servizi:

- installazione e configurazione delle tecnologie di nuova fornitura (Cynet);

Saranno inoltre erogati i seguenti servizi di Supporto Specialistico:

- supporto alla reingegnerizzazione della rete dell'Amministrazione, incluse le necessarie attività di assessment, profilazione e documentazione dell'AS-IS e del TO-BE; - supporto al personale dell'Amministrazione nella gestione di tutti i servizi preesistenti e di nuova fornitura.

Il tutto meglio specificato nel Piano Operativo e Documento di specifiche tecniche.

SEDI PRESSO CUI SI SVOLGE L'APPALTO

- Sede Centrale via San Secondo, 29 e altre sedi Asl Città di Torino; -
Attivita di lavoro da remoto.

Il tutto meglio specificato nel Piano Operativo e Documento di specifiche tecniche.

DURATA DELL'APPALTO

La durata del servizio è fissata in mesi 24.

Il tutto meglio specificato nel Piano Operativo e Documento di specifiche tecniche.

INFORMAZIONI DEL COMMITTENTE

In generale nei confronti dei lavoratori sono stati osservati gli obblighi in conformità a quanto previsto dal D. Lgs. nº 81/08 e s.m.i. con l'adozione delle misure di prevenzione e protezione necessarie.

Tipologia di attività che I 'Azienda svolge nelle zone oggetto del servizio:
-Attività amministrative (sede via San Secondo, 29)
-Attività di tipo sanitario e di assistenza ai degenti/utenti (altre sedi)

Situazioni di interferenza

I rischi di interferenza tra il personale della ditta aggiudicataria e gli occupanti della struttura (personale ASL e utenti) possono verificarsi in casi ordinari:

- durante il transito degli operatori dell'aggiudicataria all'interno del presidio;
- durante l'esecuzione del servizio;
- durante il trasporto dei materiali e attrezzature.

Si segnala che potrebbero configurarsi rischi di interferenza anche in situazioni straordinarie quali: e emergenza;

- comportamento imprevedibile da parte degli utenti.

Nei luoghi di lavoro potrebbero operare anche imprese per la gestione di specifici servizi (quali ad esempio movimentazione/trasporto pazienti e materiale, facchinaggio, ristorazione, ecc..), nonché ditte per le attività di manutenzione. In presenza di personale di altre ditte appaltatrici adottare le misure previste per il personale ASL e utenza.

Identificazione dei potenziali rischi da interferenza

Nella seguente tabella sono stati individuati i rischi presenti nell'ambito lavorativo che potrebbero costituire potenziali rischi da interferenza e le relative misure da adottare:

Rischi da interferenza	Aree interessate	Misure di prevenzione
Biologico	Strutture Azienda Sanitaria Città di Torino	Il rischio può essere connesso al contatto con i pazienti affetti da patologie infettive sia aereotrasmesse che da contatto o con materiali contaminati e alla presenza di contaminazioni ambientali (legionella , aspergillo) Attenersi alle misure di sicurezza previste dall'azienda evitando di toccare oggetti o strumenti dei quali non si conosca l'uso o la provenienza. Interfacciarsi con i coordinatori sanitari per l'accesso ai locali interni alle aree oggetto dei servizi. In caso di sversamento sono disponibili procedure di sicurezza per il contenimento dell'evento a cui si deve attenere tutto il personale. Prestare la massima attenzione per la possibilità di contatto accidentale con materiale tagliente (vetro, aghi, etc,) potenzialmente infetto. Nel caso in cui si verifichi un incidente seguire l'apposita procedura predisposta dall'aggiudicataria e segnalare l' accaduto ai referenti della Committente. Utilizzo di idonei D.P.I.
Chimico	Strutture Azienda Sanitaria Città di Torino	Il rischio è connesso alla presenza di sostanze e preparati necessari alla attività sanitarie (detergenti, disinfettanti e sterilizzanti) e alla manipolazione di sostanze pericolose nei laboratori (solventi e reagenti). E' fatto assoluto divieto di introdurre prodotti contenenti lattice naturale al fine di evitare allergie. In caso di sversamento sono disponibili procedure di sicurezza per il contenimento dell'evento a cui si deve attenere tutto il personale. Utilizzo di idonei D.P.I.
Farmaci antiblastici	Strutture Azienda Sanitaria Città di Torino	Adottare i protocolli di prevenzione in uso nei singoli Reparti. Attenersi alle indicazioni del responsabile Attivita/Servizio o suo delegato e alla segnaletica di sicurezza presente. In caso del verificarsi di sversamento, avvisare il responsabile attivita]servizio aziendale, il proprio responsabile e seguire le procedure previste dall'azienda e dalla propria azienda e in caso di contatto con mucosa orale recarsi al Pronto Soccorso. Utilizzo di idonei D.P.I.
Radiazioni ionizzanti	Strutture Azienda Sanitaria Città di Torino	La presenza di sorgenti/apparecchiature radiologiche è segnalata da apposita cartellonistica riportante il simbolo delle radiazioni ionizzanti. Nelle aree così contrassegnate è fatto divieto al personale non autorizzato di accedere con le apparecchiature in funzione. Interfacciarsi con i coordinatori sanitari/tecnici per l'accesso ai locali interni alle aree oggetto dei servizi. In relazione alle attività svolte il personale dovrà attenersi alle norme specifiche in materia di radioprotezione previste. In occasione di esami RX al letto del paziente Si dispone il rispetto delle procedure predisposte dall'Esperto Qualificato Aziendale.

Laser/R.O.A.	Strutture Azienda Sanitaria	Il rischio radiazioni non ionizzanti è presente solo ad apparecchiature attive in locali adeguatamente segnalati. Si

	Città di Torino	dispone il rispetto della segnaletica e divieto di acceso a zone con luce accesa indicante il funzionamento. Interfacciarsi con i coordinatori sanitari/tecnici per l'accesso ai locali interni alle aree oggetto dei servizi. Si dispone il rispetto delle procedure predisposte dall'Esperto ualificato Aziendale.
Impiego di gas anestetici/ medicali	Strutture Azienda Sanitaria Città di Torino	Qualora si rendesse necessario utilizzare gas anestetici/medicali nello svolgimento dell'appalto, si dovranno attuare tutte le procedure di sicurezza e/o d'emergenza previste.
Campi elettromagnetici (CEM)	Strutture Azienda Sanitaria Città di Torino	Nei locali in cui sono presenti le risonanze magnetiche (RSM) non introdurre materiale ferromagnetico e/o qualsiasi altro oggetto metallico; non accedere se si è portatori di protesi metalliche e/o "pace-maker". Attenersi alle misure di sicurezza reviste er il re arto/servizio.
Incendio	Strutture Azienda Sanitaria Città di Torino	Attenersi alle norme di comportamento definite nelle procedure di emergenza; Osservare quanto previsto dal D.M. 3 settembre 2021, "Criteri generali di progettazione, realizzazione ed esercizio della sicurezza antincendio per luoghi di lavoro" e al D.M. 29 marzo 2021, ed in particolare le misure organizzative e di tipo gestionale quali: rispetto dell'ordine e della pulizia; controllo delle misure e delle procedure di sicurezza; evitare l'accumulo di materiali combustibili od infiammabili; evitare l'ostruzione delle vie di esodo; evitare il bloccaggio delle porte resistenti al fuoco; rispettare il divieto di fumare. L'appaltatore deve seguire rigorosamente le procedure previste e deve individuare in funzione del piano di emergenza dell'ASL Città di Torino il proprio personale addetto alle emergenze e antincendio di com artimento.
Utilizzo ascensori/ montacarichi	Strutture Azienda Sanitaria Città di Torino	Si dovrà porre attenzione nel corretto uso degli impianti elevatori. Il piano di emergenza delle rispettive sedi disciplina la gestione delle situazioni di emergenza.
Elettrico	Strutture Azienda Sanitaria Città di Torino	Gli impianti e le apparecchiature sono realizzati e mantenuti in conformità alle norme CEI e al D.M. 37/08 s.m.i. Astenersi da eventuali interventi di tipo elettrico sugli impianti e verifica della possibilità di allacciamento di eventuali apparecchiature mediante richiesta alla S.C. Tecnico Area Ospedaliera e per quanto attiene il P.O. "Oftalmico" alla S.C. Tecnico Area Territoriale. Utilizzo di attrezzature marcate CE conformi alla normativa vigente. Segnalare immediatamente eventuali anomalie riscontrate sull'im ianto elettrico.

Movimentazione carichi	Strutture Azienda Sanitaria Città di Torino	La movimentazione di materiale, attrezzature, ecc deve essere effettuata in sicurezza con personale sufficiente e con utilizzo di appositi ausili atti ad evitare spandimenti, cadute o quant'altro che possa essere di pregiudizio per la salute degli operatori e degli utenti. Ris ettare i ercorsi se nalati e utilizzare attrezzature di
		dimensioni adeguate in relazione alle luci dei percorsi/passaggi individuati. Non abbandonare materiali e/o attrezzature che possono costituire fonti potenziali di pericolo in luoghi di transito e di lavoro. Non ingombrare con materiali e/o attrezzature percorsi di esodo e/o le uscite di emer enza.
Circolazione e manovra nelle aree esterne con automezzi	Strutture Azienda Sanitaria Città di Torino	Veicoli in circolazione: ambulanze, mezzi trasporto pazienti, autovetture private di pazienti, automezzi raccolta rifiuti, veicoli scarico e carico derrate cucina, automezzi trasporto farmaceutico, automezzi ditte manutenzione, macchinari per la movimentazione carichi, ecc. Nella circolazione all'interno delle strutture: procedere a passo d'uomo seguendo la segnaletica presente; impegnare le aree di carico e scarico merci solo quando queste non sono occupate da altri soggetti; in caso di manovra in retromarcia o quando la manovra risulti particolarmente difficile (spazi ridotti, scarsa visibilità, ecc..) farsi coadiuvare da un collega a terra; in mancanza di sistema di segnalazione acustica di retromarcia sul mezzo (cicalino) farsi coadiuvare da un colle a a terra.
Spostamenti a piedi	Strutture Azienda Sanitaria Città di Torino	Negli spostamenti: • camminare sui marciapiedi o lungo i percorsi pedonali indicati mediante segnaletica orizzontale; • non sostare dietro gli automezzi in sosta o in manovra; • non sostare nelle aree di de osito materiali.
Scivolamento	Strutture Azienda Sanitaria Città di Torino	Attenzione e rispetto della segnaletica mobile e/o fissa per la presenza di rischio scivolamento/inciampo/ostacoli. Le procedure per le operazioni di pulizia prevedono che il personale addetto evidenzi la presenza di pericolo di scivolamento, posizionando gli appositi cartelli indicanti "Attenzione avimento ba ato".
Organizzativo	Strutture Azienda Sanitaria Città di Torino	In considerazione dello svolgimento dell'attività sanitaria e dei servizi erogati dall'appaltatore, concordare tempestivamente con i referenti della Committente la scelta delle modalità esecutive, nonché degli orari di intervento per la programmazione delle operazioni in merito ad eventuali problemi o disguidi. Attenersi alle linee ida/ rotocolli elaborati.

Amianto	Strutture Azienda Sanitaria Città di Torino	La presenza di amianto è stata rinvenuta all'interno di alcuni manufatti di tipo "compatto", quali pavimenti in vinile, tratti di tubazioni in fibrocemento, comignoli e lastre in matrice compatta, che possono liberare fibre solo se sollecitati meccanicamente ed esempio con l'uso di utensili od attrezzature o qualora si trovino in particolare stato di degrado. La presenza di manufatti contenti amianto è indicata nella documentazione agli atti della S.C. Prevenzione e Protezione.
Emergenze in genere	Strutture Azienda Sanitaria Città di Torino	Gli operatori dell'ASL Città di Torino sono stati adeguatamente formati in merito al alle Procedure di Emergenza. Si dovranno seguire rigorosamente le procedure previste dall'azienda per eventi interessanti il complesso. L'appaltatore deve individuare in funzione delle procedure previste dai piani di emergenza il proprio personale addetto alle emer enze.
Aggressioni	Strutture Azienda Sanitaria Città di Torino	Evitare situazioni, linguaggi e/o comportamenti che possano essere travisati dai pazienti/utenti. Evitare la presenza di oggetti superflui che possano essere usati come oggetti contundenti. Organizzare l'attività di lavorazione riducendo al minimo la presenza di un solo operatore. Nei P.O. è presente H24 un servizio di vigilanza da allertare in caso di necessità.

In relazione alla tipologia di attività oggetto dell'appalto, non sono da prevedersi contatti diretti con i pazienti né con farmaci o sostanze ad uso sanitario.

In relazione all'emergenza relativa al rischio connesso all'insorgenza di patologia derivante dall'infezione da "Coronavirus 2019-(SARS-COV2), si ribadisce l'importanza dell'adozione delle principali misure di prevenzione al contenimento della diffusione dell'infezione, rappresentate dal rispetto delle precauzioni standard come l'igiene delle mani, l'etichetta tosse e l'utilizzo corretto dei dispositivi di protezione (DPI).

Si ritiene che debba essere posta particolare attenzione alle procedure da attuarsi in caso di emergenza incendi. A tale proposito si dovranno osservare le norme di comportamento elaborate e seguire le informazioni contenute nella cartellonistica affissa in cui sono richiamate semplici regole comportamentali da tenersi.

Verrà successivamente fornito un estratto del piano di emergenza che dovrà essere opportunamente divulgato agli addetti che si trovino ad operare presso le nostre strutture.

Al fine di operare in sicurezza si è ritenuto inoltre di individuare nel preposto (coordinatore infermieristico/tecnico) la figura a cui fare riferimento per le corrette procedure e informazioni necessarie nonché i soggetti individuati dall'azienda che cureranno l'esecuzione del servizio.

Accessi alle strutture

Per l'accesso alla strutture si dovranno utilizzare gli ingressi normalmente utilizzati dal personale dell'azienda.

Dovranno essere presi specifici accordi con i soggetti che cureranno l'esecuzione del servizio qualora si renda necessaria l'introduzione o il transito all'interno della struttura di attrezzature particolarmente ingombranti

Disponibilità di servizi igienici

Non è prevista la disponibilità di servizi igienici diversi da quelli presenti per il pubblico presso le varie sedi né la messa a disposizione di spogliatoi o di aree di stoccaggio, né del servizio mensa.

Primo soccorso e assistenza medica di emergenza

Ferme restando le misure di primo soccorso che l'aggiudicataria intende organizzare per il proprio personale si segnala che presso i Presidi Ospedalieri "Maria Vittoria", "Martini" "San Giovanni Bosco" e "Oftalmico" è presente un Pronto Soccorso.

Utilizzo impianti

Gli impianti presenti nelle strutture, necessari allo svolgimento del servizio sono l'impianto elettrico e di trasmissione dati; tali impianti risultano realizzati a regola d'arte e oggetto di regolare manutenzione.

Gli operatori dell'aggiudicataria sono tenuti ad utilizzarli in modo adeguato e limitatamente alle necessità dei servizi espletati, segnalando qualsiasi problema che dovessero rilevare.

Addetti aggiudicataria

Il personale occupato dall'aggiudicataria dovrà essere munito di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro.

IO

INFORMAZIONI FORNITE DALLA AGGIUDICATARIA

Dati aggiudicataria

RAGIONE SOCIALE: LANTECH LONGWAVE S.p.a.
CODICE FISCALE: 01922820350
PARTITA IVA: 01922820350
SEDE LEGALE: Reggio Emilia (RE) Via Danubio, 9 cap 42124
N.ro ISCRIZIONE C.C.I.A.A.: 01922820350 REA: RE - 235407
DATORE Dl LAVORO: LELLI LELLO
RESPONSABILE S.P.P.: BROCCA MARIO
MEDICO COMPETENTE: Dott. BERRINZONI LUCA Dott. MANENTI ANGELO
RAPPRESENTANTI DEI LAVORATORI PER LA SICUREZZA: Babetto Michele, Giovannini Giuseppe, Castagnaro Fabio
PREPOSTO REFERENTE PER IL SEGUENTE APPALTO: Sig. Rossi Alessandro

Descrizione modalità operativa dell'attività svolta presso il committente

Ulteriori informazioni che si ritiene necessario fornire in relazione ai rischi di interferenza e che si possono manifestare nello svolgimento delle attività presso il committente

La ditta Aggiudicataria fornisce l'estratto del proprio documento di valutazione dei rischi dove sono elencati i rischi lavorativi connessi all'attività oggetto dell'appalto.

II

INFORMAZIONE E FORMAZIONE

Entrambe le parti, Committente ed Aggiudicataria, provvedono ad informare i propri operatori sui possibili rischi di interferenza dovuti allo svolgimento dell'appalto in oggetto. L'Aggiudicataria attua nei confronti dei propri operatori, anche specifiche azioni di informazione e formazione riferite non solo ai rischi specifici dell'attività, ma anche ai rischi generali dovuti allo svolgimento della stessa in ambiente sanitario.

L'azienda appaltatrice si obbliga altresì ad informare e formare sul contenuto del presente documento tutti gli eventuali subappaltatori nonché coloro che a qualunque titolo eventualmente collaboreranno con la stessa.

COSTI RELATIVI ALLA SICUREZZA

Sulla base dei rischi da interferenza individuati, l'attuazione delle relative misure da adottare non comporta costi aggiuntivi per la sicurezza.

APPROVAZIONE DEL DOCUMENTO

Le parti si impegnano a darsi reciproca immediata comunicazione di ogni eventuale variazione rispetto al presente piano al fine di poter promuovere la cooperazione ed il coordinamento di cui all'art. 26 D.Lvo. 81/08 ed effettuare le revisioni del caso.

Data, firma In . PRANDI Cristina, RSPP ASL Città di Torino

2cZB

Data, timbro e firma Ditta Aggiudicataria

Lantech Longwave S.p.A.
Via Danubio, 9
42124 REGGIO EMILIA
Tel. 0522 375511 - Fax 0522 375555
Cod. Fisc. e Partita IVA 01922820350

12

DICHIARAZIONE SOSTITUTIVA DI ATTO NOTORIO

(ai sensi degli art. 19, 38, 47 e 77bis del D.P.R. n. 445 del 28 dicembre 2000 s.m.i.)

GARA A PROCEDURA APERTA PER L'AFFIDAMENTO DI UN ACCORDO QUADRO AI SENSI DELL'ART. 54 COMMA 3 DEL D. LGS. N. 50/2016, PER LA FORNITURA DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT ED EROGAZIONE DI SERVIZI CONNESSI PER LE PUBBLICHE AMMINISTRAZIONI – LOTTI 1, 2 E 3 – ID 2367

Il sottoscritto Massimiliano Materazzi, nato a Napoli il 29/09/1970 C.F. MTRMSM70P29F839Q domiciliato per la carica presso la sede societaria ove appresso, nella sua qualità di Procuratore Speciale avente i poteri necessari per impegnare la Telecom Italia S.p.A. nella presente procedura, con sede in Milano, Via Gaetano Negri n.1, iscritta al Registro delle Imprese di Milano al n. 00488410010, codice fiscale n. 00488410010, CCNL applicato: Imprese esercenti Servizi di Telecomunicazione Settore Telecomunicazioni, che partecipa alla presente iniziativa nella seguente forma: raggruppamento temporaneo ai sensi del D.Lgs. 50/2016 art. 45 – comma 2 - lett. d) in qualità di Mandataria con le imprese MATICMIND S.p.A., DGS S.P.A. e SCAI SOLUTION GROUP S.P.A., ai sensi e per gli effetti dell'art. 76 D.P.R. 445/2000 consapevole della responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci e/o formazione od uso di atti falsi e/o in caso di esibizione di atti contenenti dati non più corrispondenti a verità;

D I C H I A R A

che i prodotti offerti nella gara in oggetto, rispettano in fabbricazione i seguenti requisiti DNSH:

PRODOTTO	**Conformità alla Direttiva Bassa Tensione 2014/35/UE nota come LVD, conformemente all'allegato IV**	**Conformità alla Direttiva 2009/125/CE – Direttiva sulla progettazione ecocompatibile / possesso della marcatura CE**	**Conformità alle normative RAEE/ROHS/REACH/Compatibilità elettromagnetica**
BITDEFENDER (EPP/EDR)	N/A (fornitura software)	N/A (fornitura software)	N/A (fornitura software)
CHECK POINT (Anti-APT)	SI	SI	SI
CHECK POINT (SPP)	N/A (fornitura software)	N/A (fornitura software)	N/A (fornitura software)
CISCO (NGFW)	SI	SI	SI
CYNET (EPP/EDR)	N/A (fornitura software)	N/A (fornitura software)	N/A (fornitura software)
FORCEPOINT (NGFW)	SI	SI	SI
FORTINET (NAC/NGFW)	SI	SI	SI
HPE (NAC)	SI	SI	SI
MC AFEE (EPP/EDR)	N/A (fornitura software)	N/A (fornitura software)	N/A (fornitura software)
PAOLO ALTO (NGFW)	SI	SI	SI
TREND MICRO (Anti-APT)	SI	SI	SI
TREND MICRO (EPP/EDR, SPP)	N/A (fornitura software)	N/A (fornitura software)	N/A (fornitura software)

Firmato digitalmente da

Telecom Italia S.p.A.

Massimiliano Materazzi

Firmato digitalmente da:
MASSIMILIANO MATERAZZI
Telecom Italia S.p.A.
Firmato il: 16-07-2022 12:43:43
Seriale certificato: 580998
Valido dal 09-05-2022 al 09-05-2025

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

21-C0-C9-BE-80-2B-5F-0B-67-B6-43-B2-07-D4-EB-92-7D-69-97-FA

PAdES 1 di 1 del 16/07/2022 12:44:02

Soggetto: MASSIMILIANO MATERAZZI TINIT-MTRMSM70P29F839Q

Validità certificato dal 09/05/2022 09:45:49 al 09/05/2025 09:45:48

Rilasciato da Telecom Italia Trust Technologies S.r.l. con S.N. 8DD86

SERVIZIO SANITARIO NAZIONALE
REGIONE PIEMONTE
Azienda Sanitaria Locale "Città di Torino"
Costituita con D.P.G.R. 13/12/2016 n. 94
Cod. fiscale/P.I. 11632570013
Sede legale: Via San Secondo, 29 – 10128 Torino
☏ 011/5661566 ☏ 011/4393111

PATTO DI INTEGRITA' TRA L'A.S.L. CITTA' DI TORINO E GLI OPERATORI ECONOMICI PARTECIPANTI ALLE PROCEDURE DI AFFIDAMENTO CONTRATTUALE

Il presente Patto deve essere obbligatoriamente sottoscritto dal Rappresentante legale di ciascun Soggetto Concorrente/Affidatario diretto e presentato insieme all'offerta, di cui è da considerare elemento essenziale.

Il presente documento dovrà essere allegato al contratto a formarne parte integrante e sostanziale.

Il sottoscritto RUSSO GIUSEPPE in qualità di PROCURATORE

della Società Telecom Italia S.p.A con sede legale in MILANO, Via Gaetano Negri,1

Codice fiscale/P.IVA 00488410010

partecipante alla gara/ invitato a presentare offerta per l'affidamento/fornitura/servizi/lavori

"P.N.R.R. Missione 6 Salute, C2, Investimento 1.1. "AMMODERNAMENTO DEL PARCO TECNOLOGICO E DIGITALE OSPEDALIERO". Adesione ad Accordo Quadro Consip "Cybersecurity 2 - prodotti e servizi connessi" – Lotto 2 (ID 2367) per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi NEXT GENERATION EU per la durata di 18 mesi, Unico Fornitore R.T.I. costituendo da TELECOM ITALIA S.p.A. P.I. 00488410010 (mandataria), MATICMIND S.p.A., DGS S.p.A., SCAI SOLUTION GROUP S.p.A. Importo 663.727,58 o.f.i."

*Codice Identificativo Gara – C.I.G**: A020E7A724***

vista la normativa e gli atti di riferimento seguenti:

- *La Legge 6 novembre 2012 n. 190, art. 1, comma 17 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione";*
- *Il Piano Nazionale Anticorruzione (P.N.A.) approvato dall'Autorità Nazionale Anticorruzione (ex CIVIT) con delibera n. 72/2013 dell'11/09/2013;*
- *Il D.P.R. 16/04/2013, n. 62 col quale è stato emanato il "Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165";*

DICHIARA DI ACCETTARE QUANTO SEGUE

Articolo 1
Ambito di applicazione

1. Il presente Patto di Integrità regola i comportamenti degli operatori economici e dei dipendenti della l'Azienda Sanitaria Locale Città di Torino (nel seguito: A.S.L. Città di Torino), nell'ambito delle procedure di affidamento e gestione degli appalti di lavori, servizi e forniture di cui al d.lgs. n. 50/2016 e s.m.i..

2. Esso stabilisce la reciproca e formale obbligazione tra l'A.S.L. Città di Torino e gli operatori economici individuati al comma 1, di improntare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, nonché l'espresso impegno anticorruzione di non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio.

3. Il Patto di Integrità costituisce parte integrante e sostanziale dei contratti stipulati dall'A.S.L. Città di Torino. L'espressa accettazione dello stesso costituisce condizione di ammissione alle procedure di gara ed alle procedure negoziate ed agli affidamenti diretti di importo pari o superiori ad € 40.000,00. Tale condizione deve essere esplicitamente prevista nei bandi di gara e nelle lettere d'invito.

4. Una copia del Patto di Integrità, sottoscritta per accettazione dal legale rappresentante dell'operatore economico concorrente, deve essere consegnata unitamente alla documentazione amministrativa richiesta ai fini della procedura di affidamento. Per i consorzi ordinari o raggruppamenti temporanei l'obbligo riguarda tutti i consorziati o partecipanti al raggruppamento o consorzio.

Articolo 2
Obblighi degli operatori economici nei confronti della Stazione appaltante

1. In sede di affidamento di contratti di lavori, servizi e forniture, l'operatore economico:

1.1 dichiara di non avere influenzato il procedimento amministrativo diretto a stabilire il contenuto del bando/lettera d'invito o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte dell'Amministrazione aggiudicatrice e di non aver corrisposto né promesso di corrispondere ad alcuno – e s'impegna a non corrispondere né promettere di corrispondere ad alcuno – direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati, somme di denaro o altra utilità finalizzate a facilitare l'aggiudicazione e/o gestione del contratto;

1.2 dichiara, con riferimento alla specifica procedura di affidamento, di non avere in corso né di avere praticato intese e/o pratiche restrittive della concorrenza e del mercato vietate ai sensi della normativa vigente, ivi inclusi gli artt. 101 e segg. del Trattato sul Funzionamento dell'Unione Europea (TFUE) e gli artt. 2 e segg. della l. 287/1990, e che l'offerta è stata predisposta nel pieno rispetto della predetta normativa; dichiara altresì, che non si è accordato e non si accorderà con altri partecipanti alle procedure di gara per limitare con mezzi illeciti la concorrenza;

1.3 dichiara di aver preso visione del Codice di Comportamento aziendale e di condividere i principi in esso enunciati, impegnandosi a rispettarli;

1.4 dichiara che non risultano in servizio dipendenti che, qualora anteriormente dipendenti della Pubblica Amministrazione, negli ultimi tre anni di servizio precedenti la cessazione di rapporto di pubblico impiego abbiano esercitato poteri autoritativi o negoziale per conto dell'A.S.L. Città di Torino;

1.5 si impegna a segnalare all'Amministrazione aggiudicatrice qualsiasi illecito tentativo da parte di terzi di turbare, o distorcere le fasi di svolgimento della procedura di affidamento e/o l'esecuzione del contratto;

1.6 si impegna a segnalare all'Amministrazione aggiudicatrice qualsiasi illecita richiesta o pretesa da parte dei dipendenti dell'amministrazione o di chiunque possa influenzare le decisioni relative alla procedura di affidamento o all'esecuzione del contratto;

1.7 si impegna, qualora ritenga che i fatti di cui ai precedenti punti 1.4 e 1.5 costituiscano reato, a sporgere denuncia all'Autorità giudiziaria o alla polizia giudiziaria.

2. Nelle fasi successive all'aggiudicazione/affidamento, gli obblighi si intendono riferiti all'aggiudicatario/affidatario, il quale avrà l'onere di pretenderne il rispetto anche dai propri subcontraenti. A tal fine, la clausola che prevede il rispetto degli obblighi di cui al presente patto sarà inserita nei contratti stipulati dall'appaltatore con i propri subcontraenti.

Articolo 3
Obblighi dell'Amministrazione aggiudicatrice

1. Il personale, i collaboratori ed i consulenti dell'A.S.L. Città di Torino impiegati ad ogni livello nell'espletamento di questa gara/procedura di affidamento e nel controllo dell'esecuzione delrelativo contratto assegnato, sono consapevoli del presente Patto d'Integrità, il cui spirito condividono pienamente, nonché delle sanzioni previste a loro carico in caso di mancato rispetto diquesto Patto.

2. L'Amministrazione aggiudicatrice si obbliga a rispettare i principi di lealtà, trasparenza e correttezza e ad attivare i procedimenti disciplinari nei confronti del personale a vario titolo intervenuto nel procedimento di affidamento e nell'esecuzione del contratto in caso di violazione di detti principi e, in particolare, qualora riscontri la violazione dei contenuti dell'art. 14 del D.P.R. 16.04.2013, n. 62 o di prescrizioni analoghe per i soggetti non tenuti all'applicazione dello stesso.

3. Il Responsabile per la prevenzione per la corruzione, in adesione ai principi della trasparenza dell'attività amministrativa, vigila sull'obbligo di inserire nei bandi di gara regole di integrità sulla base delle attestazioni che devono pervenire dai dirigenti interessati entro il 31 gennaio di ciascun anno.

Articolo 4
Violazione del Patto di Integrità

1. La violazione di uno degli impegni previsti dal presente documento da parte dell'operatore economico, in veste di concorrente/affidatario diretto, comporta l'applicazione delle sanzioni di seguito previste:

a) l'esclusione dalla procedura di affidamento e l'incameramento della cauzione provvisoria, se prevista.

2. La violazione di uno degli impegni previsti dal presente documento da parte dell'operatore economico, riscontrata in un momento successivo all'aggiudicazione/affidamento, comporta l'applicazione delle sanzioni di seguito previste, che potranno essere applicate congiuntamente o alternativamente in base alla gravità o alle modalità con cui viene perpetrata la violazione:

a) revoca dell'aggiudicazione/affidamento;

b) applicazione di una penale da determinarsi, a seconda della gravità dell'infrazione, sulla base dei criteri che saranno stabiliti nell'ambito di ciascun capitolato di gara. Tale penale potrà eventualmente essere detratta dall'importo ancora dovuto all'aggiudicatario;

c) risoluzione di diritto del contratto eventualmente sottoscritto ai sensi e per gli effetti dell'art. 1456 del Codice Civile e incameramento della cauzione definitiva;

d) valutazione della violazione del presente Patto ai fini dell'esclusione degli operatori economici dalle procedure di affidamento previste dall'articolo 80 del D.lgs. 50/2016.

3. L'Amministrazione aggiudicatrice può non avvalersi della risoluzione del contratto qualora la ritenga pregiudizievole rispetto agli interessi pubblici, quali quelli indicati all'art. 121, comma 2, d.lgs. 104/2010 e s.m.i..

È fatto salvo in ogni caso l'eventuale diritto al risarcimento del danno.

4. La violazione di cui al presente articolo è dichiarata in esito ad un processo di verifica condotto dalla struttura aziendale responsabile del relativo procedimento, in cui venga garantito adeguato contraddittorio con l'operatore economico interessato.

L'accertamento della violazione può anche essere successivo alla completa esecuzione del contratto e valevole sia ai fini dell'applicazione della penale sia con riferimento all'irrogazione della sanzione accessoria comportante l'esclusione dell'operatore economico dalla partecipazione alle successive procedure di gara indette dall' l'A.S.L. Città di Torino, ai sensi dell'art. 4, comma 2,lett. d) del presente Patto.

Ogni controversia relativa all'interpretazione ed esecuzione del presente Patto d'Integrità tra l'A.S.L. Città di Torino e i concorrenti e tra gli stessi concorrenti sarà risolta dall'Autorità Giudiziaria competente.

Torino, _____

PER ACCETTAZIONE
IL CONTRAENTE

_____

(firma leggibile)

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

A8-63-C0-D9-2B-4E-7A-71-F6-14-7A-54-F9-A6-99-5E-0A-C1-76-FA

CAdES 1 di 1 del 12/12/2023 11:25:24

Soggetto: GIUSEPPE RUSSO RSSGPP67L29I480H

Validità certificato dal 09/05/2022 17:45:10 al 08/05/2025 17:45:10

Rilasciato da TI Trust Technologies QTSP CA, Telecom Italia Trust Technologies S.r.l., IT con S.N. 5C

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

E6-F2-F8-82-93-BE-6E-11-CE-94-00-6F-58-CB-1D-EB-84-83-7A-B1

CAdES 1 di 2 del 14/12/2023 09:42:51

Soggetto: GIUSEPPE RUSSO RSSGPP67L29I480H

Validità certificato dal 09/05/2022 17:45:10 al 08/05/2025 17:45:10

Rilasciato da TI Trust Technologies QTSP CA, Telecom Italia Trust Technologies S.r.l., IT con S.N. 5C

CAdES 2 di 2 del 13/12/2023 18:50:37

Soggetto: Carlo Picco PCCCRL60E17L013P

Validità certificato dal 28/12/2022 11:18:43 al 28/12/2025 01:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT con S.N. 00E1 6942

La presente copia e' conforme all'originale depositato presso gli archivi dell'Azienda ASL Citta' di Torino

44-95-9A-5F-8D-C7-44-99-C4-85-B4-33-CC-CF-3B-CA-62-8E-A8-EE

CAdES 1 di 6 del 28/12/2023 17:22:29

Soggetto: Carlo Picco

S.N. Certificato: E16942

Validità certificato dal 28/12/2022 10:18:43 al 28/12/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 2 di 6 del 27/12/2023 17:49:36

Soggetto: Stefano Taraglio

S.N. Certificato: E5BBC7

Validità certificato dal 13/01/2023 11:01:07 al 13/01/2026 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 3 di 6 del 27/12/2023 16:20:10

Soggetto: Elena Teresa Tropiano

S.N. Certificato: 15F9887

Validità certificato dal 28/07/2021 10:38:02 al 28/07/2024 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 4 di 6 del 22/12/2023 15:35:31

Soggetto: Stefania Marino

S.N. Certificato: BDF488

Validità certificato dal 02/09/2022 12:48:30 al 16/09/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT

CAdES 5 di 6 del 21/12/2023 14:36:37

Soggetto: Francesco Pensalfini

S.N. Certificato: 16E5129

Validità certificato dal 30/03/2022 16:57:33 al 08/04/2025 00:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT

CAdES 6 di 6 del 21/12/2023 12:23:29

Soggetto: Simona Iaropoli

S.N. Certificato: B2B41D

Validità certificato dal 21/07/2022 09:52:51 al 21/07/2025 00:00:00

Rilasciato da InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT
