

APPALTO SPECIFICO INDETTO DA ACI INFORMATICA PER L’AFFIDAMENTO DELLA FORNITURA DI ACCESSI INTERNET PROTETTI DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI ROMA IN VIA FIUME DELLE PERLE E SULLA SEDE DEL CONSORZIO NAMEX DI ROMA IN VIA DEI TIZII NELL’AMBITO DEL SISTEMA DINAMICO DI ACQUISIZIONE DELLA PUBBLICA AMMINISTRAZIONE PER LA FORNITURA DI PRODOTTI E SERVIZI PER L’INFORMATICA E LE TELECOMUNICAZIONI - ID SIGEF 2681 – CODICE AFFIDAMENTO ICT0966A25

PROGETTO DEL SERVIZIO

Allegati:

- 1) Relazione tecnica generale
- 2) Quadro economico dell’Appalto Specifico
- 3) Capitolato tecnico_ Via Fiume delle Perle_Lotto 1
- 4) Capitolato tecnico_ Via Dei Tizii_Lotto 2
- 5) Schema di contratto_ Lotto 1
- 6) Schema di contratto_ Lotto 2
- 7) Capitolato Speciale di Appalto di Servizi (CSA) - Parte generale

Il Responsabile Unico del Progetto

Gianluca Romeo Stefani

APPALTO SPECIFICO INDETTO DA ACI INFORMATICA PER L’AFFIDAMENTO DELLA FORNITURA DI ACCESSI INTERNET PROTETTI DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI ROMA IN VIA FIUME DELLE PERLE E SULLA SEDE DEL CONSORZIO NAMEX DI ROMA IN VIA DEI TIZII NELL’AMBITO DEL SISTEMA DINAMICO DI ACQUISIZIONE DELLA PUBBLICA AMMINISTRAZIONE PER LA FORNITURA DI PRODOTTI E SERVIZI PER L’INFORMATICA E LE TELECOMUNICAZIONI - ID SIGEF 2681 – CODICE AFFIDAMENTO ICT0966A25

ALLEGATO 1_RELAZIONE TECNICA GENERALE DI PROGETTO
(ex art. 41, d.lgs. 36/2023)

Sommario

PREMESSE	4
1) QUADRO DEGLI STRUMENTI CONSIP ATTIVI	4
2) OBIETTIVI DEI SERVIZI IN AFFIDAMENTO	5
3) SUDDIVISIONE IN LOTTI	6
3.1 Criteri di suddivisione in Lotti	6
3.2 Partecipazione e Vincolo di Aggiudicazione	6
4) DESCRIZIONE DEL SERVIZIO	7
4.1 LOTTO 1_ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI VIA FIUME DELLE PERLE	7
4.1.1 Caratteristiche dell'accesso internet	7
4.1.2 Servizio di assistenza sulla connettività	7
4.1.3 Caratteristiche del servizio DDOS	8
4.2 ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI VIA DEI TIZII	8
4.2.1 Caratteristiche dell'accesso internet	8
4.2.2 Servizio di assistenza sulla connettività	8
4.2.3 Caratteristiche del servizio DDOS	9
5) ANALISI ECONOMICA E VALORI DI GARA	10
6) QUADRO ECONOMICO GENERALE E DI LOTTO	11
7) PROCEDURA DI GARA PRESCELTA	15
8) CRITERIO DI AGGIUDICAZIONE	15
9) RELAZIONE TECNICA DI CONFORMITA'	15
10) SOGGETTI AMMESSI ALLA GARA	15
11) REQUISITI DI PARTECIPAZIONE DI ORDINE GENERALE E SPECIALE	16
12) DURATA	16
13) CONTRATTO	16
14) LIVELLI DI SERVIZIO E PENALI LOTTO 1	16
15) LIVELLI DI SERVIZIO E PENALI LOTTO 2	18
16) SOPRALLUOGO FACOLTATIVO	19
17) GARANZIA PROVVISORIA E DEFINITIVA	19
18) POLIZZA ASSICURATIVA	19
19) SEGGIO DI GARA	19

PREMESSE

ACI Informatica S.p.A., per l'esercizio delle funzioni istituzionali e nella sua qualità di società in house providing dell'Automobile Club Italia – ACI, è tenuta a porre in essere ogni utile iniziativa gestionale, organizzativa o acquisitiva volta al mantenimento del ruolo di conservatore del Pubblico Registro Automobilistico, sia in veste di fornitore di servizi di gestione degli archivi di riscossione tasse auto alle Regioni/Province autonome sue clienti, sia come gestore dei canali di incasso della tassa automobilistica (Internet, con il servizio BolloNet, pagoPA, delegazioni ACI, poli telematici, etc.).

In tal contesto, ACI Informatica ha necessità di rinnovare e potenziare la propria infrastruttura di connessione ad Internet mantenendo la medesima architettura attualmente in uso che prevede due diversi fornitori su due diverse sedi dotata anche del servizio DDoS (Distributed Denial-of-Service) che prevede l'uso di strumenti e servizi di cybersecurity per prevenire o risolvere rapidamente gli attacchi informatici di tipo DDoS, che chiudono data center, app, siti web e altre risorse inondandoli di traffico fraudolento.

Pertanto, con Richiesta di Acquisto (RdA) n. 211 del 29/10/2025 il Direttore Esercizio Sistemi e Applicazioni Centrali, Soci e Federazioni, stante la prossima scadenza degli analoghi contratti attualmente in essere, ha richiesto la fornitura di due nuovi accessi Internet più servizi accessori da attestare in Roma nelle sale del proprio data center di Roma via Fiume delle Perle 24 e nelle sale del data center del Consorzio Namex di Roma via dei Tizii nello spazio riservato e a disposizione della committente.

Il presente documento illustra l'analisi economica e le ulteriori clausole disciplinanti le prestazioni da fornire nell'ambito del contratto avente ad oggetto la fornitura di due accessi internet protetti da servizio di sicurezza anti DDoS da attestare sulla sede di via Fiume delle Perle e sulla sede del Consorzio Namex di via dei Tizii.

1) QUADRO DEGLI STRUMENTI CONSIG ATTIVI

L'art. 1, comma 449, della L. n. 296/2006, così come modificato dall'art. 1, comma 495, lett. a) della L. n. 208/2015 (c.d. legge di stabilità per il 2016) ha ulteriormente esteso per gli organismi di diritto pubblico di cui all'art. 1, D. Lgs. 165/2001 la facoltà/obbligo di aderire alle convenzioni Consip, ove vigenti *rationae materiae*.

Allo stato attuale, non ci sono Convenzioni Consip attive per la fornitura oggetto della presente procedura.

Ai fini dell'affidamento dei servizi di accesso internet protetto da servizio di sicurezza anti DDoS, ACI Informatica procederà con autonoma procedura di gara, suddivisa in due lotti, tramite indizione di Appalto Specifico a valersi sul Sistema Dinamico di Acquisizione della Pubblica Amministrazione (SDAPA) messo a disposizione da Consip S.p.A. ai sensi delle previsioni di cui all'art. 32 del d.lgs. 36/2023.

In tal contesto è attivo il SDA per la fornitura di prodotti e servizi per l'Informatica e le Telecomunicazioni con ID SIGEF 2681 che include, la categoria "Sicurezza informatica", CPV: 72000000-5 (Servizi informatici: consulenza, sviluppo di software, Internet e supporto) che risponde alle esigenze della Stazione Appaltante.

L'acquisizione in oggetto, stante i valori stimati come di seguito riportati, è inserita nell'ambito della programmazione triennale dei lavori, beni e dei servizi 2025-2026-2027 (CUI

S00405030586202500028). Essa trova la copertura economica nell'ambito del Budget 2025 di spesa della Direzione Richiedente.

2) OBIETTIVI DEI SERVIZI IN AFFIDAMENTO

I servizi in affidamento hanno lo scopo di garantire per ciascuna delle sedi sopra indicate la fornitura di accesso Internet in fibra ottica con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente, la fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico e un servizio di sicurezza di tipo anti DDoS (Distributed Denial-of-Service) attivo sul tutto il traffico trasportato dall'accesso ovvero per tutti gli IP pubblici annunciati della committente e quelli messi a disposizione del fornitore.

3) SUDDIVISIONE IN LOTTI

3.1 Criteri di suddivisione in Lotti

Al fine di differenziare gli operatori economici per le due sedi per ragioni di sicurezza dell'approvvigionamento e resilienza operativa si è ritenuto opportuno, ai sensi dell'art. 58 del D.Lgs. 36/2023, procedere alla suddivisione dell'appalto nei seguenti 2 (due) Lotti:

N. LOTTO	OGGETTO
LOTTO 1	ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE VIA FIUME DELLE PERLE
LOTTO 2	ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI VIA DEI TIZII

In particolare, la suddetta articolazione in lotti è stata individuata secondo i seguenti criteri direttivi:

- criterio funzionale e territoriale: la suddivisione delle prestazioni è basata sulle specifiche sedi/siti della Committente. Tale scelta è finalizzata a garantire la Business Continuity e la ridondanza delle infrastrutture di rete e sicurezza (routing IP e difesa perimetrale).
- criterio di cyber-resilienza: la necessità di diversificare i fornitori risponde all'esigenza di prevenire fenomeni di single point of failure. La diversificazione tecnologica e infrastrutturale permette di mitigare l'impatto di attacchi informatici mirati a vulnerabilità specifiche di un singolo fornitore o guasti infrastrutturali localizzati (es. eventi atmosferici, lavori stradali).
- criterio di proporzionalità e accesso al Mercato: la ripartizione è coerente con la struttura dello SDAPA, essendo finalizzata a rendere i lotti dimensionalmente proporzionati. In combinazione con i requisiti minimi di fatturato della piattaforma, tale struttura garantisce l'effettiva partecipazione delle micro, piccole e medie imprese (PMI), favorendo una competizione basata sull'efficienza e sulla qualità del servizio.

3.2 Partecipazione e Vincolo di Aggiudicazione

Ciascun Operatore Economico potrà presentare offerta per uno o più lotti, senza limitazioni. Tuttavia, al fine di garantire la massima continuità operativa e la resilienza complessiva della Committente, viene stabilito un vincolo di aggiudicazione in base al quale a ciascun concorrente non potrà essere aggiudicato più di un singolo lotto. Questa limitazione è strettamente funzionale a garantire la resilienza (in quanto in caso di disservizi generalizzati o vulnerabilità critiche sull'infrastruttura di un operatore, l'altro sito rimarrà operativo) ed a diversificare le soluzioni al fine di ridurre l'impatto di attacchi informatici mirati a specifiche vulnerabilità hardware/software di un singolo vendor.

Qualora un operatore economico risulti primo in graduatoria per più di un lotto, la Stazione Appaltante procederà all'individuazione del lotto da aggiudicare applicando i seguenti criteri in ordine gerarchico:

- massimo vantaggio economico complessivo: il lotto verrà assegnato in base alla combinazione di aggiudicazioni che genererà il maggior ribasso complessivo per l'Amministrazione su tutti i lotti

interessati dalla sovrapposizione.

- importo a base di gara: qualora le combinazioni di spesa risultino equivalenti, si procederà all'aggiudicazione del lotto avente l'importo a base di gara più elevato.

4) DESCRIZIONE DEL SERVIZIO

4.1 LOTTO 1_ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI VIA FIUME DELLE PERLE

Il Lotto 1 riguarda la fornitura ad ACI Informatica di un nuovo accesso Internet più servizi accessori da attestare nelle sale del proprio data center sito in Roma alla via Fiume delle Perle 24. In particolare, trattasi dei seguenti servizi:

1. Un accesso Internet in fibra ottica in doppia via con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente.
2. Fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico.
3. Un servizio di sicurezza di tipo anti DDoS (Distributed Denial-of-Service) attivo sul tutto il traffico trasportato dall'accesso ovvero per tutti gli IP pubblici annunciati della committente e quelli messi a disposizione del fornitore al punto due.

Il circuito dovrà essere consegnato ad ACI Informatica in doppia via protetta secondo specifiche meglio indicate nel capitolato tecnico, con accesso differenziato allo stabile su due lati e civici differenti. In particolare, il fornitore dovrà utilizzare i due seguenti accessi al data center:

- Primo accesso, lato via della Grande Muraglia n. 580;
- Secondo accesso, lato via Fiume delle Perle n. 24.

4.1.1 Caratteristiche dell'accesso internet

L'accesso Internet richiesto dovrà avere le caratteristiche generali minime previste al paragrafo 2 del capitolato tecnico allegato.

4.1.2 Servizio di assistenza sulla connettività

Il fornitore deve garantire un Help Desk in lingua italiana attivo h24, 7 giorni su 7 tramite numero unico, per segnalazioni su guasti o routing BGP. Ogni richiesta deve generare un "Trouble ticket" con presa in carico entro 30 minuti e aggiornamenti costanti via email. I recapiti operativi saranno scambiati alla firma del contratto. Per un maggiore dettaglio di tale servizio si rinvia all'art. 3 del capitolato tecnico allegato.

Il servizio di connettività deve essere garantito h24, 7 giorni su 7 con una disponibilità mensile minima del 99,9%. Il circuito è considerato non disponibile anche in caso di forte degrado delle performance con perdita di pacchetti superiore al 2%.

Il fornitore dovrà garantire il ripristino del servizio entro 4 ore per guasti bloccanti (indisponibilità totale, perdita pacchetti >2% o problemi al routing BGP) ed entro 12 ore per guasti non bloccanti (degrado lieve), come meglio specificato al paragrafo 4 del capitolato tecnico allegato

Per un maggiore dettaglio di tale servizio di assistenza, sulla disponibilità dello stesso, sui tempi di ripristino e sulle performance richieste si rinvia all'art. 4 del capitolato tecnico allegato.

4.1.3 Caratteristiche del servizio DDOS

Sul circuito di accesso fornito dovrà essere attivato un servizio di sicurezza finalizzato alla protezione contro attacchi di tipo DDoS (Distributed Denial-of-Service). Il servizio dovrà essere realizzato sulla rete del carrier in modo da selezionare e bloccare il traffico "malevolo" prima che arrivi ad interferire o saturare l'accesso in sede cliente. Non sono richiesti apparati dedicati da installare presso la committente.

Il sistema nel suo complesso dovrà prevedere quindi un sistema di monitoraggio del traffico per rilevare eventi DDoS e un sistema di verifica e "ripulitura" del traffico (scrubbing).

Una volta sottoposto alla verifica e ripulitura il traffico dovrà essere riconsegnato verso l'accesso fornito.

Il servizio deve essere realizzato su infrastruttura del fornitore e gestito direttamente da proprie strutture sistemiche, **non è ammesso un servizio offerto tramite terze parti**.

Per i livelli di servizio minimi che il fornitore si deve impegnare a garantire per tutta la durata del contratto per la protezione DDoS e per gli indicatori di qualità del servizio di sicurezza anti DDos si rinvia al paragrafo 6 del capitolato tecnico allegato.

4.2 ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI VIA DEI TIZII

Il Lotto 2 riguarda la fornitura ad ACI Informatica di un nuovo accesso Internet più servizi accessori da attestare nelle sale del datacenter del CONSORZIO NAMEX di Roma via dei Tizii nello spazio riservato e a disposizione della committente.

In particolare, trattasi dei seguenti servizi:

1. Un accesso Internet in fibra ottica con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente.
2. Fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico.
3. Un servizio di sicurezza di tipo anti DDoS (Distributed Denial-of-Service) attivo sul tutto il traffico trasportato dall'accesso fornito e per tutti gli IP pubblici a disposizione della committente compresi quelli messi a disposizione del fornitore al punto due.

4.2.1 Caratteristiche dell'accesso internet

L'accesso Internet richiesto dovrà avere le caratteristiche generali minime previste al paragrafo 2 del Capitolato tecnico allegato.

4.2.2 Servizio di assistenza sulla connettività

Il fornitore deve garantire un Help Desk in lingua italiana attivo h24, 7 giorni su 7 tramite numero unico, per segnalazioni su guasti o routing BGP. Ogni richiesta deve generare un "Trouble ticket" con presa in carico entro 30 minuti e aggiornamenti costanti via email. I recapiti operativi saranno scambiati alla firma del contratto. Per un maggiore dettaglio di tale servizio di assistenza si rinvia all'art. 3 del Capitolato tecnico allegato.

Il servizio di connettività deve essere garantito h24, 7 giorni su 7 con una disponibilità mensile minima del 99,8%. Il circuito è considerato non disponibile anche in caso di forte degrado delle

performance con perdita pacchetti superiore al 2%.

Il fornitore dovrà garantire il ripristino del servizio entro 8 ore per guasti bloccanti (indisponibilità totale, perdita pacchetti >2% o problemi al routing BGP) ed entro 12 ore per guasti non bloccanti (degrado lieve), come meglio specificato al paragrafo 4 del capitolato tecnico allegato.

Per un maggiore dettaglio di tale servizio di assistenza, sulla disponibilità dello stesso, sui tempi di ripristino e sulle performance richieste si rinvia all'art. 4 del Capitolato tecnico allegato

4.2.3 Caratteristiche del servizio DDOS

Sul circuito di accesso fornito dovrà essere attivato un servizio di sicurezza finalizzato alla protezione contro attacchi di tipo DDoS (Distributed Denial of Service). Il servizio dovrà essere realizzato sulla rete del carrier in modo da selezionare e bloccare il traffico "malevolo" prima che arrivi ad interferire o saturare l'accesso in sede cliente. Non sono richiesti apparati dedicati da installare presso la committente.

Il sistema nel suo complesso dovrà prevedere quindi un sistema di monitoraggio del traffico per rilevare

eventi ddos e un sistema di verifica e "ripulitura" del traffico (scrubbing).

Una volta sottoposto alla verifica e ripulitura il traffico dovrà essere riconsegnato verso l'accesso fornito.

Il servizio deve essere realizzato su infrastruttura del fornitore e gestito direttamente da proprie strutture sistemistiche, **non è ammesso un servizio offerto tramite terze parti.**

Per i livelli di servizio minimi che il fornitore si deve impegnare a garantire per tutta la durata del contratto per la protezione DDoS. e per gli indicatori di qualità del servizio di sicurezza anti DDos si rinvia al paragrafo 6 del capitolato tecnico allegato.

5) ANALISI ECONOMICA E VALORI DI GARA

Si riporta in seguito la costruzione e l'analisi della base d'asta da inviare a gara per ciascun lotto.

5.1 Lotto 1

Con riferimento al Lotto 1, per la determinazione dei prezzi a base di gara, sono state utilizzate le tariffe di riferimento del mercato oggetto del servizio nonché dalle tariffe, rivalutate, attualmente in essere a seguito di precedenti iniziative acquisitive.

L'importo a base d'asta per il lotto 1 è pari ad € 95.000,00 al netto di Iva e/o di altre imposte e contributi di legge, per una durata pari a 36 mesi a partire dalla data di rilascio del circuito e del servizio anti DDoS, determinata secondo il seguente dettaglio.

Pr.	Descrizione	Unità di misura	Durata anni	Canone annuale	Base d'asta Una tantum /Canone per 3 anni	Peso relativo % rispetto la base d'asta totale
1	Realizzazione ed attivazione del collegamento di accesso ad Internet	una tantum	—		€ 20.000,00	21,00%
2	Servizio di accesso ad Internet e servizio di sicurezza anti-DDoS da erogare con le modalità previste nel capitolato tecnico (canone unico)	Canone	3	€ 25.000	€ 75.000,00	79,00%
Totale importo a base d'asta lotto 1					€ 95.000,00	100%

In merito all'attività oggetto del presente appalto riferita alla sede di via Fiume delle Perle non si riscontra alcun rischio interferenziale, trattandosi di locali CED attrezzati con impianti e logistica, dotati di elevata sicurezza ed accesso controllato. Pertanto, gli oneri per la sicurezza sono pari a zero.

L'importo a base di gara è pari a 95.000,00, di cui **€ 3.220,00** per i costi della manodopera, stimati ai sensi dell'art. 41, comma 14, del D.Lgs. 36/2023 sulla base dei minimi salariali definiti dal CCNL per il personale dipendente da imprese esercenti servizi di Telecomunicazioni, codice univoco n. K411 e riferiti al profilo professionale associato al codice ATECO 61.90.10 (erogazione di servizi di accesso a Internet) secondo gli elementi di seguito indicati:

Figura professionale	Livello	Costo medio orario minimo [€/h]	N. di addetti	Ore/ die	GG/ uomo	Costo Manodopera parziale	Incidenza rispetto la base d'asta (%)
Commerciale	6	29,5	1	8,00	3,00	€ 708,00	3,39%
Project manager	6	29,5	1	8,00	5,00	€ 1.180,00	
Sales Support	5	26,0	1	8,00	1,00	€ 208,00	
Pre Sales	6	29,5	1	8,00	3,00	€ 708,00	
Tecnico - operaio	5	26,0	2	8,00	1,00	€ 416,00	
TOTALE COSTO DEL PERSONALE						€ 3.220,00	

5.2 Lotto 2

Con riferimento al Lotto 2, per la determinazione dei prezzi a base di gara, sono state utilizzate le tariffe di riferimento del mercato oggetto del servizio nonché dalle tariffe, rivalutate, attualmente in essere a seguito di precedenti iniziative acquisitive.

L'importo a base d'asta per il lotto 2 è pari ad € 85.000,00 al netto di Iva e/o di altre imposte e contributi di legge, per una durata pari a 36 mesi a partire dalla data di rilascio del circuito e del servizio anti DDoS, determinata secondo il seguente dettaglio.

Pr.	Descrizione	Unità di misura	Durata in anni	Canone annuale	Base d'asta una tantum/Canone per 3 anni	Peso % rispetto la base d'asta totale
1	Realizzazione ed attivazione del collegamento di accesso ad Internet	una tantum	—		€ 10.000,00	11,76
2	Servizio di accesso ad Internet e servizio di sicurezza anti-DDoS da erogare con le modalità previste nel capitolato tecnico (canone unico)	canone	3	€ 25.000,00	€ 75.000,00	88,24
Totale base d'asta lotto 2					€ 85.000,00	100%

In merito all'attività oggetto del presente appalto per la sede di via dei Tizii non si riscontra alcun rischio interferenziale, trattandosi di locali CED attrezzati con impianti e logistica, dotati di elevata sicurezza ed accesso controllato. Pertanto, gli oneri per la sicurezza sono paria zero.

L'importo a base di gara è pari a € 85.000,00, di cui **€ 3.012,00** per costi della manodopera, stimati ai sensi dell'art. 41, comma 14, del D.Lgs. 36/2023 sulla base dei minimi salariali definiti dal CCNL per il personale dipendente da imprese esercenti servizi di Telecomunicazioni codice univoco n. K411, e riferiti al profilo professionale associato al codice ATECO 61.90.10 (erogazione di servizi di accesso a Internet) secondo gli elementi di seguito indicati.

Figura professionale	Livello	Costo medio orario minimo [€/h]	N. di addetti	Ore/ die	GG/ uomo	Costo Manodopera parziale	Incidenza rispetto la base d'asta (%)
Commerciale	6	29,5	1	8,00	3,00	€ 708,00	3,54%
Project manager	6	29,5	1	8,00	5,00	€ 1.180,00	
Sales Support	5	26,0	1	8,00	1,00	€ 208,00	
Pre Sales	6	29,5	1	8,00	3,00	€ 708,00	
Tecnico - operaio	5	26,0	1	8,00	1,00	€ 208,00	
TOTALE COSTO DEL PERSONALE						€ 3.012,00	

6) QUADRO ECONOMICO GENERALE E DI LOTTO

Di seguito si espone il conto economico dell'appalto:

QUADRO ECONOMICO DI PROGETTO - LOTTO 1 e 2

1)	VALORE SERVIZI LOTTO 1 [36 mesi]		€ 95.000,00
1.1)	DI CUI MANODOPERA ART.41		€ 3.220,00
2)	VALORE SERVIZI LOTTO 2 [36 mesi]		€ 85.000,00
2.1)	DI CUI MANODOPERA ART.41		€ 3.012,00
A)	TOTALE BASE D'ASTA SERVIZI RIBASSABILE		€ 180.000,00
	Oneri attuazione dei piani di sicurezza ordinari/interf.	0,00% di A)	€ 0,00
A2)	TOTALE SERVIZI A BASE al lordo degli oneri sicurezza		€ 180.000,00
B)	SOMME A DISPOSIZIONE DELL' AMM.NE :		
B 2	Oneri derivanti dell'eventuale quinto d'obbligo	0,00% di A)	€ 0,00
B 2.1	Opzione ripetizione servizi analoghi		€ 150.000,00
B 3	Indagini :		
B 3.1	Indagini geologiche		€ 0,00
B 3.2	Accertamenti		€ 0,00
B 3.3	Rilievi		€ 0,00
		tot.	€ 0,00
B 4	Allacciamenti ai pubblici servizi :		€ 0,00
B 5	Imprevisti (CCT ex c.1 art. 215 dlgs. 36/2023 e art.7bis L. 120/2020)	0,50% del totale	€ 0,00
B 6	Acquisizione aree o immobili		€ 0,00
B 7	Art.45 D.Lgs. n.36/2023:	2,00% di A2+B2+B2.1	
B 7.1	RUP		
B 7.2	Direttore Lavori/DEC		€
B 7.3	Assistenti tecnici/amministrativi		
B 7.4	accantonamento (20% del 2%)		€ 1.320,00
		tot.	€ 6.600,00
B 8	Spese per tecnici esterni	0,00% di A)	€ 0,00
B 9	Spese per attività di consulenza o di supporto		€ 0,00
B 10	Spese per commissioni giudicatrici		€ 0,00
B 11	Spese per pubblicità/CONTRIBUTO ANAC		€ 500,00
B 12	Accertamenti di laboratorio, verifiche, collaudi		€ 0,00
B 13	I.V.A ed eventuali altre imposte :		
B 13.1	Inpdap/Inps/CP	0,00% di A	€ 0,00
B 13.2	I.V.A.	22,00% di A2+B2+B2.1	€ 72.600,00
B 13.3	I.V.A. su spese tecniche	0,00% di B8	€ 0,00
B 13.4	I.V.A. su spese B3.1	22,00% di B3.1	€ 0,00
		tot.	€ 72.600,00
	TOTALE SOMME A DISPOSIZIONE		€ 79.700,00

TOTALE PROGETTO (A+B) **€ 259.700,00**

ROMA, Li 6/02/2026

il Responsabile di fase della progettazione

Gianluca Romeo Stefani

QUADRO ECONOMICO DI PROGETTO - LOTTO 1

1)	VALORE SERVIZI LOTTO 1 [36 mesi]	€ 95.000,00
1.1)	DI CUI MANODOPERA ART.41	€ 3.220,00
A)	TOTALE BASE D'ASTA SERVIZI RIBASSABILE	€ 95.000,00
	Oneri attuazione dei piani di sicurezza ordinari/interf. 0,00% di A)	€ 0,00
A2)	TOTALE SERVIZI A BASE al lordo degli oneri sicurezza	€ 95.000,00
B)	SOMME A DISPOSIZIONE DELL' AMM.NE :	
B 2	Opzione ripetizione servizi analoghi	€ 75.000,00
B 3	Indagini :	
B 3.1	Indagini geologiche	€ 0,00
B 3.2	Accertamenti	€ 0,00
B 3.3	Rilievi	€ 0,00
	tot.	€ 0,00
B 4	Allacciamenti ai pubblici servizi :	€ 0,00
B 5	Imprevisti (CCT ex c.1art. 215 dlgs. 36/2023 e art.7bis L.120/2020)	del totale € 0,00
B 6	Acquisizione aree o immobili	€ 0,00
B 7	Art.45 D.Lgs. n.36/2023:	2,00% di A2+B2
B 7.1	RUP	
B 7.2	Direttore Lavori/DEC	€
B 7.3	Assistenti tecnici/amministrativi	
B 7.4	Accantonamento (20% del 2%)	€ 680,00
	tot.	€ 3.400,00
B 8	Spese per tecnici esterni	0,00% di A) € 0,00
B 9	Spese per attività di consulenza o di supporto	€ 0,00
B 10	Spese per commissioni giudicatrici	€ 0,00
B 11	Spese per pubblicità/Contributo ANAC	€ 250,00
B 12	Accertamenti di laboratorio, verifiche, collaudi	€ 0,00
B 13	I.V.A ed eventuali altre imposte :	
B 13.1	Inpdap/Inps/CP	0,00% di A € 0,00
B 13.2	I.V.A.	22,00% di A2+B2+B5+B1 € 37.400,00
B 13.3	I.V.A. su spese tecniche	0,00% di B8 € 0,00
B 13.4	I.V.A. su spese B3.1	22,00% di B3.1 € 0,00
	tot.	€ 37.400,00
	TOTALE SOMME A DISPOSIZIONE	€ 116.050,00
	TOTALE PROGETTO (A+B)	€ 211.050,00
ROMA, Lì 6/02/2026		il Responsabile di fase della progettazione
		Gianluca Romeo Stefani

QUADRO ECONOMICO DI PROGETTO - LOTTO 2

2)	VALORE SERVIZI LOTTO 2 [36 mesi]	€ 85.000,00
2.1)	DI CUI MANODOPERA ART.41	€ 3.012,00
A)	TOTALE BASE D'ASTA SERVIZI RIBASSABILE	€ 85.000,00
	Oneri attuazione dei piani di sicurezza ordinari/interf. 0,00% di A)	€ 0,00
A2)	TOTALE SERVIZI A BASE al lordo degli oneri sicurezza	€ 85.000,00
B)	SOMME A DISPOSIZIONE DELL' AMM.NE :	
B 2	Opzione ripetizione servizi analoghi	€ 75.000,00
B 3	<i>Indagini :</i>	
B 3.1	<i>Indagini geologiche</i>	€ 0,00
B 3.2	<i>Accertamenti</i>	€ 0,00
B 3.3	<i>Rilievi</i>	€ 0,00
	tot.	€ 0,00
B 4	Allacciamenti ai pubblici servizi :	€ 0,00
B 5	Imprevisti (CCT ex c.1art. 2°5 dlgs. 36/2023 e art.7bis L. 120/2020) 0,50% del totale	€ 0,00
B 6	Acquisizione aree o immobili	€ 0,00
B 7	Art.45 D.Lgs. n.36/2023: 2,00% di A2+B2	
B 7.1	<i>RUP</i>	
B 7.2	<i>Direttore Lavori/DEC</i>	€
B 7.3	<i>Assistenti tecnici/amministrativi</i>	
B 7.4	<i>accantonamento (20% del 2%)</i>	€ 640,00
	tot.	€ 3.200,00
B 8	Spese per tecnici esterni 0,00% di A)	€ 0,00
B 9	Spese per attività di consulenza o di supporto	€ 0,00
B 10	Spese per commissioni giudicatrici	€ 0,00
B 11	Spese per pubblicità/Contributo ANAC	€ 250,00
B 12	Accertamenti di laboratorio, verifiche, collaudi	€ 0,00
B 13	I.V.A ed eventuali altre imposte :	
B 13.1	<i>Inpdap/Inps/CP</i> 0,00% di A	€ 0,00
B 13.2	<i>I.V.A.</i> 22,00% di A2+B2+B5+B13.1	€ 35.200,00
B 13.3	<i>I.V.A. su spese tecniche</i> 0,00% di B8	€ 0,00
B 13.4	<i>I.V.A. su spese B3.1</i> 22,00% di B3.1	€ 0,00
	tot.	€ 35.200,00
	TOTALE SOMME A DISPOSIZIONE	€ 113.650,00

TOTALE PROGETTO (A+B) **€ 198.650,00**

ROMA, Li 6/02/2026

il Responsabile di fase della progettazione
Gianluca Romeo Stefani

7) PROCEDURA DI GARA PRESCELTA

Sarà indetto un appalto specifico nell'ambito del sistema dinamico di acquisizione della pubblica amministrazione (SDAPA) per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni ID SIGEF 2681, per la categoria "Sicurezza informatica", CPV: 72000000-5 (Servizi informatici: consulenza, sviluppo di software, Internet e supporto) che risponde alle esigenze della Stazione Appaltante.

8) CRITERIO DI AGGIUDICAZIONE

In relazione all'oggetto dell'affidamento si ritiene che il criterio di aggiudicazione più indicato sia quello del minor prezzo, tenuto conto che, ai sensi dell'art. 108 comma 3 del D.Lgs. 36/2023, si tratta di servizi/forniture con caratteristiche standardizzate o le cui condizioni sono definite dal mercato e che non si tratta di servizi ad alta intensità di manodopera.

9) RELAZIONE TECNICA DI CONFORMITA'

I concorrenti dovranno presentare, **a pena di esclusione**, per ciascun lotto d'interesse, una relazione tecnica finalizzata esclusivamente a consentire alla Stazione Appaltante/RUP di verificare la conformità dei servizi proposti alle specifiche tecniche e ai requisiti minimi obbligatori stabiliti nel Capitolato.

Non essendo prevista nella piattaforma SDAPA la possibilità di configurare a sistema una busta tecnica a fronte del criterio di aggiudicazione prescelto del minor prezzo, tale documentazione tecnica di conformità dovrà essere inserita all'interno della **Busta Amministrativa**.

La relazione tecnica, debitamente compilata e sottoscritta digitalmente, dovrà illustrare dettagliatamente la rispondenza dell'offerta a ciascun requisito indicato nella tabella riepilogativa di cui al paragrafo 13 del capitolato tecnico di ciascun lotto.

La relazione tecnica dovrà contenere un **numero massimo di 15 pagine** e dovrà essere organizzata per sezioni, una sezione per ciascuna macrocategoria indicata al paragrafo 13 del capitolato tecnico di ciascun lotto (dalla lettera A alla lettera N per il lotto 1 e dalla lettera A alla lettera M per il lotto 2).

La relazione tecnica non dovrà contenere varianti migliorative rispetto al Capitolato tecnico, ma solo la descrizione analitica di come l'Operatore economico intende soddisfare i requisiti minimi e non dovrà contenere alcun riferimento a prezzi, costi o elementi economici.

La relazione tecnica non darà luogo all'attribuzione di punteggi di merito, ma sarà oggetto di una valutazione di tipo "on/off" (conforme/non conforme).

10) SOGGETTI AMMESSI ALLA GARA

Alla procedura esperita mediante l'indizione di appalto specifico nell'ambito del Sistema Dinamico di Acquisizione (SDAPA) saranno inviati tutti gli operatori economici qualificati per la categoria merceologica prescelta dalla Stazione Appaltante.

11) REQUISITI DI PARTECIPAZIONE DI ORDINE GENERALE E SPECIALE

I criteri di selezione, i requisiti generali, i requisiti speciali ovvero i requisiti professionali e quelli economico-finanziari di partecipazione alla presente procedura sono riportati in sede di Capitolato d'Oneri allegato alla Lettera di Invito dell'AS.

12) DURATA

La durata del Contratto per ciascun lotto è fissata in 36 mesi a partire dalla data di rilascio del circuito e del servizio anti DDoS che dovrà avvenire entro e non oltre 90 giorni solari dalla sottoscrizione del contratto e dovrà essere certificato da un apposito verbale di collaudo positivo sottoscritto dalle parti.

La stazione appaltante si riserva per ciascun lotto, ai sensi dell'articolo 76, comma 6, del D.lgs. 36/2023 e s.m.i., la facoltà di affidare all'aggiudicatario entro il triennio successivo alla stipula del contratto originale, per 36 mesi, nuovi servizi consistenti nella ripetizione dei servizi analoghi relativi al canone di accesso ad Internet e di sicurezza anti-DDoS per un importo stimato complessivamente non superiore ad € 75.000,00, per ciascun lotto, al netto di Iva, oltre gli oneri della sicurezza.

In casi eccezionali, il contratto in corso di esecuzione può essere prorogato per il tempo strettamente necessario alla conclusione della procedura di individuazione del nuovo contraente se si verificano le condizioni indicate all'articolo 120, comma 11, del Codice. In tal caso, il contraente è tenuto all'esecuzione delle prestazioni oggetto del contratto agli stessi prezzi, patti e condizioni previsti nel contratto.

13) CONTRATTO

ACI Informatica sottoscriverà un contratto che ai sensi dell'art. 18, comma 1, del D.Lgs. 366/2023 e s.m.i., sarà stipulato mediante scrittura privata in modalità elettronica.

14) LIVELLI DI SERVIZIO E PENALI LOTTO 1

Accesso ad Internet	Tempi di rilascio del servizio	Penale
Attivazione collegamento di accesso ad Internet	90 giorni solari dall'ordine	Per ogni giorno di ritardo nella consegna dell'attivazione del circuito, verrà applicata una penale pari al 1,5 per mille del canone annuo per ogni giorno di ritardo

Servizio di connettività Internet	Valore atteso	Penale
Disponibilità del servizio	h24, 7 giorni su 7 con un livello di servizio garantito di almeno il 99,9% calcolato su base mensile.	Il mancato rispetto di tale requisito comporterà l'applicazione di una penale proporzionale alla diminuzione della disponibilità reale rilevata. La penale viene

	Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%	calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per ogni scostamento in diminuzione dello 0,1%
Tempi di risoluzione anomalie bloccanti	4 ore nel caso di guasti bloccanti	Il mancato rispetto di tale requisito comporta l'applicazione di una penale pari 2% del canone mensile per ogni ora eccedente le 4 previste come tempo massimo per la risoluzione dell'anomalia bloccante.

Servizio anti DDoS	Valore atteso	Penale
Disponibilità del servizio	Il servizio di protezione dovrà essere disponibile per almeno il 99,5% del tempo (H24 x 7 gg) su base mensile.	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale che dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.
Evento DDoS	A fronte di un evento l'operatore deve intervenire con il proprio sistema di "mitigation" entro e non oltre 10 minuti dall'inizio di un evento, individuato e segnalato dai sistemi di monitoraggio e analisi dell'operatore stesso ed entro 30 minuti dall'apertura della chiamata al proprio SOC nel caso l'evento venga rilevato solamente dal cliente. Tali tempi di risoluzione devono essere garantiti almeno nel 90% dei casi	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale proporzionale alla diminuzione della percentuale di casi di intervento nei tempi concordati. La penale dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.

15) LIVELLI DI SERVIZIO E PENALI LOTTO 2

Accesso ad Internet	Tempi di rilascio del servizio	Penale
Attivazione collegamento di accesso ad Internet	90 giorni solari dall'ordine	Per ogni giorno di ritardo nella consegna dell'attivazione del circuito, verrà applicata una penale pari al 1,5 per mille del canone annuo per ogni giorno di ritardo

Servizio di connettività Internet	Valore atteso	Penale
Disponibilità del servizio	Disponibile h24, 7 giorni su 7 con un livello di servizio garantito di almeno il 99,8% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale proporzionale alla diminuzione della disponibilità reale rilevata. La penale dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per ogni scostamento in diminuzione dello 0,1%.
Tempi di risoluzione anomalie	8 ore nel caso di guasti bloccanti	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale pari 2% del canone mensile per ogni ora eccedente le 8 previste come massimo per la risoluzione dell'anomalia bloccante.

Servizio anti DDoS	Valore atteso	Penale
Disponibilità del servizio	Il servizio di protezione dovrà essere disponibile per almeno il 99,5% del tempo (H24 x 7 gg) su base mensile.	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale che dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.
Evento DDoS	A fronte di un evento l'operatore deve intervenire con il proprio sistema di "mitigation" entro e non oltre 10 minuti dall'inizio di un evento, individuato e segnalato dai sistemi di monitoraggio e analisi dell'operatore stesso entro 30	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale proporzionale alla diminuzione della percentuale di casi di intervento nei tempi concordati. La penale dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone

	minuti dall'apertura della chiamata al proprio SOC nel caso l'evento venga rilevato solamente dal cliente. Tali tempi di risoluzione devono essere garantiti almeno nel 90% dei casi.	mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.
--	---	--

16) SOPRALLUOGO FACOLTATIVO

Al fine di poter correttamente quantificare le infrastrutture da realizzare, il fornitore può richiedere alla committente di poter effettuare sopralluoghi tecnici sulle sedi oggetto dell'appalto. Si rinvia al paragrafo 10 del capitolato per le modalità, termini e orari di espletamento del sopralluogo, nonché alla disciplina specifica dello stesso che sarà contenuta nel "Capitolato d'oneri per PA".

17) GARANZIA PROVVISORIA E DEFINITIVA

La Stazione Appaltante prevede che, tenuto conto della natura e dell'entità dell'appalto specifico, sia rilasciata per ciascun lotto la garanzia provvisoria da parte di tutti i partecipanti e quella definitiva da parte dell'aggiudicatario di ciascun lotto secondo le misure e le modalità rispettivamente previste agli artt. 106 e 117 del D. Lgs. n. 36/2023 e s.m.i.

18) POLIZZA ASSICURATIVA

L'affidatario dovrà presentare una polizza assicurativa di importo non inferiore all'importo contrattuale a copertura di tutti i rischi e responsabilità connesse all'esecuzione delle attività di gara, secondo le modalità dettagliate nello schema di contratto.

19) SEGGIO DI GARA

La Stazione Appaltante nominerà il Seggio di gara, nel rispetto dell'art. 93, comma 7, del Codice, dopo la scadenza del termine per la presentazione delle offerte, composto da un numero pari a 3 membri. Il Seggio è responsabile della verifica della documentazione amministrativa e della valutazione delle offerte economiche dei concorrenti e può riunirsi con modalità telematiche che salvaguardino la riservatezza delle comunicazioni ed opera attraverso la piattaforma di approvvigionamento digitale. Per la procedura non opererà la cd. inversione procedimentale: pertanto nella prima seduta pubblica e nelle successive riservate, il Seggio controllerà la completezza e correttezza della documentazione amministrativa presentata dagli operatori partecipanti. Il Seggio è responsabile della valutazione delle economiche dei concorrenti e fornisce ausilio al RUP, ove da questi richiesto, nella valutazione della congruità delle offerte.

Il Direttore Richiedente

Dott. Oronzo Scannificio

Il Responsabile Unico del Progetto

Gianluca Romeo Stefani

QUADRO ECONOMICO DI PROGETTO - LOTTO 1 e 2

1)	VALORE SERVIZI LOTTO 1 [36 mesi]			€ 95.000,00
1.1)	DI CUI MANODOPERA ART.41			€ 3.220,00
2)	VALORE SERVIZI LOTTO 2 [36 mesi]			€ 85.000,00
2.1)	DI CUI MANODOPERA ART.41			€ 3.012,00
A)	TOTALE BASE D'ASTA SERVIZI RIBASSABILE			€ 180.000,00
	Oneri attuazione dei piani di sicurezza ordinari/interf.	0,00%	di A)	€ 0,00
A2)	TOTALE SERVIZI A BASE	al lordo degli oneri sicurezza		€ 180.000,00

B)	SOMME A DISPOSIZIONE DELL' AMM.NE :			
B 2	Oneri derivanti dell'eventuale quinto d'obbligo	0,00%	di A)	€ 0,00
B 2.1	Opzione ripetizione servizi analoghi			€ 150.000,00
B 3	<i>Indagini :</i>			
B 3.1	<i>Indagini geologiche</i>			€ 0,00
B 3.2	<i>Accertamenti</i>			€ 0,00
B 3.3	<i>Rilievi</i>			€ 0,00
			tot.	€ 0,00
B 4	Allacciamenti ai pubblici servizi :			€ 0,00
B 5	Imprevisti (CCT ex c.1 art. 215 dlgs. 36/2023 e art.7bis L. 120/2020)	0,50%	del totale	€ 0,00
B 6	Acquisizione aree o immobili			€ 0,00
B 7	Art.45 D.Lgs. n.36/2023:	2,00%	di A2+B2+B2.1	
B 7.1	<i>RUP</i>			
B 7.2	<i>Direttore Lavori/DEC</i>			
B 7.3	<i>Assistenti tecnici/amministrativi</i>			
B 7.4	<i>accantonamento (20% del 2%)</i>			€ 1.320,00
			tot.	€ 6.600,00
B 8	Spese per tecnici esterni	0,00%	di A)	€ 0,00
B 9	Spese per attività di consulenza o di supporto			€ 0,00
B 10	Spese per commissioni giudicatrici			€ 0,00
B 11	Spese per pubblicità/CONTRIBUTO ANAC			€ 500,00
B 12	Accertamenti di laboratorio, verifiche, collaudi			€ 0,00
B 13	I.V.A ed eventuali altre imposte :			
B 13.1	<i>Inpdap/Inps/CP</i>	0,00%	di A	€ 0,00
B 13.2	<i>I.V.A.</i>	22,00%	di A2+B2+B2.1	€ 72.600,00
B 13.3	<i>I.V.A. su spese tecniche</i>	0,00%	di B8	€ 0,00
B 13.4	<i>I.V.A. su spese B3.1</i>	22,00%	di B3.1	€ 0,00
			tot.	€ 72.600,00
	TOTALE SOMME A DISPOSIZIONE			€ 79.700,00

TOTALE PROGETTO (A+B) **€ 259.700,00**

ROMA, Lì 6/02/2026

il Responsabile di fase della progettazione

Gianluca Romeo Stefani

QUADRO ECONOMICO DI PROGETTO - LOTTO 1

1) VALORE SERVIZI LOTTO 1 [36 mesi] € **95.000,00**

1.1) DI CUI MANODOPERA ART.41 € 3.220,00

A) TOTALE BASE D'ASTA SERVIZI RIBASSABILE € 95.000,00

Oneri attuazione dei piani di sicurezza ordinari/interf. 0,00% di A) € 0,00

A2) TOTALE SERVIZI A BASE al lordo degli oneri sicurezza € 95.000,00

B) SOMME A DISPOSIZIONE DELL' AMM.NE :

B 2 Opzione ripetizione servizi analoghi € 75.000,00

B 3 *Indagini :*

B 3.1 *Indagini geologiche* € 0,00

B 3.2 *Accertamenti* € 0,00

B 3.3 *Rilievi* € 0,00

tot. € **0,00**

B 4 Allacciamenti ai pubblici servizi : € **0,00**

B 5 Imprevisti (CCT ex c.1 art. 215 dlgs. 36/2023 e art.7bis L.120/2020) del totale € **0,00**

B 6 Acquisizione aree o immobili € **0,00**

B 7 Art.45 D.Lgs. n.36/2023: 2,00% di A2+B2

B 7.1 *RUP*

B 7.2 *Direttore Lavori/DEC*

B 7.3 *Assistenti tecnici/amministrativi*

B 7.4 *Accantonamento (20% del 2%)* € 680,00

tot. € **3.400,00**

B 8 Spese per tecnici esterni 0,00% di A) € **0,00**

B 9 Spese per attività di consulenza o di supporto € **0,00**

B 10 Spese per commissioni giudicatrici € **0,00**

B 11 Spese per pubblicità/Contributo ANAC € **250,00**

B 12 Accertamenti di laboratorio, verifiche, collaudi € **0,00**

B 13 I.V.A ed eventuali altre imposte :

B 13.1 *Inpdap/Inps/CP* 0,00% di A € 0,00

B 13.2 *I.V.A.* 22,00% di A2+B2+B5+B13 € 37.400,00

B 13.3 *I.V.A. su spese tecniche* 0,00% di B8 € 0,00

B 13.4 *I.V.A. su spese B3.1* 22,00% di B3.1 € 0,00

tot. € **37.400,00**

TOTALE SOMME A DISPOSIZIONE € 116.050,00

TOTALE PROGETTO (A+B) € 211.050,00

ROMA, Lì 6/02/2026

il Responsabile di fase della progettazione

Gianluca Romeo Stefani

QUADRO ECONOMICO DI PROGETTO - LOTTO 2

2) VALORE SERVIZI LOTTO 2 [36 mesi] € **85.000,00**

2.1) DI CUI MANODOPERA ART.41 € 3.012,00

A) TOTALE BASE D'ASTA SERVIZI RIBASSABILE € 85.000,00

Oneri attuazione dei piani di sicurezza ordinari/interf. 0,00% di A) € 0,00

A2) TOTALE SERVIZI A BASE al lordo degli oneri sicurezza € 85.000,00

B) SOMME A DISPOSIZIONE DELL' AMM.NE :

B 2 Opzione ripetizione servizi analoghi € 75.000,00

B 3 Indagini :

B 3.1 Indagini geologiche € 0,00

B 3.2 Accertamenti € 0,00

B 3.3 Rilievi € 0,00

tot. € **0,00**

B 4 Allacciamenti ai pubblici servizi :

€ **0,00**

B 5 Imprevisti (CCT ex c.1 art. 215 dlgs. 36/2023 e art.7bis L.120/2020) 0,50% del totale € **0,00**

B 6 Acquisizione aree o immobili € **0,00**

B 7 Art.45 D.Lgs. n.36/2023: 2,00% di A2+B2

B 7.1 RUP

B 7.2 Direttore Lavori/DEC

B 7.3 Assistenti tecnici/amministrativi

B 7.4 accantonamento (20% del 2%)

€ 640,00

tot. € **3.200,00**

B 8 Spese per tecnici esterni 0,00% di A) € **0,00**

B 9 Spese per attività di consulenza o di supporto € **0,00**

B 10 Spese per commissioni giudicatrici € **0,00**

B 11 Spese per pubblicità/Contributo ANAC € **250,00**

B 12 Accertamenti di laboratorio, verifiche, collaudi € **0,00**

B 13 I.V.A ed eventuali altre imposte :

B 13.1 Inpdap/Inps/CP 0,00% di A € 0,00

B 13.2 I.V.A. 22,00% di A2+B2+B5+B13.1 € 35.200,00

B 13.3 I.V.A. su spese tecniche 0,00% di B8 € 0,00

B 13.4 I.V.A. su spese B3.1 22,00% di B3.1 € 0,00

tot. € **35.200,00**

TOTALE SOMME A DISPOSIZIONE € 113.650,00

TOTALE PROGETTO (A+B) € 198.650,00

ROMA, Lì 6/02/2026

il Responsabile di fase della progettazione

Gianluca Romeo Stefani

ALLEGATO 3 AL PROGETTO

**CAPITOLATO TECNICO PER LA FORNITURA DI UN ACCESSO INTERNET
PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI ROMA VIA FIUME DELLE PERLE**

LOTTO 1

Codice Affidamento: ICT0966A25

**Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS
sulla sede di via Fiume delle Perle**

Sommario

1	Premessa.....	3
2	Caratteristiche generali dell'accesso Internet	3
2.1	Accesso fisico e banda garantita	3
2.2	Routing BGP.....	4
2.3	Routing IPV6	4
2.4	Indirizzamento IP.....	4
2.5	Caratteristiche degli apparati di consegna	5
2.6	Dettagli ingresso alla sede dei circuiti	5
2.7	Dettaglio instradamento urbano dei circuiti	5
3	Servizio di assistenza sulla connettività Internet.....	6
4	Livelli di servizio richiesti sulla connettività Internet.....	6
4.1	Disponibilità.....	6
4.2	Tempi di ripristino guasti.....	6
4.3	Performance del servizio di connettività richieste.....	6
5	Caratteristiche del servizio di sicurezza anti "Distributed Denial of Service"	7
5.1	Monitoraggio e analisi del traffico	7
5.2	Intervento di mitigazione dell'evento DDoS	8
5.3	Reportistica.....	8
5.4	Servizio di assistenza sistema anti DDoS	8
6	Livelli di servizio richiesti per la protezione DDoS	9
6.1	Disponibilità.....	9
6.2	Tempo di intervento della "mitigation"	9
6.3	Percentuale di rilevamento	9
6.4	Tabella riassuntiva SLA richiesti sul servizio anti DDoS:	10
7	Tempi di rilascio del servizio	10
8	Relazione tecnica	10
9	Durata dei servizi richiesti.....	11
10	Sopralluoghi	11
11	Requisiti di Sicurezza e Resilienza delle Infrastrutture	11
11.1	Affidabilità e Sicurezza del Servizio.....	11
11.2	Localizzazione del Traffico e Gestione dei Flussi (Scrubbing Center)	12
11.3	Sicurezza della Catena di Approvvigionamento (Supply Chain).....	12
11.4	Governance e Supporto alla Sicurezza (SPOC).....	12
11.5	Verifiche di Compliance e Audit	12
12	Riepilogo SLA con Penali	12
13	Tabella riepilogativa dei requisiti minimi inderogabili	14

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

1 Premessa

ACI Informatica, intende rinnovare e potenziare la propria infrastruttura di connessione ad Internet mantenendo la medesima architettura attualmente in uso che prevede diversi fornitori su due diverse sedi.

Oggetto della presente gara è la fornitura ad ACI Informatica di un nuovo accesso Internet più servizi accessori da attestare nelle sale del proprio data center di via Fiume delle Perle 24.

Il circuito dovrà essere consegnato alla committente in doppia via protetta secondo specifiche indicate di seguito, con accesso differenziato allo stabile su due lati e civici differenti.

In particolare, il fornitore dovrà utilizzare i due seguenti accessi al datacenter:

- Primo accesso, lato via della Grande Muraglia 580;
- Secondo accesso, via Fiume delle Perle 24.

Il circuito di accesso fornito dovrà essere protetto da un servizio di sicurezza contro attacchi di tipo DDoS (Distributed Denial of Service) con le caratteristiche minime meglio descritte di seguito.

La procedura di gara prevede quindi la fornitura dei seguenti servizi:

1. Un accesso Internet in fibra ottica in doppia via con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente.
2. Fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico.
3. Un servizio di sicurezza di tipo anti "Distributed Denial of Service" attivo sul tutto il traffico trasportato dall'accesso ovvero per tutti gli IP pubblici annunciati della committente e quelli messi a disposizione del fornitore al punto due.

2 Caratteristiche generali dell'accesso Internet

L'accesso Internet richiesto dovrà avere le seguenti caratteristiche generali minime.

2.1 Accesso fisico e banda garantita

- Circuito di trasporto in doppia via sulla sede cliente realizzato su portanti in fibra ottica
- Doppio apparato di consegna
- Consegna del servizio lato cliente su due porte LAN 10Gbps Ethernet (LAN PHY) con ottica di tipo SR e connettori LC;
- Banda di accesso Internet indistinto di almeno 8Gbps simmetrico (8Gbps upstream, 8Gbps downstream);
- Garanzia di disponibilità della banda richiesta fino ai peering-point nazionali ed internazionali del fornitore.

2.2 Routing BGP

Al fine di permettere alla committente l'utilizzo dei prefissi del proprio AS e di quello dei clienti ospitati nel datacenter, il fornitore dovrà utilizzare sull'accesso una configurazione che preveda l'utilizzo di routing dinamico di tipo BGP4.

Al momento ACI Informatica annuncerà i seguenti due "Autonomous System":

- AS Number 42515 (ACI Informatica) con prefissi:
 - 77.73.56.0/21
 - 185.39.188.0/22
- AS Number 34405 (ANCI Digitale) con prefissi:
 - 91.226.108.0/23

La committente annuncerà verso il carrier i prefissi indicati sopra, mentre il fornitore dovrà inviare agli apparati della committente la propria "full internet table".

La committente dovrà avere la possibilità, in caso necessità e nel corso di validità del contratto, di apportare modifiche alla configurazione del peering BGP che prevedano l'aggiunta o la modifica di prefissi o Asn.

Al fine di garantire una più elevata disponibilità, e permettere una agevole manutenzione dei gateway BGP della committente, dovranno essere instaurate dal fornitore due sessioni di peering verso i due router del cliente.

2.3 Routing IPV6

Al fine di poter sperimentare ed eventualmente implementare annunci di previsti IPV6 nel corso del periodo di validità del contratto, è richiesto che tutti gli apparati forniti siano compatibili con il protocollo IPV6.

E richiesta inoltre la disponibilità da parte del fornitore a supportare la committente nell'eventuale aggiornamento delle configurazioni per permettere l'annuncio ed il routing del protocollo ipv6 contemporaneamente a quello ipv4. Non è richiesta la fornitura di prefissi ipv6 in quanto già nella disponibilità della committente.

La configurazione del routing ipv6 non è richiesta in fase di installazione e rilascio iniziale del servizio, non è richiesto nessun collaudo di questa funzionalità al fine del rilascio ufficiale del servizio.

L'implementazione del routing ipv6 potrà essere richiesta, a discrezione della committente, nel corso del periodo di validità del contratto e non dovrà comportare aggravio o revisioni dei costi da parte della committente.

2.4 Indirizzamento IP

Anche se la committente utilizzerà indirizzamento pubblico proprio è comunque richiesto al fornitore la disponibilità di alcune classi di IP Pubblici, in particolare sono richiesti:

- Fornitura degli IP pubblici necessari alla configurazione dei collegamenti punto-punto layer3 tra i router del cliente e quelli del fornitore.

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

- Fornitura di una ulteriore classe IP da almeno 64 indirizzi da utilizzare sul circuito in aggiunta a quelli di proprietà della committente da instradare attraverso routing statico, così come indicato in premessa.

2.5 Caratteristiche degli apparati di consegna

I circuiti dovranno essere terminati su doppi apparati indipendenti, uno per la prima via ed uno per la seconda. Tali apparati dovranno essere installati negli spazi messi a disposizione della committente nel proprio datacenter in due diverse sale, una per via.

È data facoltà al fornitore di prevedere soluzioni di consegna con apparati di tipo wdm prima di quelli di swithing/routing. In questo caso anche tali sistemi dovranno essere doppi ed indipendenti, uno per accesso.

Tutti gli apparati attivi forniti dovranno avere le seguenti caratteristiche:

- Doppia alimentazione elettrica monofase 220 Volts;
- Doppio alimentatore sostituibile “a caldo” senza interruzione del servizio (protezione 1+1);
- Fattore di forma per installazione in armadio tecnico standard da 19 pollici;
- Somma della dimensione massima verticale di 6 unità rack per ogni accesso.

Per quanto riguarda l'apparato di consegna questo dovrà avere:

- Porte LAN di consegna verso il cliente con velocità 10Gbps;
- Capacità di inoltro di almeno 10Gbps;

Il trasporto, montaggio e configurazione degli apparati di accesso sarà in carico al fornitore. La committente offrirà tutto il supporto necessario per la ricezione delle merci ed il presidio durante le fasi di installazione, configurazione, e attivazione del servizio.

2.6 Dettagli ingresso alla sede dei circuiti

Il circuito fisico in fibra ottica dovrà essere rilasciato in doppia via protetta, presso il Datacenter ACI Informatica, **utilizzando due accessi allo stabile, uno lato via della grande Muraglia e l'altro lato Fiume delle Perle**. Gli apparati di terminazione ed i cassetti ottici dovranno essere installati presso le sale tecniche che saranno indicate dalla committente in fase di sopralluogo. Tutto il cablaggio necessario alla realizzazione dei circuiti, anche all'interno dello stabile, dovrà essere a cura del fornitore su indicazione dei passaggi a cura della committente.

È in carico e responsabilità della committente la predisposizione dei passaggi e delle canalizzazioni necessarie a raggiungere la sala tecnica di attestazione a partire dal confine della proprietà.

In fase di realizzazione o sopralluogo verranno forniti tutti gli ulteriori dettagli tecnici, le posizioni specifiche, le canalizzazioni esistenti, i passaggi interni ed esterni da utilizzare.

2.7 Dettaglio instradamento urbano dei circuiti

Al fine di aumentare l'affidabilità del sistema e di soddisfare nuove normative sulla disponibilità dei servizi erogati dalla committente è necessario che il percorso urbano dei due cavi in fibra ottica (primario e protezione) prevedano instradamento differenziato fino alla centrale del fornitore.

È richiesto che nella documentazione tecnica fornita a corredo dell'offerta presentata, siano contenute le planimetrie e comunque le informazioni necessarie alla committente per verificare che siano rispettati i vincoli richiesti al presente paragrafo.

Al fine di poter predisporre correttamente l'offerta tecnica ed economica è data possibilità al fornitore di effettuare uno o più sopralluoghi tecnici presso la sede di ACI Informatica così come meglio specificato di seguito.

3 Servizio di assistenza sulla connettività Internet

Il fornitore dovrà garantire un servizio di assistenza a cui inoltrare eventuali segnalazioni di malfunzionamento del circuito o problemi di routing BGP. Il servizio di Help Desk dovrà rispondere ad un numero unico nazionale, in lingua italiana ed essere disponibile h24, 7 giorni su 7. Ad ogni chiamata del cliente al centro di assistenza dovrà corrispondere da parte del fornitore l'apertura e la gestione di una segnalazione individuata da un numero di "Trouble ticket". L'apertura e gli aggiornamenti relativi alla segnalazione aperta dovranno essere notificati alla committente anche tramite email. In fase di perfezionamento del contratto, la committente, fornirà gli indirizzi email e i numeri telefonici da contattare. Il servizio di help desk dovrà prendere in carico la segnalazione al massimo entro trenta minuti dalla chiamata del cliente.

4 Livelli di servizio richiesti sulla connettività Internet

4.1 Disponibilità

La connettività alla rete pubblica dovrà essere disponibile h24, 7 giorni su 7 con un livello di servizio garantito di almeno il 99,9% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%.

4.2 Tempi di ripristino guasti

A fronte di guasti o anomalie che si dovessero presentare sull'accesso internet il fornitore si dovrà impegnare alla risoluzione del problema ed il ripristino completo del servizio nel più breve tempo possibile garantendo comunque i seguenti tempi di ripristino:

- 12 ore nel caso di guasti non bloccanti;
- 4 ore nel caso di guasti bloccanti.

Con guasti non bloccanti si intendono quelle anomalie che comportano un degrado non significativo delle performance del servizio, si intendono invece bloccanti le anomalie che comportano completa indisponibilità del servizio o forte degrado dello stesso (tasso di perdita di pacchetti maggiore del 2%). Vengono considerati guasti bloccanti anche le anomalie sulle sessioni di routing BGP. La caduta contemporanea di entrambe le sessioni BGP, con l'impossibilità di annuncio da parte del cliente delle proprie reti è da considerarsi guasto bloccante e quindi da ripristinare al più presto possibile e comunque non oltre le 4 ore.

4.3 Performance del servizio di connettività richieste

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

Di seguito vengono riportate le performance minime che il fornitore si deve impegnare a garantire per tutta la durata del contratto. In particolare, come indicatori di qualità del servizio vengono individuati i seguenti parametri tecnici:

- Tempo di attraversamento dei pacchetti;
- Percentuale di perdita di pacchetti;
- Variazione di latenza o "Jitter".

I parametri individuati si riferiscono a misure effettuate in condizione di utilizzo del circuito inferiore al 80% della banda garantita contrattualizzata (8Gbps), quindi non in condizione di saturazione.

I parametri individuati devono essere garantiti all'interno della rete del fornitore, dall'accesso cliente fino ai punti di interconnessione nazionali ed internazionali.

Di seguito vengono riportati i parametri di qualità minimi richiesti:

Parametro di valutazione	Valore
Tempi di attraversamento End-to-End	≤10ms
Percentuale di perdita di pacchetti	≤ 0,1%
Variazione di latenza o Jitter	≤ 5 ms

5 Caratteristiche del servizio di sicurezza anti "Distributed Denial of Service"

Sul circuito di accesso fornito dovrà essere attivato un servizio di sicurezza finalizzato alla protezione contro attacchi di tipo DDoS (Distributed Denial of Service). Il servizio dovrà essere realizzato sulla rete del carrier in modo da selezionare e bloccare il traffico "malevolo" prima che arrivi ad interferire o saturare l'accesso in sede cliente. Non sono richiesti apparati dedicati da installare presso la committente.

Il sistema nel suo complesso dovrà prevedere quindi un sistema di monitoraggio del traffico per rilevare eventi ddos e un sistema di verifica e "ripulitura" del traffico (scrubbing).

Una volta sottoposto alla verifica e ripulitura il traffico dovrà essere riconsegnato verso l'accesso fornito.

Il servizio deve essere realizzato su infrastruttura del fornitore e gestito direttamente da proprie strutture sistemistiche, **non è ammesso un servizio offerto tramite terze parti.**

5.1 Monitoraggio e analisi del traffico

Il fornitore dovrà quindi avere a disposizione un sistema di monitoraggio e analisi del traffico diretto al cliente al fine di poter rilevare eventi di attacco informatico di tipo DDoS. Tale sistema di monitoraggio deve essere attivo su tutta l'infrastruttura del fornitore. L'offerta deve comprendere il monitoraggio continuo del traffico mediante strumenti automatizzati e la gestione di un numero di eventi di mitigazione illimitati. Il traffico "malevolo" dovrà essere individuato sia tramite analisi di tipo quantitativo che qualitativo.

Il servizio deve comprendere il monitoraggio e l'attivazione di contromisure per tutti gli indirizzi IP in uso alla committente:

- 77.73.56.0/21;
- 185.39.188.0/22;
- 91.226.108.0/23;

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

- Indirizzi assegnati dal fornitore (almeno 64 ip);
- Eventuali nuove classi annunciate dalla committente fino ad un massimo di una ulteriore subnet /21.

È richiesto che il sistema di analisi e monitoraggio, finalizzato all'individuazione di traffico di tipo ddos, sia configurabile su richiesta della committente con diversi profili distinti per gruppi di indirizzi ip. Questo al fine di stabilire, congiuntamente con il fornitore, soglie di traffico diverso per servizi diversi e minimizzare quindi i casi di falso positivo o negativo.

5.2 Intervento di mitigazione dell'evento DDoS

Al rilevamento di un evento DDoS, destinato alle sottoreti della committente, il servizio fornito dovrà avere la capacità di innescare in autonomia il reinstradamento verso i sistemi di "scrubbing" del fornitore e la "ripulitura" del traffico.

Il traffico di tipo malevolo destinato ad uno o più indirizzi IP del cliente dovrà essere "selezionato" e "separato" accuratamente da quello lecito, che dovrà essere correttamente consegnato. In caso non si riesca a separare perfettamente il traffico lecito da quello illecito e quindi la policy applicata potrebbe avere impatti sul servizio, il centro di gestione di sicurezza del fornitore dovrà contattare le strutture tecniche della committente per chiedere la conferma di attivazione della policy potenzialmente bloccante.

Qualora la committente rilevi in autonomia un evento di tipo DDoS, non segnalato come tale dal fornitore, dovrà essere comunque possibile l'attivazione su richiesta della mitigation da parte del fornitore. Il traffico classificato come "malevolo" dai sistemi di scrubbing del fornitore dovrà in ogni caso essere bloccato/scartato direttamente sull'infrastruttura del carrier prima di arrivare a saturare la capacità del circuito di accesso fornito al cliente.

Non è richiesta l'installazione di apparati o sonde presso la sede della committente.

5.3 Reportistica

A seguito di eventi DDoS il fornitore dovrà essere in grado, su richiesta del cliente, di inviare o mettere a disposizione su un proprio portale web i report contenenti i dati statistici più significativi dell'evento. Il report dovrà specificare almeno i seguenti parametri:

- Tipo di attacco;
- IP address di destinazione;
- Tempo di intervento della "mitigation";
- Volume del traffico coinvolto;
- Durata totale dell'evento.

Il report richiesto dovrà essere messo a disposizione entro 24 ore dalla richiesta.

5.4 Servizio di assistenza sistema anti DDoS

Il fornitore dovrà garantire un servizio di assistenza tramite un centro di controllo "SOC" a cui rivolgersi 24 ore su 24, 7 giorni la settimana per avere informazioni o richiedere verifiche a fronte di possibili anomalie rilevate o attacchi segnalati in atto. Il servizio dovrà rispondere ad un numero unico nazionale, in lingua italiana. L'apertura e gli aggiornamenti sulle segnalazioni di sicurezza dovranno essere notificati alla

committente anche tramite email. La committente fornirà in fase di perfezionamento del contratto gli indirizzi email da contattare.

6 Livelli di servizio richiesti per la protezione DDoS

Di seguito vengono riportati i livelli di servizio minimi che il fornitore si deve impegnare a garantire per tutta la durata del contratto. In particolare, come indicatori di qualità del servizio di sicurezza anti DDoS vengono individuati i seguenti parametri:

- Disponibilità del servizio;
- Tempo di intervento delle procedure di mitigazione;
- Percentuale di individuazione degli eventi.

6.1 Disponibilità

Per disponibilità del servizio si intende il corretto funzionamento sia della piattaforma di monitoraggio e analisi del traffico che dei sistemi attivi per l'applicazione delle policy di mitigation. Il servizio di protezione dovrà essere disponibile per almeno 99,5% del tempo (H24 x 7 gg) su base mensile. In caso di manutenzioni non programmate o di anomalie della piattaforma il fornitore dovrà, nel più breve tempo possibile, notificare al cliente lo stato di indisponibilità della piattaforma. Tutte le attività di manutenzione programmate, che comportino indisponibilità del servizio, dovranno essere comunicate al cliente con un anticipo di almeno 10 giorni.

6.2 Tempo di intervento della "mitigation"

Per tempo di intervento della "mitigation" si intende il tempo che intercorre tra l'inizio dell'anomalia e l'effettiva attivazione del sistema di protezione. Nel caso di evento individuato e segnalato dai sistemi di monitoraggio e analisi del fornitore, la policy deve essere attivata nel più breve tempo possibile e comunque entro 10 minuti dall'evento in almeno il 90% dei casi (Tempo di presa in carico Proattiva). Nel caso l'evento venga rilevato solamente dal cliente, il fornitore dovrà prendere in carico la segnalazione entro 30 minuti dall'apertura della chiamata al proprio SOC in almeno il 90% dei casi (Tempo di presa in carico Reattiva).

6.3 Percentuale di rilevamento

Il servizio fornito dovrà essere in grado di rilevare almeno il 90% degli attacchi di tipo DDoS su base mensile. Sono da considerare attacchi non rilevati tutti gli eventi non notificati o non analizzati dai sistemi del fornitore, ma che vengano rilevati dal cliente e segnalati tramite chiamata al SOC.

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

6.4 Tabella riassuntiva SLA richiesti sul servizio anti DDoS:

Indicatore Livello di servizio	Unità di misura	Valore
Disponibilità	Percentuale di up-time su base mensile (h24 x7)	99,5%
Tempo di intervento proattivo	Tempo di presa in carico in minuti (>90% dei casi)	10
Tempo di intervento reattivo	Tempo di presa in carico in minuti (>90% dei casi)	30
Percentuale di rilevamento	Percentuale di rilevamento	90%
Disponibilità Reportistica sull'attacco	Ore	24 h

7 Tempi di rilascio del servizio

Il tempo massimo ammesso per il rilascio del servizio è di 90 giorni solari. Per tempo di rilascio si intende il tempo necessario al fornitore per la realizzazione ed il collaudo di tutte le componenti del servizio a partire dalla data di formalizzazione dell'ordine. Il servizio sarà considerato collaudabile al termine della predisposizione di entrambe le componenti: accesso e sicurezza.

8 Relazione tecnica

I concorrenti dovranno presentare, **a pena di esclusione**, una relazione tecnica **finalizzata esclusivamente a consentire alla Stazione Appaltante/RUP di verificare la conformità dei servizi proposti alle specifiche tecniche e ai requisiti minimi obbligatori stabiliti nel Capitolato**.

In particolare, i concorrenti dovranno inserire nella **Busta Amministrativa** la Relazione Tecnica, debitamente compilata e sottoscritta digitalmente, che illustri dettagliatamente la rispondenza dell'offerta a ciascun requisito indicato nella tabella riepilogativa di cui al successivo paragrafo 13 come riferito alle seguenti macro-categorie:

- A) REQUISITI GENERALI
- B) ACCESSO INTERNET (FISICO E BANDA)
- C) ROUTING E INDIRIZZAMENTO
- D) CARATTERISTICHE APPARATI DI CONSEGNA
- E) INSTALLAZIONE E PERCORSI
- F) SERVIZIO DI ASSISTENZA CONNETTIVITÀ
- G) SLA CONNETTIVITÀ INTERNET
- H) SERVIZIO ANTI-DDoS
- I) REPORTISTICA E ASSISTENZA ANTI-DDoS
- L) SLA ANTI-DDoS
- M) TEMPI E CONTENUTI DELL'OFFERTA TECNICA
- N) REQUISITI DI SICUREZZA E RESILIENZA DELLE INFRASTRUTTURE

La relazione tecnica dovrà contenere, per ciascun Lotto di interesse, una relazione obbligatoria di un numero massimo di 15 pagine, organizzata per sezioni, una sezione per ciascuna macrocategoria sopra indicata.

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

La Relazione Tecnica non dovrà contenere varianti migliorative rispetto al Capitolato tecnico, ma solo la descrizione analitica di come l'Operatore economico intende soddisfare i requisiti minimi e non dovrà contenere alcun riferimento a prezzi, costi o elementi economici.

La relazione tecnica non darà luogo all'attribuzione di punteggi di merito, ma sarà oggetto di una valutazione di tipo "on/off" (conforme/non conforme).

9 Durata dei servizi richiesti

La durata richiesta per il servizio (accesso internet più anti DDoS) è di 36 mesi a partire dalla data di collaudo del circuito e del servizio anti DDoS.

10 Sopralluoghi

Al fine di poter correttamente quantificare le infrastrutture da realizzare, il fornitore può richiedere alla committente di poter effettuare sopralluoghi tecnici sulla sede oggetto della fornitura.

Gli orari previsti per i sopralluoghi sono:

- lunedì – giovedì dalla 9:00 alle 15:30;
- venerdì dalle 9:00 alle 13:30;

I sopralluoghi vanno richiesti e concordati a mezzo email all'indirizzo tlc@informatica.aci.it con almeno due giorni lavorativi di anticipo rispetto alla data prevista. Nella richiesta, oltre alla data ed orario previsto, vanno indicati i nominativi dei tecnici che interverranno. La committente indicherà volta per volta il nome del proprio riferimento che seguirà le attività di sopralluogo nella sede.

I sopralluoghi saranno accordati fino a 5 giorni solari prima del termine di presentazione dell'offerta.

11 Requisiti di Sicurezza e Resilienza delle Infrastrutture

11.1 Affidabilità e Sicurezza del Servizio

I servizi di connettività e di protezione DDoS dovranno essere erogati attraverso infrastrutture gestite in conformità con le strategie nazionali di cybersecurity. L'aggiudicatario dovrà:

- Assicurare la resilienza dei nodi di rete e dei sistemi di trasporto rispetto a incidenti informatici, garantendo la continuità operativa dei flussi dati della Committente.
- Operare in linea con le disposizioni vigenti in materia di sicurezza delle reti e dei sistemi informativi (attuazione Direttiva NIS2 e, ove applicabile, norme sul Perimetro di Sicurezza Nazionale Cibernetica).

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle**11.2 Localizzazione del Traffico e Gestione dei Flussi (Scrubbing Center)**

Per i servizi di mitigazione degli attacchi DDoS, l'aggiudicatario dovrà garantire un'architettura di rete che privilegi la protezione della sovranità dei dati e la bassa latenza. Ed inoltre:

- L'instradamento del traffico verso i centri di pulizia (Scrubbing Center) dovrà avvenire prioritariamente su nodi situati all'interno del territorio dell'Unione Europea.
- Qualora la natura dell'attacco richieda l'instradamento su reti globali, l'aggiudicatario dovrà garantire l'adozione di misure tecniche idonee a inibire l'accesso ai contenuti del traffico da parte di soggetti terzi, assicurando la piena conformità al GDPR e agli standard di sicurezza nazionali.

11.3 Sicurezza della Catena di Approvvigionamento (Supply Chain)

In conformità con gli orientamenti dell'Agenzia per la Cybersicurezza Nazionale (ACN) sulla sicurezza della filiera, l'aggiudicatario dovrà garantire che Gli apparati critici utilizzati (Router, apparati di core network, sistemi di mitigazione) non provengano da vendor oggetto di restrizioni o specifiche segnalazioni di rischio da parte delle Autorità di Sicurezza Nazionale.

In tal contesto, l'aggiudicatario dovrà fornire, su richiesta della Committente, la mappatura dei sub-fornitori tecnologici critici coinvolti nell'erogazione del servizio per consentire la valutazione dell'esposizione al rischio della catena del valore.

11.4 Governance e Supporto alla Sicurezza (SPOC)

L'aggiudicatario dovrà designare e comunicare alla Committente, entro 48 ore dalla stipula del contratto, un Referente Tecnico per la Sicurezza (Single Point of Contact) operativo H24/7. Tale figura avrà il compito di:

- Coordinare le attività di risposta agli incidenti informatici con le strutture tecniche della Committente.
- Collaborare attivamente con lo CSIRT Italia per la notifica e la gestione degli incidenti, garantendo il supporto necessario alla protezione degli asset della Pubblica Amministrazione.

11.5 Verifiche di Compliance e Audit

La Committente si riserva la facoltà di richiedere evidenze documentali riguardanti le policy di sicurezza adottate e di effettuare, previo preavviso e secondo modalità concordate, verifiche sulla resilienza delle configurazioni dedicate alla fornitura, per accertare il mantenimento degli standard di sicurezza dichiarati.

12 Riepilogo SLA con Penali

I livelli di servizio con le relative penali sono di seguito dettagliati:

Accesso ad Internet	Tempi di rilascio del servizio	Penale
Attivazione collegamento di accesso ad Internet	90 giorni solari dall'ordine	Per ogni giorno di ritardo nella consegna dell'attivazione del circuito, verrà applicata

**Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS
sulla sede di via Fiume delle Perle**

		una penale pari al 1,5 per mille del canone annuo per ogni giorno di ritardo
--	--	--

Servizio di connettività Internet	Valore atteso	Penale
Disponibilità del servizio	h24, 7 giorni su 7 con un livello di servizio garantito di almeno il 99,9% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%	Il mancato rispetto di tale requisito comporterà l'applicazione di una penale proporzionale alla diminuzione della disponibilità reale rilevata. La penale viene calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile l'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per ogni scostamento in diminuzione dello 0,1%
Tempi di risoluzione anomalie bloccanti	4 ore nel caso di guasti bloccanti	Il mancato rispetto di tale requisito comporta l'applicazione di una penale pari 2% del canone mensile per ogni ora eccedente le 4 previste come tempo massimo per la risoluzione dell'anomalia bloccante

Servizio anti DDoS	Valore atteso	Penale
Disponibilità del servizio	Il servizio di protezione dovrà essere disponibile per almeno il 99,5% del tempo (H24 x 7 gg) su base mensile.	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale che dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.
Evento DDoS	A fronte di un evento l'operatore deve intervenire con il proprio sistema di "mitigation" entro e non oltre 10 minuti dall'inizio di un evento, individuato e	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale proporzionale alla diminuzione della percentuale di casi di intervento nei tempi

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

	segnalato dai sistemi di monitoraggio e analisi dell'operatore stesso ed entro 30 minuti dall'apertura della chiamata al proprio SOC nel caso l'evento venga rilevato solamente dal cliente. Tali tempi di risoluzione devono essere garantiti almeno nel 90% dei casi	concordati. La penale dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.
--	--	--

13 Tabella riepilogativa dei requisiti minimi inderogabili

Di seguito si riporta la tabella riepilogativa dei requisiti minimi inderogabili previsti a pena di esclusione.

Prog.	Categoria Requisito	Riferimento Paragrafo
A	REQUISITI GENERALI	
A.1	Circuito consegnato in doppia via protetta e con accesso differenziato allo stabile.	1 Premessa
A.2	Primo accesso: lato Via della Grande Muraglia 580.	1 Premessa
A.3	Secondo accesso: lato Via Fiume delle Perle 24.	1 Premessa
A.4	Il circuito di accesso deve essere protetto da un servizio di sicurezza anti-DDoS.	1 Premessa
B	ACCESSO INTERNET (FISICO E BANDA)	
B.1	Accesso Internet in fibra ottica in doppia via.	2.1
B.2	Banda garantita di almeno 8 Gbps simmetrico (upstream/downstream).	2.1
B.3	Doppio apparato di consegna.	2.1
B.4	Consegna del servizio lato cliente su due porte LAN 10Gbps Ethernet (LAN PHY).	2.1 / 2.5
B.5	Ottica di tipo SR e connettori LC.	2.1
B.6	Garanzia di disponibilità della banda richiesta fino ai peering-point nazionali e internazionali del fornitore.	2.1
C	ROUTING E INDIRIZZAMENTO	
C.1	Utilizzo di routing dinamico di tipo BGP4 sull'accesso.	2.2
C.2	Peering BGP4 con l'ASN della committente.	2.2
C.3	Doppia sessione di peering BGP verso i due router del cliente.	2.2
C.4	Il fornitore deve inviare la propria "full internet table".	2.2
C.5	Apparati forniti compatibili con il protocollo IPV6.	2.3
C.6	Disponibilità a supportare l'eventuale implementazione del routing IPV6 senza aggravio di costi.	2.3
C.7	Fornitura degli IP pubblici necessari per i collegamenti punto-punto layer3.	2.4
C.8	Fornitura di una ulteriore classe IP di tipo PA da almeno 64 indirizzi da instradare tramite routing statico.	2.4
D	CARATTERISTICHE APPARATI DI CONSEGNA	
D.1	Circuiti terminati su due apparati indipendenti (uno per via).	2.5
D.2	Se il fornitore prevede sistemi WDM questi devono essere doppi e indipendenti.	2.5
D.3	Tutti gli apparati attivi con doppia alimentazione elettrica monofase 220 Volts.	2.5
D.4	Tutti gli apparati attivi con doppi alimentatori sostituibili "a caldo" (protezione 1+1).	2.5
D.5	Fattore di forma per installazione in armadio tecnico standard da 19 pollici.	2.5
D.6	Dimensione massima verticale totale di 6 unità rack per ogni accesso.	2.5
D.7	Apparato di consegna con Capacità di inoltro di almeno 10Gbps.	2.5
D.8	Trasporto, montaggio e configurazione degli apparati a carico del Fornitore.	2.5
E	INSTALLAZIONE E PERCORSI	

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

E.1	Percorso urbano dei due cavi in fibra ottica con instradamento differenziato fino alla centrale del fornitore.	2.7
E.2	Fornire in offerta tecnica planimetrie e informazioni per verificare l'instradamento urbano differenziato.	2.7
E.3	Tutto il cablaggio necessario, anche all'interno dello stabile, a cura del Fornitore.	2.6
F	SERVIZIO DI ASSISTENZA CONNETTIVITÀ	
F.1	Help Desk con numero unico nazionale.	3
F.2	Servizio disponibile h24, 7 giorni su 7.	3
F.3	Risposta in lingua italiana.	3
F.4	Apertura e gestione di un Trouble Ticket per ogni chiamata.	3
F.5	Notifica (apertura e aggiornamenti) della segnalazione anche tramite email.	3
F.6	Presa in carico della segnalazione entro un massimo di 30 minuti dalla chiamata.	3
G	SLA CONNETTIVITÀ INTERNET	
G.1	Disponibilità garantita: almeno 99,9% su base mensile.	4.1
G.2	Tempo di ripristino guasti non bloccanti: 12 ore.	4.2
G.3	Tempo di ripristino guasti bloccanti: 4 ore.	4.2
G.4	Tempi di attraversamento End-to-End: ≤10ms.	4.3
G.5	Percentuale di perdita di pacchetti: ≤0,1%.	4.3
G.6	Variazione di latenza o Jitter: ≤5ms.	4.3
H	SERVIZIO ANTI-DDoS	
H.1	Servizio realizzato sulla rete del carrier (per bloccare il traffico malevolo prima che saturi l'accesso cliente).	5
H.2	Servizio realizzato su infrastruttura del fornitore e gestito da proprie strutture sistemiche (Non ammesso servizio tramite terze parti).	5
H.3	Monitoraggio continuo del traffico mediante strumenti automatizzati.	5.1
H.4	Gestione di un numero di eventi di mitigazione illimitati.	5.1
H.5	Monitoraggio attivo per tutti gli IP in uso (classi attuali e future/21).	5.1
H.6	Sistema di analisi e monitoraggio configurabile con diversi profili distinti per gruppi di indirizzi IP.	5.1
H.6	Sistema di analisi e monitoraggio configurabile con diversi profili distinti per gruppi di indirizzi IP.	5.1
H.7	Al rilevamento di un evento, attivazione in autonomia del reinstradamento verso i sistemi di scrubbing.	5.2
H.8	Il traffico malevolo deve essere bloccato/scartato direttamente sull'infrastruttura del carrier.	5.2
I	REPORTISTICA E ASSISTENZA ANTI-DDoS	
I.1	Servizio di assistenza tramite centro di controllo "SOC" h24, 7 giorni la settimana.	5.4
I.2	Servizio SOC con risposta in lingua italiana e con numero unico nazionale.	5.4
I.3	Notifiche (apertura/aggiornamenti) sulle segnalazioni di sicurezza anche tramite email.	5.4
I.4	Reportistica su eventi DDoS disponibile entro 24 ore dalla richiesta.	5.3
I.5	Il report deve includere almeno: Tipo di attacco, IP di destinazione, Tempo di intervento della "mitigation", Volume e Durata totale dell'evento.	5.3
L	SLA ANTI-DDoS	
L.1	Disponibilità del servizio di protezione: almeno 99,5% su base mensile.	6.1
L.2	Comunicazione di manutenzioni programmate (con indisponibilità) con almeno 10 giorni di anticipo.	6.1
L.3	Tempo di intervento proattivo (se rilevato dal Fornitore): attivazione policy entro 10 minuti dall'evento (≥90% dei casi).	6.2
L.4	Tempo di intervento reattivo (su chiamata del Cliente): presa in carico entro 30 minuti (≥90% dei casi).	6.2
L.5	Percentuale di rilevamento (eventi DDoS): almeno 90% su base mensile.	6.3
M	TERMINI E CONTENUTI DELLA RELAZIONE TECNICA	
M.1	Rilascio del servizio (realizzazione e collaudo) incluso l'anti DDoS entro 90 giorni solari dalla formalizzazione dell'ordine.	7
M.2	L'offerta tecnica deve includere planimetrie e descrizione dei percorsi urbani.	2.7
N	REQUISITI DI SICUREZZA E RESILIENZA DELLE INFRASTRUTTURE	

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via Fiume delle Perle

N.1	<i>Affidabilità e Sicurezza del Servizio.</i> • I servizi di connettività e di protezione DDoS dovranno essere erogati attraverso infrastrutture gestite in conformità con le strategie nazionali di cybersecurity. • Dovrà essere assicurata la resilienza dei nodi di rete e dei sistemi di trasporto rispetto a incidenti informatici, garantendo la continuità operativa dei flussi dati della Committente. • Si dovrà operare in linea con le disposizioni vigenti in materia di sicurezza delle reti e dei sistemi informativi (attuazione Direttiva NIS2 e, ove applicabile, norme sul Perimetro di Sicurezza Nazionale Cibernetica)	11
N.2	<i>Localizzazione del Traffico e Gestione dei Flussi (Scrubbing Center)</i> • Per i servizi di mitigazione degli attacchi DDoS, dovrà essere garantita un'architettura di rete che privilegi la protezione della sovranità dei dati e la bassa latenza. • L'instradamento del traffico verso i centri di pulizia (Scrubbing Center) dovrà avvenire prioritariamente su nodi situati all'interno del territorio dell'Unione Europea. • Qualora la natura dell'attacco richieda l'instradamento su reti globali, dovrà garantirsi l'adozione di misure tecniche idonee a inibire l'accesso ai contenuti del traffico da parte di soggetti terzi, assicurando la piena conformità al GDPR e agli standard di sicurezza nazionali.	11
N.3	<i>Sicurezza della Catena di Approvvigionamento (Supply Chain)</i> • In conformità con gli orientamenti dell'Agenzia per la Cybersicurezza Nazionale (ACN) sulla sicurezza della filiera, dovrà garantirsi che gli apparati critici utilizzati (Router, apparati di core network, sistemi di mitigazione) non provengano da vendor oggetto di restrizioni o specifiche segnalazioni di rischio da parte delle Autorità di Sicurezza Nazionale. • Su richiesta della Committente, l'aggiudicatario dovrà fornire, la mappatura dei sub-fornitori tecnologici critici coinvolti nell'erogazione del servizio per consentire la valutazione dell'esposizione al rischio della catena del valore.	11

ALLEGATO 4 AL PROGETTO

CAPITOLATO TECNICO PER LA FORNITURA DI UN ACCESSO INTERNET PROTETTO DA SERVIZIO DI SICUREZZA ANTI DDOS SULLA SEDE DI ROMA IN VIA DEI TIZII Lotto 2

Codice Affidamento: ICT0966A25

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via dei Tizii

Sommario

1	Premessa.....	3
2	Caratteristiche generali dell'accesso Internet	3
2.1	Accesso fisico e banda garantita	3
2.2	Routing BGP.....	3
2.3	Routing IPV6	4
2.4	Indirizzamento IP.....	4
2.5	Caratteristiche degli apparati di consegna	4
2.6	Dettaglio della sede di attestazione	5
3	Servizio di assistenza sulla connettività Internet.....	5
4	Livelli di servizio richiesti sulla connettività Internet.....	6
4.1	Disponibilità.....	6
4.2	Tempi di ripristino guasti.....	6
4.3	Performance del servizio di connettività richieste.....	6
5	Caratteristiche del servizio di sicurezza anti "Distributed Denial of Service"	7
5.1	Monitoraggio e analisi del traffico	7
5.2	Intervento di mitigazione dell'evento DDoS	7
5.3	Reportistica.....	8
5.4	Servizio di assistenza sistema anti DDoS	8
6	Livelli di servizio richiesti per la protezione DDoS	8
6.1	Disponibilità.....	9
6.2	Tempo di intervento della "mitigation"	9
6.3	Percentuale di rilevamento	9
6.4	Tabella riassuntiva SLA richiesti sul servizio anti DDoS:	9
7	Tempi di rilascio del servizio	9
8	Relazione tecnica	10
9	Durata dei servizi richiesti.....	10
10	Sopralluoghi	10
11	Requisiti di Sicurezza e Resilienza delle Infrastrutture	11
11.1	Affidabilità e Sicurezza del Servizio.....	11
11.2	Localizzazione del Traffico e Gestione dei Flussi (Scrubbing Center)	11
11.3	Sicurezza della Catena di Approvvigionamento (Supply Chain).....	11
11.4	Governance e Supporto alla Sicurezza (SPOC).....	11
11.5	Verifiche di Compliance e Audit.....	12
12	Riepilogo SLA Penali.....	12
13	Tabella riepilogativa dei requisiti minimi inderogabili	13

1 Premessa

ACI Informatica, intende rinnovare e potenziare la propria infrastruttura di connessione ad Internet mantenendo la medesima architettura attualmente in uso che prevede diversi fornitori su due diverse sedi.

Oggetto della presente gara è la fornitura ad ACI Informatica di un nuovo accesso Internet più servizi accessori da attestare nelle sale del datacenter del CONSORZIO NAMEX di Roma via dei Tizii nello spazio riservato e a disposizione della committente.

Il circuito di accesso fornito dovrà essere protetto da un servizio di sicurezza contro attacchi di tipo DDoS (Distributed Denial of Service) con le caratteristiche minime meglio descritte di seguito.

La procedura di gara prevede quindi la fornitura dei seguenti servizi:

1. Un accesso Internet in fibra ottica con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente.
2. Fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico.
3. Un servizio di sicurezza di tipo anti “Distributed Denial of Service” attivo sul tutto il traffico trasportato dall’accesso fornito e per tutti gli IP pubblici a disposizione della committente compresi quelli messi a disposizione del fornitore al punto due.

2 Caratteristiche generali dell’accesso Internet

L’accesso Internet richiesto dovrà avere le seguenti caratteristiche generali minime.

2.1 Accesso fisico e banda garantita

- Circuito di trasporto verso il datacenter del Namex in via dei Tizii in doppia via;
- Consegna su singolo o doppio CPE;
- Consegna del servizio lato cliente su una o due porte LAN 10Gbps Ethernet (LAN PHY) con ottica di tipo SR e connettori LC;
- Banda di accesso Internet indistinto di almeno 8Gbps simmetrico (8Gbps upstream, 8Gbps downstream);
- Garanzia di disponibilità della banda richiesta fino ai peering-point nazionali ed internazionali del fornitore.

2.2 Routing BGP

Al fine di permettere alla committente l’utilizzo dei prefissi del proprio AS e di quello dei clienti ospitati nel datacenter, il fornitore dovrà utilizzare sull’accesso una configurazione che preveda l’utilizzo di routing dinamico di tipo BGP4.

Al momento ACI Informatica annuncerà i seguenti due “Autonomous System”:

- AS Number 42515 (ACI Informatica) con prefissi:
 - 77.73.56.0/21
 - 185.39.188.0/22
- AS Number 34405 (ANCI Digitale) con prefissi:
 - 91.226.108.0/23

La committente annuncerà verso il carrier i prefissi indicati sopra, mentre il fornitore dovrà inviare agli apparati della committente la propria “full internet table”.

La committente dovrà avere la possibilità, in caso necessità e nel corso di validità del contratto, di apportare modifiche alla configurazione del peering BGP che prevedano l’aggiunta o la modifica di prefissi o Asn.

Al fine di garantire una più elevata disponibilità, e permettere una agevole manutenzione dei gateway BGP della committente, dovranno essere instaurate dal fornitore due sessioni di peering verso i due router del cliente.

2.3 Routing IPV6

Al fine di poter sperimentare ed eventualmente implementare annunci di previsti IPV6 nel corso del periodo di validità del contratto, è richiesto che tutti gli apparati forniti siano compatibili con il protocollo IPV6.

E richiesta inoltre la disponibilità da parte del fornitore a supportare la committente nell’eventuale aggiornamento delle configurazioni per permettere l’annuncio ed il routing del protocollo ipv6 contemporaneamente a quello ipv4. Non è richiesta la fornitura di prefissi ipv6 in quanto già nella disponibilità della committente.

La configurazione del routing ipv6 non è richiesta in fase di installazione e rilascio iniziale del servizio, non è richiesto nessun collaudo di questa funzionalità al fine del rilascio ufficiale del servizio.

L’implementazione del routing ipv6 potrà essere richiesta, a discrezione della committente, nel corso del periodo di validità del contratto e non dovrà comportare aggravio o revisioni dei costi da parte della committente.

2.4 Indirizzamento IP

Anche se la committente utilizzerà indirizzamento pubblico proprio è comunque richiesto al fornitore la disponibilità di alcune classi di IP Pubblici, in particolare sono richiesti:

- Fornitura degli IP pubblici necessari alla configurazione dei collegamenti punto-punto layer3 tra i router del cliente e quelli del fornitore.
- Fornitura di una ulteriore classe IP da almeno 64 indirizzi da utilizzare sul circuito in aggiunta a quelli di proprietà della committente da instradare attraverso routing statico, così come indicato in premessa.

2.5 Caratteristiche degli apparati di consegna

Il circuito dovrà essere terminato su apparati attivi installati negli spazi messi a disposizione della committente nel datacenter del Consorzio Namex (armadio AK9)

Tutti gli apparati attivi forniti dovranno avere le seguenti caratteristiche:

- Doppia alimentazione elettrica monofase 220 Volts;
- Doppio alimentatore sostituibile “a caldo” senza interruzione del servizio (protezione 1+1);
- Fattore di forma per installazione in armadio tecnico standard da 19 pollici;
- Somma della dimensione massima verticale di 4 unità rack.

Per quanto riguarda l'apparato di consegna questo dovrà avere:

- Porte LAN di consegna verso il cliente con velocità 10Gbps;
- Capacità di inoltro di almeno 10Gbps;

Il trasporto, montaggio e configurazione degli apparati di accesso sarà in carico al fornitore. La committente offrirà tutto il supporto necessario per la ricezione delle merci ed il presidio durante le fasi di installazione, configurazione, e attivazione del servizio.

2.6 Dettaglio della sede di attestazione

Il circuito dovrà essere rilasciato nell'area riservata al Consorzio NAMEX del Datacenter CINECA di Roma sito in via dei Tizii, 6. Gli apparati di terminazione dovranno essere installati all'interno della porzione di armadio tecnico riservato dal NAMEX alla Committente (armadio AK9). Tutto il cablaggio necessario alla realizzazione dell'impianto, anche all'interno delle sale, dovrà essere compreso nell'offerta e realizzato a cura del fornitore in accordo con le direttive indicate nei regolamenti tecnici del Consorzio NAMEX e comunque sotto la supervisione del personale del Consorzio.

Anche se la consegna dai sistemi del fornitore verso l'apparato della committente è richiesto in singola via, la connettività Internet del fornitore presso la sede NAMEX deve essere realizzata con infrastruttura in alta affidabilità e dotata di doppio accesso in fibra ottica alla sede.

È richiesto che nella documentazione tecnica fornita a corredo dell'offerta presentata, siano contenute eventuali e comunque le informazioni necessarie alla committente per verificare che siano rispettati i vincoli richiesti al presente paragrafo.

Al fine di poter predisporre correttamente l'offerta tecnica ed economica è data possibilità al fornitore di effettuare un sopralluogo tecnico presso la sede NAMEX così come meglio specificato di seguito.

3 Servizio di assistenza sulla connettività Internet

Il fornitore dovrà garantire un servizio di assistenza a cui inoltrare eventuali segnalazioni di malfunzionamento del circuito o problemi di routing BGP. Il servizio di Help Desk dovrà rispondere ad un numero unico nazionale, in lingua italiana ed essere disponibile h24, 7 giorni su 7. Ad ogni chiamata del cliente al centro di assistenza dovrà corrispondere da parte del fornitore l'apertura e la gestione di una segnalazione individuata da un numero di “Trouble ticket”. L'apertura e gli aggiornamenti relativi alla segnalazione aperta dovranno essere notificati alla committente anche tramite email. In fase di perfezionamento del contratto, la committente, fornirà gli indirizzi email e i numeri telefonici da contattare.

Il servizio di help desk dovrà prendere in carico la segnalazione al massimo entro trenta minuti dalla chiamata del cliente.

4 Livelli di servizio richiesti sulla connettività Internet

4.1 Disponibilità

La connettività alla rete pubblica dovrà essere disponibile h24, 7 giorni su 7 con un livello di servizio garantito di almeno il 99,8% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%.

4.2 Tempi di ripristino guasti

A fronte di guasti o anomalie che si dovessero presentare sull'accesso internet il fornitore si dovrà impegnare alla risoluzione del problema ed il ripristino completo del servizio nel più breve tempo possibile garantendo comunque i seguenti tempi di ripristino:

- 12 ore nel caso di guasti non bloccanti;
- 8 ore nel caso di guasti bloccanti.

Con guasti non bloccanti si intendono quelle anomalie che comportano un degrado non significativo delle performance del servizio, si intendono invece bloccanti le anomalie che comportano completa indisponibilità del servizio o forte degrado dello stesso (tasso di perdita di pacchetti maggiore del 2%). Vengono considerati guasti bloccanti anche le anomalie sulle sessioni di routing BGP. La caduta contemporanea di entrambe le sessioni BGP, con l'impossibilità di annuncio da parte del cliente delle proprie reti è da considerarsi guasto bloccante e quindi da ripristinare al più presto possibile e comunque non oltre le 4 ore.

4.3 Performance del servizio di connettività richieste

Di seguito vengono riportate le performance minime che il fornitore si deve impegnare a garantire per tutta la durata del contratto. In particolare, come indicatori di qualità del servizio vengono individuati i seguenti parametri tecnici:

- Tempo di attraversamento dei pacchetti;
- Percentuale di perdita di pacchetti;
- Variazione di latenza o "Jitter".

I parametri individuati si riferiscono a misure effettuate in condizione di utilizzo del circuito inferiore al 80% della banda garantita contrattualizzata (8Gbps), quindi non in condizione di saturazione.

I parametri individuati devono essere garantiti all'interno della rete del fornitore, dall'accesso cliente fino ai punti di interconnessione nazionali ed internazionali.

Di seguito vengono riportati i parametri di qualità minimi richiesti:

Parametro di valutazione	Valore
Tempi di attraversamento End-to-End	≤10ms
Percentuale di perdita di pacchetti	≤ 0,1%
Variazione di latenza o Jitter	≤ 5 ms

5 Caratteristiche del servizio di sicurezza anti “Distributed Denial of Service”

Sul circuito di accesso fornito dovrà essere attivato un servizio di sicurezza finalizzato alla protezione contro attacchi di tipo DDoS (Distributed Denial of Service). Il servizio dovrà essere realizzato sulla rete del carrier in modo da selezionare e bloccare il traffico “malevolo” prima che arrivi ad interferire o saturare l’accesso in sede cliente. Non sono richiesti apparati dedicati da installare presso la committente.

Il sistema nel suo complesso dovrà prevedere quindi un sistema di monitoraggio del traffico per rilevare eventi ddos e un sistema di verifica e “ripulitura” del traffico (scrubbing).

Una volta sottoposto alla verifica e ripulitura il traffico dovrà essere riconsegnato verso l’accesso fornito.

Il servizio deve essere realizzato su infrastruttura del fornitore e gestito direttamente da proprie strutture sistemistiche, **non è ammesso un servizio offerto tramite terze parti.**

5.1 Monitoraggio e analisi del traffico

Il fornitore dovrà quindi avere a disposizione un sistema di monitoraggio e analisi del traffico diretto al cliente al fine di poter rilevare eventi di attacco informatico di tipo DDoS. Tale sistema di monitoraggio deve essere attivo su tutta l’infrastruttura del fornitore. L’offerta deve comprendere il monitoraggio continuo del traffico mediante strumenti automatizzati e la gestione di un numero di eventi di mitigazione illimitati. Il traffico “malevolo” dovrà essere individuato sia tramite analisi di tipo quantitativo che qualitativo.

Il servizio deve comprendere il monitoraggio e l’attivazione di contromisure per tutti gli indirizzi IP in uso alla committente:

- 77.73.56.0/21;
- 185.39.188.0/22;
- 91.226.108.0/23;
- Indirizzi assegnati dal fornitore (almeno 64 ip);
- Eventuali nuove classi annunciate dalla committente fino ad un massimo di una ulteriore subnet /21.

È richiesto che il sistema di analisi e monitoraggio, finalizzato all’individuazione di traffico di tipo ddos, sia configurabile su richiesta della committente con diversi profili distinti per gruppi di indirizzi ip.

Questo al fine di stabilire, congiuntamente con il fornitore, soglie di traffico diverso per servizi diversi e minimizzare quindi i casi di falso positivo o negativo.

5.2 Intervento di mitigazione dell’evento DDoS

Al rilevamento di un evento DDoS, destinato alle sottoreti della committente, il servizio fornito dovrà avere la capacità di innescare in autonomia il reinstradamento verso i sistemi di “scrubbing” del fornitore e la “ripulitura” del traffico.

Il traffico di tipo malevolo destinato ad uno o più indirizzi IP del cliente dovrà essere “selezionato” e “separato” accuratamente da quello lecito, che dovrà essere correttamente consegnato. In caso non si riesca a separare perfettamente il traffico lecito da quello illecito e quindi la policy applicata potrebbe avere impatti sul servizio, il centro di gestione di sicurezza del fornitore dovrà contattare le strutture tecniche della committente per chiedere la conferma di attivazione della policy potenzialmente bloccante.

Qualora la committente rilevi in autonomia un evento di tipo DDoS, non segnalato come tale dal fornitore, dovrà essere comunque possibile l'attivazione su richiesta della mitigation da parte del fornitore. Il traffico classificato come “malevolo” dai sistemi di scrubbing del fornitore dovrà in ogni caso essere bloccato/scartato direttamente sull'infrastruttura del carrier prima di arrivare a saturare la capacità del circuito di accesso fornito al cliente.

Non è richiesta l'installazione di apparati o sonde presso la sede della committente.

5.3 Reportistica

A seguito di eventi DDoS il fornitore dovrà essere in grado, su richiesta del cliente, di inviare o mettere a disposizione su un proprio portale web i report contenenti i dati statistici più significativi dell'evento. Il report dovrà specificare almeno i seguenti parametri:

- Tipo di attacco;
- IP address di destinazione;
- Tempo di intervento della “mitigation”;
- Volume del traffico coinvolto;
- Durata totale dell'evento.

Il report richiesto dovrà essere messo a disposizione entro 24 ore dalla richiesta.

5.4 Servizio di assistenza sistema anti DDoS

Il fornitore dovrà garantire un servizio di assistenza tramite un centro di controllo “SOC” a cui rivolgersi 24 ore su 24, 7 giorni la settimana per avere informazioni o richiedere verifiche a fronte di possibili anomalie rilevate o attacchi segnalati in atto. Il servizio dovrà rispondere ad un numero unico nazionale, in lingua italiana. L'apertura e gli aggiornamenti sulle segnalazioni di sicurezza dovranno essere notificati alla committente anche tramite email. La committente fornirà in fase di perfezionamento del contratto gli indirizzi email da contattare.

6 Livelli di servizio richiesti per la protezione DDoS

Di seguito vengono riportati i livelli di servizio minimi che il fornitore si deve impegnare a garantire per tutta la durata del contratto. In particolare come indicatori di qualità del servizio di sicurezza anti DDoS vengono individuati i seguenti parametri:

- Disponibilità del servizio;
- Tempo di intervento delle procedure di mitigazione;
- Percentuale di individuazione degli eventi.

6.1 Disponibilità

Per disponibilità del servizio si intende il corretto funzionamento sia della piattaforma di monitoraggio e analisi del traffico che dei sistemi attivi per l'applicazione delle policy di mitigation. Il servizio di protezione dovrà essere disponibile per almeno 99,5% del tempo (H24 x 7 gg) su base mensile. In caso di manutenzioni non programmate o di anomalie della piattaforma il fornitore dovrà, nel più breve tempo possibile, notificare al cliente lo stato di indisponibilità della piattaforma. Tutte le attività di manutenzione programmate, che comportino indisponibilità del servizio, dovranno essere comunicate al cliente con un anticipo di almeno 10 giorni.

6.2 Tempo di intervento della "mitigation"

Per tempo di intervento della "mitigation" si intende il tempo che intercorre tra l'inizio dell'anomalia e l'effettiva attivazione del sistema di protezione. Nel caso di evento individuato e segnalato dai sistemi di monitoraggio e analisi del fornitore, la policy deve essere attivata nel più breve tempo possibile e comunque entro 10 minuti dall'evento in almeno il 90% dei casi (Tempo di presa in carico Proattiva). Nel caso l'evento venga rilevato solamente dal cliente, il fornitore dovrà prendere in carico la segnalazione entro 30 minuti dall'apertura della chiamata al proprio SOC in almeno il 90% dei casi (Tempo di presa in carico Reattiva).

6.3 Percentuale di rilevamento

Il servizio fornito dovrà essere in grado di rilevare almeno il 90% degli attacchi di tipo DDoS su base mensile. Sono da considerare attacchi non rilevati tutti gli eventi non notificati o non analizzati dai sistemi del fornitore, ma che vengano rilevati dal cliente e segnalati tramite chiamata al SOC.

6.4 Tabella riassuntiva SLA richiesti sul servizio anti DDoS:

Indicatore Livello di servizio	Unità di misura	Valore
Disponibilità	Percentuale di up-time su base mensile (h24 x7)	99,5%
Tempo di intervento proattivo	Tempo di presa in carico in minuti (>90% dei casi)	10
Tempo di intervento reattivo	Tempo di presa in carico in minuti (>90% dei casi)	30
Percentuale di rilevamento	Percentuale di rilevamento	90%
Disponibilità Reportistica sull'attacco	Ore	24 h

7 Tempi di rilascio del servizio

Il tempo massimo ammesso per il rilascio del servizio è di 90 giorni solari. Per tempo di rilascio si intende il tempo necessario al fornitore per la realizzazione ed il collaudo di tutte le componenti del servizio a partire dalla data di formalizzazione dell'ordine. Il servizio sarà considerato collaudabile al termine della predisposizione di entrambe le componenti: accesso e sicurezza.

8 Relazione tecnica

I concorrenti dovranno presentare, **a pena di esclusione**, una relazione tecnica **finalizzata esclusivamente a consentire alla Stazione Appaltante/RUP di verificare la conformità dei servizi proposti alle specifiche tecniche e ai requisiti minimi obbligatori stabiliti nel Capitolato**.

In particolare, i concorrenti dovranno inserire nella **Busta Amministrativa**, la Relazione Tecnica, debitamente compilata e sottoscritta digitalmente, che illustri dettagliatamente la rispondenza dell'offerta a ciascun requisito indicato nella tabella riepilogativa di cui al successivo paragrafo 13 come riferito alle seguenti macro-categorie:

- A) REQUISITI GENERALI
- B) ACCESSO INTERNET (FISICO E BANDA)
- C) ROUTING E INDIRIZZAMENTO
- D) CARATTERISTICHE APPARATI DI CONSEGNA
- E) SERVIZIO DI ASSISTENZA CONNETTIVITÀ
- F) SLA CONNETTIVITÀ INTERNET
- G) SERVIZIO ANTI-DDoS
- H) REPORTISTICA E ASSISTENZA ANTI-DDoS
- I) SLA ANTI-DDoS
- L) TEMPI E CONTENUTI DELL'OFFERTA TECNICA
- M) REQUISITI DI SICUREZZA E RESILIENZA DELLE INFRASTRUTTURE

La relazione tecnica dovrà contenere, per ciascun Lotto di interesse, una relazione obbligatoria di un numero massimo di 15 pagine, organizzata per sezioni, una sezione per ciascuna macrocategoria sopra indicata.

La Relazione Tecnica non dovrà contenere varianti migliorative rispetto al Capitolato tecnico, ma solo la descrizione analitica di come l'Operatore economico intende soddisfare i requisiti minimi e non dovrà contenere alcun riferimento a prezzi, costi o elementi economici.

La relazione tecnica non darà luogo all'attribuzione di punteggi di merito, ma sarà oggetto di una valutazione di tipo "on/off" (conforme/non conforme).

9 Durata dei servizi richiesti

La durata richiesta per il servizio (accesso internet più anti DDoS) è di 36 mesi a partire dalla data di collaudo del circuito e del servizio anti DDoS.

10 Sopralluoghi

Al fine di poter correttamente quantificare le infrastrutture da realizzare, il fornitore può richiedere alla committente di poter effettuare sopralluoghi tecnici sulla sede oggetto della fornitura.

Gli orari previsti per i sopralluoghi sono:

- Lunedì – Giovedì dalle 9:00 alle 13:00;

I sopralluoghi vanno richiesti e concordati a mezzo email all'indirizzo tlc@informatica.aci.it con almeno due giorni lavorativi di anticipo rispetto alla data prevista. Nella richiesta, oltre alla data ed orario previsto, vanno indicati i nominativi dei tecnici che interverranno. La committente indicherà volta per volta il nome del proprio riferimento che seguirà le attività di sopralluogo nella sede.

I sopralluoghi saranno accordati fino a 5 giorni solari prima del termine di presentazione dell'offerta.

11 Requisiti di Sicurezza e Resilienza delle Infrastrutture

11.1 Affidabilità e Sicurezza del Servizio

I servizi di connettività e di protezione DDoS dovranno essere erogati attraverso infrastrutture gestite in conformità con le strategie nazionali di cybersecurity. L'aggiudicatario dovrà:

- Assicurare la resilienza dei nodi di rete e dei sistemi di trasporto rispetto a incidenti informatici, garantendo la continuità operativa dei flussi dati della Committente.
- Operare in linea con le disposizioni vigenti in materia di sicurezza delle reti e dei sistemi informativi (attuazione Direttiva NIS2 e, ove applicabile, norme sul Perimetro di Sicurezza Nazionale Cibernetica).

11.2 Localizzazione del Traffico e Gestione dei Flussi (Scrubbing Center)

Per i servizi di mitigazione degli attacchi DDoS, l'aggiudicatario dovrà garantire un'architettura di rete che privilegi la protezione della sovranità dei dati e la bassa latenza. Ed inoltre:

- L'instradamento del traffico verso i centri di pulizia (Scrubbing Center) dovrà avvenire prioritariamente su nodi situati all'interno del territorio dell'Unione Europea.
- Qualora la natura dell'attacco richieda l'instradamento su reti globali, l'aggiudicatario dovrà garantire l'adozione di misure tecniche idonee a inibire l'accesso ai contenuti del traffico da parte di soggetti terzi, assicurando la piena conformità al GDPR e agli standard di sicurezza nazionali.

11.3 Sicurezza della Catena di Approvvigionamento (Supply Chain)

In conformità con gli orientamenti dell'Agenzia per la Cybersicurezza Nazionale (ACN) sulla sicurezza della filiera, l'aggiudicatario dovrà garantire che Gli apparati critici utilizzati (Router, apparati di core network, sistemi di mitigazione) non provengano da vendor oggetto di restrizioni o specifiche segnalazioni di rischio da parte delle Autorità di Sicurezza Nazionale.

In tal contesto, l'aggiudicatario dovrà fornire, su richiesta della Committente, la mappatura dei sub-fornitori tecnologici critici coinvolti nell'erogazione del servizio per consentire la valutazione dell'esposizione al rischio della catena del valore.

11.4 Governance e Supporto alla Sicurezza (SPOC)

L'aggiudicatario dovrà designare e comunicare alla Committente, entro 48 ore dalla stipula del contratto, un Referente Tecnico per la Sicurezza (Single Point of Contact) operativo H24/7. Tale figura avrà il compito di:

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via dei Tizii

- Coordinare le attività di risposta agli incidenti informatici con le strutture tecniche della Committente.
- Collaborare attivamente con lo CSIRT Italia per la notifica e la gestione degli incidenti, garantendo il supporto necessario alla protezione degli asset della Pubblica Amministrazione.

11.5 Verifiche di Compliance e Audit

La Committente si riserva la facoltà di richiedere evidenze documentali riguardanti le policy di sicurezza adottate e di effettuare, previo preavviso e secondo modalità concordate, verifiche sulla resilienza delle configurazioni dedicate alla fornitura, per accertare il mantenimento degli standard di sicurezza dichiarati.

12 Riepilogo SLA Penali

I livelli di servizio con le relative penali sono di seguito dettagliati:

Accesso ad Internet	Tempi di rilascio del servizio	Penale
Attivazione collegamento di accesso ad Internet	90 giorni solari dall'ordine	Per ogni giorno di ritardo nella consegna dell'attivazione del circuito, verrà applicata una penale pari al 1,5 per mille del canone annuo per ogni giorno di ritardo

Servizio di connettività Internet	Valore atteso	Penale
Disponibilità del servizio	h24, 7 giorni su 7 con un livello di servizio garantito di almeno il 99,8% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%	Il mancato rispetto di tale requisito comporterà l'applicazione di una penale proporzionale alla diminuzione della disponibilità reale rilevata. La penale viene calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per ogni scostamento in diminuzione dello 0,1%
Tempi di risoluzione anomalie bloccanti	8 ore nel caso di guasti bloccanti	Il mancato rispetto di tale requisito comporta l'applicazione di una penale pari 2% del canone mensile per ogni ora eccedente le 8 previste

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via dei Tizii

		come tempo massimo per la risoluzione dell'anomalia bloccante
--	--	---

Servizio anti DDoS	Valore atteso	Penale
Disponibilità del servizio	Il servizio di protezione dovrà essere disponibile per almeno il 99,5% del tempo (H24 x 7 gg) su base mensile.	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale che dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.
Evento DDoS	A fronte di un evento l'operatore deve intervenire con il proprio sistema di "mitigation" entro e non oltre 10 minuti dall'inizio di un evento, individuato e segnalato dai sistemi di monitoraggio e analisi dell'operatore stesso ed entro 30 minuti dall'apertura della chiamata al proprio SOC nel caso l'evento venga rilevato solamente dal cliente. Tali tempi di risoluzione devono essere garantiti almeno nel 90% dei casi	Il mancato rispetto di tale requisito dovrà comportare l'applicazione al fornitore di una penale proporzionale alla diminuzione della percentuale di casi di intervento nei tempi concordati. La penale dovrà essere calcolata in funzione dello scostamento percentuale e dell'importo del canone mensile dell'accesso. In particolare, la penale sarà uguale al 2% del canone mensile dovuto per il servizio anti-DDoS per ogni scostamento in diminuzione dello 1%.

13 Tabella riepilogativa dei requisiti minimi inderogabili

Di seguito si riporta la tabella riepilogativa dei requisiti minimi inderogabili previsti a pena di esclusione.

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via dei Tizii

Pr.	Categoria Requisito	Riferimento Paragrafo
A	REQUISITI GENERALI	
A.1	Fornitura di un accesso Internet con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente.	1 Premessa
A.2	Attestazione del servizio nelle sale del datacenter del CONSORZIO NAMEX di Roma via dei Tizii.	1 Premessa
A.3	Il circuito di accesso fornito dovrà essere protetto da un servizio di sicurezza anti-ddos	1 Premessa
B	ACCESSO INTERNET (FISICO E BANDA)	
B.1	Circuito di trasporto verso il datacenter del Namex in via dei Tizii in singola via	2.1
B.2	Consegna su singolo oppure doppio CPE.	2.1
B.3	Connettività Internet del fornitore presso la sede NAMEX realizzata con infrastruttura in alta affidabilità e dotata di doppio accesso in fibra ottica alla sede.	2.6
B.4	Banda di accesso Internet indistinto di almeno 8 Gbps simmetrico	2.1
B.5	Consegna del servizio lato cliente su una o due porte LAN 10Gbps Ethernet (LAN PHY)	2.1
B.6	Ottica di tipo SR e connettori LC.	2.1
B.7	Garanzia di disponibilità della banda richiesta fino ai peering-point nazionali e internazionali del fornitore.	2.1
C	ROUTING E INDIRIZZAMENTO	
C.1	Utilizzo di routing dinamico di tipo BGP4 sull'accesso.	2.2
C.2	Peering BGP4 con l'ASN della committente.	2.2
C.3	Instaurare due sessioni di peering BGP verso i due router del cliente.	2.2
C.4	Il fornitore deve inviare agli apparati della committente la propria "full internet table".	2.2
C.5	Apparati forniti compatibili con il protocollo IPV6.	2.3
C.6	Disponibilità a supportare l'eventuale implementazione del routing IPV6 senza aggravio di costi.	2.3
C.7	Fornitura degli IP pubblici necessari per i collegamenti punto-punto layer3.	2.4
C.8	Fornitura di una ulteriore classe IP di tipo PA da almeno 64 indirizzi da instradare tramite routing statico.	2.4
D	CARATTERISTICHE APPARATI DI CONSEGNA	
D.1	Apparati attivi installati negli spazi messi a disposizione della committente nel datacenter del Consorzio Namex (armadio AK9).	2.5 / 2.6
D.2	Tutti gli apparati attivi con Doppia alimentazione elettrica monofase 220 Volts.	2.5
D.3	Tutti gli apparati attivi con Doppi alimentatori sostituibili "a caldo" (protezione 1+1).	2.5
D.4	Fattore di forma per installazione in armadio tecnico standard da 19 pollici.	2.5
D.5	Somma della dimensione massima verticale per tutti gli apparati: 4 unità rack.	2.5
D.6	Apparato di consegna con Capacità di inoltro di almeno 10Gbps.	2.5
D.7	Trasporto, montaggio e configurazione degli apparati di accesso a carico del Fornitore.	2.5
D.8	Cablaggio interno alle sale compreso nell'offerta e realizzato a cura del fornitore.	2.6
E	SERVIZIO DI ASSISTENZA CONNETTIVITÀ	
E.1	Help Desk con numero unico nazionale.	3
E.2	Servizio disponibile h24, 7 giorni su 7.	3
E.3	Risposta in lingua italiana.	3
E.4	Apertura e gestione di un Trouble Ticket per ogni chiamata.	3
E.5	Notifica (apertura e aggiornamenti) della segnalazione anche tramite email.	3
E.6	Presa in carico della segnalazione entro un massimo di 30 minuti dalla chiamata.	3
F	SLA CONNETTIVITÀ INTERNET	
F.1	Disponibilità garantita: almeno 99,8% su base mensile.	4.1
F.2	Tempo di ripristino guasti non bloccanti: 12 ore.	4.2

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via dei Tizii

F.3	Tempo di ripristino guasti bloccanti: 8 ore.	4.2
F.4	Tempi di attraversamento End-to-End: ≤10ms.	4.3
F.5	Percentuale di perdita di pacchetti: ≤0,1%.	4.3
F.6	Variazione di latenza o Jitter: ≤5ms.	4.3
G	SERVIZIO ANTI-DDoS	
G.1	Servizio realizzato sulla rete del carrier (per bloccare il traffico malevolo prima che saturi l'accesso).	5
G.2	Servizio realizzato su infrastruttura del fornitore e gestito da proprie strutture sistemistiche (Non ammesso tramite terze parti).	5
G.3	Monitoraggio continuo del traffico mediante strumenti automatizzati.	5.1
G.4	Gestione di un numero di eventi di mitigazione illimitati.	5.1
G.5	Monitoraggio attivo per tutti gli IP in uso (classi attuali e future/21).	5.1
G.6	Sistema di analisi e monitoraggio configurabile con diversi profili distinti per gruppi di indirizzi IP.	5.1
G.7	Al rilevamento di un evento, attivazione in autonomia del reinstradamento verso i sistemi di scrubbing.	5.2
G.8	Il traffico malevolo deve essere bloccato/scartato direttamente sull'infrastruttura del carrier	5.2
H	REPORTISTICA E ASSISTENZA ANTI-DDoS	
H.1	Servizio di assistenza tramite centro di controllo "SOC" h24, 7 giorni la settimana.	5.4
H.2	Servizio SOC con risposta in lingua italiana e con numero unico nazionale.	5.4
H.3	Reportistica su eventi DDoS disponibile entro 24 ore dalla richiesta.	5.3 / 6.4
H.4	Il report deve specificare Tipo di attacco, IP di destinazione, Tempo di intervento, Volume e Durata totale dell'evento.	5.3
I	SLA ANTI-DDoS	
I.1	Disponibilità del servizio di protezione: almeno 99,5% su base mensile.	6.1 / 6.4
I.2	Comunicazione di manutenzioni programmate (con indisponibilità) con almeno 10 giorni di anticipo.	6.1
I.3	Tempo di intervento proattivo (se rilevato dal Fornitore): attivazione policy entro 10 minuti dall'evento (≥90% dei casi).	6.2 / 6.4
I.4	Tempo di intervento reattivo (su chiamata del Cliente): presa in carico entro 30 minuti (≥90% dei casi).	6.2 / 6.4
I.5	Percentuale di rilevamento (eventi DDoS): almeno 90% su base mensile.	6.3 / 6.4
L	TEMPI E CONTENUTI DELL'OFFERTA TECNICA	
L.1	Rilascio del servizio (realizzazione e collaudo) incluso l'anti DDoS entro 90 giorni solari dalla formalizzazione dell'ordine.	7
L.2	L'offerta tecnica deve includere planimetrie e descrizione dei percorsi urbani.	2.6
M	REQUISITI DI SICUREZZA E RESILIENZA DELLE INFRASTRUTTURE	
M.1	Affidabilità e Sicurezza del Servizio. - I servizi di connettività e di protezione DDoS dovranno essere erogati attraverso infrastrutture gestite in conformità con le strategie nazionali di cybersecurity. - Dovrà essere assicurata la resilienza dei nodi di rete e dei sistemi di trasporto rispetto a incidenti informatici, garantendo la continuità operativa dei flussi dati della Committente. - Si dovrà operare in linea con le disposizioni vigenti in materia di sicurezza delle reti e dei sistemi informativi (attuazione Direttiva NIS2 e, ove applicabile, norme sul Perimetro di Sicurezza Nazionale Cibernetica)	11
M.2	Localizzazione del Traffico e Gestione dei Flussi (Scrubbing Center) - Per i servizi di mitigazione degli attacchi DDoS, dovrà essere garantita un'architettura di rete che privilegi la protezione della sovranità dei dati e la bassa latenza. - L'instradamento del traffico verso i centri di pulizia (Scrubbing Center) dovrà avvenire prioritariamente su nodi situati all'interno del territorio dell'Unione Europea. - Qualora la natura dell'attacco richieda l'instradamento su reti globali, dovrà garantirsi l'adozione di misure tecniche idonee a inibire l'accesso ai contenuti del traffico da parte di soggetti terzi, assicurando la piena conformità al GDPR e agli standard di sicurezza	11

Capitolato tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di via dei Tizii

	nazionali.	
M.3	<i>Sicurezza della Catena di Approvvigionamento (Supply Chain)</i> • In conformità con gli orientamenti dell'Agenzia per la Cybersicurezza Nazionale (ACN) sulla sicurezza della filiera, dovrà garantirsi che gli apparati critici utilizzati (Router, apparati di core network, sistemi di mitigazione) non provengano da vendor oggetto di restrizioni o specifiche segnalazioni di rischio da parte delle Autorità di Sicurezza Nazionale. • Su richiesta della Committente, l'aggiudicatario dovrà fornire, la mappatura dei sub-fornitori tecnologici critici coinvolti nell'erogazione del servizio per consentire la valutazione dell'esposizione al rischio della catena del valore.	11



Codice affidamento ICT0966A25

ALLEGATO 5 AL PROGETTO

LOTTO 1

SCHEMA DI CONTRATTO PER SERVIZI E FORNITURE

TRA

ACI Informatica S.p.A. con sede in Roma, via Fiume delle Perle n. 24, Codice Fiscale 00405030586 e Partita IVA 00883311003, in persona del Direttore Approvvigionamenti e Centrale di Committenza, Ing. Stefano Carosi (di seguito per brevità ACI Informatica), autorizzato al presente atto giusta Procura speciale autenticata nelle firme dal Notaio Marco Pinto di Roma in data 17 marzo 2025, Repertorio n. 18254, Raccolta n. 12941,

- Stazione Appaltante -

E

l'impresa, con sede legale in (.....),
Via CAP, capitale sociale €.....,
iscritta nel Registro delle Imprese di Codice fiscale n.°
....., partita IVA....., rappresentata dain qualità
di..... giusti poteri risultanti da
[eventuale, in caso di R.T.I.] in qualità di mandataria del RTI costituito con l'impresa
..... con sede legale in (.....), Via
.....C.a.p.iscritta nel Registro delle Imprese di
..... con Codice fiscale n.°partita
IVA.....(Mandante) e l'impresa con sede
legale in (.....), Via CAPiscritta
nel Registro delle Imprese di con Codice fiscale n.°
.....partita IVA.....(Mandante)

- Appaltatore -

La Stazione Appaltante e l'Appaltatore (nel prosieguo, unitamente denominati "Parti")

PREMESSO CHE

- A.** la Stazione Appaltante ha approvato con disposizione a firma del Direttore Approvvigionamenti e Centrale di Committenza del .../.../....., l'avvio del procedimento concorsuale per l'affidamento della fornitura di accessi internet protetti dal servizio di sicurezza anti DDoS per il data center di Roma sito in via Fiume delle Perle 24 e per il data center sito presso il Consorzio Namex in Roma in via dei Tizii, da espletarsi, ai sensi dell'art. 32 del D. Lgs. n. 36/2023, mediante appalto specifico sul "Sistema Dinamico di Acquisizione della Pubblica Amministrazione" (SDAPA) per la fornitura di prodotti e servizi per l'informatica



e le telecomunicazioni, da aggiudicare con il criterio del minor prezzo, suddivisi in due Lotti i cui importi complessivi a base d'appalto sono pari ad € 95.000,000 per il Lotto 1, di cui € 0,00 per oneri relativi alla sicurezza non soggetti a ribasso ed € 85.000,00 per il Lotto 2, di cui € 0,00 per oneri relativi alla sicurezza non soggetti a ribasso;

- B.** ACI Informatica, con lettera del _____ ha invitato tutti gli operatori economici ammessi alla categoria merceologica oggetto dell'Appalto Specifico e in possesso dei requisiti indicati nella documentazione di gara, a presentare un'offerta avente ad oggetto quanto descritto nella medesima documentazione, da aggiudicarsi con il criterio del minor prezzo di cui al comma 3 dell'art. 108 del D.Lgs. n. 36/2023 e s.m.i.;
- C.** nei confronti dell'appaltatore, risultato aggiudicatario del Lotto 1, sono state esperite con esito positivo le verifiche dei requisiti di carattere generale e speciale concernenti la veridicità delle dichiarazioni presentate in sede di gara;
- D.** ai sensi del D.Lgs. n.159/2011, sussistono anche i presupposti di legge per la stipulazione del presente Contratto, giuste le informazioni antimafia rilasciate dall'U.T.G.-Prefettura di _____, in data ____/____/____ con Prot. n. _____, relativa all'Impresa _____ (in caso di RTI ripetere per ognuno dei componenti il Raggruppamento, in caso di avvalimento ripetere anche per l'impresa ausiliaria) (oppure decorso il termine previsto e procedendo anche in assenza delle informazioni antimafia) ACI Informatica S.p.A., tramite il portale della Banca Dati Nazionale Antimafia (B.D.N.A.) ha richiesto per l'impresa _____ in data _____ l'informazione ai sensi dell'art. 85 del Decreto Legislativo 159/2011 e s.m.i e, trascorsi più di 30 (trenta) giorni da detta richiesta ACI Informatica S.p.A., è legittimata a procedere alla stipula del presente Contratto (in caso di RTI ripetere per ognuno dei componenti il Raggruppamento e in caso di avvalimento per l'impresa ausiliaria)
- E.** all'esito dell'anzidetta procedura è stata disposta dal Direttore Approvvigionamenti e Centrale di Committenza di ACI Informatica, l'aggiudicazione in favore di _____, comunicata ex art. 90 del D.Lgs. n. 36/2023 e s.m.i. a tutti i concorrenti, ivi compreso il predetto Aggiudicatario, con nota del _____ prot. _____;
- F.** l'Aggiudicatario ha presentato quanto previsto nel Capitolato d'Oneri e nei suoi allegati per la stipula del contratto;
- G.** l'Appaltatore conferma e ribadisce tutte le dichiarazioni formulate con la propria offerta in sede di gara, ed in particolare di avere offerto il prezzo di € _____, di cui € _____ per oneri relativi alla sicurezza, non soggetti a ribasso;
- H.** (eventuale, in caso di R.T.I.) con scrittura privata munita di autentica delle firme Rep. n. _____/_____ in data ____/____/____ per Dott. _____ Notaio in _____, iscritto al Collegio Notarile di _____, le Imprese _____ e _____ si sono costituite, ai sensi dell'art. 68 D.Lgs. n. 36/2023 e s.m.i., in Raggruppamento Temporaneo di Imprese, designando quale Capogruppo l'Impresa _____, conferendo al legale rappresentante di quest'ultima mandato collettivo speciale irrevocabile con rappresentanza, affinché possa compiere in nome proprio e per conto della mandante tutte le operazioni e gli atti di qualsiasi natura dipendenti dal presente affidamento, fino all'estinzione di ogni rapporto;
- I.** alla luce di quanto riportato alle precedenti lettere si può procedere con la stipula del contratto;



- J. il Responsabile Unico del Progetto (RUP) è il Dott. Angelo Marrucci;
- K. il Direttore dell'Esecuzione del contratto (DEC) è il Sig. Mauro Reali;
- L. tutti i predetti atti devono aversi qui per integralmente richiamati e trascritti.

Tutto ciò premesso, tra le Parti sopra costituite si conviene quanto segue:

ART. 1 VALIDITÀ DELLE PREMESSE. ALLEGATI. NORME REGOLATRICI

Le premesse e gli allegati costituiscono parte integrante e sostanziale del presente Contratto ed hanno ad ogni effetto valore di patto.

L'esecuzione del Contratto è disciplinata, oltre che da quanto disposto nel medesimo e in tutti i documenti che fanno parte del Contratto stesso ai sensi del successivo art. 3, dalle disposizioni di cui al D.Lgs. 36/2023 e s.m.i., dal Codice Civile, e dalle altre disposizioni normative in materia di contratti di diritto privato, per quanto non regolato dalle disposizioni sopra richiamate.

ACI Informatica, ai sensi della normativa e prassi vigente, provvederà a comunicare all'Autorità Nazionale Anticorruzione (ANAC) i fatti riguardanti la fase di esecuzione del presente Contratto.

ART. 2 OGGETTO DEL CONTRATTO E CONSEGNA

ACI Informatica S.p.A., ai sensi del D.Lgs. n. 36/2023, affida all'Appaltatore, che accetta senza riserva alcuna, l'esecuzione della fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di Roma via Fiume delle Perle, 24 secondo quanto meglio precisato nel presente Contratto e nei relativi allegati, con particolare riferimento al Capitolato Speciale di Appalto di Servizi - Parte Generale sub lett. "A" e al "Capitolato Tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di Roma via Fiume delle Perle - Lotto 1", sub lett. "B".

In particolare, trattasi, a titolo esemplificativo e non esaustivo, dei seguenti servizi:

1. Un accesso Internet in fibra ottica in doppia via con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente;
2. Fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico.
3. Un servizio di sicurezza di tipo anti "Distributed Denial of Service" attivo sul tutto il traffico trasportato dall'accesso ovvero per tutti gli IP pubblici annunciati della committente e quelli messi a disposizione del fornitore al punto due. Il servizio dovrà essere realizzato su infrastruttura del fornitore e gestito direttamente da proprie strutture sistemistiche, non è ammesso un servizio offerto tramite terze parti.

Il circuito dovrà essere rilasciato ad ACI Informatica in doppia via protetta secondo specifiche meglio indicate nel capitolato tecnico, con accesso differenziato allo stabile su due lati e civici differenti. In particolare, il fornitore dovrà utilizzare i due seguenti accessi al data center:

- Primo accesso, lato via della Grande Muraglia n. 580;
- Secondo accesso, lato via Fiume delle Perle n. 24.



Il rilascio del circuito e del servizio anti DDoS deve avvenire entro e non oltre 90 giorni solari dal presente ordine.

L'Appaltatore si impegna ad eseguire le anzidette attività in ottemperanza alla normativa vigente, alla disciplina del procedimento concorsuale, alle prescrizioni del presente Contratto e relativi allegati, in particolare del Capitolato Speciale di Appalto di Servizi Parte Generale e del Capitolato Tecnico.

ART. 3 DOCUMENTI COSTITUENTI IL CONTRATTO

Fanno parte integrante e sostanziale del presente Contratto e si intendono allegati allo stesso, ancorché non materialmente e fisicamente uniti al medesimo, gli atti e i documenti del procedimento concorsuale, che si hanno per integralmente richiamati e trascritti, nonché i documenti tecnici ed amministrativi e in particolare i seguenti atti, qui allegati in copia informatica:

- a. Capitolato Speciale di Appalto (d'ora in poi CSA) di Servizi Parte Generale
- b. Capitolato Tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di Roma via Fiume delle Perle Lotto 1;
- c. (*eventuale*, in caso di RTI) Mandato costitutivo del Raggruppamento di imprese, qui allegato in originale o copia conforme all'originale sub lett. "___";
- d. Offerta economica allegata al presente atto sotto la lettera "___";
- e. Garanzia definitiva – ai sensi dell'art.117 del D.Lgs. n.36/2023 - prodotta dall'Appaltatore con Polizza fidejussoria a garanzia della buona esecuzione del presente Contratto, qui allegata unitamente alla/e Certificazione/i di qualità prodotte ai sensi dell'art. 106 comma 8 del D.Lgs. n. 36/2023;
- f. Dichiarazione dell'Appaltatore, presentata in sede di offerta con cui è stata manifestata l'intenzione di subappaltare nei limiti di cui all'art.119 del D.Lgs. n. 36/2023;
- g. (*eventuale, in caso di avvalimento*) Contratto di avvalimento stipulato tra l'Appaltatore e l'impresa ausiliaria ai sensi dell'art. 104 del D.Lgs. n. 36/2023;
- h. Polizza assicurativa.

L'affidamento viene accettato dall'Appaltatore con l'osservanza piena, assoluta, incondizionata ed inderogabile delle norme, condizioni, patti, obblighi, oneri e modalità previsti nel Contratto ed in tutti gli atti e documenti in esso richiamati, siano o meno essi qui materialmente allegati, con particolare riferimento al CSA di Servizi– Parte Generale ed al Capitolato Tecnico.

ART. 4 IMPORTO DELL'AFFIDAMENTO

L'importo complessivo dell'affidamento, al netto dell'I.V.A., è pari ad €....., comprensivo di €..... per oneri della sicurezza ed è così composto:

1. €....., determinato sulla base del ribasso del _____% offerto rispetto alla base d'asta indicata per l'attivazione del collegamento di accesso ad Internet, come il tutto dettagliato nel capitolato tecnico;



2. € _____ determinato sulla base del ribasso del _____% offerto rispetto alla base d'asta indicata per l'accesso internet protetto da servizio di sicurezza anti DDoS come il tutto dettagliato dal capitolato tecnico.

L'importo complessivo offerto che sarà corrisposto per la fornitura/servizi richiesti è espresso in Euro, onnicomprensivo e si intende, tra l'altro:

- una tantum: per l'attivazione del servizio di connettività di cui al punto 1 della precedente tabella;
- a canone per l'accesso internet protetto da servizio di sicurezza anti DDoS di cui al punto 2 della precedente tabella.

ACI Informatica si riserva la facoltà, nei limiti di cui all'art. 76, comma 6 del D.Lgs. 36/2023 e s.m.i., di affidare all'aggiudicatario, nei successivi tre anni dalla stipula del contratto, nuovi servizi consistenti nella ripetizione di servizi analoghi, secondo quanto previsto nel progetto posto alla base del presente affidamento, per una durata pari a 36 mesi per un importo stimato complessivamente non superiore ad € al netto di Iva e/o di altre imposte e contributi di legge, nonché degli oneri per la sicurezza dovuti a rischi da interferenze

ACI Informatica si riserva la facoltà di esercizio delle opzioni di cui sopra comunicandola all'appaltatore mediante posta elettronica certificata almeno 2 giorni prima della scadenza del contratto originario.

ACI Informatica S.p.A., ai sensi dell'art. 60, del D.Lgs. n. 36/2023, applicherà la formula di revisione prezzi, calcolata sugli indici indicati nel comma 3 dell'art 60 del D.Lgs. n. 36/2023, come di seguito riportata:

qualora, al verificarsi di particolari condizioni di natura oggettiva, che determinano una variazione del costo dell'appalto, l'indice riporti una variazione percentuale superiore al 5% rispetto al valore del medesimo indice nel mese di stipula del contratto, i prezzi unitari saranno adeguati in misura pari al 80% della variazione riportata a partire dal mese successivo a quello di rilevazione.

ART. 5 ONERI A CARICO DELL'APPALTATORE RELATIVI ALL'ESECUZIONE

Rientrano tra gli obblighi a carico dell'Appaltatore e si intendono, pertanto, adeguatamente remunerati nel corrispettivo di cui all'articolo 4 del presente Contratto, tutte le prestazioni afferenti all'esecuzione di quanto proposto in sede di offerta.

ART. 6 DURATA DEL CONTRATTO

La durata del presente Contratto è fissata in 36 mesi a partire dalla data di rilascio del circuito e del servizio anti DDoS che dovrà avvenire entro e non oltre 90 giorni solari dalla sottoscrizione del contratto e dovrà essere certificata da un apposito verbale di collaudo positivo sottoscritto dalle parti.

ART. 7 PAGAMENTO E TRACCIABILITÀ

7 a) Termini di pagamento



Le fatture dovranno essere emesse con le seguenti modalità:

- per le eventuali attività una-tantum in unica soluzione all'attivazione del collegamento di accesso ad Internet risultante dal collaudo positivo del circuito;
- per il servizio a canone di accesso ad Internet e di sicurezza anti-DDoS fatture di pari importo con cadenza trimestrale posticipata.

Il pagamento delle predette fatture sarà effettuato secondo quanto riportato nel CSA di Servizi – Parte Generale.

7 b) Tracciabilità dei flussi finanziari

I corrispettivi spettanti all'Appaltatore saranno accreditati unicamente a mezzo bonifico bancario/postale sul conto corrente dedicato ed intrattenuto presso, di cui al seguente codice IBAN:, esonerando ACI Informatica da ogni responsabilità per i pagamenti eseguiti in tal modo, ai sensi del combinato disposto di cui agli artt. 21 e 125 del D.Lgs. 36/2023 sulla tracciabilità dei flussi finanziari ai sensi dell'articolo 3 della legge 13 agosto 2010, n. 136.

La/le persona/e delegata/e ad operare sul conto corrente di cui sopra sono:

- a) Sig. – nato a.....il .././....., c.f.;
- b) Sig. – nato a.....il .././....., c.f.;
- c)

ART. 8 RESPONSABILE DEL CONTRATTO E REFERENTE TECNICO DELLA SICUREZZA

Ai fini dell'esecuzione del Contratto l'Appaltatore ha nominato quale Responsabile del Contratto l'Ing./il Dott./Sig., nato a (.....) il giorno (C.F.:).

Ai sensi di quanto previsto al paragrafo 11.1 del Capitolato tecnico, l'Appaltatore dovrà designare e comunicare alla Committente, entro 48 ore dalla stipula del contratto, un Referente Tecnico per la Sicurezza.

ART. 9 TERMINI PER L'ESECUZIONE DELLE PRESTAZIONI E PENALI

9 a) Termini.

Accesso ad internet

- Attivazione del collegamento di accesso ad internet

L'attivazione del collegamento di accesso ad Internet dovrà essere effettuata entro 90 giorni solari dall'ordine.

Servizio di assistenza sulla connettività Internet e anti DDoS



Il servizio di Help Desk dovrà essere disponibile h24, 7 giorni su 7.

Il servizio di Help Desk dovrà prendere in carico la segnalazione per la mancata connettività Internet e/o per la protezione DDoS al massimo entro trenta minuti dalla chiamata del cliente.

Livelli di servizio richiesti sulla connettività Internet

- *Disponibilità*

Il servizio di connettività Internet dovrà essere disponibile h24, 7 giorni su 7, con un livello di servizio garantito di almeno il 99,9% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%

- *Tempi di ripristino guasti*

A fronte di guasti o anomalie che si dovessero presentare sull'accesso internet il fornitore si dovrà risolvere il problema e ripristinare completamente il servizio nel più breve tempo possibile garantendo comunque i seguenti tempi di ripristino:

- 12 ore nel caso di guasti non bloccanti;
- 4 ore nel caso di guasti bloccanti.

Livelli di servizio richiesti per la protezione DDoS

- Il servizio di protezione DDOS dovrà essere disponibile per almeno il 99,5% del tempo (H24 x 7 gg) su base mensile. Tutte le attività di manutenzione programmate, che comportino indisponibilità del servizio, dovranno essere comunicate al cliente con un anticipo di almeno 10 giorni.

- *Tempo di intervento della "mitigation":*

- Nel caso di evento individuato e segnalato dai sistemi di monitoraggio e analisi del fornitore, la policy deve essere attivata nel più breve tempo possibile e comunque entro 10 minuti dall'evento in almeno il 90% dei casi (Tempo di presa in carico Proattiva).
- Nel caso di evento rilevato solamente dal cliente, il fornitore dovrà prendere in carico la segnalazione entro 30 minuti dall'apertura della chiamata al proprio SOC in almeno il 90% dei casi (Tempo di presa in carico Reattiva).

- *Percentuale di rilevamento:*

Il servizio fornito dovrà essere in grado di rilevare almeno il 90% degli attacchi di tipo DDoS su base mensile.

- *Disponibilità Reportistica sull'attacco:*

A seguito di eventi DDoS il fornitore dovrà essere in grado, su richiesta del cliente, di inviare o mettere a disposizione su un proprio portale web i report contenenti i dati statistici più significativi dell'evento che dovrà essere messo a disposizione entro 24 ore dalla richiesta.

Governance e Supporto alla Sicurezza (SPOC)

- Entro 48 ore dalla stipula del contratto, l'Appaltatore dovrà designare e comunicare alla Committente, un Referente Tecnico per la Sicurezza.



b) Penali.

Si rinvia a quanto previsto al paragrafo 12 del capitolato tecnico_Lotto 1.

ART. 10 GARANZIA DEFINITIVA

L'Appaltatore, ai sensi dell'art.117 del D.Lgs. n. 36/2023, a garanzia delle obbligazioni assunte con il presente Contratto e degli impegni comunque previsti negli allegati al medesimo, ha prestato, con le modalità indicate nei documenti della procedura concorsuale, apposita garanzia cauzionale mediante Polizza fidejussoria n., emessa in data dalla compagnia, per l'importo di € con firma legalizzata ai sensi di legge, allegata al presente atto sotto la *sub lett.*

“ ”
___.

ART. 11 RESPONSABILITÀ CIVILE VERSO TERZI E ASSICURAZIONI

Ai sensi dell'art. 117, comma 10 del D.Lgs 36/2023 l'Appaltatore ha stipulato una polizza di assicurazione per danni di esecuzione e responsabilità civile verso terzi causati nel corso dell'esecuzione dell'appalto avente validità dalla data di stipula del Contratto e per tutta la durata dello stesso.

La predetta copertura è costituita mediante Polizza Car/Rct n.° emessa in data dalla Compagnia – con firma regolarmente legalizzata ai sensi di legge - e qui allegata con la *sub lett.* “___” - per una somma assicurata pari all'ammontare del Contratto (€.....) [*l'importo della somma da assicurare può essere superiore all'importo del Contratto qualora sussistano motivate particolari circostanze che lo impongano*] e per un massimale contro la responsabilità civile verso terzi di €.....

ART. 13 SUBAPPALTO, COTTIMO E SUB-CONTRATTI

Ai sensi dell'art.119 del D. Lgs. n. 36/2023 e s.m.i., l'Appaltatore intende subappaltare le seguenti prestazioni:

- inserire prestazioni di.....
-

Aci Informatica provvederà alla verifica che nei contratti di subappalto e/o subcontratti sia inserita, a pena di nullità, la clausola con la quale ciascuno dei subappaltatori e/o subcontraenti assume gli obblighi di tracciabilità dei flussi finanziari, ai sensi e per gli effetti dell'articolo 3 della Legge 136/2010. A tal fine, sarà cura dell'appaltatore inviare alla Rappresentanza di Aci Informatica, copia conforme all'originale del Contratto subappalto e/o subcontratto.

L'appaltatore si impegna affinché nel Contratto di subappalto e/o subcontratti sia inserita anche la seguente clausola:

“L'impresa [...], in qualità di subappaltatore/subcontraente dell'impresa [...], si impegna a dare immediata comunicazione alla rappresentanza di Aci Informatica ed alla competente Prefettura-



ufficio territoriale del Governo della notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria".

ART. 14 AVVALIMENTO [EVENTUALE]

Ai sensi dell'art.104 del D.Lgs. n. 36/2023, l'Appaltatore si obbliga nei confronti di ACI Informatica affinché l'impresa ausiliaria metta a disposizione per tutta la durata dell'appalto i requisiti e le risorse necessarie di cui è carente l'Appaltatore medesimo, in adempimento del contratto stipulato fra l'Aggiudicatario e l'impresa ausiliaria, allegato al presente atto sotto la lettera "....".

Inoltre, ai sensi dell'art. 104 co.11 del D.Lgs. n. 36/2023 l'Appaltatore si obbliga comunque a svolgere i seguenti compiti essenziali:

Infine, ai sensi dell'art. 104, co. 7 del D.Lgs. n. 36/2023, l'Appaltatore e l'impresa ausiliaria sono responsabili in solido nei confronti di ACI Informatica in relazione alle prestazioni oggetto del Contratto. Gli obblighi previsti dalla normativa antimafia a carico dell'Appaltatore si applicano anche nei confronti del soggetto ausiliario, in ragione dell'importo dell'appalto posto a base di gara.

La violazione delle suddette disposizioni costituisce grave inadempimento contrattuale e comporta la risoluzione di diritto del presente Contratto ai sensi dell'art.1456 cod. civ..

Laddove il RUP dovesse accertare che le prestazioni oggetto del Contratto non sono svolte direttamente dalle risorse umane e strumentali dell'impresa ausiliaria che l'Appaltatore utilizza in adempimento degli obblighi derivanti dal contratto di avvalimento, la Stazione Appaltante risolve il Contratto di appalto ai sensi dell'art. 1456 cod. civ..

ART. 15 SICUREZZA E SALUTE DEI LAVORATORI NEI LUOGHI DI LAVORO

Le attività esecutive devono essere realizzate in ottemperanza alla normativa vigente.

ART. 16 RISOLUZIONE DEL CONTRATTO

Resta fermo quanto previsto nell'art. 5.1 del CSA Servizi – Parte Generale.

ART. 17 RECESSO PER INFILTRAZIONE MAFIOSA

Il Committente recederà dal presente Contratto qualora pervenga, dalla Prefettura competente, la documentazione antimafia attestante, in capo all'Appaltatore, la sussistenza delle cause di divieto, di decadenza o di sospensione di cui all'art. 67 del D.Lgs. n. 159/2011 e ss.mm.ii. nonché la sussistenza di tentativi di infiltrazione mafiosa secondo quanto previsto dal medesimo D.Lgs. n. 159/2011. In tal caso, l'Appaltatore avrà diritto al pagamento delle prestazioni correttamente eseguite al momento del recesso ed il pagamento dei materiali utili esistenti in magazzino.



ART. 18 COMUNICAZIONI TRA LE PARTI

Per gli effetti del presente Contratto, tutte le comunicazioni e tutti gli scambi di informazioni tra Stazione Appaltante e Appaltatore si intendono validamente ed efficacemente effettuate qualora rese all'indirizzo PEC acquisti.tec@pec.aci.informatica.it di ACI Informatica e all'indirizzo PEC _____ dell'Appaltatore.

L'Appaltatore dichiara che l'indirizzo PEC comunicato corrisponde al domicilio digitale presente negli indici di cui agli articoli 6-bis e 6-ter del decreto legislativo 7 marzo 2005, n. 82 o, per l'operatore economico transfrontaliero, un indirizzo di servizio elettronico di recapito certificato qualificato ai sensi del Regolamento eIDAS.

Le comunicazioni della Stazione Appaltante si intendono conosciute dall'Appaltatore al momento del loro ricevimento al predetto indirizzo PEC.

ART. 19 FORO COMPETENTE

Tutte le controversie, di qualsiasi natura e specie, derivanti dall'esecuzione del Contratto saranno devolute alla competenza esclusiva del Giudice Ordinario, Foro di Roma.

ART. 20 SPESE DI CONTRATTO E TRATTAMENTO FISCALE

Per il presente contratto è prevista l'imposta di bollo di euro _____ secondo quanto indicato nell'Allegato I.4 del D.Lgs. 36/2023.

Fascia di importo contratto (euro)	Imposta (euro)
< 40.000	esente
≥ 40.000 < 150.000	40
≥ 150.000 < 1.000.000	120
≥ 1.000.000 < 5.000.000	250
≥ 5.000.000 < 25.000.000	500
≥ 25.000.000	1.000

Resta inteso che tutte le spese di bollo e di registro se dovute, ivi comprese quelle non espressamente previste, sono a carico dell'Appaltatore che dovrà provvedere al loro assolvimento nei termini di legge.

ART. 21 FIRMA DIGITALE

Ai sensi dell'art. 18, comma 1, del D.Lgs. 36/2023 e s.m.i., il Contratto sarà stipulato con scrittura privata e sottoscritto con firma digitale anche ai sensi del D.Lgs. 82/2005 e s.m.i..

L'appaltatore
Il Legale rappresentante

ACI Informatica S.p.A.



APPROVAZIONE SPECIFICA

Si approvano specificamente, ai sensi e per gli effetti degli articoli 1341 e 1342 cod. civ., le clausole contenute nei seguenti articoli:

Art. 2 Oggetto del Contratto.

Art. 3 Documenti costituenti il Contratto.

Art. 4 Importo dell'affidamento e invariabilità del corrispettivo.

Art. 5 Oneri a carico dell'Appaltatore relativi all'esecuzione.

Art. 6 Durata del Contratto.

Art. 7 Pagamento e tracciabilità.

Art. 9 Termini per l'esecuzione delle prestazioni e penali.

Art. 10 Garanzia definitiva.

Art. 11 Responsabilità civile verso terzi e assicurazioni.

Art. 13 Subappalto, cottimo e sub-contratti.

[eventuale] Art. 14 Avvalimento.

Art. 15 Sicurezza e salute dei lavoratori nei luoghi di lavoro.

Art. 16 Risoluzione del Contratto.

Art. 17 Recesso per infiltrazione mafiosa.

Art. 19 Foro competente.

Art. 20 Spese di Contratto e trattamento fiscale.

Art. 21 Firma digitale.

Si approvano altresì, ai sensi e per gli effetti degli articoli 1341 e 1342 cod. civ., le clausole contenute nei seguenti articoli del CSA di Servizi - Parte Generale:

Art. 1.3 Osservanza di leggi, regolamenti e norme.

Art. 1.4 Assicurazioni.

Art. 1.5 Pretese di terzi e clausola di manleva.

Art. 1.6.1 Uso di licenze.

Art. 1.6.2 Proprietà industriale e commerciale.

Art. 1.6.3 Proprietà, copyright, software.

Art. 1.6.4 Brevetti.

Art. 1.7 Doveri di riservatezza.

Art. 1.8.1 Variazioni richieste da ACI Informatica.

Art. 1.8.2 Variazioni richieste dall'Appaltatore.

Art. 1.8.3 Modifica soggettiva dell'Appaltatore e divieto di cessione del Contratto.

Art. 1.9.1 Subappalto.

Art. 1.9.2 Responsabilità dell'Appaltatore per il subappalto.

Art. 1.9.3 Pagamento dei subappaltatori.

Art. 1.10 Codice Etico e Modello Organizzativo. Patto di Integrità.

Art. 1.12 Trattamento dei dati personali.

Art. 2.1 Avvio dell'esecuzione del Contratto.

Art. 2.2 Obblighi dell'Appaltatore nell'espletamento del Servizio.

Art. 2.4 Programma cronologico e termini contrattuali del Servizio.

Art. 2.5 Spostamento dei termini contrattuali dei singoli servizi.

Art. 2.6 Piano di Esecuzione del Servizio ICT.

Art. 2.7 Imballo e trasporto delle forniture.

Art. 2.8.1 Consegna.

Art. 2.8.2 Verifica di conformità e accettazione della fornitura.

Art. 2.8.3 Non conformità – difetti.

Art. 2.8.4 Prove e test per il servizio di installazione.

Art. 2.9 Verifica di conformità e presa in carico del Servizio.

Art. 2.10 Sorveglianza.

Art. 2.12 Rappresentanza dell'Appaltatore.

Art. 2.13 Svolgimento delle attività.

Art. 2.14.1 Misure per la salute e sicurezza nei luoghi di lavoro.

Art. 2.14.2 Regole comportamentali per l'accesso e l'utilizzo dei sistemi informativi di ACI Informatica.

Art. 2.14.3 Monitoraggio per la sicurezza e conseguenze di una violazione delle regole.

Art. 2.14.4 Accettazione delle clausole sistemi per la sicurezza delle informazioni di ACI Informatica.

Art. 2.15.1 Generalità.

Art. 2.15.2 Clausola sociale.

Art. 2.15.3 Trattamento economico del personale.

Art. 2.15.4 Tutela del personale e relative provvidenze.

Art. 2.15.5 Prova degli adempimenti.

Art. 2.15.6 Personale dei Subappaltatori.

Art. 2.15.7 Orario di lavoro.

Art. 2.16 Soggezioni particolari.

Art. 2.17 Coordinamento e subordinazione rispetto ad altre attività di ACI Informatica.

Art. 2.18 Sospensione del Servizio.

Art. 2.19 Esecuzione in danno.



- Art. 3.1 Condizioni ambientali.
- Art. 3.2 Remuneratività dei prezzi contrattuali.
- Art. 3.3 Revisione prezzi.
- Art. 3.4 Nuovi prezzi.
- Art. 4.1 Responsabilità e danni.
- Art. 4.2 Penali.
- Art. 4.3 Modalità di fatturazione e pagamento. Interessi sui pagamenti.
- Art. 4.4 Tracciabilità dei flussi finanziari.
- Art. 4.5 Cauzione.
- Art. 4.6 Cessione dei crediti.
- Art. 4.7 Contestazioni.
- Art. 4.8 Imposte e tasse.
- Art. 4.9 Adempimenti ex art. 17-bis del D.Lgs. 9 luglio 1997, n. 241
- Art. 5.1 Risoluzione del Contratto.
- Art. 5.2 Procedimento di risoluzione del Contratto.
- Art. 5.3.1 Recesso ordinario.
- Art. 5.3.2 Recesso per fallimento dell'Appaltatore.
- Art. 5.3.3 Recesso per altre procedure concorsuali dell'Appaltatore.
- Art. 5.3.4 Obbligo di recesso.

L'appaltatore

Il Legale rappresentante

ACI Informatica S.p.A.



Allegati:

- A) Capitolato Speciale di Appalto di Servizi Parte Generale V 1.
- B) Capitolato Tecnico
- C) *[Eventuale]* Mandato di RTI
- D) *[Eventuale]* Contratto di Avvalimento
- E) Offerta economica
- F) Garanzia definitiva
- G) Dichiarazione dell'Appaltatore di subappalto
- H) Polizza assicurativa



Codice affidamento ICT0966A25

ALLEGATO 6 AL PROGETTO

LOTTO 2

SCHEMA DI CONTRATTO PER SERVIZI E FORNITURE

TRA

ACI Informatica S.p.A. con sede in Roma, via Fiume delle Perle n. 24, Codice Fiscale 00405030586 e Partita IVA 00883311003, in persona del Direttore Approvvigionamenti e Centrale di Committenza, Ing. Stefano Carosi (di seguito per brevità ACI Informatica), autorizzato al presente atto giusta Procura speciale autenticata nelle firme dal Notaio Marco Pinto di Roma in data 17 marzo 2025, Repertorio n. 18254, Raccolta n. 12941,

- Stazione Appaltante -

E

l'impresa, con sede legale in (.....),
Via CAP, capitale sociale €.....,
iscritta nel Registro delle Imprese di Codice fiscale n.°
....., partita IVA....., rappresentata dain qualità
di..... giusti poteri risultanti da
[eventuale, in caso di R.T.I.] in qualità di mandataria del RTI costituito con l'impresa
..... con sede legale in (.....), Via
.....C.a.p.iscritta nel Registro delle Imprese di
..... con Codice fiscale n.°partita
IVA.....(Mandante) e l'impresa con sede
legale in (.....), Via CAPiscritta
nel Registro delle Imprese di con Codice fiscale n.°
.....partita IVA.....(Mandante)

- Appaltatore -

La Stazione Appaltante e l'Appaltatore (nel prosieguo, unitamente denominati "Parti")

PREMESSO CHE

- A.** la Stazione Appaltante ha approvato con disposizione a firma del Direttore Approvvigionamenti e Centrale di Committenza del .../.../....., l'avvio del procedimento concorsuale per l'affidamento della fornitura di accessi internet protetti dal servizio di sicurezza anti DDoS per il data center di Roma sito in via Fiume delle Perle 24 e per il data center sito presso il Consorzio Namex in Roma in via dei Tizii, da espletarsi, ai sensi dell'art. 32 del D. Lgs. n. 36/2023, mediante appalto specifico sul "Sistema Dinamico di Acquisizione della Pubblica Amministrazione" (SDAPA) per la fornitura di prodotti e servizi per l'informatica



e le telecomunicazioni, da aggiudicare con il criterio del minor prezzo, suddivisi in due Lotti i cui importi complessivi a base d'appalto sono pari ad € 95.000,000 per il Lotto 1, di cui € 0,00 per oneri relativi alla sicurezza non soggetti a ribasso ed € 85.000,00 per il Lotto 2, di cui € 0,00 per oneri relativi alla sicurezza non soggetti a ribasso;

- B.** ACI Informatica, con lettera del _____ ha invitato tutti gli operatori economici ammessi alla categoria merceologica oggetto dell'Appalto Specifico e in possesso dei requisiti indicati nella documentazione di gara, a presentare un'offerta avente ad oggetto quanto descritto nella medesima documentazione, da aggiudicarsi con il criterio del minor prezzo di cui al comma 3 dell'art. 108 del D.Lgs. n. 36/2023 e s.m.i.;
- C.** nei confronti dell'appaltatore, risultato aggiudicatario del Lotto 2, sono state esperite con esito positivo le verifiche dei requisiti di carattere generale e speciale concernenti la veridicità delle dichiarazioni presentate in sede di gara;
- D.** ai sensi del D.Lgs. n.159/2011, sussistono anche i presupposti di legge per la stipulazione del presente Contratto, giuste le informazioni antimafia rilasciate dall'U.T.G.-Prefettura di _____, in data ____/____/____ con Prot. n. _____, relativa all'Impresa _____ (in caso di RTI ripetere per ognuno dei componenti il Raggruppamento, in caso di avalimento ripetere anche per l'impresa ausiliaria) (oppure decorso il termine previsto e procedendo anche in assenza delle informazioni antimafia) ACI Informatica S.p.A., tramite il portale della Banca Dati Nazionale Antimafia (B.D.N.A.) ha richiesto per l'impresa _____ in data _____ l'informazione ai sensi dell'art. 85 del Decreto Legislativo 159/2011 e s.m.i e, trascorsi più di 30 (trenta) giorni da detta richiesta ACI Informatica S.p.A., è legittimata a procedere alla stipula del presente Contratto (in caso di RTI ripetere per ognuno dei componenti il Raggruppamento e in caso di avalimento per l'impresa ausiliaria)
- E.** all'esito dell'anzidetta procedura è stata disposta dal Direttore Approvvigionamenti e Centrale di Committenza di ACI Informatica, l'aggiudicazione in favore di _____, comunicata ex art. 90 del D.Lgs. n. 36/2023 e s.m.i. a tutti i concorrenti, ivi compreso il predetto Aggiudicatario, con nota del _____ prot. _____;
- F.** l'Aggiudicatario ha presentato quanto previsto nel Capitolato d'Oneri e nei suoi allegati per la stipula del contratto;
- G.** l'Appaltatore conferma e ribadisce tutte le dichiarazioni formulate con la propria offerta in sede di gara, ed in particolare di avere offerto il prezzo di €....., di cui €..... per oneri relativi alla sicurezza, non soggetti a ribasso;
- H.** (eventuale, in caso di R.T.I.) con scrittura privata munita di autentica delle firme Rep. n. _____/_____ in data ____/____/____ per Dott. _____ Notaio in _____, iscritto al Collegio Notarile di _____, le Imprese _____ e _____ si sono costituite, ai sensi dell'art. 68 D.Lgs. n. 36/2023 e s.m.i., in Raggruppamento Temporaneo di Imprese, designando quale Capogruppo l'Impresa _____, conferendo al legale rappresentante di quest'ultima mandato collettivo speciale irrevocabile con rappresentanza, affinché possa compiere in nome proprio e per conto della mandante tutte le operazioni e gli atti di qualsiasi natura dipendenti dal presente affidamento, fino all'estinzione di ogni rapporto;
- I.** alla luce di quanto riportato alle precedenti lettere si può procedere con la stipula del contratto;



- J. il Responsabile Unico del Progetto (RUP) è il Dott. Angelo Marrucci;
- K. il Direttore dell'Esecuzione del contratto (DEC) è il Sig. Mauro Reali;
- L. tutti i predetti atti devono aversi qui per integralmente richiamati e trascritti.

Tutto ciò premesso, tra le Parti sopra costituite si conviene quanto segue:

ART. 1 VALIDITÀ DELLE PREMESSE. ALLEGATI. NORME REGOLATRICI

Le premesse e gli allegati costituiscono parte integrante e sostanziale del presente Contratto ed hanno ad ogni effetto valore di patto.

L'esecuzione del Contratto è disciplinata, oltre che da quanto disposto nel medesimo e in tutti i documenti che fanno parte del Contratto stesso ai sensi del successivo art. 3, dalle disposizioni di cui al D.Lgs. 36/2023 e s.m.i., dal Codice Civile, e dalle altre disposizioni normative in materia di contratti di diritto privato, per quanto non regolato dalle disposizioni sopra richiamate.

ACI Informatica, ai sensi della normativa e prassi vigente, provvederà a comunicare all'Autorità Nazionale Anticorruzione (ANAC) i fatti riguardanti la fase di esecuzione del presente Contratto.

ART. 2 OGGETTO DEL CONTRATTO

ACI Informatica S.p.A., ai sensi del D.Lgs. n. 36/2023, affida all'Appaltatore, che accetta senza riserva alcuna, l'esecuzione della fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di Roma del Consorzio Namex in Via dei Tizii, n. 6, secondo quanto meglio precisato nel presente Contratto e nei relativi allegati, con particolare riferimento al Capitolato Speciale di Appalto di Servizi - Parte Generale sub lett. "A" e al "Capitolato Tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di Roma via dei Tizii - Lotto 2", sub lett. "B".

In particolare, trattasi, a titolo esemplificativo e non esaustivo, dei seguenti servizi:

1. Un accesso Internet in fibra ottica con banda garantita di almeno 8Gbps e peering BGP4 con ASN della committente.
2. Fornitura di una classe IP di tipo PA (Provider Aggregable) da almeno 64 indirizzi da utilizzare sullo stesso accesso ed instradare mediante routing statico, in aggiunta al predetto routing dinamico.
3. Un servizio di sicurezza di tipo anti "Distributed Denial of Service" attivo sul tutto il traffico trasportato dall'accesso fornito e per tutti gli IP pubblici a disposizione della committente compresi quelli messi a disposizione del fornitore al punto due. Il servizio dovrà essere realizzato su infrastruttura del fornitore e gestito direttamente da proprie strutture sistemistiche, non è ammesso un servizio offerto tramite terze parti.

Il rilascio del circuito e del servizio anti DDoS deve avvenire entro e non oltre 90 giorni solari dal presente ordine.

L'Appaltatore si impegna ad eseguire le anzidette attività in ottemperanza alla normativa vigente, alla disciplina del procedimento concorsuale, alle prescrizioni del presente Contratto e



relativi allegati, in particolare del Capitolato Speciale di Appalto di Servizi Parte Generale e del Capitolato Tecnico.

ART. 3 DOCUMENTI COSTITUENTI IL CONTRATTO

Fanno parte integrante e sostanziale del presente Contratto e si intendono allegati allo stesso, ancorché non materialmente e fisicamente uniti al medesimo, gli atti e i documenti del procedimento concorsuale, che si hanno per integralmente richiamati e trascritti, nonché i documenti tecnici ed amministrativi e in particolare i seguenti atti, qui allegati in copia informatica:

- a. Capitolato Speciale di Appalto (d'ora in poi CSA) di Servizi Parte Generale
- b. Capitolato Tecnico per la fornitura di un accesso internet protetto da servizio di sicurezza anti DDoS sulla sede di Roma via Fiume delle Perle Lotto 2;
- c. (*eventuale*, in caso di RTI) Mandato costitutivo del Raggruppamento di imprese, qui allegato in originale o copia conforme all'originale sub lett. "___";
- d. Offerta economica generata dal sistema allegata al presente atto sotto la lettera "___";
- e. Relazione tecnica e Scheda Sintetica "Dichiarazione possesso requisiti minimi" presentate in fase di gara;
- f. Garanzia definitiva – ai sensi dell'art.117 del D.Lgs. n.36/2023 - prodotta dall'Appaltatore con Polizza fidejussoria a garanzia della buona esecuzione del presente Contratto, qui allegata unitamente alla/e Certificazione/i di qualità prodotte ai sensi dell'art. 106 comma 8 del D.Lgs. n. 36/2023;
- g. Dichiarazione dell'Appaltatore, presentata in sede di offerta con cui è stata manifestata l'intenzione di subappaltare nei limiti di cui all'art.119 del D.Lgs. n. 36/2023;
- h. (*eventuale, in caso di avvalimento*) Contratto di avvalimento stipulato tra l'Appaltatore e l'impresa ausiliaria ai sensi dell'art. 104 del D.Lgs. n. 36/2023;
- i. Polizza assicurativa

L'affidamento viene accettato dall'Appaltatore con l'osservanza piena, assoluta, incondizionata ed inderogabile delle norme, condizioni, patti, obblighi, oneri e modalità previsti nel Contratto ed in tutti gli atti e documenti in esso richiamati, siano o meno essi qui materialmente allegati, con particolare riferimento al CSA di Servizi– Parte Generale ed al Capitolato Tecnico.

ART. 4 IMPORTO DELL'AFFIDAMENTO

L'importo complessivo dell'affidamento, al netto dell'I.V.A., è pari ad €....., comprensivo di €..... per oneri della sicurezza ed è così composto:

1. €....., determinato sulla base del ribasso del _____% offerto rispetto alla base d'asta indicata per l'attivazione del collegamento di accesso ad Internet, come il tutto dettagliato nel capitolato tecnico;
2. €..... determinato sulla base del ribasso del _____% offerto rispetto alla base d'asta indicata per l'accesso internet protetto da servizio di sicurezza anti DDoS come il



tutto dettagliato dal capitolato tecnico.

L'importo complessivo offerto che sarà corrisposto per la fornitura/servizi richiesti è espresso in Euro, onnicomprensivo e si intende, tra l'altro:

- una tantum per l'attivazione del servizio di connettività di cui al precedente punto 1;
- a canone per l'accesso internet protetto da servizio di sicurezza anti DDoS di cui al precedente punto 2.

ACI Informatica si riserva la facoltà, nei limiti di cui all'art. 76, comma 6 del D.Lgs. 36/2023 e s.m.i., di affidare all'aggiudicatario, nei successivi tre anni dalla stipula del contratto, nuovi servizi consistenti nella ripetizione di servizi analoghi, secondo quanto previsto nel progetto posto alla base del presente affidamento, per una durata pari a 36 mesi per un importo stimato complessivamente non superiore ad € al netto di Iva e/o di altre imposte e contributi di legge, nonché degli oneri per la sicurezza dovuti a rischi da interferenze

ACI Informatica si riserva la facoltà di esercizio delle opzioni di cui sopra comunicandola all'appaltatore mediante posta elettronica certificata almeno 2 giorni prima della scadenza del contratto originario.

ACI Informatica S.p.A., ai sensi dell'art. 60, del D.Lgs. n. 36/2023, applicherà la formula di revisione prezzi, calcolata sugli indici indicati nel comma 3 dell'art 60 del D.Lgs. n. 36/2023, come di seguito riportata:

qualora, al verificarsi di particolari condizioni di natura oggettiva, che determinano una variazione del costo dell'appalto, l'indice riporti una variazione percentuale superiore al 5% rispetto al valore del medesimo indice nel mese di stipula del contratto, i prezzi unitari saranno adeguati in misura pari al 80% della variazione riportata a partire dal mese successivo a quello di rilevazione.

ART. 5 ONERI A CARICO DELL'APPALTATORE RELATIVI ALL'ESECUZIONE

Rientrano tra gli obblighi a carico dell'Appaltatore e si intendono, pertanto, adeguatamente remunerati nel corrispettivo di cui all'articolo 4 del presente Contratto, tutte le prestazioni afferenti all'esecuzione di quanto proposto in sede di offerta.

ART. 6 DURATA DEL CONTRATTO

La durata del presente Contratto è fissata in 36 mesi a partire dalla data di rilascio del circuito e del servizio anti DDoS che dovrà avvenire entro e non oltre 90 giorni solari dalla sottoscrizione del contratto e dovrà essere certificata da un apposito verbale di collaudo positivo sottoscritto dalle parti.

ART. 7 PAGAMENTO E TRACCIABILITÀ

7 a) Termini di pagamento

Le fatture dovranno essere emesse con le seguenti modalità:

- per le eventuali attività una-tantum in unica soluzione all'attivazione del collegamento di accesso ad Internet risultante dal collaudo positivo del circuito;



- per il servizio a canone di accesso ad Internet e di sicurezza anti-DDoS fatture di pari importo con cadenza trimestrale posticipata.

Il pagamento delle predette fatture sarà effettuato secondo quanto riportato nel CSA di Servizi – Parte Generale.

7 b) Tracciabilità dei flussi finanziari

I corrispettivi spettanti all'Appaltatore saranno accreditati unicamente a mezzo bonifico bancario/postale sul conto corrente dedicato ed intrattenuto presso, di cui al seguente codice IBAN:, esonerando ACI Informatica da ogni responsabilità per i pagamenti eseguiti in tal modo, ai sensi del combinato disposto di cui agli artt. 21 e 125 del D.Lgs. 36/2023 sulla tracciabilità dei flussi finanziari ai sensi dell'articolo 3 della legge 13 agosto 2010, n. 136.

La/le persona/e delegata/e ad operare sul conto corrente di cui sopra sono:

- a) Sig. – nato a.....il .././....., c.f.;
- b) Sig. – nato a.....il .././....., c.f.;
- c)

ART. 8 RESPONSABILE DEL CONTRATTO E REFERENTE TECNICO DELLA SICUREZZA

Ai fini dell'esecuzione del Contratto l'Appaltatore ha nominato quale Responsabile del Contratto l'Ing./il Dott./Sig., nato a (.....) il giorno (C.F.:).

Ai sensi di quanto previsto al paragrafo 11.1 del Capitolato tecnico, l'Appaltatore dovrà designare e comunicare alla Committente, entro 48 ore dalla stipula del contratto, un Referente Tecnico per la Sicurezza

ART. 9 TERMINI PER L'ESECUZIONE DELLE PRESTAZIONI E PENALI

9 a) Termini.

Accesso ad internet

- *Attivazione del collegamento di accesso ad internet*

L'attivazione del collegamento di accesso ad Internet dovrà essere effettuata entro 90 giorni solari dall'ordine.

Servizio di assistenza sulla connettività Internet e anti DDoS

- Il servizio di Help Desk dovrà essere disponibile h24, 7 giorni su 7.



- Il servizio di Help Desk dovrà prendere in carico la segnalazione per la mancata connettività Internet e/o per la protezione DDoS al massimo entro trenta minuti dalla chiamata del cliente.

Livelli di servizio richiesti sulla connettività Internet

- Disponibilità

Il servizio di connettività Internet dovrà essere disponibile h24, 7 giorni su 7, con un livello di servizio garantito di almeno il 99,8% calcolato su base mensile. Ai fini del calcolo dei livelli di servizio, il circuito si intende indisponibile anche in caso di forte degrado delle performance ovvero un tasso di perdita di pacchetti > 2%.

- Tempi di ripristino guasti

A fronte di guasti o anomalie che si dovessero presentare sull'accesso internet il fornitore si dovrà risolvere il problema e ripristinare completamente il servizio nel più breve tempo possibile garantendo comunque i seguenti tempi di ripristino:

- 12 ore nel caso di guasti non bloccanti;
- 8 ore nel caso di guasti bloccanti.

Livelli di servizio richiesti per la protezione DDoS

- Il servizio di protezione DDOS dovrà essere disponibile per almeno il 99,5% del tempo (H24 x 7 gg) su base mensile. Tutte le attività di manutenzione programmate, che comportino indisponibilità del servizio, dovranno essere comunicate al cliente con un anticipo di almeno 10 giorni.

- Tempo di intervento della "mitigation":

- Nel caso di evento individuato e segnalato dai sistemi di monitoraggio e analisi del fornitore, la policy deve essere attivata nel più breve tempo possibile e comunque entro 10 minuti dall'evento in almeno il 90% dei casi (Tempo di presa in carico Proattiva).
- Nel caso di evento rilevato solamente dal cliente, il fornitore dovrà prendere in carico la segnalazione entro 30 minuti dall'apertura della chiamata al proprio SOC in almeno il 90% dei casi (Tempo di presa in carico Reattiva).

- Percentuale di rilevamento:

Il servizio fornito dovrà essere in grado di rilevare almeno il 90% degli attacchi di tipo DDoS su base mensile.

- Disponibilità Reportistica sull'attacco

A seguito di eventi DDoS il fornitore dovrà essere in grado, su richiesta del cliente, di inviare o mettere a disposizione su un proprio portale web i report contenenti i dati statistici più significativi dell'evento che dovrà essere messo a disposizione entro 24 ore dalla richiesta.

Governance e Supporto alla Sicurezza (SPOC)

- Entro 48 ore dalla stipula del presente contratto, l'Appaltatore dovrà designare e comunicare alla Committente, un Referente Tecnico per la Sicurezza.

9 b) Penali.

Si rinvia a quanto previsto al paragrafo 12 del capitolato tecnico_Lotto 2.

ART. 10 GARANZIA DEFINITIVA

L'Appaltatore, ai sensi dell'art.117 del D.Lgs. n. 36/2023, a garanzia delle obbligazioni assunte con il presente Contratto e degli impegni comunque previsti negli allegati al medesimo, ha prestato, con le modalità indicate nei documenti della procedura concorsuale, apposita garanzia cauzionale mediante Polizza fidejussoria n., emessa in data .../.../..... dalla compagnia, per l'importo di € con firma legalizzata ai sensi di legge, allegata al presente atto sotto la *sub* lett. "___".

ART. 11 RESPONSABILITÀ CIVILE VERSO TERZI E ASSICURAZIONI

Ai sensi dell'art. 117, comma 10 del D.Lgs 36/2023 l'Appaltatore ha stipulato una polizza di assicurazione per danni di esecuzione e responsabilità civile verso terzi causati nel corso dell'esecuzione dell'appalto avente validità dalla data di stipula del Contratto e per tutta la durata dello stesso.

La predetta copertura è costituita mediante Polizza Car/Rct n.° emessa in data .../.../..... dalla Compagnia – con firma regolarmente legalizzata ai sensi di legge - e qui allegata con la *sub* lett. "___" - per una somma assicurata pari all'ammontare del Contratto (€.....) e per un massimale contro la responsabilità civile verso terzi di €.....

ART. 13 SUBAPPALTO, COTTIMO E SUB-CONTRATTI

Ai sensi dell'art.119 del D. Lgs. n. 36/2023 e s.m.i., l'Appaltatore intende subappaltare le seguenti prestazioni:

- inserire prestazioni di.....
-

Aci Informatica provvederà alla verifica che nei contratti di subappalto e/o subcontratti sia inserita, a pena di nullità, la clausola con la quale ciascuno dei subappaltatori e/o subcontraenti assume gli obblighi di tracciabilità dei flussi finanziari, ai sensi e per gli effetti dell'articolo 3 della Legge 136/2010. A tal fine, sarà cura dell'appaltatore inviare alla Rappresentanza di Aci Informatica, copia conforme all'originale del Contratto subappalto e/o subcontratto.

L'appaltatore si impegna affinché nel Contratto di subappalto e/o subcontratti sia inserita anche la seguente clausola:

"L'impresa [...], in qualità di subappaltatore/subcontraente dell'impresa [...], si impegna a dare immediata comunicazione alla rappresentanza di Aci Informatica ed alla competente Prefettura-ufficio territoriale del Governo della notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria".



ART. 14 AVVALIMENTO [EVENTUALE]

Ai sensi dell'art.104 del D.Lgs. n. 36/2023, l'Appaltatore si obbliga nei confronti di ACI Informatica affinché l'impresa ausiliaria metta a disposizione per tutta la durata dell'appalto i requisiti e le risorse necessarie di cui è carente l'Appaltatore medesimo, in adempimento del contratto stipulato fra l'Aggiudicatario e l'impresa ausiliaria, allegato al presente atto sotto la lettera "....".

Inoltre, ai sensi dell'art. 104 co.11 del D.Lgs. n. 36/2023 l'Appaltatore si obbliga comunque a svolgere i seguenti compiti essenziali:

Infine, ai sensi dell'art. 104, co. 7 del D.Lgs. n. 36/2023, l'Appaltatore e l'impresa ausiliaria sono responsabili in solido nei confronti di ACI Informatica in relazione alle prestazioni oggetto del Contratto. Gli obblighi previsti dalla normativa antimafia a carico dell'Appaltatore si applicano anche nei confronti del soggetto ausiliario, in ragione dell'importo dell'appalto posto a base di gara.

La violazione delle suddette disposizioni costituisce grave inadempimento contrattuale e comporta la risoluzione di diritto del presente Contratto ai sensi dell'art.1456 cod. civ..

Laddove il RUP dovesse accertare che le prestazioni oggetto del Contratto non sono svolte direttamente dalle risorse umane e strumentali dell'impresa ausiliaria che l'Appaltatore utilizza in adempimento degli obblighi derivanti dal contratto di avvalimento, la Stazione Appaltante risolve il Contratto di appalto ai sensi dell'art. 1456 cod. civ..

ART. 15 SICUREZZA E SALUTE DEI LAVORATORI NEI LUOGHI DI LAVORO

Le attività esecutive devono essere realizzate in ottemperanza alla normativa vigente.

ART. 16 RISOLUZIONE DEL CONTRATTO

Resta fermo quanto previsto nell'art. 5.1 del CSA Servizi – Parte Generale.

ART. 17 RECESSO PER INFILTRAZIONE MAFIOSA

Il Committente recederà dal presente Contratto qualora pervenga, dalla Prefettura competente, la documentazione antimafia attestante, in capo all'Appaltatore, la sussistenza delle cause di divieto, di decadenza o di sospensione di cui all'art. 67 del D.Lgs. n. 159/2011 e ss.mm.ii. nonché la sussistenza di tentativi di infiltrazione mafiosa secondo quanto previsto dal medesimo D.Lgs. n. 159/2011. In tal caso, l'Appaltatore avrà diritto al pagamento delle prestazioni correttamente eseguite al momento del recesso ed il pagamento dei materiali utili esistenti in magazzino.

ART. 18 COMUNICAZIONI TRA LE PARTI

Per gli effetti del presente Contratto, tutte le comunicazioni e tutti gli scambi di informazioni tra Stazione Appaltante e Appaltatore si intendono validamente ed efficacemente effettuate qualora



rese all'indirizzo PEC acquisti.tec@pec.aci.informatica.it di ACI Informatica e all'indirizzo PEC _____ dell'Appaltatore.

L'Appaltatore dichiara che l'indirizzo PEC comunicato corrisponde al domicilio digitale presente negli indici di cui agli articoli 6-bis e 6-ter del decreto legislativo 7 marzo 2005, n. 82 o, per l'operatore economico transfrontaliero, un indirizzo di servizio elettronico di recapito certificato qualificato ai sensi del Regolamento eIDAS.

Le comunicazioni della Stazione Appaltante si intendono conosciute dall'Appaltatore al momento del loro ricevimento al predetto indirizzo PEC.

ART. 19 FORO COMPETENTE

Tutte le controversie, di qualsiasi natura e specie, derivanti dall'esecuzione del Contratto saranno devolute alla competenza esclusiva del Giudice Ordinario, Foro di Roma.

ART. 20 SPESE DI CONTRATTO E TRATTAMENTO FISCALE

Per il presente contratto è prevista l'imposta di bollo di euro _____ secondo quanto indicato nell'Allegato I.4 del D.Lgs. 36/2023.

Fascia di importo contratto (euro)	Imposta (euro)
< 40.000	esente
≥ 40.000 < 150.000	40
≥ 150.000 < 1.000.000	120
≥ 1.000.000 < 5.000.000	250
≥ 5.000.000 < 25.000.000	500
≥ 25.000.000	1.000

Resta inteso che tutte le spese di bollo e di registro se dovute, ivi comprese quelle non espressamente previste, sono a carico dell'Appaltatore che dovrà provvedere al loro assolvimento nei termini di legge.

ART. 21 FIRMA DIGITALE

Ai sensi dell'art. 18, comma 1, del D.Lgs. 36/2023 e s.m.i., il Contratto sarà stipulato con scrittura privata e sottoscritto con firma digitale anche ai sensi del D.Lgs. 82/2005 e s.m.i..

L'appaltatore

Il Legale rappresentante

ACI Informatica S.p.A.



APPROVAZIONE SPECIFICA

Si approvano specificamente, ai sensi e per gli effetti degli articoli 1341 e 1342 cod. civ., le clausole contenute nei seguenti articoli:

Art. 2 Oggetto del Contratto.

Art. 3 Documenti costituenti il Contratto.

Art. 4 Importo dell'affidamento e invariabilità del corrispettivo.

Art. 5 Oneri a carico dell'Appaltatore relativi all'esecuzione.

Art. 6 Durata del Contratto.

Art. 7 Pagamento e tracciabilità.

Art. 9 Termini per l'esecuzione delle prestazioni e penali.

Art. 10 Garanzia definitiva.

Art. 11 Responsabilità civile verso terzi e assicurazioni.

Art. 13 Subappalto, cottimo e sub-contratti.

[eventuale] Art. 14 Avvalimento.

Art. 15 Sicurezza e salute dei lavoratori nei luoghi di lavoro.

Art. 16 Risoluzione del Contratto.

Art. 17 Recesso per infiltrazione mafiosa.

Art. 19 Foro competente.

Art. 20 Spese di Contratto e trattamento fiscale.

Art. 21 Firma digitale.

Si approvano altresì, ai sensi e per gli effetti degli articoli 1341 e 1342 cod. civ., le clausole contenute nei seguenti articoli del CSA di Servizi - Parte Generale:

Art. 1.3 Osservanza di leggi, regolamenti e norme.

Art. 1.4 Assicurazioni.

Art. 1.5 Pretese di terzi e clausola di manleva.

Art. 1.6.1 Uso di licenze.

Art. 1.6.2 Proprietà industriale e commerciale.

Art. 1.6.3 Proprietà, copyright, software.

Art. 1.6.4 Brevetti.

Art. 1.7 Doveri di riservatezza.

Art. 1.8.1 Variazioni richieste da ACI Informatica.

Art. 1.8.2 Variazioni richieste dall'Appaltatore.

Art. 1.8.3 Modifica soggettiva dell'Appaltatore e divieto di cessione del Contratto.

Art. 1.9.1 Subappalto.

Art. 1.9.2 Responsabilità dell'Appaltatore per il subappalto.



- Art. 1.9.3 Pagamento dei subappaltatori.
- Art. 1.10 Codice Etico e Modello Organizzativo. Patto di Integrità.
- Art. 1.12 Trattamento dei dati personali.
- Art. 2.1 Avvio dell'esecuzione del Contratto.
- Art. 2.2 Obblighi dell'Appaltatore nell'espletamento del Servizio.
- Art. 2.4 Programma cronologico e termini contrattuali del Servizio.
- Art. 2.5 Spostamento dei termini contrattuali dei singoli servizi.
- Art. 2.6 Piano di Esecuzione del Servizio ICT.
- Art. 2.7 Imballo e trasporto delle forniture.
- Art. 2.8.1 Consegna.
- Art. 2.8.2 Verifica di conformità e accettazione della fornitura.
- Art. 2.8.3 Non conformità – difetti.
- Art. 2.8.4 Prove e test per il servizio di installazione.
- Art. 2.9 Verifica di conformità e presa in carico del Servizio.
- Art. 2.10 Sorveglianza.
- Art. 2.12 Rappresentanza dell'Appaltatore.
- Art. 2.13 Svolgimento delle attività.
- Art. 2.14.1 Misure per la salute e sicurezza nei luoghi di lavoro.
- Art. 2.14.2 Regole comportamentali per l'accesso e l'utilizzo dei sistemi informativi di ACI Informatica.
- Art. 2.14.3 Monitoraggio per la sicurezza e conseguenze di una violazione delle regole.
- Art. 2.14.4 Accettazione delle clausole sistemi per la sicurezza delle informazioni di ACI Informatica.
- Art. 2.15.1 Generalità.
- Art. 2.15.2 Clausola sociale.
- Art. 2.15.3 Trattamento economico del personale.
- Art. 2.15.4 Tutela del personale e relative provvidenze.
- Art. 2.15.5 Prova degli adempimenti.
- Art. 2.15.6 Personale dei Subappaltatori.
- Art. 2.15.7 Orario di lavoro.
- Art. 2.16 Soggezioni particolari.
- Art. 2.17 Coordinamento e subordinazione rispetto ad altre attività di ACI Informatica.
- Art. 2.18 Sospensione del Servizio.
- Art. 2.19 Esecuzione in danno.
- Art. 3.1 Condizioni ambientali.
- Art. 3.2 Remuneratività dei prezzi contrattuali.
- Art. 3.3 Revisione prezzi.

Art. 3.4 Nuovi prezzi.
Art. 4.1 Responsabilità e danni.
Art. 4.2 Penali.
Art. 4.3 Modalità di fatturazione e pagamento. Interessi sui pagamenti.
Art. 4.4 Tracciabilità dei flussi finanziari.
Art. 4.5 Cauzione.
Art. 4.6 Cessione dei crediti.
Art. 4.7 Contestazioni.
Art. 4.8 Imposte e tasse.
Art. 4.9 Adempimenti ex art. 17-bis del D.Lgs. 9 luglio 1997, n. 241
Art. 5.1 Risoluzione del Contratto.
Art. 5.2 Procedimento di risoluzione del Contratto.
Art. 5.3.1 Recesso ordinario.
Art. 5.3.2 Recesso per fallimento dell'Appaltatore.
Art. 5.3.3 Recesso per altre procedure concorsuali dell'Appaltatore.
Art. 5.3.4 Obbligo di recesso.

L'appaltatore

Il Legale rappresentante

ACI Informatica S.p.A.

Allegati:

- A) Capitolato Speciale di Appalto di Servizi Parte Generale V 1.
- B) Capitolato Tecnico
- C) *[Eventuale]* Mandato di RTI
- D) *[Eventuale]* Contratto di Avvalimento
- E) Offerta economica generata dal sistema
- F) Garanzia definitiva
- G) Dichiarazione dell'Appaltatore di subappalto
- H) Polizza assicurativa



CAPITOLATO SPECIALE DI APPALTO DI SERVIZI PARTE GENERALE

Versione 1.8

Sommario

1	DEFINIZIONI E NORME GENERALI	5
1.1	DEFINIZIONI	5
1.1.1	ACI INFORMATICA	5
1.1.2	RAPPRESENTANZA DI ACI INFORMATICA	5
1.1.3	APPALTATORE	5
1.1.4	RESPONSABILE DEL CONTRATTO	5
1.1.5	DOCUMENTI CONTRATTUALI	5
1.1.6	DUVRI E PSC	6
1.1.7	SERVIZIO	6
1.2	DIFFORMITÀ TRA DOCUMENTI CONTRATTUALI	7
1.3	OSSERVANZA DI LEGGI, REGOLAMENTI E NORME	7
1.4	ASSICURAZIONI	8
1.5	PRETESE DI TERZI E CLAUSOLA DI MANLEVA	9
1.6	USO DI LICENZE, PROPRIETÀ INDUSTRIALE, COMMERCIALE, BREVETTI, SOFTWARE E COPYRIGHT	9
1.6.1	USO DI LICENZE	9
1.6.2	PROPRIETÀ INDUSTRIALE E COMMERCIALE	9
1.6.3	PROPRIETÀ, COPYRIGHT, SOFTWARE	11
1.6.4	BREVETTI	13
1.7	DOVERE DI RISERVATEZZA	13
1.8	VARIAZIONI	14
1.8.1	VARIAZIONI RICHIESTE DA ACI INFORMATICA	14
1.8.2	VARIAZIONI RICHIESTE DALL'APPALTATORE	15
1.8.3	MODIFICA SOGGETTIVA DELL'APPALTATORE E DIVIETO DI CESSIONE DEL CONTRATTO	16
1.9	SUBAPPALTO	17
1.9.1	SUBAPPALTO	17
1.9.2	RESPONSABILITÀ DELL'APPALTATORE PER IL SUBAPPALTO	19
1.9.3	PAGAMENTO DEI SUBAPPALTATORI	20
1.10	CODICE ETICO E MODELLO ORGANIZZATIVO. PATTO DI INTEGRITÀ	21
1.11	VARIAZIONI DELLA COMPAGINE SOCIETARIA E/O DEGLI ORGANI SOCIETARI DELL'APPALTATORE	21
1.12	TRATTAMENTO DEI DATI PERSONALI	22
1.12.1	NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI	22
1.12.2	NOMINA A SUB-RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI	22
2	ESECUZIONE DEL SERVIZIO	23
2.1	AVVIO DELL'ESECUZIONE DEL CONTRATTO	23
2.2	OBBLIGHI DELL'APPALTATORE NELL'ESPLETAMENTO DEL SERVIZIO	23
2.3	OBBLIGHI DI ACI INFORMATICA	24
2.4	PROGRAMMA CRONOLOGICO E TERMINI CONTRATTUALI DEL SERVIZIO	25
2.5	SPOSTAMENTO DEI TERMINI CONTRATTUALI DEI SINGOLI SERVIZI	26



2.6	PIANO DI ESECUZIONE DEL SERVIZIO ICT	26
2.7	IMBALLO E TRASPORTO DELLE FORNITURE	27
2.8	RICEVIMENTO DELLE FORNITURE	28
2.8.1	CONSEGNA	28
2.8.2	VERIFICA DI CONFORMITÀ E ACCETTAZIONE DELLA FORNITURA	28
2.8.3	NON CONFORMITÀ – DIFETTI	29
2.8.4	PROVE E TEST PER IL SERVIZIO DI INSTALLAZIONE	29
2.9	VERIFICA DI CONFORMITÀ E PRESA IN CARICO DEL SERVIZIO	30
2.10	SORVEGLIANZA	30
2.11	COMPITI DELLA RAPPRESENTANZA DI ACI INFORMATICA	31
2.12	RAPPRESENTANZA DELL'APPALTATORE	31
2.13	SVOLGIMENTO DELLE ATTIVITÀ	32
2.14	SICUREZZA	32
2.14.1	MISURE PER LA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	32
2.8.5	REGOLE COMPORTAMENTALI PER L'ACCESSO E L'UTILIZZO DEI SISTEMI INFORMATIVI DI ACI INFORMATICA	36
2.8.6	MONITORAGGIO PER LA SICUREZZA E CONSEGUENZE DI UNA VIOLAZIONE DELLE REGOLE	36
2.8.7	ACCETTAZIONE DELLE CLAUSOLE SISTEMI PER LA SICUREZZA DELLE INFORMAZIONI DI ACI INFORMATICA	37
2.15	PERSONALE ADDETTO AL SERVIZIO	37
2.15.1	GENERALITÀ	37
2.15.2	CLAUSOLA SOCIALE	39
2.15.3	TRATTAMENTO ECONOMICO DEL PERSONALE	39
2.15.4	TUTELA DEL PERSONALE E RELATIVE PROVVIDENZE	40
2.15.5	PROVA DEGLI ADEMPIMENTI	40
2.15.6	PERSONALE DEI SUBAPPALTATORI	40
2.15.7	ORARIO DI LAVORO	40
2.16	SOGGEZIONI PARTICOLARI	41
2.17	COORDINAMENTO E SUBORDINAZIONE RISPETTO AD ALTRE ATTIVITÀ DI ACI INFORMATICA	41
2.18	SOSPENSIONE DEL SERVIZIO	41
2.19	ESECUZIONE IN DANNO	43
3	PREZZI CONTRATTUALI	43
3.1	CONDIZIONI AMBIENTALI	44
3.2	REMUNERATIVITÀ DEI PREZZI CONTRATTUALI	44
3.3	REVISIONE PREZZI	45
3.4	NUOVI PREZZI	45
4	ACCETTAZIONE DEL SERVIZIO E CONTABILITÀ DELLE PRESTAZIONI	46
4.1	RESPONSABILITÀ E DANNI	46
4.2	PENALI	47
4.3	MODALITÀ DI FATTURAZIONE E PAGAMENTO. INTERESSI SUI PAGAMENTI	49
4.4	TRACCIABILITÀ DEI FLUSSI FINANZIARI	51
4.5	CAUZIONE	52
4.6	CESSIONE DEI CREDITI	53
4.7	CONTESTAZIONI	54
4.8	IMPOSTE E TASSE	54



4.9	ADEMPIMENTI EX ART. 17-BIS DEL D.LGS. 9 LUGLIO 1997, N. 241	55
5	SCIoglimento DEL CONTRATTO	56
5.1	RISOLUZIONE DEL CONTRATTO	56
5.2	PROCEDIMENTO DI RISOLUZIONE DEL CONTRATTO	56
5.3	RECESSO DAL CONTRATTO	57
5.3.1	RECESSO ORDINARIO	57
5.3.2	RECESSO PER FALLIMENTO DELL'APPALTATORE	58
5.3.3	RECESSO PER ALTRE PROCEDURE CONCORSUALI DELL'APPALTATORE	58
5.3.4	OBBLIGO DI RECESSO	58
6	LEGGE APPLICABILE	59



1 DEFINIZIONI E NORME GENERALI

1.1 Definizioni

Si conviene che le seguenti dizioni ed espressioni menzionate nei documenti contrattuali stiano rispettivamente ad indicare e a definire:

1.1.1 ACI Informatica

ACI Informatica S.p.A. (nel seguito denominata “*ACI Informatica*” o “*Stazione Appaltante*”).

1.1.2 Rappresentanza di ACI Informatica

Per “Rappresentanza di ACI Informatica S.p.A.” si intendono il Responsabile Unico del Progetto di ACI Informatica (nel seguito denominato anche “*RUP*” o “*Responsabile Unico del Progetto*”), il Responsabile della fase di Esecuzione del Contratto di ACI Informatica (di seguito anche “*RE*” o “*Responsabile della fase di Esecuzione del Contratto*”) ed il Direttore dell'Esecuzione del Contratto (di seguito anche DEC), cui competono le funzioni di cui all'art. 2.11.

1.1.3 Appaltatore

Per “Appaltatore” si intende la persona fisica o giuridica o altro soggetto, anche nella forma del Raggruppamento temporaneo tra imprese, o consorzio o altra forma di cui all'articolo 65 del D.Lgs. n. 36/2023 e s.m.i., che, con la firma del Contratto di appalto/Accordo quadro, si impegna ad eseguire il Servizio.

1.1.4 Responsabile del Contratto

Il Responsabile del Contratto è il rappresentante dell'Appaltatore, designato all'atto della accettazione del Contratto/Accordo quadro, cui competono tutte le responsabilità che, a norma delle vigenti disposizioni, derivano dalla conduzione tecnica ed amministrativa del Servizio.

1.1.5 Documenti contrattuali

Il complesso degli atti da cui risulta l'accordo tra i contraenti per l'esecuzione dei servizi appaltati, comprendente, di norma, i seguenti documenti:

- a) Contratto / Accordo Quadro di appalto di servizi: il documento in cui sono precisati l'oggetto del Contratto di appalto e le specifiche clausole che lo disciplinano sul piano economico ed amministrativo.



- b) Offerta economica allegata al contratto, con elenco dei prezzi, i.e. il documento che contiene i prezzi unitari delle componenti oggetto del Servizio, le descrizioni, i codici di posizione e i prezzi delle singole prestazioni.
- c) Offerta tecnica allegata al contratto, con eventuale Programma Cronologico (PC) nel quale sono riportati la data di inizio e il termine finale delle attività, nonché le varie scadenze a cui è soggetto l'Appaltatore nel corso del rapporto contrattuale, per tutta la durata del Contratto.
- d) Capitolato Speciale di Appalto (CSA) di Servizi – Parte Generale: il presente documento contenente le condizioni generali che regolano il Contratto di appalto di servizi o l'Accordo Quadro.
- e) Capitolato Speciale di Appalto (CSA) di Servizi – Parte Tecnica, ovvero Specifiche Tecniche e Capitolati Tecnici Capitolati Tecnici per singolo Accordo Attuativo (in caso di Accordo Quadro), contenenti le caratteristiche tecniche e funzionali, le eventuali norme di costruzione e di accettazione dei servizi forniti.
- f) Polizza fideiussoria: il documento che garantisce ACI Informatica, in qualità di Stazione Appaltante, circa la buona esecuzione del Servizio appaltato.
- g) Polizza assicurativa: il documento che garantisce ACI Informatica, in qualità di Stazione Appaltante, circa il pagamento dei danni - diretti o indiretti - eventualmente da corrispondere nei confronti dei terzi e/o di ACI Informatica stessa, derivanti dall'esecuzione del Servizio.
- h) Eventuale la Dichiarazione dell'Appaltatore, presentata in sede di offerta con cui è stata manifestata l'intenzione di subappaltare nei limiti di cui all'art.119 del D.Lgs. n. 36/2023;
- i) *Eventuale* contratto di avvalimento stipulato tra l'Appaltatore e l'impresa ausiliaria ai sensi dell'art. 104 del D.Lgs. n. 36/2023
- j) *Eventuale, nel caso in cui, ai fini dell'esecuzione delle prestazioni oggetto del Contratto, l'Appaltatore debba effettuare un trattamento di dati personali dei quali ACI Informatica sia Titolare*, Nomina a Responsabile del trattamento dei dati personali;
- k) *Eventuale, nel caso in cui, ai fini dell'esecuzione delle prestazioni oggetto del Contratto, l'Appaltatore debba effettuare un trattamento di dati personali dei quali ACI Informatica sia Responsabile*, Nomina a Sub-Responsabile del trattamento dei dati personali;

1.1.6 DUVRI e PSC

Il DUVRI è il Documento Unico di Valutazione dei Rischi da Interferenze redatto dal RUP ai sensi del D.Lgs n. 81/2008 e s.m.i..

Il PSC è il Piano di Sicurezza e Coordinamento redatto dal RUP ai sensi del D.Lgs. n. 81/2008 e s.m.i..

1.1.7 Servizio



Con il termine “Servizio”, si intende il complesso di attività, articolate ed organizzate, svolte dall’Appaltatore con proprio personale e, in generale, con mezzi e strumenti, il cui scopo può essere, anche contemporaneamente, fornire prodotti materiali (ad esempio documenti) o immateriali (ad esempio supporto ad attività di ACI Informatica), secondo requisiti, caratteristiche e tempistiche specifiche del Contratto.

1.2 Difformità tra documenti contrattuali

Con riferimento ai documenti contrattuali si precisa che, in caso di difformità o incompatibilità tra le pattuizioni del Contratto e i termini e/o le condizioni di alcuno dei documenti allegati e/o richiamati, prevarranno le pattuizioni presenti nel Contratto. In caso di difformità o incompatibilità tra taluni dei documenti contrattuali menzionati nell’art. 1.1.5, la prevalenza è determinata dall’ordine secondo il quale i documenti stessi vi si trovano elencati.

1.3 Osservanza di leggi, regolamenti e norme

L’Appaltatore, sotto la sua esclusiva responsabilità, deve ottemperare alle disposizioni legislative come pure osservare tutti i regolamenti, le norme, le prescrizioni delle competenti Autorità in materia di servizi, di contratti di lavoro, di sicurezza ed igiene del lavoro e di quanto altro possa comunque interessare l’appalto di servizi.

A nessun effetto saranno considerati come dipendenti di ACI Informatica coloro della cui opera si avvarrà l’Appaltatore ai fini dell’espletamento del Servizio ad esso affidato, intendendosi ACI Informatica del tutto estranea rispetto ad ogni e qualsiasi rapporto intercorrente fra l’Appaltatore medesimo e le persone anzidette.

Il Contratto / Accordo quadro deve essere espletato nel completo rispetto di tutte le disposizioni vigenti in materia di prevenzione della delinquenza di tipo mafioso.

In particolare, nei confronti del rappresentante legale, dei componenti dell’organo di amministrazione dell’Appaltatore, dei membri del Collegio Sindacale o, nei casi contemplati dall’art. 2477 del Codice Civile, del Sindaco, nonché nei confronti dei soggetti che svolgono compiti di vigilanza, non dovranno essere stati emessi provvedimenti definitivi o provvisori che dispongano misure di prevenzione o divieti, sospensioni o decadenze di cui alla predetta normativa, né dovranno essere pendenti procedimenti per l’applicazione delle medesime disposizioni, ovvero pronunciate condanne che comportino l’incapacità di contrattare con la Pubblica Amministrazione.

Per tutta la durata del Contratto / Accordo quadro, inoltre, l’Appaltatore deve garantire il permanere dei requisiti di idoneità/qualificazione richiesti in sede di affidamento del Contratto.

Il mancato rispetto, da parte dell’Appaltatore, dei requisiti e delle obbligazioni poste a carico dello stesso ai sensi del presente articolo, legittima ACI Informatica alla risoluzione del Contratto / Accordo quadro ai sensi e per gli effetti dell’art. 1456 codice civile.



1.4 Assicurazioni

Prima di dare inizio a qualsiasi attività inerente il Contratto, l'Appaltatore è tenuto, senza che per questo siano comunque limitate le sue responsabilità contrattuali, a costituire una polizza assicurativa di importo non inferiore al corrispettivo complessivo del Contratto stesso, rilasciata da imprese bancarie o assicurative che rispondano ai requisiti di solvibilità previsti dalle leggi che ne disciplinano le rispettive attività o rilasciata dagli intermediari finanziari iscritti nell'albo di cui all'art. 106 del D.Lgs. n. 385/1993, che svolgano, in via esclusiva o prevalente, attività di rilascio di garanzie e che siano sottoposti a revisione contabile da parte di una società di revisione iscritta nel Registro dei Revisori Legali presso il Ministero dell'Economia e delle Finanze e che abbiano i requisiti minimi di solvibilità richiesti dalla vigente normativa bancaria assicurativa, a copertura di ogni tipologia di danno derivante, direttamente o indirettamente, dall'espletamento delle proprie attività.

Inoltre, qualora le prestazioni oggetto del Contratto / Accordo quadro vengano svolte presso sedi ACI Informatica, l'Appaltatore deve dimostrare il possesso di una polizza assicurativa a copertura degli infortuni professionali, attraverso apposita dichiarazione rilasciata su carta intestata dalla compagnia stessa.

A tal fine, l'Appaltatore si impegna a produrre l'originale dell'appendice di dichiarazione della polizza assicurativa dove sia riportata esplicita attestazione dell'avvenuto pagamento dei premi assicurativi, la rinuncia al diritto di rivalsa da parte della stessa Compagnia di assicurazione/Istituto di credito nei confronti di ACI Informatica e dei terzi coinvolti a diverso titolo nell'esecuzione delle attività.

Resta comunque inteso che qualora l'Appaltatore non costituisca una garanzia in conformità alle disposizioni di cui sopra, sarà sua cura e onere provvedere quanto prima a stipularla. In mancanza, sarà facoltà di ACI Informatica risolvere il Contratto ai sensi e per gli effetti dell'art. 1456 del codice civile.

Resta inteso che la mancata costituzione delle suddette garanzie prima del termine fissato per la stipula del Contratto comporterà, in ogni caso, la decadenza dell'affidamento e l'acquisizione della cauzione provvisoria eventualmente presentata in sede di offerta da parte della Stazione Appaltante, con conseguente scorrimento della graduatoria.

Ogni indennizzo a terzi a titolo di risarcimento deve essere liquidato senza deduzione di alcuna franchigia che si intende a totale carico dell'Appaltatore.

Durante l'esecuzione dell'appalto e allo scadere del termine di validità del contratto di assicurazione, sarà cura dell'Appaltatore inviare alla Rappresentanza di ACI Informatica la prova del rinnovo dello stesso, mediante dichiarazione emessa dalla Compagnia di assicurazione/Istituto di credito, pena, in difetto, la risoluzione del Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

Resta inteso che lo stesso Appaltatore dovrà comunicare alla suddetta Rappresentanza di ACI Informatica, con congruo anticipo, ogni evento che modifichi i termini e/o le condizioni afferenti la polizza assicurativa, nel rispetto delle previsioni di cui al presente artico-



lo, mediante l'emissione di una nuova appendice di dichiarazione della polizza assicurativa stessa.

1.5 Pretese di terzi e clausola di manleva

L'Appaltatore tiene indenne ACI Informatica da ogni responsabilità per danni a persone, luoghi ed a cose, sia per quanto riguarda i propri dipendenti, ausiliari, collaboratori e/o subappaltatori e contraenti ed eventuali materiali o strumenti di sua proprietà, sia per quanto riguarda i danni che esso dovesse arrecare a terzi in conseguenza dell'esecuzione dell'appalto e delle attività connesse e, in ogni caso, per qualunque altro rischio di esecuzione da qualsiasi causa determinato. L'Appaltatore assume altresì la responsabilità per i danni subiti da ACI Informatica a causa del danneggiamento o della distruzione totale o parziale di impianti ed opere, anche preesistenti, verificatisi nel corso dell'esecuzione dell'appalto.

1.6 Uso di licenze, proprietà industriale, commerciale, brevetti, software e copyright

1.6.1 Uso di licenze

Qualora il Servizio sia espletato sulla base di una licenza, l'Appaltatore si impegna a comunicare alla Rappresentanza di ACI Informatica, per iscritto, le modalità del relativo utilizzo e ad utilizzarla secondo modalità tali da consentire l'esecuzione del Servizio in forma equivalente a quella che eventualmente potrebbe essere messa in atto dalla Licenziante.

L'Appaltatore, a sue spese, è altresì obbligato ad ottenere le eventuali concessioni, licenze ed autorizzazioni necessarie all'esecuzione del Contratto e a darne prova alla Rappresentanza di ACI Informatica.

L'Appaltatore garantisce in ogni tempo ACI Informatica, in nome proprio e dei propri Subappaltatori, e si impegna a tenere quest'ultima manlevata ed indenne, contro ogni rivendicazione e/o pretesa da parte di titolari o concessionari di brevetti, licenze, disegni, modelli, marchi di fabbrica ed altro, adottati per l'espletamento del Servizio nonché i materiali, i procedimenti ed i mezzi utilizzati nell'esecuzione del Contratto.

L'Appaltatore si impegna altresì ad intervenire in ogni eventuale giudizio che venisse promosso nei confronti di ACI Informatica, salvo sempre il diritto di quest'ultima ad essere indennizzata dall'Appaltatore dei danni e delle spese che fosse stata costretta per tali motivi a sostenere.

1.6.2 Proprietà industriale e commerciale



L'Appaltatore dichiara e garantisce che quanto offerto in sede di partecipazione alla procedura di selezione e realizzato in esecuzione del Contratto / Accordo quadro è originale e non viola, in tutto o in parte, diritti di terzi, ed all'uopo sin d'ora assume in proprio tutti gli oneri e le spese derivanti dalla eventuale violazione dei suddetti diritti di terzi, manlevando e tenendo indenne ACI Informatica da ogni conseguente responsabilità e da ogni e qualsiasi onere e spesa, anche legale.

Gli eventuali elaborati forniti dall'Appaltatore e/o i documenti forniti in esecuzione del Contratto e non coperti da brevetto o altro titolo di privativa intellettuale registrato si intendono trasferiti in proprietà a ACI Informatica, la quale potrà utilizzarli e disporne per qualsiasi scopo, senza che l'Appaltatore possa pretendere alcun compenso, a qualsivoglia titolo e, in particolare, rivendicare diritti di autore, proprietà industriale ed artistica, etc.

Tutti gli elaborati e la documentazione di progetto relativi al Servizio, non potranno essere né riprodotti né riutilizzati dall'Appaltatore, in tutto o in parte, per altre commesse anche se con caratteristiche analoghe, senza specifica autorizzazione scritta di ACI Informatica.

In ragione delle dichiarazioni e garanzie rese, l'Appaltatore si impegna a manlevare e tenere indenne la Stazione Appaltante, da ogni e qualsivoglia pretesa, diritto o azione che terzi dichiarino di vantare su quanto realizzato in esecuzione del Contratto / Accordo quadro e, a tal fine 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.

Qualora venga promossa nei confronti della Stazione Appaltante azione giudiziaria da parte di terzi che vantino diritti su beni acquistati o in licenza d'uso, l'Appaltatore si impegna a manlevare e tenere indenne la Stazione Appaltante, assumendo a proprio carico tutti gli oneri conseguenti, inclusi i danni verso terzi e le spese giudiziali e legali a carico di ACI Informatica.

La Stazione Appaltante si obbliga ad informare prontamente per scritto l'Appaltatore delle iniziative giudiziarie di cui al precedente comma; in caso di difesa congiunta, la Stazione Appaltante riconosce all'Appaltatore la facoltà di nominare un proprio legale di fiducia da affiancare al difensore scelto dalla Stazione Appaltante.

Nell'ipotesi di azione giudiziaria di cui al precedente comma, la Stazione Appaltante, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare la risoluzione di diritto del Contratto / Accordo Quadro, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per l'avvenuto uso.

ACI Informatica si riserva, in ogni caso, il diritto, in pendenza delle azioni di cui sopra, di richiedere all'Appaltatore di realizzare a propria cura e spese un prodotto che abbia caratteristiche analoghe a quello fornito o di acquisire, sempre a propria cura e spese, il consenso alla continuazione dell'uso delle apparecchiature e dei programmi, il cui diritto di esclusiva è giudizialmente contestato.



L'Appaltatore si impegna a rispettare i diritti di proprietà intellettuale e industriale in capo ad ACI Informatica. Tali diritti restano di esclusiva titolarità della stessa ACI Informatica. L'Appaltatore si impegna, pertanto, a non fare – direttamente o per interposta persona – alcun uso delle competenze di ACI Informatica non espressamente autorizzato, o che possa – anche indirettamente - recare danno o pregiudizio ad ACI Informatica, o per finalità estranee all'attuazione ed esecuzione del Contratto, o secondo modalità diverse da quelle previste dal Contratto stesso.

In caso di inadempimento da parte dell'Appaltatore a quanto stabilito nei precedenti commi, fermo restando il diritto al risarcimento del danno, la Stazione Appaltante avrà facoltà di dichiarare risolto il Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

1.6.3 Proprietà, copyright, software

Con l'accettazione del Contratto / Accordo quadro, l'Appaltatore riconosce ed accetta che i prodotti software e/o informatici in genere ed altri elaborati analoghi, prodotti dall'Appaltatore e/o dai suoi ausiliari per ACI Informatica in esecuzione del Contratto/ Accordo quadro e gli eventuali sviluppi degli stessi sono di esclusiva proprietà di ACI Informatica, senza bisogno di ulteriori formalità, e che quest'ultima ne potrà disporre liberamente e senza alcun vincolo fermo restando il diritto dell'Appaltatore ad esserne riconosciuto autore.

Il diritto di proprietà di ACI Informatica sui prodotti software e/o informatici in genere si intende esteso ai relativi manuali operativi, alle specifiche funzionali e a qualunque documento o informazione, su qualunque supporto riportati, predisposti e consegnati dall'Appaltatore a ACI Informatica nell'ambito dell'esecuzione del Servizio.

E' fatto quindi divieto all'Appaltatore di utilizzare, concedere l'uso a terzi, vendere o concedere in licenza, a titolo oneroso o gratuito, quanto realizzato in esecuzione del Contratto /Accordo quadro.

In particolare, al di fuori dell'utilizzo dei summenzionati prodotti software e/o informatici in genere nell'ambito dell'esecuzione del Servizio, l'Appaltatore si impegna a non utilizzare né a disporre, in qualsiasi modo e a qualsiasi titolo, dei prodotti software, degli eventuali sviluppi e dei relativi supporti, quali che essi siano, senza il preventivo consenso scritto di ACI Informatica. Gli stessi non potranno quindi essere commercializzati né utilizzati da parte di Terzi senza il previo consenso scritto di ACI Informatica, alla quale spetterebbero in tal caso le relative royalties, il cui importo dovrebbe essere determinato d'accordo con ACI Informatica stessa.

In ogni caso l'Appaltatore, laddove venisse a conoscenza di eventuali violazioni da parte di Terzi dei diritti di ACI Informatica sui prodotti software e/o informatici in genere, si impegna a darne tempestiva comunicazione a ACI Informatica stessa e a collaborare con quest'ultima a tutela dei suoi diritti.



Nel caso in cui, ai fini dell'esecuzione del Servizio, l'Appaltatore utilizzi prodotti software allo stesso ceduti o concessi in sublicenza d'uso da parte di Terzi, l'Appaltatore garantisce che gli stessi siano stati a loro volta ricevuti dall'Appaltatore con espressa autorizzazione del titolare alla cessione ovvero alla sublicenza, senza che ciò comporti oneri aggiuntivi per ACI Informatica e si impegna a fornire adeguata informativa a quest'ultima in merito alle garanzie previste nei relativi contratti.

L'Appaltatore si impegna in ogni caso a tenere ACI Informatica manlevata e indenne rispetto a qualsiasi pretesa e/o azione che dovesse essere avanzata da terzi in relazione ai prodotti software e/o informatici in genere oggetto del Contratto/Accordo quadro. A tal fine ACI Informatica comunicherà per iscritto all'Appaltatore ogni eventuale azione promossa o pretesa avanzata nei confronti della stessa ACI Informatica.

Ferma restando la paternità dell'opera in capo all'Appaltatore, la Stazione Appaltante acquisisce – interamente, gratuitamente, incondizionatamente e definitivamente - il diritto di proprietà e di utilizzazione e sfruttamento economico di tutto quanto realizzato dall'Appaltatore in esecuzione del Contratto /Accordo quadro (a titolo meramente esemplificativo ed affatto esaustivo, trattasi dei prodotti software e dei Sistemi sviluppati, degli elaborati, delle procedure software e più in generale di creazioni intellettuali ed opere dell'ingegno), dei relativi materiali e della documentazione creati, inventati, predisposti o realizzati dall'Appaltatore o dai suoi dipendenti nell'ambito o in occasione dell'esecuzione del Contratto/ Accordo Quadro.

La Stazione Appaltante potrà, pertanto, utilizzare quanto realizzato in esecuzione del Contratto / Accordo quadro non solo per le finalità specificate nel Bando di Gara, nel Contratto / Accordo quadro e nel presente Capitolato o nelle Specifiche Tecniche, ma anche e senza alcuna limitazione, per finalità diverse, ivi incluso il diritto di concederne il diritto a terzi, a titolo gratuito o oneroso, il diritto di modifica e integrazione anche con altri prodotti e sistemi, senza alcuna limitazione temporale e/o territoriale, a prescindere dalla durata del Contratto /Accordo quadro che inerisce i termini entro i quali il Contraente deve adempiere alle proprie obbligazioni, ma in nessun modo incide sul diritto di utilizzo di quanto realizzato da parte della Stazione Appaltante.

I menzionati diritti devono, pertanto, intendersi acquisiti dalla Stazione Appaltante in modo perpetuo, illimitato ed irrevocabile.

L'Appaltatore si obbliga espressamente a fornire alla Stazione Appaltante tutti i codici sorgenti del software sviluppato in esecuzione del Contratto /Accordo quadro, indicando esplicitamente quali software di proprietà di Terzi sono stati eventualmente utilizzati. Tale consegna, che dovrà avvenire in occasione di tutte le emissioni di nuove versioni del software e, comunque, a seguito di esplicita richiesta della Stazione Appaltante, dovrà essere corredata dalla documentazione atta a rendere agevole la verifica e la gestione della configurazione e dovrà essere completata con una lettera nella quale il Contraente dichiara di aver consegnato tutti i codici sorgenti del software sviluppato alla data.



L'Appaltatore si obbliga espressamente a fornire alla Stazione Appaltante tutta la documentazione ed il materiale necessario all'effettivo sfruttamento di detti diritti di titolarità esclusiva, nonché a sottoscrivere tutti i documenti necessari all'eventuale trascrizione di detti diritti a favore della Stazione Appaltante in eventuali registri od elenchi pubblici.

Tutti i report e, comunque, tutta la documentazione di rendicontazione e di monitoraggio del Contratto /Accordo Quadro, anche fornita e/o predisposta e/o realizzata dall'Appaltatore in esecuzione degli adempimenti contrattuali, tutti i dati e le informazioni ivi contenute, nonché la documentazione di qualsiasi tipo derivata dall'esecuzione del Contratto / Accordo Quadro, sono e rimarranno di titolarità esclusiva della Stazione Appaltante che potrà, quindi, disporre senza alcuna limitazione.

In caso di inadempimento da parte dell'Appaltatore a quanto stabilito nei precedenti commi, fermo restando il diritto al risarcimento del danno, la Stazione Appaltante avrà facoltà di dichiarare risolto il Contratto / Accordo quadro ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

1.6.4 Brevetti

Qualora, nel corso dell'esecuzione del Servizio, l'Appaltatore sviluppi programmi e/o progetti che possano essere considerati invenzioni brevettabili, ACI Informatica potrà richiedere all'Appaltatore, in alternativa:

- i. che l'Appaltatore stesso prontamente richieda, a propria cura e spesa, il rilascio di un brevetto e trasferisca ad ACI Informatica, a titolo gratuito ed in via esclusiva, il diritto di utilizzo dello stesso;
- ii. che l'Appaltatore ceda a ACI Informatica, a titolo gratuito, ogni e qualsiasi documentazione e informazione necessaria affinché ACI Informatica possa ottenere il relativo brevetto;
- iii. che l'Appaltatore ottenga, in nome e per conto di ACI Informatica e a spese della stessa, il relativo brevetto.

1.7 Dovere di riservatezza

L'Appaltatore è tenuto a mantenere la più assoluta riservatezza per quanto concerne tutti i documenti di qualsiasi tipo (tecnico, amministrativo, gestionale, di presentazione, report, etc), forma di rappresentazione (testo, grafica, audio, multimediale) e supporto (cartaceo, digitale) connessi all'appalto e/o prodotti in esecuzione dello stesso e ad astenersi, salvo esplicito benestare di ACI Informatica, dal pubblicare o comunque diffondere fotografie ed articoli su quanto fosse venuto a sua conoscenza in relazione all'espletamento dell'appalto medesimo. Egli deve inoltre astenersi dall'effettuare fotografie e/o filmati delle opere eseguite da terzi per conto di ACI Informatica, salvo esplicito benestare di ACI Informatica stessa.



Tutte le notizie relative alle attività comunicate da ACI Informatica o, comunque, apprese dall'Appaltatore e dal suo personale durante l'esecuzione del Contratto e/o in forza di esso e tutte le informazioni che transiteranno per i sistemi di elaborazione dei dati non debbono essere in alcun modo ed in qualsiasi forma comunicate o divulgate a terzi, né debbono essere utilizzate sia da parte dell'Appaltatore sia da parte di chiunque altro collabori al suo lavoro per fini diversi da quelli contemplati dall'appalto.

L'Appaltatore si impegna a diffidare tutti i propri dipendenti e chiunque collabori all'esecuzione delle prestazioni, alla più rigorosa osservanza del segreto d'ufficio in conformità alle vigenti norme, richiamando l'attenzione dei propri dipendenti su quanto disposto dall'art. 326 del codice penale, così come modificato dalla legge 26.4.1990 n.86, che punisce la violazione, l'uso illegittimo e lo sfruttamento delle notizie riservate.

La violazione dell'obbligo di cui al presente articolo legittima ACI Informatica alla risoluzione del Contratto di appalto/Accordo quadro ai sensi e per gli effetti dell'art. 1456 codice civile.

1.8 Variazioni

1.8.1 Variazioni richieste da ACI Informatica

Il Contratto d'appalto può essere modificato, senza necessità di una nuova procedura di affidamento, nei casi previsti dall'art. 120 del D.Lgs. n. 36/2023.

Con l'accettazione del Contratto, l'Appaltatore s'impegna ad eseguire tutte le aggiunte e/o variazioni, anche in diminuzione, fino a concorrenza del quinto dell'importo del Contratto che verranno eventualmente richieste da ACI Informatica in corso d'esecuzione, agli stessi prezzi, patti e condizioni previsti nel Contratto medesimo, senza possibilità di far valere il diritto alla risoluzione e senza diritto ad alcuna indennità ad eccezione del corrispettivo relativo alle nuove prestazioni.

Ai fini della determinazione del quinto, l'importo dell'appalto è formato dalla somma risultante dal Contratto, aumentato dell'importo degli atti aggiuntivi per varianti già intervenute, nonché dell'ammontare degli importi diversi da quelli a titolo risarcitorio, eventualmente riconosciuti all'Appaltatore in sede di Accordo bonario ex art. 206 e/o transazione ex art. 212 del D.Lgs. n. 36/2023.

Qualora dette modifiche comportino aumenti o diminuzioni di costo e/o modifiche nelle caratteristiche del Servizio eccedenti il quinto dell'importo contrattuale, le eventuali differenze di prezzo e le relative modalità di pagamento, i nuovi termini contrattuali, le nuove caratteristiche e le eventuali nuove garanzie dovranno essere concordate tra le Parti e formalizzate tramite appositi atti aggiuntivi al Contratto. A tal fine, ACI Informatica procede alla redazione di un atto aggiuntivo al Contratto, che il RUP, tramite la Direzione Approvvigionamenti e Logistica, provvederà a comunicare all'Appaltatore.



Entro il termine di 15 giorni dal ricevimento dello schema di atto aggiuntivo, l'Appaltatore deve dichiarare, per iscritto, se intende accettare la prosecuzione del Contratto e a quali condizioni. Nel termine di 15 giorni dal ricevimento di tale comunicazione, ACI Informatica comunica all'Appaltatore le proprie determinazioni.

Qualora l'Appaltatore non risponda alla comunicazione di ACI Informatica, si intende manifestata la volontà di accettare la modifica agli stessi prezzi, patti e condizioni del Contratto originario.

Indipendentemente dalle ipotesi previste dall'art. 120 del D.Lgs. n. 36/2023, la Rappresentanza di ACI Informatica può ordinare l'esecuzione di prestazioni in misura inferiore rispetto a quanto previsto nel Contratto, entro il limite del - 20% dell'importo contrattuale, come determinato ai sensi del comma 4 dello stesso art. 120 del D.Lgs. n. 36/2023, dandone comunicazione all'Appaltatore prima del raggiungimento del quarto quinto dell'importo contrattuale, senza che nulla spetti all'Appaltatore a titolo di indennizzo.

Resta inteso che in caso di contratto a consumo, se nel contratto è prevista una % dell'importo contrattuale minima garantita l'eventuale conclusione del contratto al raggiungimento di tale % minima non potrà in ogni caso giustificare alcuna richiesta di indennizzo da parte dell'Appaltatore.

In ogni caso, è obbligo dell'Appaltatore eseguire tutte le modifiche di dettaglio disposte dalla Rappresentanza di ACI Informatica che non comportano aumento o diminuzione dell'importo contrattuale nonché tutte quelle variazioni di carattere non sostanziale ritenute opportune dalla Stazione Appaltante e ordinate dalla Rappresentanza di ACI Informatica che non mutino sostanzialmente la natura delle attività oggetto del Contratto / Accordo quadro e non comportino a carico dell'Appaltatore maggiori oneri.

Nessun compenso sarà in ogni caso dovuto da ACI Informatica all'Appaltatore per le varianti al progetto originario che si rendessero eventualmente necessarie per rispondere alle prescrizioni tecniche originariamente richieste dalla stessa ACI Informatica nel Capitolato Speciale di Appalto (CSA) di Servizi – Parte Tecnica, indipendentemente dai costi, anche maggiori, che l'Appaltatore dovesse eventualmente sostenere.

1.8.2 Variazioni richieste dall'Appaltatore

L'Appaltatore non può, senza preventiva autorizzazione scritta di ACI Informatica, apportare alcuna variazione, di qualsiasi natura o entità, al Contratto / Accordo quadro, sia con riguardo alle prescrizioni tecniche e/o contrattuali sia con riguardo ai documenti approvati da ACI Informatica in relazione al Servizio. Le variazioni non previamente autorizzate da ACI Informatica non danno titolo a pagamenti o rimborsi di sorta e comportano comunque l'obbligo di eseguire la prestazione secondo quanto previsto dalle prescrizioni tecniche e/o contrattuali e di rimettere in pristino la situazione originaria preesistente, con spese a carico dell'Appaltatore.

Eventuali variazioni al Servizio conseguenti all'applicazione di norme di legge e/o regolamentari intervenute successivamente alla data del Contratto, dovranno in ogni caso essere autorizzate da ACI Informatica e alle stesse si applicheranno le disposizioni di cui al precedente articolo 1.8.1.

Qualora l'Appaltatore individuasse modifiche e/o soluzioni realizzative diverse da quelle previamente stabilite, utilizzando altre tipologie di componenti ovvero modalità realizzative alternative, dovrà produrre una nuova documentazione da sottoporre all'approvazione di ACI Informatica che quindi potrà decidere di autorizzare o non autorizzare. Nel caso in cui ACI Informatica autorizzi quanto proposto dall'Appaltatore ACI Informatica potrà stabilire o richiedere nuove prove, verifiche e/o controlli da eseguire a completa cura e spesa dell'Appaltatore.

1.8.3 Modifica soggettiva dell'Appaltatore e divieto di cessione del Contratto

In conformità a quanto previsto dall'articolo 120, co. 1, lett. d), del D.Lgs. n. 36/2023, al contraente originario può subentrare un nuovo contraente senza la necessità di una nuova procedura di affidamento al ricorrere delle seguenti circostanze:

- 1) se le modifiche soggettive implicanti la sostituzione del contraente originario sono previste in clausole chiare, precise e inequivocabili dei documenti di gara;
- 2) se all'aggiudicatario succede, per causa di morte o insolvenza o a seguito di ristrutturazioni societarie, che comportino successione nei rapporti pendenti, un altro operatore economico che soddisfi gli iniziali criteri di selezione, purché ciò non implichi ulteriori modifiche sostanziali al contratto e non sia finalizzato ad eludere l'applicazione del codice, fatto salvo quanto previsto dall'articolo 124;
- 3) nel caso in cui la stazione appaltante assume gli obblighi del contraente principale nei confronti dei suoi subappaltatori ,

In tutti i casi di cui al precedente punto 2 le modifiche soggettive dell'Appaltatore dovranno essere notificate con formale comunicazione ad ACI Informatica da parte dell'Appaltatore stesso unitamente a tutta la documentazione necessaria a comprovare la variazione soggettiva occorsa, di cui ACI Informatica, previa verifica della regolarità formale, prenderà eventualmente atto con proprio provvedimento.

Entro il termine di 60 giorni dalla comunicazione dell'Appaltatore, ACI Informatica, previa valutazione della trasformazione societaria sulla base della documentazione elencata, notificherà la propria opposizione al subentro di altro soggetto nella titolarità del Contratto con conseguente provvedimento di recesso o risoluzione dello stesso o, al contrario, accettazione della nuova situazione soggettiva. In quest'ultimo caso ACI Informatica procederà a prenderne atto mediante proprio provvedimento.

Salvo quanto previsto nel presente articolo in merito alla modifica soggettiva del Contratto ai sensi dell'articolo 120, co. 1, lett. d), punto 2) del D.Lgs. n. 36/2023, è vietata la cessione del Contratto sotto qualsiasi forma. Ogni atto contrario è nullo di diritto.



In caso di inadempimento da parte dell'Appaltatore a quanto stabilito nei precedenti commi, fermo restando il diritto al risarcimento del danno, la Stazione Appaltante avrà facoltà di dichiarare risolto il Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

1.9 Subappalto

1.9.1 Subappalto

Il subappalto non è consentito per quelle prestazioni che ACI Informatica, nella documentazione di gara, motivandone le ragioni, abbia previsto a carico esclusivo dell'Appaltatore.

Al di fuori delle ipotesi di cui sopra, qualora l'Appaltatore intenda affidare in subappalto, alle condizioni previste dall'art. 119 del D.Lgs. n. 36/2023 e s.m.i., l'esecuzione di alcune attività facenti parte delle prestazioni contrattualmente previste e si sia riservato, in tal senso, in sede di offerta, questi deve depositare presso ACI Informatica, da intendersi quale istanza formale di subappalto, il contratto di subappalto (originale o copia autenticata), corredato dalla documentazione di cui al medesimo articolo 119, commi 5 e 16 del D.Lgs. n. 36/2023, in coerenza con quanto già dichiarato in sede di offerta e successivamente recepito nel Contratto di appalto. Ai sensi e per gli effetti del comma 17 dell'art. 119 del D.Lgs. 36/2023, è vietato il subappalto a cascata in ragione delle specifiche motivazioni qualora indicate dalla stazione appaltante nella documentazione di gara.

Al momento del deposito del contratto, l'Appaltatore dovrà inoltre presentare la certificazione attestante l'eventuale possesso, da parte del subappaltatore, dei requisiti di micro, piccola o media impresa di cui all'Allegato I.1 art. 1, comma 1, lettera 0) del D.Lgs. n. 36/2023.

Il deposito del contratto deve aver luogo almeno 20 (venti) giorni prima della data dell'inizio dell'esecuzione delle attività oggetto del contratto di subappalto.

Per l'autorizzazione del subappalto, è necessario che l'affidatario del subappalto (i) sia idoneamente qualificato per eseguire la prestazione; (ii) in sede di offerta siano indicati i servizi/forniture o le parti di servizi/forniture che si intendono affidare in subappalto; (iii) il subappaltatore dimostri l'assenza a suo carico delle cause di esclusione ex art. 94, 95 e 98 D.Lgs. 36/2023 e s.m.i. e il possesso dei requisiti speciali di cui all'articolo 100 D.Lgs. 36/2023 e s.m.i..

L'Appaltatore è tenuto ad inserire, nei contratti sottoscritti con i propri subappaltatori e subcontraenti della filiera delle imprese a qualsiasi titolo interessate all'appalto, a pena di nullità assoluta, apposita clausola con cui ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge n.136/2010.



ACI Informatica provvederà alla verifica che nei contratti di subappalto e/o subcontratti sia inserita, a pena di nullità, la clausola con la quale ciascuno dei subappaltatori e/o subcontraenti assume gli obblighi di tracciabilità dei flussi finanziari, ai sensi e per gli effetti dell'articolo 3 della Legge 136/2010. A tal fine, sarà cura dell'Appaltatore inviare alla Rappresentanza di ACI Informatica, copia conforme all'originale del contratto di subappalto e/o subcontratto.

Si applicano all'Appaltatore, ai subappaltatori, ai cottimisti ed ai sub contraenti le verifiche previste dalla vigente normativa antimafia e, in particolare, dal D.Lgs. n. 159/2011 e s.m.i., e nella Legge n. 136/2010 e s.m.i. nonché le prescrizioni contenute nel presente Capitolato.

Resta fermo che, ai sensi dell'art. 95, comma 3 del citato D.Lgs. n. 159/2011, l'affidamento in subappalto o in cottimo nonché l'attivazione di sub-contratti restano vietati, a prescindere dall'importo dei servizi, qualora per l'impresa subappaltatrice/subcontraente/cottimista sia accertata una delle situazioni indicate dall'art. 91 comma 6 dello stesso D.Lgs. n. 159/2011.

ACI Informatica si riserva di dare, entro 30 (trenta) giorni dalla data di deposito del contratto di subappalto, termine dimezzato in caso di subappalti di importo inferiore al 2% dell'importo delle prestazioni affidate o di importo inferiore a € 100.000, la propria eventuale autorizzazione espressa, che deve essere esibita alla Rappresentanza di ACI Informatica, al fine di consentire l'accesso al subappaltatore ai siti ACI Informatica, per lo svolgimento del Servizio. ACI Informatica si riserva la facoltà di prorogare tale termine, per una sola volta, ove ricorrano giustificati motivi.

ACI Informatica tuttavia ha sempre la facoltà di rimuovere l'autorizzazione qualora accerti, in qualsiasi momento, l'esistenza di cause ostative al subappalto ai sensi della normativa vigente in materia.

Nel caso in cui l'Appaltatore affidi anche solo parte delle attività in subappalto senza la preventiva autorizzazione, espressa o tacita, oppure nel caso in cui il subappaltatore autorizzato subappalti, a sua volta, le prestazioni affidate, ACI Informatica può avvalersi della facoltà di risoluzione del Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile, costituendo tale fattispecie grave inadempimento agli obblighi contrattuali dell'Appaltatore.

Con riferimento ai servizi attinenti all'architettura e all'ingegneria, ferma restando la responsabilità del progettista, è fatto divieto all'Appaltatore di avvalersi del subappalto, fatta eccezione per le attività relative alle indagini geologiche, geotecniche e sismiche, a sondaggi, a rilievi, a misurazioni e picchettazioni, alla predisposizione di elaborati specialistici e di dettaglio, con l'esclusione delle relazioni geologiche, nonché per la sola redazione grafica degli elaborati progettuali.

Per tutto quanto non previsto dal presente capitolato si applicano le disposizioni di cui all'art. 119 del D.Lgs. 36/2023 e s.m.i..



1.9.2 Responsabilità dell'Appaltatore per il subappalto

L'autorizzazione espressa al subappalto da parte di ACI Informatica non apporta nessuna modifica agli obblighi e agli oneri contrattuali dell'Appaltatore il quale diventa responsabile in solido con il subappaltatore nei confronti di ACI Informatica in relazione alle prestazioni oggetto del contratto di subappalto.

L'Appaltatore è tenuto ad osservare integralmente il 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. E', altresì, responsabile in solido in merito all'osservanza delle norme anzidette, con particolare riferimento agli obblighi retributivi e contributivi dei subappaltatori nei confronti dei loro dipendenti per le prestazioni rese nell'ambito del subappalto.

ACI Informatica acquisisce d'ufficio il DURC in corso di validità relativo all'Appaltatore e a tutti i subappaltatori, ai fini del pagamento delle prestazioni rese nell'ambito dell'appalto o del subappalto.

Ai sensi dell'art. 11, commi 5 e 6 del D.Lgs. n. 36/2023, in caso di ritardo nel pagamento delle retribuzioni dovute al personale dipendente dell'Appaltatore o del subappaltatore o dei soggetti titolari di subappalti e cottimi, impiegato nell'esecuzione del Contratto, il RUP invita per iscritto il soggetto inadempiente, ed in ogni caso l'Appaltatore, a provvedervi entro i successivi 15 giorni. Ove non sia stata contestata formalmente e motivatamente la fondatezza della richiesta entro detto termine, ACI Informatica provvederà al pagamento diretto, anche in corso d'opera, ai lavoratori delle retribuzioni arretrate, detraendo il relativo importo dalle somme dovute all'Appaltatore ovvero dalle somme dovute al subappaltatore inadempiente nel caso in cui sia previsto il pagamento diretto ai sensi dell'art. 1.9.3 del presente Capitolato.

Ai sensi dell'art. 11, commi 5 e 6 del D.Lgs. n. 36/2023, in caso di inadempienza contributiva risultante dal DURC relativo a personale dipendente dell'affidatario o del subappaltatore o dei soggetti titolari di subappalti e cottimi, impiegato nell'esecuzione del Contratto, ACI Informatica provvederà a trattenere dal certificato di pagamento l'importo corrispondente all'inadempienza per il successivo versamento diretto agli enti previdenziali e assicurativi, compresa, nei lavori, la cassa edile. Sull'importo netto progressivo delle prestazioni sarà operata una ritenuta dello 0,50 %. Tali ritenute potranno essere svincolate soltanto in sede di liquidazione finale, dopo l'approvazione da parte di ACI Informatica del certificato di verifica di conformità, previo rilascio del DURC.

Il subappaltatore, per le prestazioni affidate in subappalto, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconosce 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, ovvero un differente contratto collettivo, purché garantisca ai dipen-



denti le stesse tutele economiche e normative di quello applicato dall'appaltatore, 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.

L'Appaltatore deve corrispondere i costi della sicurezza e della manodopera, relativi alle prestazioni affidate in subappalto, alle imprese subappaltatrici senza alcun ribasso ed è solidalmente responsabile con il subappaltatore degli adempimenti, da parte di quest'ultimo, degli obblighi di sicurezza previsti dalla normativa vigente. ACI Informatica, tramite il Responsabile della fase di Esecuzione del contratto, provvede alla verifica dell'effettiva applicazione della presente disposizione.

Qualora, durante l'esecuzione delle attività ed in qualsiasi momento, ACI Informatica accerti che l'Appaltatore risulti inadempiente con riferimento alle attività affidate in subappalto, l'Appaltatore, a seguito della ricezione di comunicazione scritta in merito, deve porre in essere quanto necessario per eliminare l'inadempimento, ivi inclusa la risoluzione immediata del relativo subappalto e l'allontanamento dal luogo dell'esecuzione dell'attività del Subappaltatore medesimo.

La risoluzione del subappalto comporta da parte dell'Appaltatore, ove qualificato per l'esecuzione delle attività oggetto del contratto di subappalto, l'assunzione diretta delle relative attività, senza alcun onere aggiuntivo per ACI Informatica e fatto salvo il risarcimento di eventuali danni da ACI Informatica subiti e non dà alcun diritto all'Appaltatore di pretendere da ACI Informatica indennizzi, risarcimento di danni o spostamento dei termini contrattualmente previsti.

L'affidamento delle attività da parte dei soggetti di cui all'art. 65, comma 2, lettere b), c) e d) del D.Lgs. n. 36/2023 ai propri consorziati non costituisce subappalto. Si applicano comunque le disposizioni di cui all'art. 119 del citato D.Lgs. n. 36/2023.

1.9.3 Pagamento dei subappaltatori

ACI Informatica provvede al pagamento dell'importo dovuto per le prestazioni affidate in subappalto direttamente nei confronti dell'Appaltatore. In deroga a quanto previsto nel precedente comma, ACI Informatica procederà a corrispondere direttamente al subappaltatore e/o al subfornitore l'importo dovuto per le prestazioni dagli stessi eseguite qualora:

- a) in sede di autorizzazione al subappalto, l'Appaltatore dimostri che il subappaltatore è una micro impresa o piccola impresa secondo la definizione di cui all'Allegato I.1 art. 1, comma 1, lettera 0) del D.Lgs. n. 36/2023;
- b) in caso di inadempimento da parte dell'Appaltatore;
- c) su richiesta del subappaltatore solo nel caso in cui la natura del Contratto lo consenta.



Nel caso di pagamento diretto, l'Appaltatore comunica alla Stazione Appaltante le prestazioni eseguite dal subappaltatore o dal cottimista, con specificazione del relativo importo e con proposta motivata di pagamento, corredata di tutti gli elaborati tecnico-economici da cui risultino in dettaglio le prestazioni eseguite dal subcontraente.

In ogni caso, il pagamento diretto del subappaltatore o del subcontraente non potrà avvenire prima della maturazione del diritto dell'Appaltatore al pagamento della fattura ai sensi dell'art. 4.3, in cui siano ricomprese le prestazioni del subcontratto.

In applicazione della Legge sulla tracciabilità dei Flussi finanziari, l'Appaltatore dovrà indicare a ACI Informatica i conti correnti dedicati da parte del subappaltatore ed il nominativo del personale preposto alla gestione dello stesso.

Per quanto non espressamente indicato nel presente documento si rinvia alla disciplina di cui all'art. 119 del D.Lgs 36/2023

1.10 Codice Etico e Modello organizzativo. Patto di Integrità

L'Appaltatore dichiara di aver preso visione e di impegnarsi a rispettare e a far osservare ai soggetti che operano, per conto dell'Appaltatore stesso, in relazione all'esecuzione del Contratto, tutte le prescrizioni contenute nel Piano di Prevenzione della Corruzione, nel Modello Organizzativo e nel Codice Etico adottato da ACI Informatica ai sensi del D.Lgs. 231/2001 e pubblicato sul sito di ACI Informatica www.informatica.aci.it, nella sezione Trasparenza, e sul Portale Acquisti. L'inosservanza delle suddette prescrizioni costituirà inadempienza agli obblighi del Contratto, e legittimerà ACI Informatica a valutare l'adozione delle opportune misure di tutela, tra cui la risoluzione di diritto del Contratto stesso ai sensi e per gli effetti dell'art. 1456 del Codice Civile, fermo restando il risarcimento degli eventuali maggiori danni.

L'Appaltatore dichiara, altresì, di aver preso visione e di impegnarsi a rispettare e a far osservare ai soggetti che operano, per conto dell'Appaltatore stesso, in relazione all'esecuzione del presente Contratto, tutte le prescrizioni contenute nel "Patto di Integrità" pubblicato sul sito di ACI Informatica www.informatica.aci.it, nella sezione trasparenza, e sul Portale Acquisti, la cui inosservanza legittimerà ACI Informatica a valutare l'adozione delle misure di tutela in esso previste, tra cui la risoluzione di diritto del Contratto stesso e la segnalazione dei fatti all'Autorità Nazionale Anticorruzione.

1.11 Variazioni della compagine societaria e/o degli organi societari dell'Appaltatore

L'Appaltatore è tenuto a comunicare tempestivamente a ACI Informatica eventuali variazioni, che intervengano durante la validità del Contratto / Accordo quadro, nella composizione societaria, negli organi sociali (anche delle eventuali società controllanti), nonché in



ogni altro documento o dichiarazione forniti in sede di perfezionamento del Contratto / Accordo quadro.

Le variazioni dovranno essere comunicate con lo stesso dettaglio con il quale sono state prodotte in sede di perfezionamento del Contratto / Accordo quadro.

1.12 Trattamento dei dati personali

Tutte le informazioni di carattere personale utilizzate per le finalità di cui al Contratto / Accordo Quadro dovranno essere gestite in coerenza con la normativa vigente in materia di trattamento e di protezione dei dati personali.

Ai fini dell'espletamento delle attività e dei servizi oggetto del Contratto / Accordo Quadro, ACI Informatica potrebbe acquisire e trattare i dati personali riferiti ai dipendenti e ai collaboratori dell'Appaltatore.

A tal proposito, l'Appaltatore assicura di aver reso adeguata informativa, ai sensi del Regolamento UE 2016/679, agli interessati, manlevando espressamente ACI Informatica da ogni responsabilità derivante dall'illegittima comunicazione dei dati personali riferiti agli stessi.

1.12.1 Nomina a Responsabile del trattamento dei dati personali

L'Appaltatore, nel caso in cui, ai fini dell'esecuzione delle prestazioni oggetto del Contratto / Accordo Quadro, debba effettuare un trattamento di dati personali dei quali ACI Informatica sia Titolare, su incarico della stessa ACI Informatica (Titolare del trattamento) opererà in qualità di Responsabile in relazione al trattamento dei dati rientranti nella titolarità di ACI Informatica.

Le Parti si obbligano a regolare con separato atto la nomina dell'Appaltatore da parte di ACI Informatica a Responsabile del Trattamento, ai sensi dell'articolo 28 del Regolamento UE n. 679/2016.

1.12.2 Nomina a Sub-Responsabile del trattamento dei dati personali

L'Appaltatore, nel caso in cui, ai fini dell'esecuzione delle prestazioni oggetto del Contratto / Accordo Quadro, debba effettuare un trattamento di dati personali dei quali ACI Informatica sia Responsabile, su incarico della stessa ACI Informatica (Responsabile del trattamento) opererà in qualità di Sub-Responsabile in relazione al trattamento dei dati rientranti nella titolarità dell'Automobile Club d'Italia (Titolare del trattamento) effettuato per conto dello stesso Automobile Club d'Italia.

Le Parti si obbligano a regolare con separato atto la nomina dell'Appaltatore da parte di ACI Informatica a Sub-Responsabile del Trattamento, ai sensi dell'articolo 28 del Regolamento UE n. 679/2016.



2 ESECUZIONE DEL SERVIZIO

2.1 Avvio dell'esecuzione del Contratto

L'Appaltatore è tenuto a seguire le istruzioni e le direttive fornite dalla Rappresentanza di ACI Informatica per l'avvio dell'esecuzione del Contratto.

Ove si renda necessario in considerazione della natura e del luogo dell'esecuzione delle prestazioni, il DEC provvede alla redazione di un verbale di avvio dell'esecuzione, recante l'indicazione delle aree e degli eventuali ambienti in cui si svolge l'attività, la descrizione dei mezzi e degli strumenti eventualmente messi a disposizione dalla Stazione Appaltante e la dichiarazione attestante che lo stato degli ambienti è tale da non impedire l'avvio e la prosecuzione del Servizio.

Qualora, per l'estensione delle aree o dei locali, o per l'importanza dei mezzi strumentali all'esecuzione del Contratto, l'inizio dell'attività debba avvenire in luoghi o tempi diversi, il DEC provvede a dare le necessarie istruzioni nel verbale di avvio dell'esecuzione del Contratto.

Nei casi in cui sia disposta l'esecuzione anticipata a norma dell'art. 17, comma 8 del D.Lgs. n. 36/2023, il DEC indica nel verbale di avvio quanto predisposto e somministrato dall'Appaltatore ai fini del rimborso delle relative spese nonché le prestazioni che l'Appaltatore deve immediatamente eseguire.

Resta inteso che, qualora l'Appaltatore intenda far valere pretese derivanti dalla riscontrata difformità dello stato dei luoghi o dei mezzi o degli strumenti rispetto a quanto previsto dai documenti contrattuali, lo stesso è tenuto ad iscrivere riserva nel verbale di avvio dell'esecuzione, a pena di decadenza.

2.2 Obblighi dell'Appaltatore nell'espletamento del Servizio

Il Servizio deve essere conforme, nel suo complesso e in ogni sua parte, oltre che alle prescrizioni contrattuali, a tutte le disposizioni legislative e/o regolamentari e alle prescrizioni stabilite dalle competenti Autorità nazionali, vigenti alla data dell'espletamento del Servizio medesimo.

L'Appaltatore deve provvedere, ove occorra, all'ottenimento di tutti i permessi, autorizzazioni e/o licenze necessari per l'espletamento del Servizio, ad eccezione di quelli che la



legge pone espressamente in capo alla Stazione Appaltante, per l'ottenimento dei quali l'Appaltatore si impegna comunque a fornire, ove richiesta, la necessaria assistenza e/o documentazione.

Tutti gli obblighi e gli oneri inerenti l'esecuzione del Contratto / Accordo quadro devono intendersi a completo ed esclusivo carico dell'Appaltatore, ad esclusione di quelli esplicitamente posti dal presente Capitolato a carico di ACI Informatica; resta inteso, pertanto, che l'enunciazione, nel presente Capitolato, degli obblighi ed oneri a carico dell'Appaltatore deve intendersi a titolo meramente esemplificativo e non limitativo.

Se non previsto diversamente dal presente Capitolato, tutte le fasi relative allo svolgimento del Servizio saranno effettuate dall'Appaltatore, con proprie risorse e mezzi, salva la possibilità di acquistare presso terzi le materie prime, i materiali di serie, le eventuali apparecchiature, prodotti *hardware* e le eventuali licenze di prodotti *software* necessari all'espletamento del Servizio nonché i mezzi di trasporto e sollevamento.

A tal fine, l'Appaltatore deve dotarsi di tutto quanto necessario (ad esempio strumentazione, *software*, materiale di consumo) per l'esecuzione del Servizio; il materiale utilizzato dall'Appaltatore dovrà essere tenuto in buono stato di efficienza e non costituire fonte di pericolo per l'ambiente di lavoro.

L'Appaltatore adempirà al Contratto con l'impiego dei capitali e dei mezzi necessari e assumendosi il rischio dell'impresa ai sensi e per gli effetti dell'art. 29 del D.Lgs. 10.09.2003, n. 276.

In caso di inadempimento da parte dell'Appaltatore a quanto stabilito nei precedenti commi, fermo restando il diritto al risarcimento del danno, la Stazione Appaltante avrà facoltà di dichiarare risolto il Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

2.3 Obblighi di ACI Informatica

La Stazione Appaltante si impegna ad adempiere gli obblighi previsti a suo carico dal presente Capitolato e dalle disposizioni normative applicabili al rapporto.

In particolare, ACI Informatica provvede alla nomina dei soggetti che seguiranno l'esecuzione del Contratto. La direzione di tale esecuzione è affidata al RUP, che controlla i livelli di qualità delle prestazioni.

Il RUP, nella fase dell'esecuzione, si avvale, secondo i rispettivi compiti stabiliti al successivo art. 2.11, del Responsabile della fase di Esecuzione del Contratto, ove necessario, del Direttore dell'Esecuzione del Contratto, del coordinatore in materia di salute e di sicurezza durante l'esecuzione previsto dal D.Lgs. n. 81/2008, nonché del collaudatore ovvero della commissione di collaudo, del verificatore della conformità e accerta il corretto ed effettivo svolgimento delle funzioni ad ognuno affidate.



2.4 Programma cronologico e termini contrattuali del Servizio

Il Programma cronologico allegato al Contratto stabilisce, per ogni fase del Servizio, le date di espletamento del medesimo.

Il Programma cronologico del Servizio (o dell'insieme dei servizi che costituiscono l'oggetto del Contratto / Accordo quadro) è elaborato sulla base di quanto stabilito nelle Specifiche Tecniche, considerando che possono essere richiesti servizi con caratteristiche diverse che non sempre hanno una medesima modalità di svolgimento.

Il Programma cronologico approvato da ACI Informatica ha carattere esecutivo e impegna, in ogni caso, l'Appaltatore al rispetto di tutti i termini e scadenze temporali in esso indicati e connessi al raggiungimento di specifici risultati.

Nel concordare termini e scadenze, l'Appaltatore ha tenuto debitamente conto di tutte le alee connesse con l'esecuzione del Contratto / Accordo quadro ed in particolare di quelle relative alle condizioni ambientali e alla eventuale necessità di coordinamento con altri fornitori e/o appaltatori e con le strutture di ACI Informatica.

In caso di ritardo rispetto ai termini indicati nel Programma cronologico relativi a ciascuna fase del Servizio approvati dalla Rappresentanza di ACI Informatica, potranno essere applicate le penali secondo quanto previsto nel successivo art. 4.2 e nel Contratto/ Accordo quadro.

Ove per effetto delle variazioni di cui all'art. 1.8 si determinino variazioni nell'entità di alcuni servizi, i termini di ultimazione relativi sono, se necessario e previa specifica autorizzazione di ACI Informatica, congruamente differiti.

Nel Programma cronologico allegato al Contratto sono esplicitati i seguenti termini contrattuali, il cui significato è di seguito precisato:

- Inizio Programma Cronologico (IPC): *coincidente con la data di stipula del Contratto o, nei casi ove ricorra, con la Data di consegna anticipata delle attività;*
- Presa in Carico del Servizio (PCS), per ogni singolo servizio attivato: *coincidente con il momento in cui l'Appaltatore può effettivamente avviare l'erogazione dello specifico servizio, a valle delle eventuali attività di presa in carico avviate subito dopo l'IPC.*

Il Piano cronologico può prevedere scadenze diverse e specifiche in relazione ai singoli servizi oggetto del Contratto.

Tutti i suddetti termini dovranno essere accertati da appositi Verbali debitamente sottoscritti dalle Parti, con l'esplicita indicazione della conclusione di tutte le attività/fasi previste, della consegna di tutti i prodotti, dell'eventuale trasferimento di conoscenze e dell'esito finale; inoltre dovranno essere dettagliati gli eventuali ritardi rispetto ai termini contrattualmente previsti, intermedi e finali, nonché le eventuali anomalie relative a non soddisfacimento di requisiti (prestazionali, di qualità, ecc) previsti nelle Specifiche Tecniche ai fini dell'applicazione di quanto previsto nel successivo articolo 4.2.



A tale Programma cronologico deve conformarsi il Piano di Esecuzione del Servizio.

2.5 Spostamento dei termini contrattuali dei singoli servizi

Nel caso di interruzione o ritardo nell'esecuzione di un servizio, determinati da una o più delle cause non imputabili all'Appaltatore, di seguito elencate, l'Appaltatore ha il diritto di chiedere una proroga dei termini contrattuali del servizio interessato per un periodo da concordare, ma comunque non superiore alla durata dell'evento che ha determinato detta interruzione o ritardo.

In particolare, sono considerate cause legittime di ritardo o interruzione i seguenti eventi:

- a) eventi di forza maggiore: scioperi nazionali, calamità naturali, etc. Non sono invece assimilabili a questa fattispecie i ritardi imputabili ai subcontraenti;
- b) opere ed attività che, pur non rientrando nell'oggetto del Contratto / Accordo quadro, sono strumentali all'esecuzione del Servizio e si trovino in uno stato di avanzamento tale da non consentire all'Appaltatore l'inizio delle attività alla data prevista nel Programma Cronologico;
- c) altri eventuali eventi esplicitamente precisati nel Contratto/Accordo quadro.

L'Appaltatore è tenuto, in ogni caso, a presentare alla Rappresentanza di ACI Informatica, a pena di decadenza, domanda di proroga scritta, debitamente motivata e documentata, entro 10 (dieci) giorni dall'evento impeditivo ovvero, se diversa, dalla data in cui ne è venuto a conoscenza, e comunque con congruo anticipo rispetto al termine contrattuale.

Accertato il diritto dell'Appaltatore alla proroga, la Rappresentanza ACI Informatica definirà – entro un termine di tempo coerente con il Piano Cronologico delle attività, e comunque non oltre il termine di 30 giorni dal ricevimento dell'istanza di proroga - un nuovo termine contrattuale, che sostituisce a tutti gli effetti quello originario previsto dal Contratto, richiedendo in ogni caso all'Appaltatore la ripianificazione e l'emissione del Programma Cronologico delle attività che sarà verificato dalla Rappresentanza di ACI Informatica e, se ritenuto congruo, approvato.

Non sono consentiti anticipi sull'espletamento del Servizio rispetto ai termini contrattuali, se non espressamente concordati con ACI Informatica o da quest'ultima richiesti per iscritto. In particolare, l'esecuzione anticipata del Servizio potrà avvenire solo su esplicita autorizzazione scritta del Responsabile Unico del Progetto.

2.6 Piano di Esecuzione del Servizio ICT

In relazione alle caratteristiche ed esigenze dei Servizi previsti nel CSA di Servizi – Parte Tecnica, l'Appaltatore deve predisporre il Piano di Esecuzione del Servizio, compresi gli



eventuali allegati, che costituisce il riferimento per le modalità di esecuzione del Servizio medesimo.

Tale Piano deve contenere una descrizione dettagliata di tutte le attività, con l'indicazione del corrispondente Programma Cronologico di esecuzione, nel rispetto dei Termini Contrattuali stabiliti nel Programma Cronologico di cui al Contratto e, in particolare, dei tempi previsti per le eventuali prestazioni in sito. In particolare, il Piano dovrà sviluppare contenuti diversi in base al grado di definizione dei servizi, approfondendo maggiormente gli aspetti metodologici per i servizi che hanno un grado di approfondimento minore, o sviluppare invece maggiormente gli aspetti operativi qualora il piano sia relativo ad un Servizio le cui caratteristiche e requisiti siano già completamente individuati e siano riportati nelle Specifiche Tecniche. Nel caso in cui il Contratto riguardi l'adeguamento di un impianto in esercizio, il Programma Cronologico dovrà anche tenere conto delle esigenze di continuità del Servizio, secondo quanto richiesto dalla documentazione tecnica di riferimento.

Il Piano di Esecuzione del Servizio sarà oggetto di revisione e aggiornamento per tutta la durata di esecuzione del Servizio. L'Appaltatore si impegna a tenere costantemente aggiornato il Piano di Esecuzione del Servizio e ad informare ACI Informatica in occasione di ogni aggiornamento intervenuto.

2.7 Imballo e trasporto delle forniture

Nel caso in cui l'oggetto del Contratto preveda anche la fornitura di prodotti, l'Appaltatore deve curare, sotto la sua esclusiva responsabilità, l'imballaggio, l'approntamento al trasporto, il carico, il trasporto dalla fabbrica al luogo di destinazione, lo scarico e la movimentazione di quanto fa parte della fornitura, nonché la conservazione e la custodia della stessa.

Per consentire l'identificazione del materiale oggetto della fornitura, sarà resa disponibile, all'interno e all'esterno dell'imballaggio, copia del documento con l'elenco di quanto contenuto nell'imballaggio stesso.

Le modalità di assemblaggio dei materiali per il trasporto saranno definite dall'Appaltatore tenendo conto della situazione logistica della specifica sede cui sono destinati (accessibilità, viabilità, condizioni atmosferiche ecc.). L'eventuale sub-fornitore commissionato dall'Appaltatore per il trasporto deve essere adeguatamente informato della situazione logistica della specifica sede cui sono destinati (accessibilità, viabilità, condizioni atmosferiche ecc.).

Il DUVRI o PSC, laddove allegato al Contratto di appalto, dovrà essere consegnato materialmente dall'Appaltatore al sub contraente trasportatore, assicurandosi che le informazioni ivi contenute vengano da quest'ultimo adeguatamente rispettate nella fase di consegna e scarico della fornitura. ACI Informatica si riserva la facoltà di non accettare la



fornitura nel caso in cui rilevi che il sub contraente trasportatore non sia stato informato dei contenuti del DUVRI o PSC.

L'Appaltatore garantisce che i trasportatori dallo stesso scelti osservino tutte le norme di legge e/o regolamentari vigenti ed applicabili e, in particolare, il Codice della Strada, i Regolamenti regionali, provinciali, comunali autostradali e ferroviari.

2.8 Ricevimento delle forniture

2.8.1 Consegna

L'Appaltatore è obbligato a consegnare l'intera fornitura, unitamente agli eventuali accessori, nel luogo e nei termini indicati nel Contratto. Non sono ammesse le consegne frazionate, senza previa autorizzazione scritta di ACI Informatica.

Se non diversamente disposto nel Contratto, la fornitura s'intende resa franco destino, con le attività di scarico a cura e spesa dell'Appaltatore, che ne risponde in modo pieno ed esclusivo.

Le consegne dovranno essere eseguite durante il normale orario di lavoro osservato dal personale di ACI Informatica, dando al destinatario un preavviso non inferiore a 3 (tre) giorni lavorativi.

In caso di fornitura proveniente da un Paese non appartenente all'Unione Europea, l'Appaltatore avrà l'obbligo, prima della spedizione, di trasmettere alla Rappresentanza di ACI Informatica, le generalità ed il recapito telefonico dello spedizioniere, il quale dovrà contattare la suddetta Rappresentanza in tempo utile per gli adempimenti di propria competenza.

2.8.2 Verifica di conformità e accettazione della fornitura

La fornitura si intende definitivamente accettata solo dopo che abbia superato con esito positivo la verifica di conformità compiuta da ACI Informatica sulla quantità e qualità della fornitura nonché sulla sua rispondenza alle prescrizioni tecniche di ACI Informatica e, più in generale, alle condizioni e termini stabiliti nel Contratto e suoi allegati, ferme restando le garanzie del fornitore.

L'accettazione della fornitura sarà normalmente effettuata sulla base dei seguenti controlli, fermo restando che nelle Specifiche Tecniche possono essere specificati altri in sostituzione o integrazione.

- esito favorevole della verifica di conformità, svolta secondo quanto previsto dalla normativa specifica e quanto ulteriormente indicato nelle Specifiche Tecniche;
- corrispondenza della fornitura a quanto indicato nelle bolle di consegna/accompagnamento, per ciò che riguarda quantità, codici, documentazione



allegata (manuali, certificazioni ecc.), e in particolare ai fini della conformità a quanto fissato contrattualmente e dalla vigente normativa in materia;

- verifica del possesso, ove presente, della Marcatura CE, con presentazione ed evidenza a cura del fornitore, del relativo Certificato o Dichiarazione di Conformità alle specifiche norme europee;
- assenza di eventuali danneggiamenti e/o imperfezioni esteriori, evidenziatisi anche dopo l'apertura degli imballaggi.

ACI Informatica si riserva di rifiutare le forniture i cui imballi siano danneggiati.

2.8.3 Non conformità – difetti

In caso di non conformità della fornitura alle prescrizioni di ACI Informatica o di danneggiamento della stessa immediatamente rilevabili, ACI Informatica potrà rifiutare i prodotti non conformi o danneggiati, e il Contratto s'intenderà in tutto o in parte ineseguito, con l'obbligo dell'Appaltatore di effettuare, a propria cura e spese, la sostituzione dei prodotti rifiutati. L'Appaltatore dovrà effettuare la sostituzione nel più breve tempo possibile e, comunque, entro il termine perentorio assegnatogli. La richiesta di sostituzione sarà effettuata da ACI Informatica, con comunicazione scritta, contenente la descrizione dei difetti, delle difformità e/o dei danni riscontrati.

Si conviene espressamente che, in deroga a quanto disposto dall'articolo 1495, c.c., eventuali vizi e/o mancanza di qualità non apparenti, rilevati durante il normale uso, potranno essere denunciati all'Appaltatore mediante comunicazione scritta, entro 10 (dieci) giorni dalla scoperta. ACI Informatica, a propria discrezione, potrà richiedere all'Appaltatore di sostituire o riparare il prodotto difettoso. Tutte le spese di riparazione o sostituzione restano a totale carico dell'Appaltatore.

ACI Informatica potrà effettuare in qualunque momento tutte le verifiche che riterrà necessarie e/o opportune sui prodotti ricevuti ovvero su campioni degli stessi, al fine di accertare che i requisiti e gli standard qualitativi dei medesimi corrispondano a quelli richiesti nel Contratto, ovvero che i relativi valori siano compresi nell'intervallo di tolleranza ammesso.

Nel caso in cui, all'esito delle verifiche, risulti che i prodotti forniti siano di qualità inferiore rispetto a quella attesa, ovvero presentino caratteristiche non conformi a quelle pattuite, ACI Informatica, a propria esclusiva discrezione, potrà accettare la fornitura, richiedendo, ai sensi dell'articolo 1492 del c.c., un'equa riduzione di prezzo, commisurata allo scostamento dei valori accertati rispetto a quelli stabiliti nel Contratto, ovvero rifiutarla, salvo il risarcimento dei danni ai sensi dell'articolo 1494 del c.c.

2.8.4 Prove e test per il servizio di installazione



L'Appaltatore, dopo aver completato l'installazione provvederà, sotto la propria esclusiva responsabilità, all'approntamento ed esecuzione delle prove test; a tale riguardo si rimanda alle Specifiche Tecniche per eventuali maggiori specificazioni.

Con particolare riferimento allo sviluppo del software, ACI Informatica intende porre in atto, in forma sempre più ampia e stringente, tecniche di Application Security Testing (AST) durante l'intero ciclo di vita dello sviluppo del software. In questa ottica ACI Informatica potrà direttamente utilizzare, o richiedere all'Appaltatore di utilizzare, specifici software di controllo finalizzati a valutare la rispondenza del software sviluppato dall'Appaltatore ai requisiti di sicurezza applicativa indicati in Specifica Tecnica o nella documentazione aggiuntiva.

2.9 Verifica di conformità e presa in carico del Servizio

Il Servizio si intende accettato e preso in carico da ACI Informatica solo dopo il positivo superamento della verifica di conformità, avente ad oggetto la rispondenza del Servizio alle Specifiche Tecniche, e, più in generale, alle condizioni e termini stabiliti nel Contratto e suoi allegati, ferme restando le garanzie dell'Appaltatore.

2.10 Sorveglianza

ACI Informatica ha diritto di controllare e verificare, anche oltre e al di fuori dei tempi indicati nei piani di test e controllo, tramite personale della Rappresentanza di ACI Informatica, la perfetta osservanza, da parte dell'Appaltatore, di tutte le pattuizioni contrattuali e di tutte le disposizioni emanate da ACI Informatica stessa nel corso dell'espletamento del Servizio, nonché il corretto e tempestivo svolgimento, da parte dell'Appaltatore medesimo di tutte le attività necessarie per l'esecuzione del Contratto. A tal fine, il personale di ACI Informatica all'uopo autorizzato può accedere in ogni momento, durante il normale orario di lavoro, nei luoghi ove si svolgono le suddette attività.

I controlli e le verifiche, eseguiti dal personale di ACI Informatica, anche in assenza di obiezioni da parte dello stesso, non liberano l'Appaltatore dagli obblighi e responsabilità inerenti il corretto espletamento del Contratto e la conformità del Servizio alle clausole contrattuali, né lo sollevano dagli obblighi derivanti dalle disposizioni di leggi e/o regolamentari vigenti.

Tali controlli e verifiche non possono, inoltre, essere invocati dall'Appaltatore a giustificazione di eventuali ritardi e/o inadempienze dell'Appaltatore, adducendo gli stessi quali causa di interferenza nelle modalità di conduzione delle prestazioni oggetto dell'appalto, ivi inclusa l'utilizzazione dei mezzi d'opera, dei macchinari e dei materiali.



2.11 Compiti della Rappresentanza di ACI Informatica

La Rappresentanza di ACI Informatica per lo svolgimento delle attività oggetto del Contratto è esercitata dal Responsabile Unico del Progetto e dal Responsabile della fase di Esecuzione del Contratto se nominato e dal Direttore dell'Esecuzione del Contratto.

Nel caso sia stato nominato, il Responsabile della fase di Esecuzione, rappresenta il delegato del RUP per la specifica fase dell'esecuzione contrattuale, sovrintende a tutte le attività finalizzate alla realizzazione degli interventi affidati, assicurando che le stesse siano svolte nell'osservanza delle disposizioni di legge, in particolare di quelle in materia di sicurezza e salute sui luoghi di lavoro, e garantendo il rispetto dei tempi di esecuzione previsti nel contratto e la qualità delle prestazioni.

Il Direttore dell'Esecuzione del Contratto ha il compito di controllare, in proprio o tramite i componenti della sua struttura di supporto, la perfetta osservanza da parte dell'Appaltatore, di tutte le disposizioni contenute nel Contratto e nel presente Capitolato, nonché di quelle comunque emanate da ACI Informatica nel corso dell'esecuzione del Servizio.

Allo stesso Responsabile della fase di Esecuzione del Contratto ed al Responsabile Unico del Progetto dovranno essere inviate, sempre per iscritto, tutte le comunicazioni inerenti il Servizio.

2.12 Rappresentanza dell'Appaltatore

Al "Responsabile del Contratto", come definito all'art. 1.1.4 del presente Capitolato, competono tutte le responsabilità che, a norma delle vigenti disposizioni, derivano dalla conduzione tecnica ed amministrativa del Servizio.

Il Responsabile del Contratto ed il suo sostituto devono essere in possesso dei requisiti di legge, essere muniti delle necessarie deleghe ed avere adeguata competenza e piena conoscenza di tutte le clausole contrattuali.

L'Appaltatore non può preporre il Responsabile del Contratto od il suo sostituto se non previo gradimento di ACI Informatica e deve provvedere immediatamente e senza oneri per ACI Informatica alla loro sostituzione, nel rispetto delle norme vigenti, ove ACI Informatica gli comunichi il venir meno del gradimento. In caso di sua sostituzione, il nuovo Responsabile del Contratto potrà operare solo previo consenso espresso di ACI Informatica. Si conviene, altresì, che il rappresentante dell'Appaltatore, o il suo sostituto, deve essere reperibile in ogni momento per tutta la durata delle attività oggetto del Servizio in modo che nessuna operazione subisca ritardi per effetto di loro assenza.



2.13 Svolgimento delle attività

Nulla sarà dovuto all'Appaltatore per eventuali interferenze dovute alla contemporanea esecuzione di attività ad opera di altri appaltatori e/o di ACI Informatica stessa.

L'Appaltatore è tenuto ad utilizzare in modo corretto e diligente le aree, i locali, gli impianti, le installazioni e tutti i mezzi e strumenti di proprietà di ACI Informatica, comunque interessati dal Servizio, e a provvedere, in caso di danneggiamento, alle conseguenti riparazioni, ripristini e indennizzi.

In particolare, in caso di danneggiamento, l'Appaltatore dovrà darne immediata comunicazione ad ACI Informatica e dovrà prontamente provvedere, a propria cura e spese, alla riparazione ed al ripristino delle parti danneggiate sulla base delle indicazioni di ACI Informatica e previo accertamento dei danni e specifico benessere da parte di ACI Informatica stessa.

ACI Informatica si riserva in ogni caso la facoltà di accettare le riparazioni o ripristini subordinatamente al buon esito dei controlli, delle prove e degli eventuali test, per l'esecuzione dei quali l'Appaltatore medesimo dovrà fornire tutta la necessaria assistenza.

2.14 Sicurezza

2.14.1 Misure per la salute e sicurezza nei luoghi di lavoro

Fermi restando gli ulteriori obblighi di cooperazione e coordinamento di cui alla vigente legislazione in materia di sicurezza e salute dei lavoratori, ACI Informatica, qualora i luoghi di esecuzione della prestazione ricadano nella sua giuridica disponibilità e sempre che sussistano interferenze tra attività connesse all'esecuzione del Contratto, elabora il Documento unico di valutazione dei rischi da interferenze (DUVRI).

Fatte salve diverse previsioni normative, il DUVRI sarà aggiornato da ACI Informatica in caso di subappalti o forniture con posa in opera intervenuti successivamente ovvero in caso di modifiche di carattere tecnico, logistico o organizzativo incidenti sulle modalità realizzative del Contratto.

Per tutti gli altri rischi non riferibili alle interferenze resta immutato l'obbligo dell'Appaltatore di elaborare il proprio documento di valutazione dei rischi e di provvedere all'attuazione delle misure di sicurezza necessarie per eliminare o ridurre al minimo i rischi specifici propri dell'attività svolta.

Ai sensi del D.Lgs. n. 81/2008 e s.m.i., l'Appaltatore è obbligato ad osservare ove applicabile, quanto previsto dal DUVRI predisposto dalla Stazione Appaltante ed allegato al Contratto.



L'Appaltatore, prima di procedere all'esecuzione dell'appalto, sulla base della propria esperienza, ove ritenga di poter meglio garantire la sicurezza del lavoro, potrà proporre ulteriori modifiche e/o integrazioni al PSC o al DUVRI. Tali proposte di integrazione, una volta valutate da ACI Informatica, saranno inserite nel PSC o nel DUVRI definitivo che verrà allegato al Contratto d'appalto/Accordo Quadro e considerato alla stregua delle Specifiche Tecniche.

Il PSC o il DUVRI definitivo e i relativi allegati dovranno essere sottoscritti per accettazione ed inviati a ACI Informatica dal datore di lavoro dell'Appaltatore, dall'impresa affidataria in caso di Consorzio o RTI.

L'Appaltatore si obbliga, ai fini della verifica dell'idoneità Tecnico professionale, a trasmettere ad ACI Informatica la documentazione di cui all'allegato XVII del Dlg. 81/08 e, presa visione dello stato dei luoghi e di tutti gli elaborati progettuali e dei documenti relativi alla sicurezza nei luoghi di lavoro, si obbliga a porre in essere tutte le misure di sicurezza previste dalla vigente normativa in materia di prevenzione dagli infortuni sul lavoro e di igiene del lavoro. L'Appaltatore si impegna ad informare adeguatamente il proprio personale ed il personale ad esso equiparato, quale è quello di eventuali subappaltatori e/o subfornitori, dei rischi specifici e ambientali ai quali potrebbero essere esposti e delle misure di prevenzione e di protezione da adottare, ai sensi del D.Lgs. n. 81/2008 e s.m.i..

Prima dell'inizio delle attività l'Appaltatore, e comunque tutte le imprese esecutrici delle prestazioni in caso di RTI o Consorzio, incluse le ausiliarie, devono presentare una dichiarazione dell'organico medio annuo, distinto per qualifica, corredata dagli estremi delle denunce dei lavoratori effettuate all'Istituto nazionale della previdenza sociale (INPS), all'Istituto nazionale assicurazione infortuni sul lavoro (INAIL) e alle casse edili, nonché una dichiarazione relativa al contratto collettivo stipulato dalle organizzazioni sindacali comparativamente più rappresentative, applicato ai lavoratori dipendenti.

Laddove è previsto il PSC, prima dell'inizio delle prestazioni ACI Informatica comunica alle ditte incaricate del Servizio il nominativo del Coordinatore della Sicurezza in fase di progettazione (CSP) e del Coordinatore per la Sicurezza in fase di esecuzione (CSE).

L'Appaltatore, ove previsto per legge, prima dell'inizio delle prestazioni, deve:

- a) consegnare al Coordinatore per l'esecuzione copia del Piano di Sicurezza e di Coordinamento (PSC), sottoscritto per accettazione, unitamente al Piano Operativo di Sicurezza (POS), predisposto dallo stesso Appaltatore e complementare al PSC; l'Appaltatore deve inserire all'interno del POS, l'elenco nominativo dei referenti per la sicurezza, nonché dei preposti, con i rispettivi ruoli.
- b) consegnare al Coordinatore per l'esecuzione apposita dichiarazione in cui si evinca il nominativo del soggetto preposto alla funzione di Responsabile della Gestione dell'Emergenza in cantiere e del suo Sostituto e la loro dichiarazione di conoscenza dei compiti che sono chiamati a svolgere. Il responsabile ed il



suo sostituto dovranno esibire l'attestato di frequenza ad un adeguato corso di formazione per addetti antincendio come previsto dal D.M. n. 64 del 10/03/98;

- c) inviare a ACI Informatica la vigente Visura camerale attestante l'iscrizione presso il registro della Camera di Commercio, Industria, Artigianato e Agricoltura (CCIAA).

ACI Informatica si riserva la facoltà di verificare in ogni momento il preciso e puntuale adempimento, da parte dell'Appaltatore, di tutte le obbligazioni in materia di sicurezza e salute dei lavoratori, in conformità a quanto previsto dalla legislazione vigente. Il RUP compie, su delega della Stazione Appaltante, in coordinamento con il RE, se nominato, o in alternativa il DEC, ove diverso dal RUP, le azioni dirette a verificare, anche attraverso la richiesta di documentazione, attestazioni e dichiarazioni, il rispetto, da parte dell'Appaltatore, delle norme sulla sicurezza e sulla salute dei lavoratori sui luoghi di lavoro, in conformità a quanto previsto dalla legislazione vigente. Resta in ogni caso inteso che in nessun modo tali verifiche sollevano l'Appaltatore dalla piena e completa responsabilità che gli compete.

Le prestazioni contrattuali che dovranno essere svolte presso gli uffici di ACI Informatica dovranno essere eseguite, di norma, nel corso del normale orario di lavoro degli uffici. L'accesso negli uffici di ACI Informatica e la disponibilità dei relativi ambienti, in relazione e ai fini dell'esecuzione delle prestazioni oggetto del Contratto / Accordo Quadro, saranno consentiti nel rispetto di tutte le relative prescrizioni di sicurezza e di accesso. In relazione a ciò, l'Appaltatore prende atto che, nel corso dell'esecuzione delle suddette prestazioni, gli uffici di ACI Informatica continueranno a essere utilizzati, per la loro destinazione istituzionale, dal personale di ACI Informatica e/o di terzi autorizzati. L'Appaltatore si impegna, pertanto, a eseguire le summenzionate prestazioni, senza alcun onere aggiuntivo, salvaguardando le esigenze di ACI Informatica e di terzi autorizzati, senza recare intralci, disturbi o interruzioni all'attività lavorativa in atto, e nel rispetto di tutte le relative prescrizioni di sicurezza e accesso.

Il personale dell'Appaltatore sarà tenuto ad osservare la normativa vigente in materia di impianti e, in particolare, le disposizioni sull'accesso e la mobilità all'interno degli immobili di ACI Informatica. Il personale preposto all'esecuzione delle attività oggetto del Contratto / Accordo Quadro da svolgersi presso gli uffici e gli ambienti di ACI Informatica potrà accedervi previa comunicazione ad ACI Informatica dei relativi nominativi e dati anagrafici unitamente agli estremi di un documento di identificazione, e sarà dotato, ai sensi del D.Lgs. n. 81/2008 e della Legge 136/2010, di una tessera di riconoscimento, da esibire durante l'esecuzione dei lavori, corredata di fotografia, contenente l'indicazione del datore di lavoro, le generalità del lavoratore, il relativo numero di matricola, nonché la data di assunzione e, in caso di subappalto, la relativa autorizzazione. Nel caso di lavoratori autonomi, la tessera di riconoscimento dovrà contenere anche l'indicazione della Stazione Appaltante. Il suddetto personale e i suddetti lavoratori si impegnano, nella frequentazione degli uffici e degli ambienti di ACI Informatica, a portare in modo visibile tale tessera di riconoscimento.



L'Appaltatore è tenuto a dettare le norme disciplinari e comportamentali alle quali il proprio personale dovrà attenersi nell'esecuzione delle attività oggetto del Contratto / Accordo Quadro, e a garantire il rispetto, da parte del personale stesso, delle disposizioni interne di ACI Informatica. In particolare, l'Appaltatore, ai sensi e per gli effetti del D. Lgs. 81/08 e s.m.i., dichiara di avere ricevuto copia integrale del 'Piano di Emergenza Sicurezza – Piano di emergenza per tutto il personale' relativo alle sedi di ACI Informatica presso cui andranno svolte le attività contrattuali, e di averne acquisito piena e adeguata conoscenza, e si obbliga a rispettarne e a farne rispettare integralmente i relativi contenuti dal proprio personale, e a far sì che il proprio personale si obblighi ad adottare tutte le misure previste dalle prescrizioni delle vigenti norme antinfortunistiche e dalle disposizioni di legge e regolamenti in materia di sicurezza.

Il personale dell'Appaltatore sarà tenuto ad osservare la normativa vigente in materia di impianti e, in particolare, le disposizioni sull'accesso e la mobilità all'interno degli immobili di ACI Informatica. Lo stesso sarà inoltre dotato, ai sensi del D.Lgs. n. 81/2008 e della Legge 136/2010, di una tessera di riconoscimento, da esibire durante l'esecuzione del servizio, corredata di fotografia, contenente l'indicazione del datore di lavoro, le generalità del lavoratore, il relativo numero di matricola, nonché la data di assunzione e, in caso di subappalto, la relativa autorizzazione.

Nel caso di lavoratori autonomi, la tessera di riconoscimento dovrà contenere anche l'indicazione della Stazione Appaltante.

Tutti i rappresentanti delle imprese esecutrici e i singoli lavoratori autonomi che operano eventualmente nell'appalto, dovranno necessariamente partecipare a tutte le riunioni di cooperazione e coordinamento indette dal CSE. La prima di tali riunioni avrà lo scopo di definire:

- la programmazione delle attività.
- eventuale integrazione dei POS e del PSC proposte dall'Appaltatore al fine di migliorare la sicurezza.
- le modalità organizzative e le procedure operative stabilite ai fini del coordinamento tra le imprese e i lavoratori autonomi.
- l'individuazione delle figure con particolari compiti all'interno del sito.

In caso di subappalto, il datore di lavoro dell'Appaltatore verifica l'idoneità tecnico professionale dei subappaltatori e dei lavoratori autonomi, e trasmette ad ACI Informatica una dichiarazione in cui attesta di aver verificato l'idoneità tecnico professionale delle imprese subappaltatrici, ai sensi dell'articolo 90, comma 9, lettere a) e b), del D.lgs. n. 81/2008. Nel caso di subappalto a Consorzi la verifica sarà limitata alle sole imprese consorziate esecutrici del subappalto, mentre nel caso di RTI la verifica verrà effettuata su tutte le imprese associate esecutrici del subappalto.



Laddove è previsto il PSC, il subappaltatore dovrà comunicare a ACI Informatica, il nominativo del proprio responsabile della sicurezza in cantiere che avrà il compito di tenere i rapporti con il CSE.

In caso di mancato rispetto delle disposizioni di legge vigenti in materia di tutela di salute e sicurezza dei lavoratori, ACI Informatica ha facoltà di risolvere il Contratto di appalto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

2.8.5 Regole comportamentali per l'accesso e l'utilizzo dei sistemi informativi di ACI Informatica

L'accesso da parte di personale dell'Appaltatore e subappaltatore alla rete ed ai sistemi di ACI Informatica nonché l'utilizzo delle applicazioni e dei servizi aziendali (computer, reti, *software* di sistema ed applicativo, servizi di comunicazione, etc), sono ammessi esclusivamente per lo svolgimento delle attività oggetto del Contratto e sono sempre vincolati al rispetto delle regole di uso "sicuro" stabilite da ACI Informatica, tra cui le seguenti regole comportamentali:

- a) l'accesso deve essere attuato nel rispetto dell'ambito assegnato e limitatamente alle componenti tecnologiche, ai trattamenti ed alle informazioni strumentali all'espletamento dell'attività oggetto del Contratto;
- b) le credenziali per l'accesso ai sistemi sono strettamente personali, non devono essere cedute ad altri e devono essere gestite e protette secondo le prescrizioni di ACI Informatica, comunicate al momento della loro consegna;
- c) l'eventuale casella di posta elettronica fornita da ACI Informatica sul server aziendale, se prevista per l'espletamento delle attività del Contratto, non deve essere utilizzata né nei confronti di interlocutori estranei alle attività oggetto del Contratto, né per attività estranee al Contratto (messaggi personali, etc.);
- d) nei casi in cui sia prevista la classificazione dei documenti, gli eventuali messaggi *e-mail* contenenti dati che ACI Informatica classifica ad uso Ristretto, ammessi se finalizzati all'espletamento delle attività oggetto del Contratto, possono essere scambiati solo se protetti per mezzo di adeguati strumenti di crittografia.

A tale scopo si rimanda anche al "Documento programmatico sulla sicurezza (DPS)" che fornisce molte informazioni e prescrizioni che trovano applicazione nei servizi di cui si tratta.

2.8.6 Monitoraggio per la sicurezza e conseguenze di una violazione delle regole

Per garantire la protezione dei propri sistemi, applicazioni e servizi, ACI Informatica attua un monitoraggio continuo della sicurezza nel rispetto delle leggi vigenti.



In presenza di violazioni alle regole comportamentali, ACI Informatica si riserva il diritto di revocare, anche con effetto immediato, l'autorizzazione di accesso ai propri sistemi informativi/informatici per l'Appaltatore ed il suo personale.

ACI Informatica inoltre segnalerà alla competente Autorità Giudiziaria, quelle costituenti un'ipotesi di reato.

2.8.7 Accettazione delle clausole sistemi per la sicurezza delle informazioni di ACI Informatica

Per poter essere autorizzato al trattamento delle informazioni di ACI Informatica e/o all'accesso ai sistemi ed all'utilizzo dei servizi e delle applicazioni di ACI Informatica facenti parte dell'ambito delle attività del Contratto, l'Appaltatore deve fornire ad ACI Informatica:

- a) al momento della destinazione del proprio personale sulle attività, la dichiarazione sottoscritta di avvenuta formazione/informazione, per il proprio personale individuato e destinato ad operare nelle attività del Contratto / Accordo quadro, sulle norme per la sicurezza delle informazioni applicabili al Contratto / Accordo quadro stesso (impegni, regole comportamentali, tracciabilità e conseguenze);
- b) al momento dell'autorizzazione all'accesso per il personale dell'Appaltatore, la dichiarazione di presa visione ed accettazione delle norme per la sicurezza delle informazioni, sottoscritta dal personale individuato.

In assenza di tali adempimenti, non sarà possibile dare seguito all'autorizzazione di accesso ai sistemi ed alle relative aree tecnologiche e ACI Informatica si riserverà di risolvere il Contratto d'appalto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

2.15 Personale addetto al Servizio

2.15.1 Generalità

L'Appaltatore deve provvedere alla conduzione delle prestazioni oggetto del Contratto con personale idoneo, qualificato e specializzato, di provate capacità ed adeguato, qualitativamente e numericamente, alle necessità connesse alla prestazione in relazione agli oneri ed obblighi derivanti dal Contratto/Accordo quadro.

I lavoratori impiegati nell'espletamento del Servizio – assunti a tempo determinato o indeterminato dall'Appaltatore in base agli usuali e regolari contratti di lavoro subordinato ovvero di prestazione di lavoro autonomo conformi alla vigente disciplina di settore - saranno soggetti, anche laddove la prestazione venga effettuata presso locali ACI Informatica, all'esclusivo potere organizzativo, direttivo e disciplinare dell'Appaltatore che risponderà dei danni alle persone e alle cose provocati nello svolgimento del Servizio, restando a suo completo ed esclusivo carico qualsiasi risarcimento, senza diritto



di rivalsa o di compensi da parte della Stazione Appaltante; in relazione a ciò, l'Appaltatore si obbliga a contrarre apposita polizza assicurativa e si obbliga espressamente a tenere indenne e a manlevare ACI Informatica da ogni e qualsivoglia azione risarcitoria e/o pretesa retributiva da chiunque proposta nei confronti della predetta Stazione Appaltante.

A seguito di esplicita richiesta di ACI Informatica, l'Appaltatore dovrà comprovare la corresponsione, ai dipendenti impiegati nell'appalto, dei trattamenti retributivi loro dovuti, inoltrando alla stessa copia della documentazione di lavoro ad essi relativa.

L'Appaltatore non ha comunque diritto ad alcun compenso se, per far fronte alle prestazioni contrattuali, risulta necessario modificare, rispetto a quanto inizialmente previsto, la consistenza del personale da impiegare, in termini qualitativi e/o quantitativi.

L'Appaltatore è tenuto ad impiegare personale di gradimento di ACI Informatica ed è tenuto a procedere all'allontanamento e/o alla sostituzione - nel rispetto delle norme vigenti e senza oneri per ACI Informatica - di quel personale per il quale ACI Informatica avanzasse apposita richiesta. Tali aspetti possono essere ulteriormente regolamentati nelle Specifiche Tecniche.

Nel caso di esercizio di tale facoltà, l'Appaltatore dovrà provvedere all'allontanamento e/o alla sostituzione delle persone non gradite entro e non oltre 2 (due) giorni dal ricevimento della comunicazione.

L'Appaltatore si impegna altresì alla sostituzione preventiva del personale assente per ferie e tempestiva in caso di malattia, etc. allo scopo di evitare disservizi nell'espletamento del Servizio.

Prima dell'inizio delle prestazioni, l'Appaltatore dovrà consegnare a ACI Informatica l'elenco del personale -proprio e di ogni sub-contraente presente sul sito o presso locali ACI Informatica- corredato da un estratto del Libro Unico del Lavoro ("LUL") dei datori di lavoro.

L'Appaltatore garantisce altresì di astenersi dall'utilizzo di lavoro minorile, manodopera in nero o forme equivalenti di sfruttamento.

L'Appaltatore è ritenuto responsabile unico dell'operato del proprio personale impiegato nello svolgimento del Servizio.

L'Appaltatore è tenuto a fornire al suddetto personale indumenti di lavoro decorosi, adeguati alle caratteristiche dell'attività da svolgere e muniti di scritta di identificazione (da concordare con ACI Informatica) che rendano evidente il nome della Ditta di appartenenza.

Il personale in servizio dovrà mantenere un contegno riguardoso e corretto. In particolare è tenuto all'assoluto riserbo in ordine agli atti e ai documenti di cui viene a conoscenza nel corso dello svolgimento della prestazione.



Al personale in parola è fatto divieto assoluto di utilizzare le attrezzature e le apparecchiature ACI Informatica (fotocopiatrici, fax, telefoni, ecc.), che esulano dall'espletamento del Servizio.

L'Appaltatore s'impegna a richiamare e, se del caso, sostituire il personale che non osserva una condotta irreprendibile.

2.15.2 Clausola sociale

Ove espressamente previsto nel Bando di Gara, al fine di garantire i livelli occupazionali esistenti, in caso di cambio di gestione, l'Appaltatore ha l'obbligo di assorbire ed utilizzare prioritariamente nell'espletamento del Servizio, qualora disponibili, i lavoratori che già vi erano adibiti quali soci lavoratori o dipendenti del precedente aggiudicatario, nel rispetto di quanto previsto dalla contrattazione collettiva in materia di riassorbimento del personale.

2.15.3 Trattamento economico del personale

L'Appaltatore deve applicare, nei confronti di tutto il personale utilizzato per l'espletamento del Servizio, condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro applicabili vigenti ai sensi dell'art. 2070 del c.c. nonché ai sensi dell'art. 41 comma 13 D.Lgs. n. 36/2023 alla categoria e nelle località in cui si svolgono le prestazioni, e le condizioni risultanti da successive modifiche e integrazioni, nonché adempiere regolarmente agli oneri assicurativi, antinfortunistici, assistenziali, previdenziali e di qualsiasi specie, in conformità delle leggi, dei regolamenti e delle norme in vigore. L'Appaltatore è il solo responsabile dell'assolvimento degli obblighi predetti.

L'Appaltatore 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.

Gli obblighi relativi ai contratti collettivi nazionali di lavoro, di cui ai precedenti commi, vincolano l'Appaltatore anche nel caso in cui l'Appaltatore stesso non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità del Contratto / Accordo Quadro.

L'Appaltatore dichiara di essere in regola con il versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti.

L'Appaltatore è tenuto a presentare il Documento Unico di Regolarità Contributiva (D.U.R.C.) di cui alla Legge n. 266/2002 e s.m.i. o Dichiarazione Sostitutiva attestante l'assolvimento, da parte dell'Appaltatore stesso, degli obblighi legislativi e contrattuali nei confronti di INPS, INAIL e Cassa Edile.



La violazione degli obblighi ed oneri imposti dal presente articolo costituisce grave inadempimento e legittima ACI Informatica alla risoluzione in danno del Contratto di appalto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

2.15.4 Tutela del personale e relative provvidenze

L'Appaltatore è tenuto a provvedere alla tutela materiale e morale del personale dipendente comunque addetto all'esecuzione delle prestazioni oggetto del Contratto. A tale fine egli è tenuto, pertanto, ad osservare ed applicare tutte le norme sulla tutela, protezione, assicurazione ed assistenza dei lavoratori.

2.15.5 Prova degli adempimenti

L'Appaltatore, ove ACI Informatica lo richieda, deve dimostrare di aver adempiuto alle disposizioni richiamate nel presente documento, restando inteso che la mancata richiesta da parte di ACI Informatica non lo esonera in alcun modo dalle sue responsabilità.

2.15.6 Personale dei Subappaltatori

L'Appaltatore deve provvedere a che siano osservate le norme di cui al presente documento, anche da parte degli eventuali Subappaltatori nei confronti del loro personale dipendente.

La violazione degli obblighi ed oneri imposti dal presente articolo costituisce grave inadempimento e legittima ACI Informatica alla risoluzione in danno del Contratto di appalto ai sensi e per gli effetti dell'art. 1456 codice civile.

2.15.7 Orario di lavoro

Le attività oggetto del Contratto / Accordo quadro verranno normalmente eseguite nelle 5 (cinque) giornate feriali settimanali durante il normale orario di lavoro giornaliero del personale ACI Informatica, salvo diversa previsione nell'offerta o nel Contratto.

Eventuali attività che, per ragioni di erogazione del Servizio, dovessero essere eseguite in giornate festive, di sabato o comunque al di fuori del suddetto orario di lavoro, verranno preventivamente concordate e non daranno luogo, per l'Appaltatore, a maggiorazioni o compensi di sorta, fatto salvo quanto diversamente previsto e regolato dal Contratto.

Qualora, per proprie particolari esigenze, l'Appaltatore intendesse effettuare le attività nelle giornate di sabato, festive o al di fuori del normale orario di lavoro, dovrà farne richiesta con congruo anticipo a ACI Informatica.

ACI Informatica si riserva - a suo insindacabile giudizio - la facoltà di accordare o meno l'esecuzione delle attività nell'orario di lavoro richiesto.



2.16 Soggezioni particolari

L'Appaltatore non ha diritto a compensi di sorta in ragione di soggezioni che possano essergli comunque causate, anche all'interno eventualmente dei cantieri, dall'uso e dall'esercizio normale dei beni, installazioni e servizi, di ACI Informatica o di terzi, nonché da servitù a favore di ACI Informatica o di terzi e ciò, in particolare, per quanto riguarda la presenza e la manutenzione di fabbricati, manufatti, strade, corsi d'acqua, condotti.

2.17 Coordinamento e subordinazione rispetto ad altre attività di ACI Informatica

L'Appaltatore è tenuto a svolgere la propria prestazione senza arrecare molestia e, comunque, in modo da non ostacolare l'attività svolta direttamente da ACI Informatica e da altri fornitori o appaltatori che si trovassero ad operare negli stessi ambienti di lavoro, per il buon andamento dell'insieme di tutte le prestazioni.

In ogni modo, l'Appaltatore deve mantenere gli opportuni contatti con i suddetti fornitori e appaltatori in maniera da non ostacolare il migliore coordinamento di tutte le attività e senza che tale circostanza possa costituire causa giustificatrice della richiesta di maggiori oneri e/o compensi da parte dell'Appaltatore.

In caso di inosservanza delle disposizioni del presente articolo, l'Appaltatore è responsabile di tutte le conseguenze che ne possano derivare.

I luoghi in cui si eseguono le prestazioni oggetto del Contratto, devono essere mantenuti adeguatamente puliti ed ordinati dall'Appaltatore durante tutto il periodo di svolgimento delle prestazioni medesime.

2.18 Sospensione del Servizio

Qualora l'esecuzione del Servizio sia temporaneamente impedita da circostanze particolari, ai sensi dell'art. 121, co. 1, del D.Lgs. n. 36/2023, il RE, se nominato in alternativa il RUP, ha il diritto di disporre, dandone comunicazione all'Appaltatore mediante PEC, la sospensione dell'esecuzione, redigendo apposito verbale nel quale sono indicate: 1) le ragioni della sospensione e l'imputabilità delle medesime, 2) le prestazioni già effettuate, 3) le eventuali cautele per la ripresa dell'esecuzione del Contratto senza che siano richiesti ulteriori oneri, 4) i mezzi e gli strumenti esistenti che rimangono eventualmente nel luogo dove l'attività contrattuale era in corso di svolgimento.

Il verbale deve essere sottoscritto dall'Appaltatore.

La sospensione del Servizio permane per il tempo strettamente necessario a far cessare le cause che hanno imposto l'interruzione del Contratto. In ogni caso - e salvo che la so-



sospensione non sia dovuta a cause imputabili all'Appaltatore - la sua durata non è calcolata nel tempo fissato dal Contratto per l'esecuzione del Servizio.

La sospensione del Servizio può, altresì, essere disposta dal RUP per ragioni di necessità o di pubblico interesse. In tale evenienza, qualora la sospensione, o le sospensioni, durino per un periodo di tempo superiore ad un quarto della durata complessiva prevista per l'esecuzione del Servizio stesso, o comunque quando superino sei mesi complessivi, l'Appaltatore può chiedere la risoluzione del Contratto senza indennità; se la Stazione Appaltante si oppone, l'Appaltatore ha diritto alla rifusione dei maggiori oneri derivanti dal prolungamento della sospensione oltre i termini suddetti da quantificarsi ai sensi del successivo comma 7.

Salvo quanto previsto all'ultimo periodo del comma precedente, per la sospensione del Servizio, qualunque sia la causa, non è dovuto all'Appaltatore alcun compenso o indennizzo.

Ove, successivamente all'inizio dell'esecuzione del Servizio, il regolare svolgimento del medesimo sia parzialmente impedito per cause imprevedibili o di forza maggiore, il RE, se nominato, o in alternativa il RUP dispone la sospensione parziale del Servizio, dandone atto in apposito verbale. In tal caso, l'Appaltatore è tenuto a proseguire la parte del Servizio ancora eseguibile. La sospensione parziale del Servizio determina un differimento dei termini contrattuali, pari ad un numero di giorni determinato dal prodotto dei giorni di sospensione per il rapporto tra l'ammontare della parte del Servizio non eseguito per effetto della sospensione parziale e l'importo totale del Servizio previsto nello stesso periodo secondo il Programma cronologico.

Nel caso di sospensioni totali o parziali del Servizio disposte per cause diverse da quelle sopra indicate, l'Appaltatore può chiedere il risarcimento dei danni subiti, quantificato sulla base dei seguenti criteri:

- a. i maggiori oneri per spese generali infruttifere si ottengono sottraendo all'importo contrattuale l'utile di impresa nella misura del 10 % e le spese generali nella misura del 15 % e calcolando sul risultato la percentuale del 6,5 %. Tale risultato va diviso per il tempo contrattuale e moltiplicato per i giorni di sospensione e costituisce il limite massimo previsto per il risarcimento quantificato sulla base del criterio di cui alla presente lettera;
- b. la lesione dell'utile è riconosciuta coincidente con la ritardata percezione dell'utile di impresa, nella misura pari agli interessi legali di mora di cui all'art. 2, co. 1, lettera e) del D.Lgs. n. 231/2002, computati sulla percentuale del dieci per cento, rapportata alla durata dell'illegittima sospensione;
- c. il mancato ammortamento e le retribuzioni inutilmente corrisposte sono riferiti rispettivamente al valore reale, all'atto della sospensione, dei mezzi e strumenti esistenti nel luogo di esecuzione del Servizio accertati dal DEC;
- d. la determinazione dell'ammortamento avviene sulla base dei coefficienti annui fissati dalle vigenti norme fiscali.



Non appena siano venute a cessare le cause della sospensione, il RUP dispone la ripresa dell'esecuzione, indicando il nuovo termine contrattuale. Entro cinque giorni dalla disposizione della ripresa dell'esecuzione a cura del RUP, il DEC provvede alla redazione del verbale di ripresa, che deve essere sottoscritto anche dall'Appaltatore e deve riportare il nuovo termine contrattuale.

Le contestazioni dell'Appaltatore in merito alle sospensioni del Servizio devono essere iscritte, a pena di decadenza, nei verbali di sospensione e di ripresa del Servizio, salvo che per le sospensioni inizialmente legittime, per le quali è sufficiente l'iscrizione nel verbale di ripresa del Servizio. Qualora l'Appaltatore non intervenga alla firma dei verbali o si rifiuti di sottoscriverli, deve farne espressa riserva sul registro di contabilità.

2.19 Esecuzione in danno

Qualora la Stazione Appaltante rilevi che l'Appaltatore non stia eseguendo correttamente il Servizio ovvero l'eventuale prestazione connessa secondo il progetto, può assegnare un termine perentorio per l'adeguamento dello stesso agli elaborati progettuali.

Inoltre, qualora ACI Informatica rilevi qualunque arbitraria sospensione o palese, reiterato, inequivocabile rallentamento della esecuzione della prestazione/del servizio, derivante a titolo esemplificativo e non esaustivo da insufficiente disponibilità di mezzi, da inadeguata presenza di personale qualificato preposto alla esecuzione dell'appalto, ovvero da inefficienze organizzative, che incida sullo svolgimento, nei termini contrattualmente previsti, della prestazione/del servizio da parte dell'Appaltatore, determinando un ritardo nel completamento degli stessi, ACI Informatica può assegnare un termine perentorio entro il quale l'Appaltatore dovrà porre in essere le necessarie misure correttive e gli interventi indispensabili per recuperare il suddetto ritardo, condivisi preliminarmente con ACI Informatica stessa.

Qualora l'Appaltatore non dia corso alla esecuzione della prestazione/del servizio ordinato da ACI Informatica e/o delle misure correttive e agli interventi necessari, anche dopo l'assegnazione di un termine perentorio commisurato all'urgenza della prestazione/del servizio, ACI Informatica – ove possibile - ha il diritto di procedere direttamente alla loro esecuzione utilizzando, a tale fine, la propria organizzazione o quella di terzi ed ha facoltà di risolvere in danno il Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile.

I maggiori oneri che la Stazione Appaltante dovesse eventualmente sopportare rispetto a quelli derivanti dalla applicazione del Contratto sono a carico dell'Appaltatore.

3 PREZZI CONTRATTUALI



3.1 Condizioni ambientali

Con la firma del Contratto, l'Appaltatore riconosce di essersi reso pienamente edotto e di avere tenuto debito conto di tutte le condizioni ambientali e delle circostanze ed allee nonché condizionamenti e soggezioni ad esse connesse che possano avere influenza sulla esecuzione del Contratto e sulla determinazione dei prezzi. Dichiara quindi di avere preso esatta conoscenza dei luoghi dove deve essere eseguito il Servizio nonché, tra l'altro, delle condizioni ambientali e sanitarie della zona, delle condizioni meteorologiche, della distanza dei luoghi di lavoro dai centri abitati, della disponibilità dei mezzi di trasporto, della disponibilità e del costo effettivo della mano d'opera e di ogni altro elemento rilevante ai fini dell'esecuzione delle prestazioni appaltate.

Resta inteso che i prezzi contrattuali si intendono per prestazioni rese in sedi, locali o aree di ACI Informatica eseguite in qualunque situazione ambientale, comprese le operazioni di carico, trasporto e scarico dalle sedi ACI Informatica, o dell'Appaltatore, e viceversa.

3.2 Remuneratività dei prezzi contrattuali

Le prestazioni comunque necessarie per l'esecuzione del Contratto sono remunerate in base ai prezzi stabiliti nel Contratto / Accordo quadro e agli eventuali nuovi prezzi, di cui al successivo art. 3.4. I prezzi dei servizi si riferiscono al Servizio reso, interamente finito, completo in ogni sua parte anche accessoria, ed eseguito a regola d'arte, secondo le prescrizioni e modalità indicate nel Contratto, in esatta rispondenza allo scopo a cui è destinato.

Pertanto i prezzi dei servizi coprono tutti gli oneri derivanti dal Contratto / Accordo quadro, salvo quelli esplicitamente stabiliti a carico di ACI Informatica, ed inoltre tutti quelli che anche se non categoricamente espressi, siano necessari al perfetto compimento delle relative prestazioni.

Con la firma del Contratto l'Appaltatore riconosce la remuneratività del complesso dei prezzi contrattuali indicati nel Contratto / Accordo Quadro e che coprono quindi nel loro insieme l'utile dell'Appaltatore, oltre alla totalità delle spese, degli oneri ed allee inerenti il compimento delle prestazioni oggetto del Contratto / Accordo quadro e dei quali l'Appaltatore ha tenuto conto, secondo le prescrizioni, con le obbligazioni ed entro i termini in esso previsti.

In relazione alla riconosciuta remuneratività del complesso dei prezzi contrattuali, nessuna riserva potrà essere avanzata in ordine alla pretesa non remuneratività di singoli prezzi, qualunque possa essere la causa che l'abbia determinata.

Pertanto l'Appaltatore dichiara che tutti i prezzi contrattuali indicati nel Contratto / Accordo Quadro relativi alle prestazioni tengono conto degli oneri previsti nel Contratto in relazione alle prestazioni medesime, e che in particolare sono comprensivi – a titolo esemplificativo ma non esaustivo - anche degli oneri relativi a:



1. qualsiasi onere relativo alla corresponsione di paghe, premi, indennità, rimborsi e somministrazioni non previsti o comunque eccedenti quanto stabilito dai contratti collettivi di lavoro, avendo pienamente valutato il costo effettivo della mano d'opera anche in base alle condizioni ambientali, nonché per ogni onere riferentesi al lavoro straordinario, festivo o notturno che fosse comunque necessario per lo svolgimento del Servizio nei termini contrattuali;
2. tutta la documentazione richiesta all'Appaltatore nei documenti tecnici;
3. apprestamento delle eventuali attrezzature per l'esecuzione del Servizio;
4. altri oneri previsti nel Contratto per eventuali altre prestazioni accessorie a carico dell'Appaltatore;
5. tutti gli oneri per lo svolgimento delle pratiche con Enti Pubblici e Privati per i depositi cauzionali previsti dalla normativa applicabile e per l'ottenimento dei permessi, nulla-osta, licenze e certificati occorrenti per l'esecuzione delle prestazioni (ad es. permessi di lavoro rilasciati da tutti gli enti interessati, etc.) come meglio precisato nelle Specifiche Tecniche e l'osservanza delle disposizioni eventualmente impartite da tutti gli Enti e/o Autorità competenti per il territorio e l'ambiente;
6. costi generali della sicurezza relativi allo svolgimento delle prestazioni;
7. tutti gli eventuali oneri derivanti dal dover provvedere - ai fini dello smaltimento, quale produttore dei rifiuti prodotti nel corso delle prestazioni - alla gestione dei rifiuti stessi conformemente alle vigenti normative.

Nel caso di prestazione di Servizio ICT, i prezzi sono altresì comprensivi – a titolo esemplificativo ma non esaustivo - di:

- a) esecuzione delle eventuali prove/attivazioni e test;
- b) altri oneri previsti nel Contratto per eventuali altre prestazioni accessorie a carico dell'Appaltatore;
- c) dell'installazione e configurazione del Servizio;
- d) ulteriori oneri eventualmente previsti dal Contratto di appalto.

3.3 Revisione prezzi

È ammessa la revisione prezzi con le modalità definite nel Contratto in accordo con l'art 60 del D.Lgs. 36/2023.

3.4 Nuovi prezzi

Le ulteriori prestazioni che si rendessero necessarie nel periodo di validità del Contratto / Accordo quadro, dovranno essere preventivamente autorizzate per iscritto da ACI Informatica mediante specifiche varianti al Contratto / Accordo quadro, nelle quali verranno



stabiliti le eventuali estensioni di attività, i nuovi elementi di costo da inserire ed i relativi nuovi prezzi.

Tali nuovi prezzi sono determinati tenendo conto di tutte le norme contrattuali, mediante ragguaglio con i prezzi contrattuali relativi a prestazioni consimili, ovvero, quando ciò non sia possibile, totalmente o parzialmente, mediante nuove analisi effettuate avendo a riferimento i prezzi alla data di formulazione dell'offerta, in contraddittorio con l'Appaltatore.

Anche in caso di disaccordo sulla valutazione degli stessi, l'Appaltatore è tenuto a dare corso all'esecuzione delle prestazioni oggetto dei nuovi prezzi.

Ove dalla determinazione dei nuovi prezzi risultino maggiori spese rispetto alle somme previste nel quadro economico, i prezzi sono approvati dalla Stazione Appaltante su proposta del RUP.

4 ACCETTAZIONE DEL SERVIZIO E CONTABILITA' DELLE PRESTAZIONI

4.1 Responsabilità e danni

Per tutta la durata di svolgimento del Servizio e fino al termine del rapporto contrattuale, l'Appaltatore è responsabile dei danni arrecati a persone e cose di ACI Informatica e/o di terzi, direttamente e/o indirettamente connessi all'appalto. Sono compresi nelle responsabilità dell'Appaltatore gli eventuali danni che dovessero verificarsi nelle diverse fasi di espletamento del Servizio conformemente a quanto previsto dal Contratto.

In caso di subappalto, l'Appaltatore e il subappaltatore sono responsabili in solido nei confronti di ACI Informatica, in relazione alle prestazioni oggetto del contratto di subappalto.

L'Appaltatore è altresì responsabile della corretta esecuzione del Servizio, anche se effettuata da terzi collaboratori, subappaltatori e/o subcontraenti. L'Appaltatore assume inoltre nei confronti di ACI Informatica la piena responsabilità per tutte le obbligazioni derivanti dal Contratto, garantendo anche per l'operato dei suoi collaboratori e/o subappaltatori e/o subcontraenti.

L'Appaltatore si impegna, conseguentemente, a tenere ACI Informatica indenne e manlevata da ogni responsabilità per incidenti e/o infortuni che, nell'esecuzione del Contratto, possano derivare al personale dell'Appaltatore stesso e/o di ACI Informatica, ovvero a loro collaboratori e/o a terzi.

L'Appaltatore si impegna ad agire con la massima diligenza e ad assumere ogni iniziativa necessaria e/o opportuna per evitare danni di qualsivoglia genere e natura a persone e cose. Ove questi si verificchino, l'Appaltatore dovrà in ogni caso provvedere al completo e sollecito risarcimento degli stessi.



Nel caso in cui, in corso di esecuzione del Servizio, si verificano sinistri alle persone o danni a cose, sarà cura della Rappresentanza di ACI Informatica compilare una relazione recante la descrizione del fatto e delle presumibili cause, e adottare gli opportuni provvedimenti finalizzati a ridurre le conseguenze dannose. Restano in ogni caso a carico dell'Appaltatore:

- a) tutte le misure e tutti gli adempimenti per evitare il verificarsi di danni all'ambiente, alle persone e alle cose nell'esecuzione dell'appalto;
- b) l'onere per il ripristino della situazione preesistente nonché il completo e sollecito risarcimento di danni ai luoghi, a cose o a terzi determinati da mancata, tardiva o inadeguata assunzione dei necessari provvedimenti. L'accertamento, la valutazione e la liquidazione dei danni saranno eseguiti dall'Appaltatore in contraddittorio con i danneggiati. L'Appaltatore si impegna in ogni caso a far firmare, all'atto della liquidazione, da persone che hanno giuridicamente la facoltà di impegnare l'Appaltatore stesso, dichiarazioni ampiamente liberatorie per ACI Informatica.

Fatti salvi i casi di caso fortuito o forza maggiore, l'Appaltatore non può pretendere indennizzi per i danni che dovessero derivare a opere e provviste. Nessun indennizzo è in ogni caso dovuto quando a determinare il danno abbia concorso la colpa dell'Appaltatore ovvero dei soggetti dei quali è tenuto a rispondere.

In caso di caso fortuito o forza maggiore, l'Appaltatore è tenuto a prendere, tempestivamente ed efficacemente, tutte le misure preventive atte ad evitare ovvero limitare i danni e a darne comunicazione alla Rappresentanza di ACI Informatica entro il termine di 5 giorni dalla data dell'evento, a pena di decadenza dal diritto all'indennizzo.

Al fine di determinare l'importo da riconoscere a titolo di indennizzo, il DEC, in presenza dell'Appaltatore, provvede alla redazione di un processo verbale, accertando lo stato delle cose dopo il danno (rapportato allo stato precedente), le cause dei danni (precisando l'eventuale caso fortuito o di forza maggiore), l'eventuale negligenza, con indicazione del responsabile, l'osservanza o meno delle regole dell'arte e delle prescrizioni del RUP o ove nominato del RE, le eventuali omissioni delle cautele necessarie a prevenire i danni.

Resta inteso che l'indennizzo è limitato alle spese sostenute e documentate per il ripristino delle opere e non potrà superare il corrispondente importo contrattuale, decurtato dell'utile d'impresa e delle spese generali come risultanti dall'offerta.

4.2 Penali

In caso di ritardo o di difformità nell'esecuzione e nel completamento del Servizio rispetto al termine finale previsto nel Contratto, l'Appaltatore dovrà corrispondere a ACI Informatica una somma a titolo di penale nella misura giornaliera indicata nel Contratto stesso.

Il Contratto potrà altresì prevedere termini intermedi il cui mancato rispetto potrà comportare l'applicazione di penali, nella misura giornaliera indicata nel Contratto medesimo, che potranno essere riaccreditate, senza interessi o indennizzi comunque denominati,



laddove l'Appaltatore provveda a recuperare i ritardi intermedi, ultimando il Servizio nel rispetto del termine finale.

È espressamente fatta salva la risarcibilità dell'ulteriore danno, in aggiunta all'importo delle penali precisate nel Contratto di appalto. Il suddetto danno potrà consistere tanto nel danno emergente che nel lucro cessante.

I relativi importi saranno trattenuti all'atto del pagamento delle fatture in corrispondenza alle prestazioni per le quali il termine contrattuale e/o le condizioni contrattuali siano disattese, ovvero all'atto del pagamento di quanto a qualsiasi titolo dovuto all'Appaltatore in relazione al Contratto, ovvero, in mancanza, avvalendosi, in tutto o in parte, della cauzione prestata.

Tutte le penali verranno applicate previa contestazione dell'addebito e valutazione delle deduzioni addotte dall'Appaltatore e comunicate dall'Appaltatore stesso ad ACI Informatica nel termine massimo di 5 (cinque) giorni dalla contestazione stessa.

ACI Informatica si riserva la facoltà, in qualunque tempo, di risolvere di diritto il Contratto ai sensi e per gli effetti dell'art. 1456 del Codice Civile, oltre a chiedere il risarcimento di tutti i danni, nei seguenti casi:

- qualora l'importo complessivo delle penali inflitte all'Appaltatore raggiunga nel periodo di un mese la somma complessiva pari al 20% del corrispettivo maturato nel periodo;
- qualora l'ammontare complessivo delle penali inflitte raggiunga il 10% del corrispettivo contrattuale massimo dell'intero Servizio. In particolare, nel caso di appalti basati su un Accordo Quadro i cui singoli servizi saranno avviati mediante Accordi Attuativi, l'importo applicato a titolo di penale non potrà eccedere il 10% rispetto all'importo del singolo Accordo Attuativo e, in ogni caso, gli importi cumulati per penalità non potranno eccedere il 10% dell'importo complessivo dell'Accordo Quadro. In ogni caso non saranno applicate penali superiori al 10% del corrispettivo complessivo del Contratto / Accordo Quadro ai sensi dell'art. 113 bis del codice appalti così come modificato dalla legge del 3 maggio 2019 n. 37.

I provvedimenti di applicazione delle penali d'importo superiore, singolarmente o cumulativamente, all'1% del valore economico del Contratto / Accordo Quadro saranno comunicate tempestivamente all'ANAC in ottemperanza all'art 95 comma 1 lettera e), ai fini dell'iscrizione sul Casellario Informatico di cui all'art. 222, comma 10, del codice appalti.

L'applicazione delle penali, non esime l'Appaltatore dall'osservanza di tutti gli obblighi contrattuali e di legge inerenti la corretta esecuzione del Contratto. Peraltro, la richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso l'Appaltatore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e/o che ha fatto sorgere l'obbligo di pagamento della penale stessa.

Ferma restando l'applicazione delle penali previste nel presente articolo, ACI Informatica si riserva di richiedere il maggior danno, sulla base di quanto disposto all'articolo 1382



del Codice Civile, nonché la risoluzione del Contratto / Accordo Quadro nell'ipotesi di grave e reiterato inadempimento.

Fatto salvo quanto previsto nei precedenti commi, l'Appaltatore si impegna espressamente a rifondere l'ammontare di eventuali oneri che ACI Informatica dovesse sostenere – anche per causali diverse da quelle di cui al presente articolo – a seguito di fatti che siano ascrivibili a responsabilità dell'Appaltatore stesso.

ACI Informatica, per i crediti derivanti dall'applicazione delle penali di cui al presente articolo, potrà, a sua insindacabile scelta, avvalersi della cauzione di cui al successivo art. 4.5, senza bisogno di diffida o procedimento giudiziario, ovvero compensare finanziariamente il credito con quanto dovuto all'Appaltatore a qualsiasi titolo, quindi anche con i corrispettivi maturati.

4.3 Modalità di fatturazione e pagamento. Interessi sui pagamenti

La fatturazione sarà effettuata elettronicamente secondo il formato "FatturaPA" nei termini previsti dalla normativa vigente secondo le modalità generali qui di seguito elencate, fermo restando che tali modalità potranno essere modificate e/o maggiormente dettagliate nel Contratto, in relazione alle specificità:

- tutti i servizi *task* chiavi in mano e tutti i servizi *task* saranno fatturati mensilmente sulla base dello stato di avanzamento;
- tutti i servizi a misura saranno fatturati mensilmente sulla base delle effettive giornate erogate dalle diverse figure professionali;
- nel caso in cui l'oggetto del Contratto preveda anche la fornitura di prodotti, sulla base dell'effettivo installato, accettato da ACI Informatica con opportuno verbale.

La fatturazione del corrispettivo relativo al Servizio verrà effettuata con riferimento al consuntivo dei servizi oggetto del Contratto correttamente eseguiti dall'Appaltatore, collaudati con esito positivo, e accettati da ACI Informatica ai sensi del precedente art. 2.9, e sulla base dei parametri quantitativi.

In particolare, il pagamento del corrispettivo relativo al Servizio sarà regolato con la presentazione di fatture emesse dall'Appaltatore in base agli stati di avanzamento delle prestazioni (SAL mensili o con le diverse cadenze eventualmente stabilite nel Contratto). Il SAL dovrà essere redatto dall'Appaltatore sul modello predisposto dal DEC di ACI Informatica, anche se sulla base di eventuali documenti preparatori e di computo predisposti dall'appaltatore e verificati dal Responsabile del Contratto nominato dall'Appaltatore. Il SAL di ciascun mese (o della diversa periodicità stabilita nel Contratto) dovrà essere presentato dall'Appaltatore entro il giorno 5 del mese successivo al periodo di riferimento. Il SAL sarà approvato integralmente o parzialmente dalla Rappresentanza di ACI Informatica entro 30 (trenta) giorni naturali consecutivi dalla data di presentazione da parte dell'Appaltatore. Il SAL approvato costituisce il riferimento per la fatturazione delle attività; in mancanza di approvazione non potranno essere emesse le fatture corrispondenti. L'Appaltatore non potrà emettere fatture per un importo superiore a quello approvato.



Ciascuna fattura elettronica, che dovrà essere emessa e resa disponibile nei termini previsti dalla normativa vigente, dovrà

- (i) indicare espressamente la causale del pagamento,
- (ii) contenere i riferimenti al Contratto relativi al numero, alla data, e al codice CIG (Codice Identificativo Gara),
- (iii) essere emessa secondo il formato “FatturaPA” nei confronti di: ACI Informatica S.p.A., Via Fiume delle Perle n. 24 – 00144 ROMA, Codice Fiscale: 00405030586, Partita IVA: 00883311003, Codice Univoco della Pubblica Amministrazione N5BL4E .

Nella Sezione Dati contratto (2.1.3) della fattura elettronica devono essere valorizzati i seguenti dati:

- (2.1.3.2) Numero ordine
- (2.1.3.3) Data dell'ordine
- (2.1.3.7) Codice CIG

inoltre, nel campo (2.2.2.7) Esigibilità IVA deve essere riportato il valore ‘S’ del file .xml, a indicare che le fatture sono state emesse in regime di scissione dei pagamenti (split payment) IVA ai sensi dell’art. 17- ter DPR 633/72.

Ai fini del pagamento del corrispettivo, e comunque ove vi siano fatture elettroniche in pagamento, ACI Informatica procederà, per quanto di competenza e secondo la normativa vigente, ad acquisire il documento unico di regolarità contributiva (D.U.R.C.), attestante la regolarità in ordine al versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti; ogni somma che, a causa della mancata produzione delle certificazioni di cui al presente comma, non venga corrisposta da ACI Informatica, non produrrà alcun interesse.

Le suddette fatture elettroniche dovranno essere corredate da una nota dell’Appaltatore attestante la perfetta esecuzione delle prestazioni richieste, il rispetto degli adempimenti previsti e dei livelli di servizio definiti, controfirmate dal responsabile dell’Ufficio interessato dell’Appaltatore stesso.

In esito alla positiva conclusione della verifica di conformità, l’importo delle fatture di cui al presente articolo sarà bonificato a 30 (trenta) giorni decorrenti dalla data della ricezione, i cui estremi identificativi, unitamente alle generalità e al codice fiscale delle persone delegate a operare su tale conto, saranno comunicati ad ACI Informatica nei termini di cui all’art. 3, comma 7, della Legge del 13 agosto 2010 n. 136, così come modificata dal D.L. del 12 novembre 2010 n. 187.

Il corrispettivo che l’Appaltatore dovrà indicare in fattura elettronica sarà pari al 99,50 % di quello maturato nel periodo di riferimento. La differenza dello 0,50% costituirà la trattenuta ex art. 11, comma 6, del D.Lgs. 36/2023 e s.m.i. che sarà svincolata soltanto in sede di liquidazione finale a conclusione ed accettazione del Servizio, previa presentazione di regolare fattura.



ACI Informatica rientra tra i soggetti nei confronti dei quali si applica la scissione dei pagamenti (split payment) IVA ai sensi dell'art. 17-ter, comma 1bis, del DPR 633/72, così come modificato dall'art. 3 del D.L. n. 148 del 16/10/2017. Pertanto le fatture elettroniche emesse nei confronti di ACI Informatica dovranno riportare la dicitura "fattura elettronica emessa in regime di scissione dei pagamenti (split payment) IVA ai sensi dell'art. 17-ter DPR 633/72".

In ottemperanza alle disposizioni previste dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973, ACI Informatica in qualità di società a totale partecipazione pubblica, per ogni pagamento di importo superiore ai limiti di legge, procederà a verificare se il beneficiario è inadempiente all'obbligo di versamento derivante dalla notifica di una o più cartelle di pagamento per un ammontare complessivo pari almeno a tale importo. Nel caso in cui l'Agenzia delle Entrate-Riscossione (già Equitalia S.p.A.), ai sensi dell'art. 3 del Decreto Ministeriale 40/2008, comunichi che risulta un inadempimento a carico del beneficiario e sospenda e/o disponga il versamento, totale o parziale, delle somme oggetto di verifica all'Agente della riscossione, ACI Informatica darà seguito a tali prescrizioni e nessuna pretesa, per interessi o altro, potrà essere avanzata nei confronti della stessa ACI Informatica.

In caso di contestazione da parte di ACI Informatica i pagamenti saranno sospesi sino alla definitiva verifica di conformità del Servizio e dell'accertamento della regolarità del Servizio stesso.

In caso di ritardo nei pagamenti oltre il termine suddetto vengono riconosciuti all'Appaltatore gli interessi legali di mora di cui al D.Lgs. n. 231/2002 e s.m.i..

4.4 Tracciabilità dei flussi finanziari

Ai sensi e per gli effetti di cui all'art. 3 della Legge 13 agosto 2010 n. 136, così come modificato e integrato dal D.L. 187/2010 e dalla relativa legge di conversione 217/2010, tutti i movimenti finanziari relativi alla realizzazione del Servizio oggetto del Contratto/ Accordo Quadro devono essere registrati dall'Appaltatore su un conto corrente dedicato e devono essere effettuati esclusivamente tramite lo strumento del bonifico bancario o postale o con altri strumenti idonei a garantire la piena tracciabilità delle operazioni (cd "obbligo di tracciabilità"), con le indicazioni richieste dalla Legge (ad esempio, il Codice CIG – Codice Identificativo Gara - della commessa, da indicare nella causale delle fatture elettroniche emesse, unitamente al riferimento al Contratto).

L'inosservanza dell'obbligo di tracciabilità di cui al precedente comma determina la nullità assoluta del Contratto/ Accordo Quadro ai sensi dell'art. 1418 del Codice Civile e dell'art. 3 comma 8 della legge n. 136/2010.

In tutti i casi in cui le transazioni finanziarie relative allo svolgimento del Servizio oggetto del Contratto/ Accordo Quadro siano state eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle opera-



zioni, si determinerà la risoluzione immediata e di diritto del Contratto/ Accordo Quadro stesso.

L'Appaltatore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità dei flussi finanziari di cui alla Legge n. 136/2010, deve darne immediata comunicazione all'ACI Informatica ed alla Prefettura - Ufficio Territoriale del Governo della provincia di Roma.

L'Appaltatore provvederà altresì a comunicare ad ACI Informatica – nei termini di cui all'art. 3 comma 7 della L. 136/2010, così come modificato dal D.L. 187/2010 e dalla relativa legge di conversione 217/2010 - gli estremi identificativi (Codice IBAN) del conto corrente dedicato intestato all'Appaltatore stesso, unitamente alle generalità e al codice fiscale delle persone delegate a operare su tale conto. L'Appaltatore dovrà utilizzare il proprio conto corrente dedicato in conformità a quanto previsto dalla Legge 13 agosto 2010 n. 136 e s.m.i.. L'Appaltatore dichiara inoltre che il predetto conto corrente è conforme a quanto previsto dalla L. 136/2010 'Piano straordinario contro le mafie, nonché Delega al Governo in materia di normativa antimafia' e s.m.i.. L'Appaltatore è obbligato a comunicare, sotto la propria esclusiva responsabilità, alla Stazione Appaltante, entro e non oltre 7 giorni, mediante PEC o Raccomandata A.R. da inoltrarsi presso ACI Informatica – Direzione Approvvigionamenti e Logistica e Direzione Amministrazione Bilancio e Controllo), via Fiume delle Perle 24, 00144 Roma - ogni modifica relativa agli estremi identificativi del conto corrente indicato, nonché alle generalità e codice fiscale delle persone delegate ad operarvi. In difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, l'Appaltatore non potrà sollevare eccezioni in ordine a eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.

Per quanto non espressamente previsto dal presente articolo, le Parti rinviano alla disciplina dettata dall'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i.

4.5 Cauzione

Entro 10 giorni dalla data di ricevimento della comunicazione di efficacia dell'aggiudicazione definitiva, l'Appaltatore dovrà costituire ed inviare a ACI Informatica apposita fidejussione nella misura prevista dal Contratto a garanzia, a titolo esemplificativo e non esaustivo:

- del corretto adempimento delle obbligazioni derivanti dall'accettazione del Contratto e della corretta esecuzione dello stesso e salvo il maggior danno;
- del risarcimento a ACI Informatica dei danni derivanti dall'inadempimento delle obbligazioni contrattuali;
- di tutte le obbligazioni che fanno capo all'Appaltatore inerenti il pagamento dei trattamenti retributivi e dei contributi previdenziali dovuti ai propri lavoratori;
- del risarcimento a ACI Informatica delle maggiori somme che questa avesse eventualmente pagato in più durante l'espletamento del Contratto, unitamente a quanto



altro dovuto, a qualsiasi titolo, dall'Appaltatore a ACI Informatica, al momento della chiusura del rapporto contrattuale.

Ai sensi dell'art. 117 comma 12 del D.Lgs. n. 36/2023, la garanzia fideiussoria/polizza assicurativa prestata per la sottoscrizione del Contratto deve essere conforme agli schemi tipo approvati con decreto del Ministro delle imprese e del made in Italy di concerto con il Ministro delle infrastrutture e dei trasporti e con il Ministro dell'economia e delle finanze

La cauzione è progressivamente svincolata a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80% dell'iniziale importo garantito.

L'ammontare residuo della cauzione definitiva deve permanere fino alla data di emissione del certificato di verifica di conformità/ / di regolare esecuzione, o comunque fino a dodici mesi dalla data di ultimazione del Servizio risultante dal relativo certificato.

Lo svincolo è automatico, senza necessità di nulla osta della Stazione Appaltante, con la sola condizione della preventiva consegna all'istituto garante, da parte dell'Appaltatore, di un documento, in originale o in copia autentica, attestante l'avvenuta positiva esecuzione.

In ogni caso l'Appaltatore è obbligato a reintegrare la cauzione di cui ACI Informatica si sia avvalsa, in tutto o in parte durante l'esecuzione del Contratto entro il termine di 10 (dieci) giorni dal ricevimento della richiesta della stessa ACI Informatica e, in caso di proroga della durata del Contratto di appalto, a produrre una fideiussione con una nuova durata che tenga conto della stessa proroga. A tal fine le parti concordano espressamente che la violazione di quanto sopra disposto dà diritto a ACI Informatica di risolvere in danno il Contratto ai sensi e per gli effetti dell'articolo 1456 c.c., con conseguente diritto di ACI Informatica stessa al risarcimento dei danni.

Il pagamento della rata di saldo è subordinato alla costituzione di una cauzione o di una garanzia fideiussoria bancaria o assicurativa, in conformità allo schema tipo approvato pari all'importo della medesima rata di saldo maggiorato del tasso di interesse legale applicato per il periodo intercorrente tra la data di emissione del certificato di verifica di conformità/di collaudo positivo/di regolare esecuzione e l'assunzione del carattere di definitività dei medesimi.

4.6 Cessione dei crediti

Previa espressa accettazione di ACI Informatica, sulla base di quanto previsto dal presente articolo, è ammessa la cessione dei crediti ai sensi dell'art. 120, comma 12 del D.Lgs. n. 36/2023 ed in applicazione di quanto disposto dalla L. n. 52/1991.

Ai fini dell'opponibilità ad ACI Informatica della cessione dei crediti, l'atto di cessione dovrà essere stipulato con atto pubblico o scrittura privata autenticata e dovrà essere notificato alla Stazione Appaltante, mediante PEC o Raccomandata A.R. da inoltrarsi presso ACI Informatica S.p.A. – Direzione Approvvigionamenti e Logistica e Direzione Ammini-



strazione, Bilancio e Controllo, via Fiume delle Perle n.° 24 – 00144 Roma, indicando espressamente il codice IBAN completo di numero di conto corrente (bancario/postale) sul quale deve essere effettuato il pagamento. Al suddetto conto corrente si applicano le disposizioni sulla tracciabilità dei flussi finanziari, di cui alla legge n. 136/2010 e s.m.i..

L'atto di cessione dovrà contenere l'indicazione del cedente, del cessionario, dell'importo e della natura del credito ceduto.

Il mancato rispetto di ciascuna delle anzidette prescrizioni determina l'inefficacia e l'inopponibilità della cessione nei confronti di ACI Informatica.

Resta inteso che l'efficacia dell'atto di cessione è subordinata all'approvazione espressa – da rendersi entro il termine di 45 giorni dalla notifica della cessione – di ACI Informatica, che si riserva di verificare, di volta in volta, la sussistenza dei presupposti giuridici e contabili per l'opponibilità della cessione medesima nonché l'effettivo pagamento, da parte del cedente, nei confronti dei subappaltatori e/o subcontraenti.

Resta inteso che, anche in caso di accettazione espressa della cessione, ACI Informatica potrà opporre al cessionario tutte le eccezioni opponibili al cedente e derivanti dall'applicazione del presente Contratto.

È fatto divieto all'Appaltatore di conferire, in qualsiasi forma, procure all'incasso.

4.7 Contestazioni

Il RE, se nominato, o il DEC, deve dare comunicazione al RUP delle contestazioni insorte in relazione a fatti o aspetti tecnici che possono influire sull'esecuzione del Contratto, redigendo, in contraddittorio con l'Appaltatore o, in difetto di quest'ultimo, in presenza di due testimoni, un processo verbale delle circostanze contestate.

Ove il processo verbale sia stato redatto in assenza dell'Appaltatore, copia del medesimo è comunicata all'Appaltatore per la formulazione di eventuali osservazioni, da rendere al RE, se nominato, o al DEC, entro il termine di 8 giorni. In mancanza di osservazioni entro il predetto termine, le risultanze del verbale si intendono definitivamente accettate.

Il processo verbale deve essere firmato dall'Appaltatore, in persona del Responsabile del Contratto, ovvero dai testimoni, ed essere trasmesso, unitamente alle eventuali osservazioni, al RUP.

La decisione del RUP è comunicata all'Appaltatore il quale ha l'obbligo di uniformarvisi, salvo il diritto di iscrivere riserva.

4.8 Imposte e tasse

Tutte le tasse, imposte, diritti ed oneri di qualsivoglia natura gravanti sul Servizio saranno a carico dell'Appaltatore, ad eccezione dell'I.V.A. e di quelle che la legge espressamente pone a carico della Stazione Appaltante.



4.9 Adempimenti ex art. 17-bis del D.Lgs. 9 luglio 1997, n. 241

Qualora l'appaltatore sia risultato affidatario da ACI Informatica di uno o più contratti, per un importo complessivo annuo superiore a 200.000 €, caratterizzati:

- dal prevalente utilizzo di manodopera prestata presso le sedi di ACI Informatica,
- dall'utilizzo di beni strumentali di proprietà del committente,

ACI Informatica richiederà all'appaltatore copia delle deleghe di pagamento relative al versamento delle ritenute fiscali per i lavoratori dipendenti direttamente impiegati nei servizi.

A tal fine, l'appaltatore effettuerà distinti versamenti, con F24 specifico per ACI Informatica, senza possibilità di compensazione delle ritenute dovute con propri crediti fiscali.

Inoltre l'appaltatore trasmetterà ad ACI Informatica entro i 5 giorni lavorativi successivi alla scadenza del versamento delle ritenute:

- copia delle deleghe di pagamento
- l'elenco nominativo di tutti i lavoratori, identificati mediante codice fiscale, coinvolti nel servizio nel mese precedente, con:
 - o il dettaglio delle ritenute eseguite nel mese precedente nei confronti dello stesso lavoratore con separata indicazione di quelle relative alla prestazione effettuata dal committente.
 - o l'ammontare della retribuzione corrisposta al dipendente in relazione alla prestazione
 - o il dettaglio delle ore di lavoro prestate da ciascun lavoratore nell'esecuzione del servizio.

In caso di mancata trasmissione dei dati di cui sopra da parte dell'appaltatore ovvero appurato l'omesso o insufficiente versamento delle ritenute da parte dell'appaltatore, ACI Informatica sospenderà il pagamento dei corrispettivi maturati (sino a concorrenza del 20% del valore complessivo del servizio, ovvero per un importo pari alle ritenute non versate ma risultanti dalla documentazione trasmessa), dandone comunicazione entro 90 giorni all'ufficio dell'Agenzia delle Entrate competente per territorio.

Gli obblighi di cui ai commi precedenti non trovano applicazione se l'appaltatore comunica ad ACI Informatica, allegando la relativa certificazione rilasciata dall'Agenzia delle Entrate, la sussistenza nell'ultimo giorno del mese precedente a quello della scadenza (5 giorni successivi alla scadenza del versamento) di entrambi i seguenti requisiti:

- di essere in attività da almeno 3 anni ed in regola con gli obblighi dichiarativi e di avere eseguito nel corso dei periodi d'imposta cui si riferiscono le dichiarazioni dei redditi presentate nell'ultimo triennio complessivi versamenti registrati nel conto fiscale per un importo superiore al 10% dell'ammontare dei ricavi e compensi risultanti dalle dichiarazioni medesime;



- di non avere iscrizioni a ruolo o accertamenti esecutivi o avvisi di accertamento, affidati agli agenti della riscossione relativi alle imposte sul reddito, IRAP, ritenute e contributi previdenziali per importi superiori a 50.000 euro, per i quali siano ancora dovuti pagamenti o per i quali non siano stati accordati provvedimenti di sospensione.

In caso di subappalto gli obblighi di cui ai commi precedenti posti in capo all'appaltatore si estendono anche al subappaltatore.

5 SCIoglimento del Contratto

5.1 Risoluzione del Contratto

Il Contratto di appalto, ivi incluso l'Accordo Quadro, può essere risolto da ACI Informatica, ai sensi delle disposizioni del Codice Civile e dell'art. 122 del D.Lgs. n. 36/2023, e in tutti i casi previsti nel presente Capitolato ove si fa espresso richiamo all'articolo 1456 codice civile e alla risoluzione di diritto, e nel Contratto, come meglio dettagliato nel Contratto stesso.

ACI Informatica si riserva di risolvere il Contratto/Accordo Quadro nel caso in cui l'Appaltatore venga a trovarsi in una delle condizioni previste dall'art. 94, 95, 97 e 98 del D.Lgs. 31 marzo 2023 n. 36 che non consentono di concludere contratti con la Pubblica Amministrazione. ACI Informatica risolverà il Contratto/Accordo Quadro nel caso che siano applicate nei confronti dell'Appaltatore misure di prevenzione di cui al D.Lgs. 06/09/2011 n 159 e s.m.i..

Nei casi di cui al comma precedente la risoluzione si verifica di diritto e con effetto immediato mediante unilaterale dichiarazione di ACI Informatica, da farsi con posta elettronica certificata.

5.2 Procedimento di risoluzione del Contratto

Nelle ipotesi di risoluzione di cui all'art. 122, comma 3 del D.Lgs. 36/2023, la Stazione Appaltante, previa eventuale acquisizione delle informazioni utili da parte della Rappresentanza di ACI Informatica, provvederà a contestare all'Appaltatore gli addebiti, assegnando al medesimo un termine non inferiore a 15 (quindici) giorni naturali e consecutivi dal ricevimento della contestazione per porre rimedio all'inadempimento in cui esso sia incorso, laddove l'inadempimento sia suscettibile di rimedio, e valutando altresì le con-



controdeduzioni che l'Appaltatore dovrà fornire alla Stazione Appaltante entro 15 (quindici) giorni naturali e consecutivi dal ricevimento della contestazione.

Ove l'Appaltatore non rimedi all'inadempimento nel termine ad esso assegnato ovvero non fornisca le controdeduzioni richieste, ovvero se ad insindacabile giudizio di ACI Informatica le medesime non siano ritenute soddisfacenti, la Stazione Appaltante potrà disporre la risoluzione del Contratto.

ACI Informatica potrà tenere conto delle controdeduzioni presentate anche per valutare se estendere il termine per rimediare all'inadempimento.

Nell'ipotesi in cui la Stazione Appaltante proceda alla risoluzione del Contratto, spetterà all'Appaltatore esclusivamente il pagamento delle prestazioni regolarmente eseguite, decurtato degli oneri aggiuntivi derivanti dalla risoluzione del Contratto; ACI Informatica avrà diritto a far completare nel modo che riterrà più opportuno le prestazioni oggetto del Contratto, addebitandone la maggiore spesa sostenuta all'Appaltatore.

In caso di risoluzione del Contratto per colpa dell'Appaltatore, ACI Informatica avrà inoltre diritto al risarcimento del danno e sarà legittimata ad escutere la cauzione definitiva dal medesimo prestata nonché a rivalersi sulle somme a qualunque titolo detenute dallo stesso.

Resta comunque espressamente inteso che il mancato esercizio della facoltà di risoluzione da parte della Stazione Appaltante non potrà mai essere invocato dall'Appaltatore al fine di escludere o limitare gli oneri e i danni che la Stazione Appaltante stessa dovesse sopportare per fatto dell'Appaltatore medesimo.

5.3 Recesso dal Contratto

5.3.1 Recesso ordinario

E' in facoltà di ACI Informatica, in ogni momento e qualunque sia lo stato di svolgimento del Servizio oggetto del Contratto, di recedere dallo stesso, ivi incluso il Contratto Quadro, secondo le modalità e criteri di cui all'art. 123 del D.Lgs. n. 36/2023.

L'Appaltatore ha l'obbligo, entro il termine di 30 (trenta) giorni naturali e consecutivi decorrenti dal ricevimento della comunicazione di cui al comma 2 dello stesso art. 123 del D.Lgs. n. 36/2023, ovvero nel diverso termine indicato nella comunicazione predetta, di consegnare ad ACI Informatica i servizi eseguiti. All'Appaltatore, a definitiva e completa tacitazione di ogni diritto e pretesa, verranno riconosciuti esclusivamente, il pagamento delle prestazioni correttamente eseguite al momento del recesso, il valore dei materiali utili esistenti in magazzino, oltre al decimo dell'importo dei servizi non ancora eseguito calcolato sulla differenza tra l'importo dei quattro quinti del prezzo posto a base di gara, depurato del ribasso d'asta e l'ammontare netto dei servizi eseguiti, con espressa esclusione di ogni altro riconoscimento, a qualsivoglia titolo richiesto. Resta inteso che in caso di contratto a consumo, se nel contratto è prevista una %



dell'importo contrattuale minima garantita di acquisto dei servizi, in caso di recesso all'Appaltatore, a definitiva e completa tacitazione di ogni diritto e pretesa, verranno riconosciuti esclusivamente, il pagamento delle prestazioni correttamente eseguite al momento del recesso, il valore dei materiali utili esistenti in magazzino oltre al decimo dell'importo dei servizi non ancora eseguito calcolato sulla differenza tra l'importo dei quattro quinti della % dell'importo contrattuale minimo garantito e l'ammontare netto dei servizi eseguiti, con espressa esclusione di ogni altro riconoscimento, a qualsivoglia titolo richiesto.

Dalla data di efficacia del recesso, l'Appaltatore dovrà cessare tutte le prestazioni oggetto del Contratto / Accordo Quadro, assicurando che tale cessazione non comporti danno alcuno ad ACI Informatica.

Al momento del recesso, la Stazione Appaltante diviene in ogni caso unico titolare della proprietà esclusiva del prodotto dei servizi resi e dell'ulteriore documentazione, nonché di ogni altro diritto sui medesimi, senza che possano essere fatte valere dall'Appaltatore a qualsivoglia titolo pretese di sorta, anche in ordine ad ulteriori riconoscimenti, compensi, indennizzi o risarcimenti comunque denominati.

5.3.2 Recesso per fallimento dell'Appaltatore

Nel caso in cui l'Appaltatore sia sottoposto a procedura di fallimento, con autorizzazione all'esercizio provvisorio, o di concordato preventivo con continuità aziendale nonché in caso di ammissione a concordato con cessione di beni o di presentazione della domanda di concordato ai sensi dell'art. 161, co. 6 del r.d. n. 267/1942, il Contratto di appalto/Accordo quadro può essere proseguito dall'Appaltatore a condizione che sia in tal senso autorizzato dal giudice delegato. In difetto di tali condizioni, il Contratto/Accordo quadro si scioglie ai sensi dell'art. 81 legge fallimentare, con salvezza di ogni altro diritto e azione in favore di ACI Informatica. In tal caso ACI Informatica si riserva anche il ricorso alla procedura di cui all'art. 124 del D. Lgs. 36/2023 e s.m.i..

5.3.3 Recesso per altre procedure concorsuali dell'Appaltatore

ACI Informatica si riserva la facoltà di recedere dal Contratto di appalto, ivi incluso l'Accordo Quadro, secondo le modalità e criteri precisati nel precedente articolo 5.3.1, qualora rilevi che l'Appaltatore sia sottoposto ad una procedura concorsuale diversa da quelle di cui all'art. 5.3.2.

5.3.4 Obbligo di recesso

La Stazione Appaltante ha l'obbligo di recedere dal Contratto qualora, al verificarsi di uno dei casi previsti dal comma 17 dell'art. 68 del D.Lgs. n. 36/2023 e s.m.i., non sussistano le condizioni che consentano di proseguire il Contratto di appalto con altro operatore economico che sia costituito mandatario nei modi previsti dal D. Lgs. 36/2023 stesso ed in possesso dei requisiti di qualificazione adeguati ai servizi o forn-



ture ancora da eseguire. In tal caso l'Appaltatore ha diritto al solo pagamento delle prestazioni correttamente eseguite al momento del recesso ed il pagamento dei materiali utili esistenti in magazzino.

6 Legge applicabile

Il Contratto / Accordo Quadro e tutti i diritti e gli obblighi da esso derivanti sono regolati, e saranno da interpretarsi, secondo la legge italiana.

Approvato da Giancarlo Di Crescenzo

il 27/06/2025 alle 14:53:19 CEST



Approvato da Gianluca Stefani

il 27/06/2025 alle 15:11:03
CEST

