CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO A
CAPITOLATO TECNICO

INDICE

1. PREMESSA

Il presente documento definisce i requisiti tecnici per la realizzazione, da parte del Fornitore aggiudicatario delle gara, dei Servizi della Rete Internazionale delle Pubbliche Amministrazioni (S-RIPA), i requisiti relativi alle modalità con cui il Fornitore stesso dovrà erogare tali servizi, nonché i requisiti che le offerte dei concorrenti dovranno rispettare.

La numerazione dei requisiti segue il formato [R.N]. dove "R" sta ad indicare "requisito" ed N la numerazione progressiva.

Per agevolare la lettura del documento viene di seguito riportato il glossario dei termini più frequentemente utilizzati:

- **Amministrazione Aggiudicatrice:** Consip S.p.A.
- **Amministrazioni Pubbliche o Pubbliche Amministrazioni**: le pubbliche amministrazioni legittimate ad utilizzare l'accordo quadro ai sensi della normativa vigente (di seguito per brevità anche Amministrazioni)
- **Accordo Quadro**: il contratto che verrà stipulato con l'Aggiudicatario della presente iniziativa di gara
- **Amministrazione/i Contraente/i**: la/e Amministrazione/i Pubblica/che che utilizza/utilizzano l'Accordo Quadro nel periodo della sua validità ed efficacia mediante stipula dei Contratti Esecutivi derivanti dall'Accordo Quadro
- **Capitolato Tecnico**: il presente documento
- **Fornitore**: l'aggiudicatario della presente gara
- **Servizi**: tutti i servizi oggetto della gara, elencati al par. 1.1 del presente Capitolato Tecnico
- **Contratto Esecutivo**: il documento, comprensivo degli eventuali allegati, con il quale le Amministrazioni Contraenti utilizzano l'accordo quadro, impegnando il Fornitore alla prestazione dei servizi richiesti nel rispetto delle modalità e delle specifiche contenute nel presente Capitolato Tecnico e nell'Offerta Tecnica del Fornitore, nonché alle condizioni economiche fissate dal Fornitore medesimo nell'Offerta Economica.

Tutti i servizi (con le loro caratteristiche) previsti nel presente capitolato tecnico, e che il concorrente descriverà nella Relazione Tecnica, sono da ritenersi inclusi nell'offerta effettuata e tariffati secondo i corrispettivi economici di cui all'Offerta Economica.

Tutte le durate e gli intervalli di tempo previsti nel presente Capitolato sono da intendersi come solari, salvo dove diversamente indicato.

Laddove non diversamente indicato, per ciascun parametro per il quale si richiede al concorrente, nell'intero capitolato, di indicare il valore caratteristico della propria offerta tecnica, il concorrente dovrà utilizzare due cifre decimali (ad es: 12,34), anche nel caso di percentuali (ad es: 56,78%).

Valori con un numero maggiore di decimali saranno arrotondati al secondo decimale, per difetto se la terza cifra decimale è compresa tra 0 e 4, e per eccesso se la terza cifra decimale è compresa tra 5 e 9. Ad esempio:

- 21,264 viene arrotondato a 21,26;
- 21,265 viene arrotondato a 21,27.

Nei casi in cui sia invece richiesta l'indicazione di un valore intero, qualora il valore indicato dal concorrente contenga delle cifre decimali, sarà arrotondato all'intero inferiore, se la prima cifra decimale è compresa tra 0 e 4, e all'intero superiore se la prima cifra decimale è compresa tra 5 e 9. Ad esempio:

- 1,4 viene arrotondato a 1;
- 1,5 viene arrotondato a 2.

1.1 Sommario dei servizi oggetto della gara

Sulla base dei servizi ad oggi fruiti dalle Amministrazioni aderenti al "Contratto Quadro n. 5/2010 – affidamento dei servizi di telecomunicazione ed informatici per la realizzazione dei servizi e della rete internazionale della pubblica amministrazione (S-RIPA)" stiupato il 22/12/2010, delle esigenze di breve/medio periodo raccolte presso le Amministrazioni interessate e dei trend di mercato, sono state individuate le tipologie di servizi descritte nel seguito, oggetto della presente gara:

- servizi di Connettività IP, le cui specifiche sono riportate nel Capitolo 2;
- servizi di Sicurezza, le cui specifiche sono riportate nel Capitolo 3;
- servizi VoIP (Voice over IP) e di Comunicazione Evoluta, le cui specifiche sono riportate nel Capitolo 4;
- servizi di Supporto, le cui specifiche sono riportate nel Capitolo 5.

Fatta eccezione per i servizi di sicurezza Anti-APT, "centralizzati" e contrattualizzabili su base Amministrazione, tutti i restanti servizi sono "locali" e contrattualizzabili su base sede.

1.2 Durata e limiti dell' erogazione dei servizi

Il massimale dei servizi oggetto dell' accordo quadro è fissato in:

- 100 milioni di € per l'insieme dei servizi oggetto di gara (connettività, sicurezza, comunicazione evoluta, supporto), ad eccezione dei servizi VoIP;
- 1.500 linee per i servizi VoIP.

L'accordo quadro avrà una durata di **60 (sessanta)** mesi e sarà eventualmente prorogabile sino ad un massimo di ulteriori **12 (dodici)** mesi, a condizione che non sia esaurito il massimale di cui sopra, eventualmente incrementato come di seguito descritto.

Nel caso in cui, prima della scadenza della durata (eventualmente prorogata) dell'accordo quadro, sia esaurito il massimale sopra indicato, Consip potrà richiedere al Fornitore, che sarà obbligato ad accettare, un incremento del predetto massimale fino alla concorrenza di un quinto del medesimo.

1.3 Architettura della rete internazionale

La Rete Internazionale S-RIPA si articola in tre ambiti di intervento complementari:

- **Connettività Internazionale** – Connettività IP tra le sedi delle Amministrazioni ed accesso ad Internet, secondo i livelli di servizio prestazionali e gestionali definiti nel presente Capitolato;
- **Sicurezza** – Servizi di presidio della sicurezza, in grado di garantire la protezione sia passiva che attiva da tentativi di intrusione e la confidenzialità delle comunicazioni tra le sedi connesse;
- **Dominio Servizi** – Servizi a valore aggiunto di comunicazione evoluta, che sfruttano le opportunità offerte dalla tecnologia IP.

Nella figura seguente è rappresentato lo schema di principio della Rete Internazionale S-RIPA.

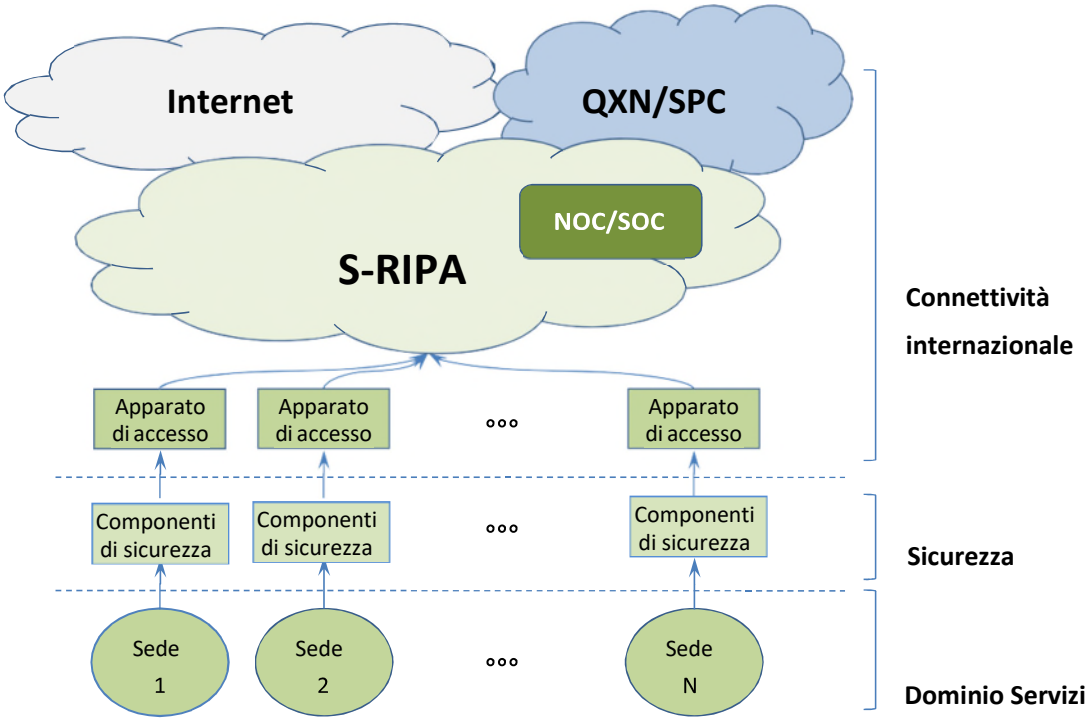

Figura 1: Schema di principio della Rete Internazionale S-RIPA

L'Appendice A al presente Capitolato tecnico contiene un quadro sintetico delle consistenze dei servizi fruiti dalle Amministrazioni aderenti al Contratto Quadro n. 5/2010 (rif. par. 1.1), aggiornato al dicembre 2017. Si precisa che, con riferimento alle colonne "Sedi/Servizi attivi", con "0" si intentende servizio non attivo/richiesto sulla sede; con "1" un servizio attivo/richiesto sulla sede; con "0,5" due servizi attivi/richiesti sulla sede.

1.4 Prescrizioni generali

Si riportano di seguito le prescrizioni di carattere generale che dovranno essere soddisfatte dal Fornitore:

[R.1] Il Fornitore è responsabile dell'erogazione dei servizi previsti dal presente Capitolato tecnico, ivi compresa l'installazione e la gestione di tutti gli apparati funzionali all'offerta dei servizi e l'implementazione delle politiche di sicurezza da applicare su tutte le infrastrutture utilizzate per l'erogazione dei servizi.

[R.2] I servizi sono specificati in termini di caratteristiche del servizio e di parametri di qualità del servizio descritti nell'ambito del presente Capitolato.

[R.3] I servizi dovranno essere forniti 24 ore su 24 per 365 giorni l'anno, e a tale orario di erogazione si riferisce la misura delle prestazioni dei servizi.

[R.4] I servizi dovranno essere *aperti all'utenza*, cioè dovranno essere accessibili secondo caratteristiche di qualità definite e formalizzate nel presente Capitolato tecnico.

[R.5] I servizi devono essere *aperti al cambiamento*, cioè devono essere erogati in modo tale da consentire una facile introduzione di elementi innovativi risultanti dall'evoluzione della tecnologia.

[R.6] La fornitura dei servizi dovrà essere *indipendente dalla tecnologia*, salvo ove espressamente prevista nel capitolato, e dovrà essere garantita la trasparenza dei servizi rispetto all'evoluzione tecnologica.

[R.7] La modalità di fornitura dei servizi dovrà essere *scalabile*: dovrà essere garantita l'espandibilità della rete S-RIPA per estensione geografica, per numero e tipologia di utenze e per numero e tipologia di servizi supportati (anche riferibili al singolo sito).

[R.8] Il Fornitore deve garantire soluzioni *conformi alle normative e agli standard vigenti*, aggiornate allo stato dell'arte della tecnologia disponibile ed in linea con l'evoluzione degli standard di riferimento ove applicabili (es. IETF, IEEE, etc.).

[R.9] Le interfacce di accesso ad ogni servizio dovranno essere *conformi ai relativi standard de jure* e *de facto*, come richiesto all'interno delle specifiche relative ad ogni servizio oggetto di fornitura, in modo da rendere possibile l'interlavoro di sottoreti basate su tecnologie diverse.

[R.10] Nella gara sarà dato particolare rilievo alle caratteristiche funzionali e ai conseguenti parametri prestazionali misurati sull'interfaccia fisica lato utente dalla quale viene erogato il singolo servizio. Ai servizi oggetto del presente capitolato, salvo ove esplicitamente escluso, è associato un punto di accesso al servizio (PAS) che:

- individua il punto di consegna del servizio da parte del Fornitore,
- delimita le frontiere di responsabilità del Fornitore e dell'Amministrazione,
- è il punto di riferimento per la misura dei parametri di SLA.

Qualora il servizio non preveda PAS, la responsabilità del servizio è totalmente a carico del Fornitore e tale specifica è da intendersi nel senso che non è individuato un punto di frontiera diretto tra l'infrastruttura per il servizio e quella dell'Amministrazione.

[R.11] Il Fornitore deve acquisire il tempo ufficiale di rete attraverso il protocollo Network Time Protocol (NTP) versione 3 (o successive) tramite sincronizzazione con il servizio NTP di SPC erogato da QXN o tramite la sincronizzazione con il tempo di riferimento nazionale dell'Istituto Elettrotecnico Nazionale "Galileo Ferraris" come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble ticket, nonché per tutte le altre funzioni di gestione dei servizi che richiedono un riferimento temporale.

2. SERVIZI DI CONNETTIVITA' IP

[R.12] I servizi di connettività IP sono dedicati alla trasmissione di qualunque tipo di dato (inclusa la fonia) e dovranno necessariamente essere basati su protocollo Internet Protocol version IPv4 e IPv6.

[R.13] Il Fornitore si impegna a prestare i servizi richiesti dalle Amministrazioni, nelle sedi e con le caratteristiche di cui al par. 2.4.

[R.14] Il Fornitore dovrà altresì prestare i servizi derivanti da nuove esigenze di connettività, secondo quanto disciplinato al par. 2.5.

[R.15] I servizi di trasporto devono essere basati su Internet Protocol version IPv4 e IPv6. I servizi standard devono comprendere il trasporto e l'indirizzamento secondo la versione IPv4. L'Amministrazione cliente può richiedere, senza differenze di prezzo, che il servizio venga fornito secondo gli standard IPv6 o con sistemi configurati con dual stack IPv4/IPv6. Il Fornitore, su richiesta dell'Amministrazione, si impegna a mettere in atto tutte le azioni atte a favorire la migrazione della rete dell'Amministrazione dalla suite protocollare IP V4 a quella IP V6

[R.16] Il fornitore dovrà garantire differenti modalità di erogazione dei servizi di Connettività IP articolati come segue:

- Servizi di connettività Satellitare (SAT);
- Servizi di connettività Terrestre Best Effort (TER BE);
- Servizi di connettività Terrestre a Banda Garantita (TER BG).

[R.17] Le diverse modalità di erogazione dei servizi sono caratterizzate da opportuni livelli di servizio (SLA) che ne prescrivono la qualità e che sono indicati nel seguito. In particolare, per ciascuna modalità di erogazione dei servizi di Connettività IP sopra elencati, il Fornitore si impegna a garantire opportuni SLA gestionali, in termini di *disponibilità unitaria* del servizio e *tempo di ripristino* del servizio, nonché, limitatamente ai servizi SAT e TER BG, SLA prestazionali, in termini di ritardo di traferimento dei pacchetti (*Round Trip Delay*) e tasso di terdita dei pacchetti (*Packet Loss*).

[R.18] Gli oneri, derivanti dalle misure tecnico-organizzative adottate per il monitoraggio e la rendicontazione dei livelli di servizio, sono a carico del Fornitore.

[R.19] Relativamente al trasporto del traffico IP (Internet Protocol), il servizio dovrà permettere la trasmissione di pacchetti IP nei seguenti tre ambiti (o sottoinsieme di essi indicato dall'Amministrazione):

- **ambito Intranet**: costituito dal dominio interno alla singola Amministrazione che connette tutte le sedi (o parte di esse), distribuite sul territorio internazionale;
- **ambito Infranet**: costituito dall'interconnessione tra le diverse Amministrazioni attestate alla S-RIPA, o al SPC attraverso la QXN (Qualified eXchange Network);
- **ambito Internet:** costituito dall'interconnessione di una specifica Amministrazione con la rete Internet pubblica.

[R.20] Le diverse modalità di erogazione dei servizi di Connettività IP devono consentire all'Amministrazione la trasmissione/ricezione di pacchetti IPv4 e IPv6 negli ambiti configurati.

Sui servizi di connettività, oltre l'ambito Intranet, incluso di default e disattivabile su richiesta, il Fornitore dovrà permettere, su richiesta dell'Amministrazione, l'abilitazione del traffico dati multiambito, cioè anche sugli ambiti Infranet e/o Internet. Ognuno degli ambiti, su richiesta dell'Amministrazione, dovrà poter essere disabilitato separatamente.

[R.21] Il Fornitore deve garantire, su accessi configurati per gestire più ambiti, la segregazione del traffico appartenente a diversi ambiti.

[R.22] La connettività verso tutti gli ambiti deve essere fornita senza limitazioni temporali e di accesso ai contenuti (*network neutrality*); non deve essere limitato il trasporto di alcun protocollo dell'intera suite di protocolli Internet, il tutto compatibilmente con il rispetto delle diverse imposizioni normative a tal proposito vigenti nei diversi paesi internazionali interessati alla fornitura.

[R.23] Non devono essere adottate politiche di *traffic shaping* sugli apparati di accesso, che impediscano, in assenza di congestione, di utilizzare la larghezza di banda massima del circuito di accesso.

[R.24] I parametri che caratterizzano i servizi di connettività IP e Internet sono:

- **BNA (Banda Nominale in Accesso)**: è definita come la banda fisica configurata sull'interfaccia geografica del servizio in oggetto. Laddove è indicata la sola BGA, si intende una BNA pari almeno alla BGA;
- **BGA (Banda Garantita in Accesso)**: è definita come il valore massimo di throughput per il quale il Fornitore è obbligato alla garanzia degli SLA prestazionali (*Round Trip Delay* e *Packet Loss*). Tale banda garantita, e i relativi SLA, sono misurati tra il Punto di Accesso al Servizio e il Border Router di attestazione alla QXB.

[R.25] Nel caso di collegamenti asimmetrici, sono definiti i valori di BNA in *uplink* e *downlink*, rispettivamente BNAu e BNAd, e di BGA in *uplink* e *downlink*, rispettivamente BGAu e BGAd, nonché i relativi valori medi:

- BNAm=(BNAu+BNAd)/2;
- BGAm=(BGAu+BGAd)/2.

[R.26] Per i collegamenti satellitari e terrestri a banda garantita, l'Amministrazione potrà richiedere l'allocazione della BGA sui diversi ambiti definiti in [R.20], con granularità di 64 Kbps.

[R.27] I servizi di connettività IP si intendono comprensivi delle attività di fornitura, installazione, gestione, manutenzione, monitoraggio e implementazione delle politiche di sicurezza, inerenti tutte le componenti necessarie alla corretta erogazione dei servizi stessi.

[R.28] Gli apparati di accesso forniti con i servizi di connettività IP, devono essere gestiti e configurati dal Fornitore come componenti integranti del servizio, devono essere ricompresi nel prezzo offerto e dovranno:

- essere allo stato dell'arte della tecnologia e del mercato;
- implementare protocolli allo stato dell'arte;
- essere dimensionati in modo da garantire il rispetto dei livelli di servizio previsti.

[R.29] Gli apparati di accesso dovranno, in particolare:

- essere dotati di una o più interfacce fisiche lato utente compatibili con l'infrastruttura di rete dell'Amministrazione (ognuna di tali interfacce deve essere conforme ad uno dei seguenti standard: Fast Ethernet 10/100 Autosensing, Gigabit Ethernet o 10Gigabit Ethernet);
- avere una capacità totale delle interfacce lato utente non inferiore alla BNA contrattualizzata sull'accesso (in caso di accesso asimmetrico della maggiore tra la banda in downstream ed upstream);
- garantire una capacità di commutazione in termini di pacchetti al secondo adeguata alle bande dei collegamenti, prendendo a riferimento distribuzioni del traffico standard quale Internet Mix (iMix).
- permettere, per i servizi di connettività Satellitare e Terrestre a Banda Garantita, la configurazione di uno o più ambiti, su richiesta dell'Amministrazione, secondo quanto previsto dal [R.20].

[R.30] I servizi di connettività IP e Internet, devono in ogni caso comprendere:

- l'apparato di accesso al servizio;
- il circuito/collegamento satellitare che permette all'Amministrazione il collegamento alla rete del Fornitore;
- l'abilitazione all'ambito Intranet (disattivabile su richiesta);

- il trasporto in modalità best effort, fino al raggiungimento della BNA;
- la garanzia del trasporto di flussi di traffico fino al raggiungimento della BGA (se prevista dallo specifico collegamento);
- i servizi di manutenzione e assistenza;
- il rispetto dei livelli di servizio.

[R.31] Per consentire la comunicazione tra le reti, il Fornitore aggiudicatario della presente gara deve connettersi alla QXN, mediante acquisizione di un'istanza di servizio di interconnessione OPA, seguendo le regole tecniche di interconnessione di cui all'Appendice B del presente Capitolato Tecnico. Il Fornitore aggiudicatario della presente procedura dovrà a tal fine sottoscrivere, con il Fornitore aggiudicatario della "Gara per la progettazione, realizzazione, fornitura, manutenzione e gestione delle Infrastrutture Condivise del Sistema Pubblico di Connettività" (IC-SPC), un Contratto attuativo del Contratto già stipulato da AgID con tale Fornitore. Le appendici C e D del presente Capitolato Tecnico sono costituite, rispettivamente, dallo Schema di Contratto attuativo e dallo Schema di Contratto cui il Contratto Attuativo si riferisce. I corrispettivi dovuti dal Fornitore aggiudicatario della presente procedura per l'interconnessione alla QXN sono quelli indicati all'art. 13, co. 2, lett. 2.a) e 2.b) dello schema di contratto di cui alla predetta appendice D.

[R.32] Il Punto di accesso al servizio (PAS) per i servizi di trasporto dati è definito come l'insieme delle interfacce lato utente messe a disposizione dal Fornitore sugli apparati di terminazione del servizio in sede della Amministrazione.

[R.33] I servizi di trasporto comprendono anche l'erogazione di un servizio *Domain Name System* (DNS) che consenta sia la pubblicazione dei nomi a dominio delle Pubbliche Amministrazioni che la risoluzione dei nomi a dominio, relativi ai soli ambiti Infranet e Internet. Il servizio deve essere disponibile sia in caso di IPv4 che IPv6.

[R.34] Il sistema DNS del Fornitore deve essere configurato in modo tale da essere suddiviso in due componenti Internet/Infranet per la gestione differenziata di ciascun ambito.

[R.35] La componente DNS Internet deve annunciare le zone di propria competenza sulla sola rete Internet.

[R.36] La componente DNS Infranet deve essere configurata in modo tale da annunciare automaticamente verso i DNS della QXN il cambiamento di una zona di propria competenza, attraverso l'utilizzo del meccanismo DNS Notify (RFC1996). Inoltre il sistema DNS del Fornitore deve essere configurato in modo tale da accettare le richieste di AXFR (Full Zone Transfer) e IXFR (Incremental Zone Transfer RFC1995), provenienti dai Name Server della QXN.

[R.37] Il sistema DNS deve essere configurato in modo da accettare lo Zone Transfer da parte dei sistemi DNS delle Amministrazioni, in modo da garantire la pubblicazione automatica dei nomi a dominio di loro competenza, tramite i meccanismi di DNS Notify (RFC1996).

[R.38] Il Fornitore deve garantire altresì la gestione dei change dei nomi a dominio su richiesta dell'Amministrazione.

[R.39] Il sistema DNS del Fornitore, per garantire il servizio di risoluzione alle Pubbliche Amministrazioni di propria competenza, deve utilizzare come "forwarders" i DNS della QXN. In caso di indisponibilità dei DNS della QXN il sistema del Fornitore deve accedere direttamente ai "root server" Internet.

[R.40] Il sistema DNS deve implementare meccanismi di cache per la risoluzione dei nomi, e meccanismi di forwarding selettivo su base dominio.

[R.41] Il piano di indirizzamento adottato nell'ambito di S-RIPA deve garantire l'univocità degli indirizzi IPv4 e/o IPv6 attribuiti ai singoli sistemi che, connessi tramite QXN, scambieranno traffico tra loro.

[R.42] Gli indirizzi IPv4 e/o IPv6 delle Amministrazioni, destinati ai servizi esposti su Internet o su Infranet, devono essere di tipo pubblico e, su richiesta dell'Amministrazione, messi a disposizione dal Fornitore all'interno del proprio spazio di indirizzi accessibile tramite QXN.

[R.43] Oltre a quelli eventualmente necessari per la gestione delle proprie Terminazioni di Rete (TdR), il Fornitore deve rendere disponibili, a richiesta dall'Amministrazione, al fine di realizzare servizi esposti su Infranet o Internet,

almeno il numero di indirizzi IPv4 pubblici correlato al numero complessivo di accessi S-RIPA secondo quanto indicato nella successiva tabella.

Numero accessi contrattualizzati	Numero di indirizzi disponibili
Fino a 2	8
Da 3 a 10	16
Da 11 a 25	32
Da 26 a 50	64
Da 51 a 100	128
Da 101 a 200	256
Oltre 200	512

Tabella 1 – Indirizzi IP da rendere disponibili

Non vi sono invece limiti specifici sul numero di indirizzi IPv6 pubblici che il Fornitore deve rendere disponibili all'Amministrazione.

2.1 Servizi di connettività Satellitare

[R.44] I servizi di connettività Satellitare sono caratterizzati da collegamenti satellitari, *always-on*, tra le sedi delle Amministrazioni e la rete del Fornitore.

[R.45] La soluzione di connettività via satellite dovrà prevedere la fornitura, installazione, gestione e manutenzione di tutte le infrastrutture ed apparati necessari per la realizzazione del collegamento satellitare: antenna, supporto fisico dell'antenna, apparato di terminazione, collegamento fisico tra l'antenna e l'apparato che interconnette la LAN.

[R.46] La soluzione di connettività via satellite dovrà prevedere una fase preliminare in cui il Fornitore sarà tenuto ad effettuare uno studio di fattibilità della soluzione presso la sede dell'Amministrazione e la successiva fornitura ed installazione di un antenna ricetrasmittente con diametro il più possibile limitato per le caratteristiche del collegamento offerto.

[R.47] Il collegamento tra il satellite e la rete del Fornitore dovrà essere incluso nel servizio e dimensionato in modo tale da rispettare gli SLA definiti nel seguito, nonché nel par. 8.

[R.48] Il fornitore dovrà rendere disponibile il servizio satellitare tramite tecnologia di accesso DVB.

[R.49] Per i collegamenti in "Affidabilità Standard", la minima Disponibilità unitaria (come definita nel par. 8) da garantire è pari al 97,00%. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par 2.4.

[R.50] Per i collegamenti in "Affidabilità Standard", il Tempo di ripristino massimo del servizio (come definito nel par. 8) da garantire è pari a 72 ore (3 giorni solari) dalla segnalazione del disservizio. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par 2.4.

[R.51] I collegamenti in "Affidabilità Elevata" prevedono che il servizio sia realizzato ridondando gli apparati di accesso, i modem e l'illuminatore.

[R.52] Per i collegamenti in "Affidabilità Elevata", la minima Disponibilità unitaria (come definita nel par. 8) da garantire è pari al 99,01%. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par 2.4.

[R.53] Per i collegamenti in "Affidabilità Elevata", il Tempo di ripristino massimo del servizio (come definito nel par. 8) da garantire è pari 24 ore (1 giorno solare) dalla segnalazione del disservizio. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par 2.4.

[R.54] Tutti i collegamenti satellitari devono garantire un Ritardo di trasferimento (RTD – come definito nel par. 8), per il 99% dei pacchetti, pari ad un massimo di 900 ms, ed un Tasso di perdita dei pacchetti (PL – come definito nel par. 8) massimo dell' 1%.

2.2 I servizi di connettività Terrestre Best Effort

[R.55] I servizi di connettività di tipo Terrestre Best Effort sono di tipo *wired*, basati su collegamenti fisici permanenti, il cui rilegamento fisico utilizzato per il circuito di accesso è su portante elettrica (realizzato con uno o più doppini in rame) o su portante ottica (realizzato in fibra ottica). Sono caratterizzati da una connessione, *always-on*, e da una Banda Nominale all'Accesso.

[R.56] Per l'accesso al servizio, il Fornitore potrà ricorrere sia a risorse di rete dedicate, sia a connessioni, di tipo VPN, che utilizzino tunnel IPSec su accessi locali alla Internet pubblica per il collegamento alla rete IP MPLS del Fornitore, e caratterizzati da:

- un apparato di accesso;
- un accesso ad Internet attraverso un ISP locale, con cui il Fonitore si fa carico di instaurare un rapporto per la gestione trasparente del servizio nei confronti dell'Amministrazione;
- una porta MPLS, per la raccolta e consegna del traffico in transito su ciascuna connessione, presso uno dei nodi internazionali della rete IP MPLS del Fornitore.
- tunnel IPSec con crittografia AES – 256 Tunnel mode, per negoziare protocolli ed algoritimi per la generazione delle chiavi di crittografia ed autenticazione.

[R.57] La minima Disponibilità unitaria (come definita nel par. 8) da garantire è pari al 97,00%. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par. 2.4.

[R.58] Il Tempo di ripristino massimo del servizio (come definito nel par. 8) da garantire è pari a 96 ore (4 giorni solari) dalla segnalazione del disservizio. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par. 2.4.

2.3 Servizi di connettività Terrestre a Banda Garantita

[R.59] I servizi di connettività Terrestre a Banda Garantita sono di tipo *wired*, basati su collegamenti fisici permanenti, il cui rilegamento fisico utilizzato per il circuito di accesso è su portante elettrica (realizzato con uno o più doppini in rame) o su portante ottica (realizzato in fibra ottica). Sono caratterizzati da una Banda Garantita all'Accesso, e da collegamenti fisici permanenti, *always-on*, tra le sedi delle Amministrazioni e la rete del Fornitore, in cui l'accesso al servizio sarà realizzato attraverso risorse di rete che saranno dedicate allo scopo per il periodo di erogazione contrattualizzato.

[R.60] Per i collegamenti in "Affidabilità Standard", la minima Disponibilità unitaria (come definita nel par. 8) da garantire è pari al 97,00%. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par. 2.4.

[R.61] Per i collegamenti in "Affidabilità Standard", il Tempo di ripristino massimo del servizio (come definito nel par. 8) da garantire è pari a 72 ore (3 giorni solari) dalla segnalazione del disservizio. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par. 2.4.

[R.62] I collegamenti in "Affidabilità Elevata" prevedono che il servizio sia realizzato ridondando completamente la soluzione tecnologica caratterizzante il servizio in Affidabilità Standard in modo da garantire, in caso di guasto singolo, funzionalità e prestazioni equivalenti. La soluzione consiste in un accesso secondario equivalente all'accesso primario, con realizzazione del collegamento tale da minimizzare i singoli punti di guasto, e la fornitura di apparati di accesso configurati in modalità active-standby, pertanto solo in caso di indisponibilità dell'accesso primario, il traffico è instradato sull'accesso secondario. L'Affidabilità Elevata deve garantire, nella centrale del Fornitore, l'attestazione dei circuiti di accesso su apparati differenti. Entrambe le componenti del servizio devono essere monitorate e gestite.

[R.63] Per i collegamenti in "Affidabilità Elevata", la minima Disponibilità unitaria (come definita nel par. 8) da garantire è pari al 99,01%. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par. 2.4.

[R.64] Per i collegamenti in "Affidabilità Elevata", il Tempo di ripristino massimo del servizio (come definito nel par. 8) da garantire è pari 24 ore (1 giorno solare) dalla segnalazione del disservizio. Tale parametro, relativamente a ciascun collegamento offerto, potrà essere migliorato come specificato nel successivo par. 2.4.

[R.65] I collegamenti terrestri devono garantire un Ritardo di trasferimento (RTD – come definito nel par. 8), per il 99% dei pacchetti, pari ad un massimo di 400 ms per collegamenti con BGA fino a 2 Mbps, e pari a un massimo di 300 ms per collegamenti con BGA superiore.

[R.66] Tutti i collegamenti terrestri devono garantire un Tasso di perdita dei pacchetti (PL – come definito nel par. 8) massimo dell' 1%.

[R.67] Nel caso in cui la legislazione locale non consenta al Prestatore di realizzare a proprio carico il *local loop*, l'Amministrazione provvederà a dotarsi del rilegamento di accesso a sue spese. In questo caso il Prestatore dovrà garantire all'Amministrazione adeguato supporto tecnico-amministrativo, nonchè proporre una modalità di fatturazione che consenta lo storno degli oneri sostenuti direttamente dall'Amministrazione.

2.4 Servizi di connettività per le sedi attuali

Le prescrizioni che seguono si riferiscono alla "**Offerta Tecnica per i servizi di connettività**" e alla "**Dichiarazione di Offerta Economica per i servizi di connettività**", parti integranti rispettivamente dell'Offerta Tecnica e della Dichairazione di Offerta Economica che il concorrente dovrà compilare, sulla base dei **modelli** allegati alla lettera di invito, e presentare con le modalità precisate nella lettera stessa.

[R.68] Per ciascuna sede indicata nei suddetti modelli, è richiesto al concorrente di formulare **una "offerta base"** a banda garantita (con un servizio in Affidabilità Standard ed uno in Affidabilità Elevata), **una "offerta avanzata"** a banda garantita (anche in questo caso con un servizio in Affidabilità Standard ed uno in Affidabilità Elevata), e **una "offerta best effort"** (con un servizio in Affidabilità Standard). Per ciascuno di tali servizi, il concorrente dovrà indicare il canone mensile offerto nella "Dichiarazione di Offerta Economica per i servizi di connettività", e le caratteristiche tecniche, come di seguito precisato, nella "Offerta Tecnica per i servizi di connettività". Per ciascuna sede, le Amministrazioni potranno acquistare uno o più servizi tra quelli offerti dal Fornitore.

Gli indirizzi delle predette sedi sono contenute nell'Appendice E del presente Capitolato Tecnico, reperibile con le modalità indicate nella Lettera di invito.

OFFERTA BASE

[R.69] Per l'**offerta base** è richiesta, per ciascuna sede, l'offerta di un collegamento, Satellitare o Terrestre a Banda Garantita, sia in Affidabilità Standard sia in Affidabilità Elevata. Più in dettaglio, per ciascuna sede il modello presenta le seguenti caratteristiche:

- La Banda Garantita in Accesso richiesta BGAr;
- Per l' Affidabilità Standard:
  - disponibilità minima richiesta;
  - tempo massimo di ripristino richiesto;
- Per l' Affidabilità Elevata:
  - disponibilità minima richiesta;
  - tempo massimo di ripristino richiesto.

Sono altresì indicate le disponibilità massime e i tempi minimi di ripristino, utilizzati per l'attribuzione dei punteggi tecnici come specificato nella lettera di invito.

[R.70] **Il concorrente dovrà indicare, per ciascuna sede**:

- **tipologia di collegamento: SAT o TER BG**, con i vincoli di cui ai seguenti [R.71] e [R.72];
- **la BGAu e la BGAd del collegamento offerto, espresse in Kbit/s**, con i vincoli di cui al [R.73], [R.74], [R.75] ed [R.76];
- **disponibilità e tempo di ripristino (valore intero, espresso in ore) per il collegamento offerto, per Affidabilità Standard**, che dovranno essere compresi negli intervalli indicati nel modello;
- **disponibilità e tempo di ripristino (valore intero, espresso in ore) per il collegamento offerto, per Affidabilità Elevata**, che dovranno essere compresi negli intervalli indicati nel modello.

[R.71] Per 13 sedi il collegamento dovrà essere esclusivamente satellitare. Tali 13 sedi sono contraddistinte, nel Modello di Offerta Tecnica, dal colore rosso, e dall'avere il campo "Tipologia di collegamento" pre-compilato con il valore "SAT".

[R.72] Il numero di collegamenti SAT non potrà essere superiore a a 52 per le sedi del MAECI (che comprendono le 11 obbligatoriamente SAT), e a 9 per le sedi del Ministero della Difesa. Tenuto conto delle due sedi obbligatoriamente SAT della Protezione Civile, il numero di collegamenti SAT massimo è di 63. Al ridursi dei collegamenti SAT (e quindi all'aumentare di quelli TER BG) verrà attribuito un punteggio tecnico, come definito nella lettera di invito.

[R.73] Per le sedi in cui la BGAr è superiore a 2 Mbit/s, il collegamento offerto dovrà avere Banda Garantita in Accesso, in uplink e downlink, pari a quella richiesta, cioè BGAu=BGAd=BGAr.

[R.74] Per le sedi in cui la BGAr è pari a 2 Mbit/s, se il collegamento offerto è SAT, dovrà avere BGAd=2 Mbit/s. La BGAu dovrà essere di minimo 512 kbit/s. Al crescere del rapporto di simmetria (BGAu/BGAd) medio dei collegamenti SAT con BGAr=2Mbit/s, sarà attribuito il punteggio tecnico definito nella lettera di invito. In caso di offerta di collegamenti SAT asimmetrici, con BGAd=2 Mbit/s e BGAu=x Mbit/s, l'Amministrazione potrà richiedere e il fornitore sia tenuto ad erogare, a parità di tutte le altre condizioni tecniche, collegamenti simmetrici con BGAd=BGAu=1 Mbit/s, e con canone mensile pari a quello offerto per il collegamento asimmetrico, moltiplicato per il fattore 2/(2+x).

[R.75] Per le sedi in cui la BGAr è pari a 2 Mbit/s, se il collegamento offerto è TER BG, il collegamento offerto dovrà avere BGAd=2Mbit/s, fatta eccezione per un massimo di 55 sedi per il Ministero degli Affari Esteri e della Cooperazione Internazionale, 18 per il Minstero della Difesa e una per l'Agenzia Dogane, in cui potranno essere offerti collegamenti con BGAd pari almeno ad 1Mbit/s. Al crescere del numero dei collegamenti complessivi, per i quali la BGAd offerta è di almeno 2Mbit/s, sarà attribuito il punteggio tecnico definito nella lettera di invito.

[R.76] Per le sedi in cui la BGAr è pari a 2 Mbit/s, se il collegamento offerto è TER BG, il collegamento offerto dovrà avere BGAu=BGAd, fatta eccezione per un massimo di 23 sedi per il Ministero degli Affari Esteri e della Cooperazione Internazionale e 7 per il Minstero della Difesa, in cui potranno essere offerti collegamenti con BGAu pari almeno alla metà della BGAd. Al crescere del rapporto di simmetria (BGAu/BGAd) medio dei collegamenti TER BG con BGAr=2Mbit/s, sarà attribuito il punteggio tecnico definito nella lettera di invito.

OFFERTA AVANZATA

[R.77] Per l'**offerta avanzata** è richiesta, per ciascuna sede, l'offerta di un collegamento, Satellitare o Terrestre a Banda Garantita, sia in Affidabilità Standard sia in Affidabilità Elevata. Più in dettaglio, per ciascuna sede il modello presenta le seguenti caratteristiche:

- La Banda Garantita in Accesso richiesta BGAr:
- Per l' Affidabilità Standard:
  - disponibilità minima richiesta;
  - tempo massimo di ripristino richiesto;
- Per l' Affidabilità Elevata:
  - disponibilità minima richiesta;
  - tempo massimo di ripristino richiesto.

Sono altresì indicate le BGAr massime, le disponibilità massime e i tempi minimi di ripristino utilizzati per l'attribuzione dei punteggi tecnici come specificato nella lettera di invito.

[R.78] **Il concorrente dovrà indicare, per ciascuna sede**:

- **tipologia di collegamento: SAT o TER BG**, con gli stessi vincoli di cui ai precedenti [R.71] e [R.72];
- **BGAd e BGAu del collegamento offerto, espresse in Kbit/s**, con i vincoli di cui ai successivi requisiti da [R.79] a [R.83];
- **disponibilità e tempo di ripristino (valore intero, espresso in ore) per il collegamento offerto, per Affidabilità Standard**, che dovranno essere compresi negli intervalli indicati nel modello;
- **disponibilità e tempo di ripristino (valore intero, espresso in ore) per il collegamento offerto, per Affidabilità Elevata**, che dovranno essere compresi negli intervalli indicati nel modello.

[R.79] I collegamenti offerti dovranno avere BGAd almeno pari alla BGAr. Fanno eccezione gli eventuali collegamenti TER BG per i quali, in virtù del [R.75], il concorrente abbia offerto, per l'offerta base, una BGAd inferiore a 2Mbit/s, ma comunque almeno pari a 1 Mbit/s. Limitatamente a tali casi, è ammessa l'offerta della stessa BGAd dell'offerta base, anche nell'offerta avanzata.

[R.80] I collegamenti SAT dovranno avere BGAu almeno pari a 0,25xBGAd. Al crescere del rapporto di simmetria (BGAu/BGAd) medio dei collegamenti SAT, sarà attribuito il punteggio tecnico definito nella lettera di invito.

[R.81] I collegamenti TER BG dovranno avere BGAu pari alla BGAd. Fanno eccezione i collegamenti per i quali, come da [R.79], il concorrente abbia offerto una BGAd pari a quella dell'offerta base. Per tali collegamenti, potrà essere offerta, anche per la BGAu, lo stesso valore offerto per l'offerta base.

[R.82] La somma delle BGAd dei collegamenti offerti per le sedi del MAECI, dovrà essere pari o superiore al 30% della somma delle relative singole BGAr massime. Per le sedi del Ministero della Difesa, la somma delle BGAd dei collegamenti offerti dovrà essere pari o superiore al 60% della somma delle relative singole BGAr massime. Alla somma delle BGAd e delle BGAu offerte per la totalità delle sedi, verrà attribuito il punteggio tecnico definito nella lettera di invito.

[R.83] Per almeno 115 sedi del MAECI, 36 sedi del Ministero della Difesa, 2 sedi dell'Agenzia Dogane e 1 sede della Protezione Civile, la BGAd dei collegamenti offerti dovrà essere almeno pari al doppio della BGAr. Al numero totale di sedi in cui la BGAd offerta sia almeno pari al doppio della BGAr sarà attribuito il punteggio tecnico definito nella lettera di invito.

OFFERTA BEST EFFORT

[R.84] Per l'**offerta best effort** è richiesta, per le sedi di cui al [R.85], l'offerta di un collegamento Terrestre Best Effort. Più in dettaglio, per ciascuna sede il modello presenta le seguenti caratteristiche:

- La Banda Nominale in Accesso richiesta BNAr:
- disponibilità minima richiesta;
- tempo massimo di ripristino richiesto;

Sono altresì indicate le BNAr massime, le disponibilità massime e i tempi minimi di ripristino utilizzati per l'attribuzione dei punteggi tecnici come specificato nella lettera di invito.

[R.85] **I collegamenti Terrestri Best Effort dovranno essere offerti per almeno 115 sedi del MAECI, almeno 36 sedi del Ministero della Difesa e 2 sedi dell'Agenzia delle Dogane**. L'offerta di ulteriori collegamenti TER BE sarà oggetto di punteggio tecnico, come specificato nella lettera di invito. Per le sedi in cui, compatibilmente comunque col predetto vincolo, il concorrente non abbia offerto un collegamento TER BE, ai fini del calcolo dell'importo complessivo offerto e, di conseguenza, del punteggio economico, verrà considerato un importo unitario di Euro 2.500,00, come meglio precisato nella lettera di invito.

[R.86] **Per ciascun collegamento TER BE offerto, il concorrente dovrà indicare**:

- **BNAu e BNAd, espresse in Kbit/s**, nel rispetto dei vincoli di cui al [R.87] e [R.88];
- **disponibilità e tempo di ripristino (valore intero, espresso in ore)**, che dovranno essere compresi negli intervalli indicati nel modello.

[R.87] La BNAd dei collegamenti offerti dovrà essere almeno pari alla La BNAr. Alla somma delle BNAd offerte per la totalità delle sedi, sarà attribuito il punteggio tecnico definito nella lettera di invito

[R.88] La BNAu di ciascun collegamento dovrà essere compresa tra 0,5 BNAd e BNAd. Al crescere del rapporto di simmetria (BNAu/BNAd) medio dei collegamenti TER BE, sarà attribuito il punteggio tecnico definito nella lettera di invito.

2.5 Nuove esigenze di connettività

[R.89] Le Amministrazioni potranno richiedere l'attivazione di servizi di connettività in sedi ulteriori rispetto a quelle di cui al precedente par. 2.4, sia in caso di traslochi delle sedi (rif. par. 5.7.1), sia in caso di incremento delle sedi da inserire nella RIPA.

[R.90] Se la nuova sede sarà situata in una città già presente tra quelle definite nel Modello di Offerta Tecnica, l'Amministrazione potrà scegliere tra i servizi di connettività offerti dal Fornitore per tale sede, alle medesime condizioni tecniche ed economiche offerte in gara. Nel caso la nuova sede si trovi in una città in cui il Modello di Offerta Tecnica presenti diverse sedi con servizi offerti alle stesse condizioni tecniche, allora l'Amministrazione dovrà corrispondere il più alto tra i canoni previsti in offerta economica, a parità di città e di caratteristiche tecniche.

[R.91] In caso di nuove esigenze di connettività in sedi al di fuori delle città presenti nel Modello di Offerta Tecnica, e/o nelle medesime sedi ma con caratteristiche tecniche diverse da quelle richieste in gara e/o offerte dal Fornitore, Consip si riserva di ampliare o modificare i servizi di connettività, ai sensi dell'art. 106 del D.Lgs 50/2016. Tali modifiche/ampliamenti potranno comportare un incremento massimo del 40% dell'importo complessivo dell'Accordo Quadro. Al fine di definire le condizioni tecniche ed economiche dei servizi ampliati/modificati, Consip potrà richiedere al Fornitore, che sarà tenuto a fornire entro 30 giorni dalla richiesta, un benchmark tecnico/economico dei servizi da ampliare/modificare, basato su almeno 3 rilevazioni di mercato.

3. SERVIZI DI SICUREZZA

I servizi di sicurezza sono volti a supportare le Amministrazioni nella prevenzione, rilevamento e gestione degli incidenti informatici.

I servizi di sicurezza richiesti dal presente capitolato si articolano in:

- Next Generation Firewall (NGFW);
- Data Loss Prevention (DLP);
- anti –APT.

Le Amministrazioni che acquisiranno i servizi di connettività di cui al par. 2, dovranno dotare i relativi collegamenti almeno dei servizi Next Generation Firewall. In alternativa, l'Amministrazione potrà fruire di sistemi di sicurezza propri in grado di garantire almeno le funzionalità di firewalling, intrusion detection, monitoraggio e registrazione degli eventi di sicurezza. In tal caso, ai fini dell'attivazione dei servizi di connettività, il Fornitore farà compilare all'Amministrazione un documento di dichiarazione, da allegare al contratto esecutivo, che attesti l'implementazione delle predette funzionalità mediante sistemi di sicurezza propri.

[R.92] Tali servizi dovranno essere erogati in modalità di "outsourcing completo" mediante l'attivazione di un Centro di Gestione della sicurezza (SOC - Security Operating Center), unico e centralizzato per tutte le Amministrazioni.

[R.93] Il Fornitore dovrà prevedere la fornitura, l'installazione/configurazione, la gestione e la manutenzione di tutti gli opportuni componenti hardware e software necessari ad implementare i servizi di sicurezza di cui sopra, da collocare presso la sede dell'Amministrazione, che potrà essere ovunque nel mondo. A mero titolo informativo, non esustivo né vincolante, vengono comunque forniti, all'interno dell'elenco degli indirizzi delle sedi delle Amministrazioni (rif. Premessa della Lettera di Invito) anche gli indirizzi degli uffici ICE dichiarati come potenzialmente interessati ai servizi di sicurezza.

[R.94] Il Punto di Accesso al Servizio (PAS) per i servizi di sicurezza è definito come l'insieme delle interfaccie messe a disposizione sul dispositivo HW di cui al precedente [R.93].

[R.95] Si precisa che per ciascuno dei servizi sopra indicati, il Fornitore, in fase di attivazione del servizio, dovrà concordare con l'Amministrazione le modalità operative e le policy di sicurezza che dovranno essere applicate per il blocco delle minacce e la definizione dei livelli di gravità degli incidenti (gravità alta, media, bassa).

In base alle esigenze espresse dall'Amministrazione nel piano dei fabbisogni, il Fornitore dovrà includere, nel progetto dei fabbisogni, la descrizione di dettaglio delle soluzioni tecniche (sistemi hw e sw impiegati, modalità operative e policy di sicurezza da implementare), nel rispetto delle prescrizioni di sicurezza vigenti.

[R.96] Il Fornitore dal SOC dovrà occuparsi di monitorare costantemente l'emissione degli upgrade/patching/hotfix necessari a risolvere le eventuali vulnerabilità presenti negli elementi architetturali adottati per erogare i servizi di sicurezza. Il Fornitore entro il giorno successivo al rilascio dell'upgrade/patching/hotfix dovrà avviare le attività di analisi e valutazioni propedeutiche all'applicazione delle stesse sui dispositivi di sicurezza che dovrà comunque avvenire tempestivamente. In particolare le patch di sicurezza devono essere applicate entro 2 giorni successivi al rilascio da parte del produttore del dispositivo.

[R.97] Il Fornitore, attraverso il SOC, dovrà erogare un servizio di monitoraggio in tempo reale in proattività degli eventi di sicurezza, in modo da rilevare tempestivamente eventuali tentativi di intrusione o attacchi di sicurezza alla sede per la quale è stato attivato il servizio e consentire l'adozione tempestiva di adeguate contromisure. Successivamente alla rilevazione di possibili attività malevoli, il Fornitore dovrà effettuare dal SOC, l'analisi degli allarmi al fine di discriminare i falsi positivi e classificare il livello di gravità dell'attacco sulla base di una serie di elementi fra cui:

- lista di signatures (qual'ora l'incidente fosse già noto) aggiornata a cura del Fornitore;

- caratteristiche della sede coinvolta e della sua configurazione in termini di rete e sistemi informativi;
- numero di utenti coinvolti

e dovrà provvedere all' apertura di un ticket di "incidente di sicurezza" con indicazione del tipo di incidente, mediante lo strumento di Trouble Ticketing gestito dal call center, monitorandone lo stato di avanzamento fino alla relativa chiusura.

[R.98] Si precisa che per quanto riguarda i tempi entro i quali il Fornitore dovrà provvedere all'apertura del ticket, il Fornitore dovrà rispettare i livelli di servizio definiti nel par. 8, differenziati in base ai seguenti livelli di gravità degli incidenti:

Livello 1 – Alta

Grave impatto sull'operatività e conseguente livello di compromissione di servizi e/o sistemi dell'Amministrazione. Di seguito si riportano a titolo esemplificativo e non esaustivo le condizioni che comportano una classificazione alta del livello di gravità dell'incidente:

- impossibilità tecnica di fornire uno o più servizi classificati come critici dall'Amministrazione;
- estesa infezione virale in grado di compromettere uno o più sistemi e di propagarsi nella rete;
- compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni riservate;
- rilevanti perdite di produttività per gli utenti;
- frode o attività criminale che coinvolga servizi forniti dall'Amministrazione;
- perdita di immagine e/o reputazione.

Livello 2 – Media

I servizi e/o sistemi sono parzialmente interrotti o seriamente degradati. Di seguito si riportano a titolo esemplificativo e non esaustivo le condizioni che comportano una classificazione media del livello di gravità dell'incidente:

- compromissione di server e degrado delle prestazioni;
- attacchi che provocano il funzionamento parziale o intermittente della rete/sistemi/applicazioni;
- impossibilità tecnica di fornire servizi classificati dall'Amministrazione come non critici;
- parziale perdita di produttività per un gruppo di utenti.

Livello 3 – Bassa

Modesto impatto sull'operatività e relativi ambienti per l'erogazione dei servizi. Di seguito si riportano a titolo esemplificativo e non esaustivo le condizioni che comportano una classificazione bassa del livello di gravità dell'incidente:

- informazione (o segnalazione) del rischio di contaminazioni da virus;
- informazione (o segnalazione) del rischio di intrusione da parte di un attaccante;
- parziale perdita di produttività per un numero ristretto di utenti.

[R.99] In particolar modo, in caso di rilevazione di un attacco di gravità elevata, il Fornitore dovrà dare opportuna notifica, tramite posta elettronica o telefono, dell'incidente rilevato e delle azioni da intraprendere, al Responsabile della Sicurezza indicato dall'Amministrazione, alle ULS ed al CERT-PA.

[R.100] Il Fornitore dovrà rendersi disponibile anche a contattare direttamente un referente indicato dall'Amministrazione presente presso la sede periferica, oggetto di attacco, nelle modalità e nei tempi concordati preventivamente con l'Amministrazione.

[R.101] In caso di attacco ad elevata gravità, il Fornitore dovrà adottare tutte le contromisure previste dal codice di comportamento concordato preventivamente con l'Amministrazione.

[R.102] L'Amministrazione potrà richiedere (anche a seguito un tentativo di intrusione o attacco) modifiche alle policy di sicurezza. E' richiesto a tal fine al concorrente di **indicare, nell'offerta tecnica – foglio "Offerta Sicurezza e Supporto"**:

- **tempo di validazione (valore intero, espresso in ore) della richiesta di una nuova regola/policy**. Tale tempo è calcolato a partire dalla richiesta dell'Amministrazione, fino al feedback del Fornitore circa l'applicabilità (validazione), o i motivi di non applicabilità, della richiesta;

- **tempo di implementazione (valore intero, espresso in ore) della richiesta di una nuova regola/policy**. Tale tempo è calcolato a partire dalla comunicazione di validazione del Fornitore all'Amministrazione, fino alla comunicazione di avvenuta implementazione della nuova regola/policy, sempre dal Fornitore all'Amministrazione.

I valori offerti dal concorrente dovranno essere compresi entro gli intervalli indicati nel modello di offerta tecnica, e concorreranno all'attribuzione del punteggio tecnico come definito nella lettera di invito.

[R.103] Il Fornitore avrà l'obbligo di verificare almeno trimestralmente l'effettiva attuazione delle policy di sicurezza al fine di assicurare l'aderenza rispetto a quanto concordato con l'Amministrazione. Dell'esito di tale verifica dovrà fornire comunicazione all'Amministrazione.

[R.104] Per ogni incidente di sicurezza dovrà essere fornito, entro il giorno successivo, un report all'Amministrazione interessata e ad AgID, che descriva la tipologia di attacco subito, le vulnerabilità sfruttate e documenti la sequenza temporale degli eventi verificatisi, e delle contromisure adottate.

[R.105] Giornalmente devono essere inviati all'Amministrazione interessata e al CERT-PA i report riepilogativi degli eventi di sicurezza avvenuti nel giorno precedente a quello dell'invio. I contenuti e la struttura del report dovranno essere concordati preventivamente con l'Amministrazione. A titolo esemplificativo si riporta di seguito l'elenco degli elemente da riportare nel report:

- Domains blocked: in questa sezione devono essere riportati esclusivamente i tentativi di connessione (bloccati) effettuati tramite proxy S-RIPA verso URL/domini segnalati dall'Amministrazione, dal CERT-PA e dal SOC;
- IP blocked: in questa sezione devono essere riportati esclusivamente i tentativi di connessione (bloccati) verso IP segnalati dall'Amministrazione, dal CERT-PA e dal SOC;
- Malicious blocked: in questa sezione devono essere consuntivati i tentativi di connessione bloccati verso destinazioni ritenute malevole (malicious) dal NGFW. Il Fornitore nella predisposizione di questa sezione dovrà occuparsi anche di analizzare e filtrare il report stesso da eventuali falsi positivi (ad esempio connessioni considerate malevole ma in realtà collegate a cookies o redirect di siti leciti);
- DNS blocked: In questa sezione vengono consuntivati tutti i tentativi di risoluzione DNS verso DNS non autorizzati;
- Mail dannose e di phising: numero di mail bloccate e indirizzi mittenti.

[R.106] Per ogni segnalazione riportata nel report giornaliero, dovrà essere riportato anche un dettaglio circa la natura dell'Indicatore di compromissione corrispondente e un'indicazione dei controlli da effetture.

[R.107] Su richiesta dell'Amministrazione, che potrebbe avvenire generalmente a seguito di un evento di sicurezza ad elevata gravità, il Fornitore dovrà rendersi disponibile a fornire i log di sistema generati dai dispositivi di sicurezza utilizzati, predisposti almeno in formato CSV o TXT. Tali log dovranno essere inviati all'Amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta.

[R.108] Per tutti i servizi di sicurezza (Next Generation Firewall, Data Loss Prevention, anti –APT) è previsto un livello di Affidabilità Standard (AS). E' richiesto al concorrente di **indicare, nell'offerta tecnica – foglio "Offerta Sicurezza e Supporto"**:

- **disponibilità (espressa in percentuale) dei servizi di sicurezza, in Affidabilità Standard**;

- **tempo di ripristino (valore intero, espresso in ore) dei servizi di sicurezza, in Affidabilità Standard**.

Entrambe le quantità sono riferite al Punto di Accesso al Servizio (PAS). Per la definizione di disponibilità e tempo di ripristino si rimanda al par. 8. I valori offerti dal concorrente dovranno essere compresi entro gli intervalli indicati nel modello di offerta tecnica, e concorreranno all'attribuzione del punteggio tecnico come definito nella lettera di invito.

[R.109] Per i servizi di Next Generation Firewall, in aggiunta all'Affidabilità Standard, è prevista l'Affidabilità Elevata (AE). E' richiesto a al concorrente di **indicare, nell'offerta tecnica – foglio "Offerta Sicurezza e Supporto"**:

- **disponibilità (espressa in percentuale) dei servizi di sicurezza, in Affidabilità Elevata**;

- **tempo di ripristino (valore intero, espresso in ore) dei servizi di sicurezza, in Affidabilità Elevata**.

Anche in questo caso, i valori offerti dal concorrente dovranno essere compresi entro gli intervalli indicati nel modello di offerta tecnica, e concorreranno all'attribuzione del punteggio tecnico come definito nella lettera di invito.

[R.110] Qualora i servizi di sicurezza di rete vengano contrattualizzati congiuntamente ai servizi di connettività IP ed Internet, il Fornitore avrà facoltà, nel rispetto delle prescrizioni del presente Capitolato tecnico, di erogare i servizi di connettività e sicurezza tramite apparati integrati. Tuttavia, su richiesta dell'Amministrazione, le funzionalità di sicurezza dovranno essere implementate da un sistema fisicamente diverso da quello di accesso alla rete.

[R.111] Tutti i dispositivi utilizzati per l'erogazione dei servizi di sicurezza devono implementare meccanismi di Autenticazione, Autorizzazione e Accounting (AAA) attraverso i quali sia possibile l'accesso logico da console e da remoto per attività di gestione e/o di Amministrazione. Per l'autenticazione possono essere supportati uno o più meccanismi tra quelli riportati di seguito:

- Accesso da console:
  - Server Radius;
  - Password statiche configurabili sul dispositivo utilizzato;
  - Password dinamiche generate per il tramite di token;
  - One Time Password (OTP).
- Accesso da remoto:
  - Password dinamiche generate per il tramite di token;
  - One Time Password (OTP).

[R.112] Le comunicazioni tra la componente di gestione remota centralizzata e la componente locale di NGFW installata presso la sede dell'Amministrazionedovranno essere cifrate. Dovrà essere possibile la gestione da remoto (es. monitoring, configuration e trouble- shoooting) di tutti gli apparati di rete attraverso il protocollo standard SNMP almeno v2.

[R.113] I sistemi adottati devono rilevare e registrare i tentativi di accesso non autorizzato al sistema stesso.

[R.114] Per quanto riguarda le attività di gestione e Amministrazione, i sistemi devono essere in grado di generare log di audit contenenti almeno le seguenti informazioni: data, ora evento, identità del soggetto, successo/fallimento dell'evento.

[R.115] I dati registrati dal sistema di sicurezza devono essere disponibili per l'uso da parte degli utenti abilitati.

[R.116] I file di log devono essere protetti da modifiche o cancellazioni non autorizzate, in conformità alla normativa vigente.

[R.117] Nei casi in cui nuove tipologie di minacce informatiche richiedano nuovo servizi di sicurezza o, comunque, l'evoluzione tecnologica renda disponibili servizi più adeguati alle esigenze delle Amministrazioni, Consip si riserva di ampliare o modificare i servizi di sicurezza, ai sensi dell'art. 106 del D.Lgs 50/2016. Tali modifiche/ampliamenti potranno comportare un incremento massimo del 40% dell'importo complessivo dell'Accordo Quadro. Al fine di definire le condizioni tecniche ed economiche dei servizi ampliati/modificati, Consip potrà richiedere al Fornitore, che

sarà tenuto a fornire entro 30 giorni dalla richiesta, un banchmark tecnico/economico dei servizi da ampliare/modificare, basato su almeno 3 rilevazioni di mercato.

3.1 Next Generation Firewall

Il servizio di "next generation firewall" deve implementare le seguenti caratteristiche di base:
[R.118] funzionalità di network firewall (es. policy enforcement, statefull inspection, packet filtering, Network Address Translation (NAT), Port Address Translation (PAT) Management, VPN client to site e site to site, etc.);

[R.119] URL Filtering che consente di abilitare la navigazione WEB che avviene per il tramite del NGFW solo a determinate postazioni, di controllare le statistiche sulla navigazione e/o di bloccare l'accesso a particolari siti Internet/Intranet;

[R.120] meccanismi antispoofing;

[R.121] meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service (ad esempio mediante funzioni di ingress/egress filtering) tesi a saturare la banda di rete disponibile o ad esaurire le risorse dei server che espongono i servizi erogati dall'Amministrazione;

[R.122] Intrusion Prevention (IPS) per il rilevamento e il blocco delle minacce attraverso l'adozione di almeno le seguenti tecniche di rilevazione degli attacchi: signature analysis (analisi basata su firma), anomaly detection (es. individuazione delle anomalie nei protocolli comunemente utilizzati nell'ambito delle reti IP), analisi euristica o comportamentale (adottata per riconoscere minacce per le quali non sono state già definite le firme). Per il riconoscimento dei potenziali attacchi, il servizio fornito dal Fornitore dovrà utilizzare informazioni presenti in una banca dati centrale costantemente aggiornata e compatibile con le Common Vulnerabilities and Exposures (CVE-compatible). In caso di rilevamento di attacco, il sistema deve essere in grado di impedirne l'esecuzione attraverso l'esecuzioni di differenti tecniche, quali ad esempio: Drop packet/session, ossia scarto del pacchetto/sessione e Close Client/Server, ossia invio di un segnale di chiusura lato client e/o server.

[R.123] deep packet inspection per scansionare l'intero payload dei pacchetti;

[R.124] SSL inspection per l'ispezione del traffico cifrato;

[R.125] rilevazione e blocco dei malware e degli spam (anti-malware e anti-spam). Il sistema deve permettere la protezione da codice dannoso che può propagarsi tramite lo scambio di posta elettronica, tramite la navigazione web e tramite il trasferimento di file mediante FTP, nonché la protezione di attacchi informativi veicolati tramite il protocollo HTTP. Il servizio fornito dal Fornitore dovrà permettere: la scansione in tempo reale; il filtraggio dei contenuti e l'esclusione basata sul tipo di file trasferito (vbs, exe, pif, bat, etc.); il controllo della presenza di codice malevolo anche nei file compressi (es. in formato zip, rar, etc); il supporto di blacklist (liste contenenti domini di mail o indirizzi di mail indesiderati);

[R.126] application filtering & monitoring. Il sistema deve permettere di effettuare un'analisi delle applicazioni in grado di di permettere il controllo e la visibilità delle applicazioni web indipendentemente dalla porta e dal protocollo utilizzati dall'applicazione stessa. Il sistema deve anche essere in grado di bloccare, e laddove possibile limitare, la banda utilizzabile e il traffico relativo alle applicazioni selezionate sulla base di politiche impostate secondo i requisiti dichiarati dalle Amministrazioni nonchè di applicare politiche basate sull'identità degli utenti, consentendo o negando l'uso di tali applicazioni sulla base del profilo dell'utente o di gruppi di utenti;

[R.127] supportare tutti i protocolli specificati nella suite di protocolli Internet;

[R.128] auditing e logging che consente l'analisi del traffico che attraversa il NGFW;

[R.129] modulo di gestione che consente di configurare e monitorare il sistema NGFW;

[R.130] possibilità di generare report sulle analisi svolte.

[R.131] Il NGFW dovrà essere configurato in modo che il flusso dati tra la rete interna dell'Amministrazione (intesa come l'insieme dei segmenti LAN protetti) e la rete del Fornitore transiti esclusivamente attraverso di esso.

[R.132] Il servizio fornito deve disporre di una struttura in grado di rilasciare aggiornamenti delle signature utilizzate per il rilevamento degli attacchi. Il sistema deve quindi essere in grado di aggiornare le signature automaticamente, senza l'intervento manuale dell'operatore.

[R.133] Il servizio deve comprendere la funzionalità di realizzazione di reti private virtuali basate sullo standard IPsec come definito dall'IPsec Working Group dell'IETF (RFC 4301). Specificatamente per il servizio VPN IPsec devono essere implementate le seguenti caratteristiche:

- supporto per IPsec "Tunnel mode" e "Transport mode" come definiti nella specifica pubblica RFC 4301;
- Data origin authentication che verifica l'autenticità del mittente di ciascun datagramma IP;
- Data integrity che verifica che il contenuto di ciascun datagramma non sia stato modificato (deliberatamente o a causa di errori di linea) durante il transito tra sorgente e destinazione;
- Data confidentiality che nasconde il testo in chiaro contenuto in un messaggio, mediante l'impiego della crittografia;
- Replay protection che assicura che una terza parte non autorizzata, intercettato un datagramma IP, non sia in grado, a posteriori, di rispedirlo a destinazione per qualche scopo illecito;
- Relativamente all'autenticazione dei nodi e alla gestione delle associazioni di sicurezza, la creazione e la negoziazione delle associazioni di sicurezza (SA, Security Association) del sistema IPsec devono essere garantite attraverso i meccanismi identificati dal protocollo Internet Key Exchange (IKE) secondo la specifica pubblica RFC 5996. Tali meccanismi devono supportare sia l'autenticazione mediante segreto condiviso ("pre-shared key") che quella mediante certificati digitali conformi allo standard ISO/IEC 9594-8 (X.509v3);
- Utilizzo di certificati X.509v3 emessi esclusivamente da una propria Certification Authority di rete, situata sul territorio italiano;
- il formato per le richieste dei certificati dovrà essere conforme allo standard PKCS#10;
- adozione di adeguati meccanismi di protezione della chiave privata e delle chiavi di sessione memorizzate nei dispositivi utilizzati
- prima dell'apertura di un nuovo tunnel crittografico, i dispositivi dovranno verificare lo stato di validità del certificato con l'ausilio delle Certification Revocation List o, in alternativa e preferibilmente, direttamente online con il supporto del protocollo OCSP.

[R.134] Il Fornitore deve erogare il servizio di sicurezza utilizzando apparati che si interfaccino con i sistemi dell'Amministrazione attraverso interfacce conformi agli standard IEEE Ethernet/Fast-Ethernet/Gigabit - Ethernet 10/100/1000 Autosensing, in particolare:

- gli apparati previsti nelle sedi centrali delle Amministrazioni dovranno essere dotati di almeno n. 6 interfacce Ethernet/Fast-Ethernet/Gigabit-Ethernet 10/100/1000 Autosensing;
- gli apparati previsti nelle sedi periferiche delle Amministrazioni dovranno essere dotati di almeno n. 4 interfacce Ethernet/Fast-Ethernet /Gigabit-Ethernet 10/100/1000 Autosensing.

Il concorrente dovrà indicare nella Dichiarazione di Offerta Economica il canone mensile del servizio per ciascuna delle seguenti fasce, definite in base alla banda nominale di accesso disponibile presso la sede dell' Amministrazione che richiederà il servizio:

- banda nominale fino a 50 Mbps, differenziata in Affidabilità Standard e Affidabilità Elevata;

- banda nominale compresa tra 51 Mbps e 100 Mbps, differenziata in Affidabilità Standard e Affidabilità Elevata;
- banda nominale compresa tra 101 Mbps e 500 Mbps (solo Affidabilità Elevata);
- banda nominale compresa tra 501 Mbps e 1000 Mbps (solo Affidabilità Elevata).

Il dispositivo NGFW adottato dal Fornitore, dovrà essere adeguatamente dimensionato in termini di throughput, tenendo in considerazione ciascuna fascia di banda nominale precedentemente indicata, per consentire la corretta e completa erogazione del servizio di sicurezza secondo i requisiti e le caratteristiche su riportate.

3.2 Data loss/leak prevention

[R.135] Il servizio di "data loss/leak prevention" (o DLP) deve consentire alle Amministrazioni la protezione dei dati da accessi non autorizzati o violazioni delle policy di sicurezza e riducendo il rischio di perdita, danno o svantaggio competitivo.

[R.136] Il servizio deve garantire supervisione e controllo dei dati indipendentemente dal fatto che siano archiviati o in transito sulla rete, includendo attività di monitoraggio e protezione dei dati in-use (accesso tramite endpoint – desktop e laptop), in-motion (traffico rete), e at-rest (sui supporti di memorizzazione).

[R.137] Si precisa inoltre che il servizio include anche l'attività di gestione degli incident descritta nel paragrafo 3.

[R.138] Il Fornitore, nell'ambito del servizio "data loss/leak prevention" deve garantire la disponibilità per l'Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- rilevazione dei dati che transitano nell'organizzazione, ovunque siano archiviati, e valutazione del rischio di perdita di dati (DLP Risk Assessment);
- analisi e classificazione dei dati (DLP Information classification);
- possibilità di creare regole predefinite per la protezione dei dati, identificando i sistemi in cui sono memorizzati (ad esempio porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, dispositivi di acquisizione immagini, modem) per assicurarsi che siano usati in conformità con le politiche di privacy e sicurezza (DLP data at rest);
- generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite, visibilità e controllo sui dati in movimento, sia che si trovino in messaggi e-mail, nella mail sul Web, nell'instant messaging, e nei protocolli di rete (DLP data in motion);
- possibilità di generare report sulle analisi svolte;
- generazione audit trail e gestione profili di audit.
- Dal punto di vista tecnico, il servizio deve prevedere almeno:
- compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport;
- compatibilità con i sistemi operativi Windows, Mac OS, Linux, Android e iOS.

Il concorrente dovrà indicare nella Dichiarazione di Offerta Economica il canone mensile per endpoint.

L'Amministrazione potrà richiedere, nell'ambito dei servizi professionali di supporto operativo di cui al par. 5.9, le attività necessarie ad implementare un sistema di Data loss / leak prevention. Le attività potranno riguardare:

- analisi, assessment e classificazione delle informazioni nonchè definizione dell'ambito di intervento;
- installazione di componenti software client DLP su endpoint.

3.3 Anti - APT

[R.139] Il servizio anti - APT, basato su SANDBOX, dovrà garantire alle Amministrazioni protezione da minacce avanzate di tipo persistente e malware zero-day.

[R.140] Tale servizio prevede l'intercettazione del traffico mediante il NGFW, di cui al precedente paragrafo, e l'invio dei file – non analizzati precedentemente – verso l'infrastruttura "sandbox" predisposta dal Fornitore.

[R.141] I file andranno eseguiti in ambiente protetto così da poter essere sottoposti ad analisi comportamentale e consentire la rilevazione di attacchi che utilizzano tecniche per mascherare la loro natura (es. eventuali polimorfismi, tecniche di evasione, offuscamento e anomalie da emulazione di codice).

[R.142] E' richiesto un feedback sul livello di rischio e l'eventuale produzione di signature utilizzabili dal dispositivo di sicurezza installato presso le PA. Deve essere possibile configurare il sistema per far sì che nessuna informazione o dato del Cliente sia trasferito all'esterno dell'ambito S-Ripa.

[R.143] Il concorrente dovrà indicare nella Dichiarazione di Offerta Economica l'una tantum di attivazione e il canone mensile del servizio "Anti - APT", corrispondente alla capacità del servizio di analizzare almeno 130 file per ora.

[R.144] Il servizio anti APT potrà essere attivato solo centralmente su base Amministrazione e non su base sede, e gestito/supervisionato dal SOC del Fornitore. Resta inteso che il servizio attivato per la singola Amministrazione, con il pagamento di una sola una tantum e un solo canone mensile, sarà comunque messo a disposizione e fruito da ciascuna sede della stessa, al fine di prottegersi da attacchi di tipo APT.

[R.145] L'Amministrazione, in base alle proprie esigenze di protezione, alla sua banda di accesso nominale, alla propria infrastruttura di rete e al numero e al tipo di file da far analizzare attraverso il servizio anti – APT, individuerà con il supporto del Fornitore secondo le modalità indicate al par. 6 del capitolato tecnico, il corretto dimensionamento del servizio Anti-APT da acquistare in termini di capacità complessiva di file per ora da analizzare.

4. SERVIZI VoIP (Voice over IP) E DI COMUNICAZIONE EVOLUTA

I servizi di *Voice over IP* consentono, alle sedi di ciascuna Amministrazione contraente, di effettuare chiamate telefoniche utilizzando il medesimo accesso attraverso il quale viene fornita la connettività IP.
Per usufruire dei servizi VoIP in una data sede, l'Amministrazione dovrà contrattualizzare un numero di linee VoIP pari al numero di chiamate effettuabili contemporaneamente da e verso la sede. E' a tal fine richiesto al concorrente di indicare, nell'Offerta Economica, il canone mensile della linea VoIP, sia in Affidabilità Standard sia in Affidabilità Elevata, da intendersi remunerativo di tutti gli eventuali adeguamenti (tra cui la configurazione dei canali voce richiesti dall'Amministrazione) necessari alla sua erogazione a livello end-to-end, nel rispetto dei parametri di qualità di cui al par. 8.
Il PAS della linea VoIP è l'interfaccia tra l'IP-PBX o l'IP Voice gateway, e l'apparato di accesso del collegamento IP.
Alla linea VoIP potrà essere associato il servizio opzionale di "gestione del traffico off-net", di cui al par. 4.3.
I servizi di comunicazione evoluta mettono a disposizione delle Amministrazioni le componenti hardware e software per realizzare soluzioni di:

- **"IP Telephony"**,che prevede la messa in opera e la gestione di una infrastruttura IP-based, con postazioni utente basate su tecnologia VoIP;
- **"IP Trunking"**, che si pone l'obiettivo di garantire il minimo impatto sull'infrastruttura esistente presso l'Amministrazione. In questo caso, infatti, il Fornitore dovrà fornire, per ogni sito, un IP Voice Gateway in grado di connettere il centralino telefonico locale, dell'Amministrazione, con la rete IP, trasf\ormando il traffico voce e fax in pacchetti IP;
- **"Videocomunicazione di qualità su IP"**, che consente la comunicazione in tempo reale ed in modalità interattiva con utenti dislocati remotamente in sale attrezzate per videoconferenze, mediante l'utilizzo di immagini e suoni e lo scambio di dati elettronici, con qualità video ad alta definizione e qualità audio CD full-duplex, offrendo un elevato livello di interattività che consente di virtualizzare l'interazione tra utenti (telepresenza).

[R.146] I servizi VoIP, acquisibili dalle Amministrazioni su base sede, dovranno consentire la trasmissione/ricezione della voce da/verso proprie sedi dell'Amministrazione, facendo uso dei servizi di connettività di cui al par. 2.

[R.147] Il Fornitore dovrà garantire l'interoperabilità tra le soluzioni IP Telephony ed IP Trunking proposte, al fine di consentire la comunicazione tra una sede con soluzione IP Telephony ed un'altra sede con soluzione IP Trunking.

[R.148] Il Fornitore dovrà considerare inclusi nei servizi VoIP tutti gli adeguamenti necessari alla sua erogazione a livello end-to-end, nel rispetto dei parametri di qualità del servizio VoIP (ri. par. 8) e senza comportare alcun degrado degli SLA previsti per gli altri servizi contrattualizzati. In particolare, dovrà essere inclusa nel servizio la configurazione dei "canali voce" richiesti dall'Amministrazione, ossia del numero di chiamate attivabili contemporaneamente da/verso la sede.

[R.149] Nel caso in cui la velocità della linea di accesso non risulti adeguata al trattamento e trasporto del traffico VoIP richiesto dall'Amministrazione (in termini di numero di "canali voce" richiesti), rimarrà a carico dell'Amministrazione stessa l'upgrade della velocità della linea di accesso.

[R.150] Il servizio VoIP non include:

- la realizzazione e la gestione delle infrastrutture di rete IP (cablaggio strutturato), fonia TDM ed alimentazione presso i siti dell'Amministrazione;
- il servizio di commutazione del traffico su rete telefonica pubblica ed il relativo rilegamento trasmissivo, a meno che non sia richiesto dall'Amministrazione il servizio di gestione del traffico Off-net (rif. 4.3).

[R.151] Le due tipologie di soluzione VoIP dovranno essere conformi ai principali standardard internazionali relativi al trasporto della voce su IP, almeno al SIP (Session Initiation Protocol - RFC 3261) e, eventualmente, anche al H.323 ITU-T Recommendations. Gli ulteriori protocolli di segnalazione supportati nonché quelli per la trasmissione in tempo reale dei dati su rete IP e per la codifica audio saranno specificati successivamente nella documentazione di riscontro.

[R.152] Il sistema dovrà prevedere meccanismi di trattamento del segnale audio (echo cancellation), tali da prevenire problematiche tipiche di "Audio di ritorno".

[R.153] Sarà completamente a carico del Fornitore l'installazione e la configurazione del sistema.

[R.154] Dovrà essere garantita la conformità a tutte le norme applicabili in vigore presso lo Stato in cui è situata la sede dell'Amministrazione nella quale viene attivato il servizio VoIP.

[R.155] Dovrà essere possibile la gestione da remoto (es. monitoring, configuration e trouble- shoooting) di tutti gli apparati di rete attraverso il protocollo standard SNMP (versione 2 o successive).

[R.156] Nel corso dell'erogazione dei servizi di VoIP e di Comunicazione Evoluta, il Fornitore dovrà implementare le modifiche di configurazione dei servizi richieste dalle Amministrazioni, con lo SLA definito nel par. 8.

4.1 Soluzione IP Telephony

[R.157] Il Fornitore dovrà mettere a disposizione di ogni singola Amministrazione richiedente, tutte le infrastrutture hardware e software necessarie per l'erogazione del servizio VoIP in modalità "IP Telephony". In particolare, la fornitura del servizio comprende la messa in opera e la gestione di un sistema organizzato secondo le seguenti componenti:

- apparati IP-PBX;
- postazioni utente basate su tecnologia VoIP;
- interfacciamento con la rete telefonica pubblica (PSTN);

[R.158] Il servizio offerto dal Fornitore dovrà inoltre integrarsi completamente con le infrastrutture pre-esistenti, sia per quanto riguarda la rete IP (piano di indirizzamento, presenza di Network Address Translation, presenza di proxy di livello applicativo), sia per quanto riguarda il piano di numerazione dei derivati telefonici. A questo scopo, laddove siano presenti componenti al di fuori dell'ambito dei servizi oggetto di gara, dovrà essere fornito supporto tecnico all'Amministrazione o ad eventuale terze parti da essa indicate per la definizione delle configurazioni da adottare.

[R.159] Le soluzioni proposte dovranno essere aperte al cambiamento, e cioè dovranno essere erogate in modo tale da consentire l'introduzione di funzionalità evolute di IP Telephony al fine di garantire l'integrazione di tutti i servizi di telefonia dell'Amministrazione sulla stessa infrastruttura VoIP.

[R.160] Il Fornitore dovrà garantire i seguenti servizi:

- **Servizi intra-dominio**, ossia tra due sedi della stessa Amministrazione per le quali è stato attivato il servizio VoIP, con traffico veicolato attraverso la rete IP del Fornitore senza transitare da rete pubblica:

  - Chiamata base
  - Trasporto dei toni DTMF
  - Presentazione dell'indirizzo/alias del chiamante
  - Presentazione del nome del chiamante

- Restrizione sulla presentazione del nome del chiamante
- Trasferimento incondizionato di chiamata
- Trasferimento condizionato di chiamata
- Redirezione di chiamata su occupato
- Redirezione di chiamata su nessuna risposta
- Trattenuta
- Parcheggio
- Chiamata presa da altro terminale
- Richiamata
- Conferenza a tre
- Autenticazione dell'utente
- Indicazione di chiamata in attesa
- Musica su attesa
- Gestione di suonerie differenziate
- Gestione lista chiamate in contemporanea
- Sbarramento delle chiamate
- Direttore segretaria
- Numeri brevi
- Rubrica personale e aziendale
- Funzioni FAX

▪ **Servizi di interfacciamento con PSTN**:

- Chiamata base
- Presentazione del numero del chiamante
- Trasporto dei toni DTMF
- Funzioni FAX

In aggiunta ai servizi sopra-elencati, il Fornitore è tenuto ad offrire il servizio di segreteria telefonica, qualora richiesto dall'Amministrazione.

[R.161] Il Fornitore dovrà prendersi carico delle seguenti attività operative:

- installazione, configurazione e gestione delle postazioni VoIP;
- installazione, configurazione e gestione di tutti gli elementi attivi facenti parte della soluzione VoIP;
- gestione del piano di numerazione;
- gestione completa di tutte le chiamate intra-dominio;
- corretto instradamento verso/da le reti telefoniche pubbliche (PSTN).

[R.162] Il Fornitore dovrà realizzare la soluzione "IP Telephony" per la fornitura dei servizi di fonia sopra specificati, includendo i seguenti elementi funzionali:

- Stazioni telefoniche IP (Wired IP phone e Wireless IP phone);
- Call Control Function (CCF): elemento funzionale, sede dell'esecuzione della logica di servizio, che gestisce la segnalazione per il controllo delle fasi di una chiamata, e l'instradamento del traffico voce attraverso la rete dati del Fornitore;
- Media Gateway (MGW): elemento funzionale cui è demandato l'interfacciamento con la rete PSTN, che dovrà avvenire localmente in ogni sede delle Amministrazioni. Il Fornitore dovrà garantire la presenza di un numero adeguato di interfacce per il break out locale verso PSTN (sulla base delle consistenze di fonia della sede).

[R.163] Il Fornitore dovrà fornire Media Gateway dimensionati sulla base delle esigenze delle singole sedi ed equipaggiati con interfacce ISDN BRI o PRI in numero tale da soddisfare i requisiti tecnologici e di traffico espressi dalle Amministrazioni.

[R.164] Il Fornitore dovrà introdurre la soluzione VoIP in modo congruente e compatibile con il piano di numerazione pre-esistente. Sulla base delle richieste dell'Amministrazione, le postazioni VoIP dovranno:

- riutilizzare numerazioni interne già assegnate in precedenza al dominio tradizionale, oppure
- utilizzare nuove estensioni, oppure
- introdurre un piano di numerazione ex-novo utilizzando una diversa radice.

[R.165] Il Fornitore dovrà fornire stazioni telefoniche IP "Wired IP phone", con le seguenti caratteristiche:

- tele-alimentazione remota attraverso l'interfaccia Ethernet (standard IEEE 802.3af);
- supporto dell'assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP (IETF RFC2131);
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- monitor con lettura a 40 caratteri;
- controllo del contrasto;
- 3 tasti sensibili al contesto (soft-key);
- tastiera alfanumerica;
- modalità di ascolto viva voce e amplificata;
- 10 tasti programmabili dall'utente e dall'Amministratore del sistema;
- rubrica personale con 15 numeri;
- controllo del volume per il ricevitore;
- servizio di guida in linea integrato per le operazioni di programmazione;
- messaggi di notifica su display multilingua (Italiano, Inglese)
- switch interno con porte Ethernet 10/100/1000 e rilevamento automatico della presenza di un PC connesso
- supporto dello standard 802.1q

[R.166] Il Fornitore dovrà fornire stazioni telefoniche IP "Wireless IP phone", che non richiedono un collegamento wired alla LAN dell'Amministrazione ma vengono connesse tramite opportuni access point, e con le seguenti caratteristiche:

- assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP;
- supporto dello standard IEEE 802.11b/g/n;
- supporto dello standard IEEE 802.1q;
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- funzionalità WPA e WPA2;
- monitor LCD;
- 2 tasti sensibili al contesto (soft-key);
- blocco tasti;
- regolazione del volume del ricevitore;
- 8 tasti programmabili dall'utente e dall'amministratore del sistema;
- range: fino a 300m in out-door, fino a 75m in in-door;
- rubrica personale con 12 numeri;
- autonomia: fino a 24 ore in stand-by e fino a 4 ore in conversazione;
- messaggi di notifica su display multilingua (Italiano, Inglese).

[R.167] Il servizio dovrà garantire funzionalità di autenticazione ed autorizzazione nei confronti degli utenti che utilizzano postazioni VoIP. Tali funzionalità dovranno essere implementate mediante comunicazioni logiche IP sicure.

[R.168] Il servizio IP Telephony potrà essere richiesto dalle Amministrazioni, su base sede, in Affidabilità Standard o Elevata, e sarà remunerato al Fornitore in base al numero di derivati gestiti. E' quindi richiesto al concorrente di indicare, in Offerta Economica, il canone mensile offerto, in Affidabilità Standard ed Elevata, per derivato. Tale importo non include i telefoni, i cui canoni saranno corrisposti a parte dalle Amministrazioni, e per i quali è richiesto al concorrente di indicare i canoni mensili offerti, in Offerta Economica, per le due tipologie previste, in Affidabilità Standard.

[R.169] Per il servizio IP Telephony non è definito un PAS. I livelli di servizio di cui al par. 8 sono relativi ai tempi di ripristino a seguito dei disservizi di una qualunque delle componenti di servizio dell'infrastruttura IP Telephony sopra descritta, e alla risultante disponibilità, su base sede, dell'infrastruttura stessa.

4.2 Soluzione IP Trunking

[R.170] Fermo restando l'obbligo per il Fornitore di rendere disponibile la soluzione di "IP Telephony", la singola Amministrazione potrà richiedere, per ciascuna sede, la realizzazione di una soluzione che prevede l'integrazione delle infrastrutture voce-dati al fine di massimizzare il riutilizzo delle esistenti infrastrutture di telefonia privata.

[R.171] Tale soluzione dovrà prevedere la fornitura, installazione e gestione di opportuni Gateway (IP Voice Gateway) per interconnettere il centralino telefonico esistente con l'apparato di accesso, trasformando il traffico voce e fax in pacchetti IP.

[R.172] L'apparato di accesso dovrà essere configurato per gestire il traffico voce in modo tale da evitare problemi di congestione di traffico della rete locale.

[R.173] L'instradamento del traffico voce attraverso la rete dati del Fornitore dovrà essere controllata da una funzione di controllo di chiamata (da ora in poi per brevità CCF). Il numero telefonico composto dall'utente verrà inoltrato dal centralino all'IP Voice Gateway che, in congiunzione col servizio offerto dal CCF, è in grado di instradare correttamente la chiamata.

[R.174] La CCF ha come funzione primaria quella di essere il sistema di gestione della registrazione, accesso e controllo di stato (RAS: Registration, Admission & Status) di tutti i gateway voce della rete dati. Inoltre, esso fornisce la corrispondenza tra indirizzo IP e numero di telefono associato, nonché il controllo della banda.

[R.175] Il servizio IP Trunking potrà essere richiesto dalle Amministrazioni, su base sede, in Affidabilità Standard o Elevata, e sarà remunerato al Fornitore in base al numero di derivati gestiti. E' quindi richiesto al concorrente di indicare, in Offerta Economica, il canone mensile offerto, in Affidabilità Standard ed Elevata, per derivato.

[R.176] Per il servizio IP Trunking non è definito un PAS. I livelli di servizio di cui al par. 8 sono relativi ai tempi di ripristino a seguito dei disservizi del Gateway, e alla risultante disponibilità, su base sede, dell'apparato.

4.3 Servizio di gestione del traffico Off-net

[R.177] Il servizio di gestione del traffico Off-net è un'opzione dei servizi VoIP descritti in precedenza, per offrire alle Amministrazioni la possibilità di effettuare/ricevere chiamate verso/da rete pubblica nelle diverse zone internazionali interessate dal traffico telefonico S-RIPA.

[R.178] Il servizio di gestione del traffico Off-net può essere acquistato dalle Amministrazioni esclusivamente come servizio opzionale con canone aggiuntivo a quello della linea VoIP. E' a tal fine richiesto al concorrente di indicare, in Offerta Economica, il canone mensile offerto per la linea VoIP Off-Net.

[R.179] Il concorrente dovrà garantire il servizio di gestione del traffico Off-net in almeno 25 Paesi tra quelli elencati nel Modello di offerta tecnica.

[R.180] **Il concorrente dovrà indicare, nell'offerta tecnica – foglio "Offerta VoIP", in quali Paesi offra il servizio di gestione del traffico Off-net, nel rispetto del vincolo di cui al precedente [R.179]**. L'offerta del servizio in un numero maggiore di Paesi rispetto al minimo richiesto, sarà oggetto di attribuzione del punteggio tecnico, come precisato nella lettera di invito.

[R.181] E' onere del Fornitore la trasduzione del traffico VoIP Off-net dell'Ammministrazione, il suo interfacciamento e la sua gestione sulla rete telefonica pubblica.

[R.182] I servizi devono essere erogati con l'obbligo del rispetto del piano di numerazione telefonica esistente.

[R.183] Il servizio deve garantire in ogni caso la presentazione del numero chiamante e la georeferenziazione dell'utente chiamante in caso di utilizzo dei servizi/numerazioni di emergenza.

[R.184] Nell'ambito di una chiamata fra una PA e un'utenza di rete pubblica devono essere garantiti almeno i servizi elencati in tabella:

- Chiamata base,
- Trasporto toni DTMF
- Presentazione dell'indirizzo/alias del chiamante
- Fax

[R.185] Il servizio dovrà prevedere, per la gestione del traffico generato dalle utenze VoIP S-RIPA e diretto verso rete telefonica internazionale, una tariffazione a minuto di chiamata per le chiamate uscenti secondo le tre seguenti direttrici:

ZONA 1 - verso l'Italia;

ZONA 2 - verso lo stesso paese di origine della chiamata;

ZONA 3 - verso il resto del mondo.

Per ciascuna di tali zone il concorrente dovrà indicare, in Offerta Economica, il prezzo al minuto offerto.

4.4 Servizio di videocomunicazione di qualità su IP

[R.186] Il servizio di Videocomunicazione di Qualità consiste nella messa a disposizione e nella gestione di tutte le infrastrutture, sia hardware che software, e di tutte le attività necessarie a rendere fruibili in modalità non esclusiva all'Amministrazione le funzionalità sopra descritte. Agli utenti del servizio dovrà essere fornita assistenza tramite un Call Center con le modalità di cui al successivo paragrafo 5.4.

[R.187] Il Fornitore dovrà erogare il servizio di Videocomunicazione di qualità su IP, contrattualizzabile su base sede, utilizzando il medesimo accesso attraverso il quale viene fornita la connettività IP.

[R.188] Il Fornitore dovrà mettere a disposizione tutte le infrastrutture hardware e software necessarie per l'erogazione del servizio end-to-end (servizio "chiavi in mano"), facendosi carico della fornitura, installazione e manutenzione dei terminali (end- point) previste presso le Amministrazioni.

[R.189] Il Fornitore dovrà considerare inclusi nel servizio di Videocomunicazione di qualità su IP tutti gli adeguamenti necessari alla sua erogazione nel rispetto dei parametri di qualità del servizio stesso (cfr. par. 8.) e senza comportare alcun degrado degli SLA previsti per gli altri servizi contrattualizzati. In particolare, dovrà essere inclusa nel servizio la configurazione dei "canali di videocomunicazione" richiesti dall'Amministrazione, ossia del numero di chiamate audio/video attivabili contemporaneamente da/verso la sede.

[R.190] Nel caso in cui la velocità della linea di accesso non risulti adeguata al trattamento e trasporto dei flussi multimediali richiesti dall'Amministrazione (in termini di numero di "canali di videocomunicazione" richiesti), rimarrà a carico dell'Amministrazione stessa l'upgrade della velocità della linea di accesso.

[R.191] Il servizio fornito dal Fornitore dovrà garantire la conformità agli standard applicabili, al fine di consentire la piena interoperabilità con sistemi di videocomunicazione eventualmente presenti nell'Amministrazione; in ogni caso, il servizio dovrà essere erogato via rete IP, garantendo la conformità almeno ai seguenti standard:

- H.323 ITU-T Recommendations ovvero SIP (Session Initiation Protocol - RFC 3261) per quanto concerne la segnalazione;
- H.460 ITU-T Recommendations per quanto concerne la funzionalità di NAT e Firewall traversal;
- RTP (Real time Transport Protocol - RFC 3550) per quanto riguarda la trasmissione in tempo reale dei dati su rete IP.

[R.192] Il sistema dovrà consentire la gestione di sessioni non solo punto – punto, ma anche multi-punto permettendo di connettere in un'unica sessione tre o più partecipanti, fino ad un massimo non inferiore a 5.

[R.193] Il sistema fornito dal Fornitore dovrà permettere il controllo totale sulle modalità di invito, partecipazione e di moderazione di una sessione di videocomunicazione.

[R.194] Il sistema dovrà prevedere meccanismi di trattamento del segnale audio (echo cancellation), tali da prevenire problematiche tipiche di "Audio di ritorno".

[R.195] Il sistema dovrà offrire la possibilità di disporre del tracciamento di ciascuna sessione, rendendo disponibili almeno le seguenti informazioni: partecipanti alla sessione, data e ora di inizio/fine sessione, esito della sessione.

[R.196] Il sistema dovrà garantire la disponibilità del repository delle registrazioni per almeno sei mesi solari; con il termine "registrazioni", si intende la tracciatura ed il salvataggio delle seguenti informazioni minime: partecipanti alla sessione; data e ora di inizio/fine sessione.

[R.197] Il sistema dovrà mettere a disposizione una interfaccia verso servizi di "directory" centralizzati, al fine di poter memorizzare e consultare (tramite protocollo LDAP) una rubrica per gli indirizzi dei soggetti contattabili nell'ambito del servizio.

[R.198] Il sistema dovrà consentire un numero di sessioni di videocomunicazione contemporanee per Amministrazione non inferiore a 10.

[R.199] Il sistema fornito dal Fornitore dovrà garantire la conformità a tutte le norme applicabili in vigore presso lo stato in cui è situata la sede dell'Amministrazione nella quale viene attivato il servizio di videocomunicazione collaborativa.

[R.200] Il sistema fornito dal Fornitore dovrà garantire la gestione del servizio anche in presenza di ambienti con vincoli di sicurezza, offrendo opportuni meccanismi di cifratura dei dati al fine di garantire la confidenzialità e l'integrità delle comunicazioni critiche.

[R.201] Il Fornitore dovrà considerare inclusi nel servizio di Videoconferenza di qualità tutti gli eventuali adeguamenti necessari alla sua erogazione a livello end-to-end, nel rispetto dei parametri di qualità del servizio stesso (cfr. par. 8.) e senza comportare alcun degrado degli SLA previsti per gli altri servizi contrattualizzati. In particolare, dovrà essere inclusa nel servizio la configurazione dei "canali di videoconferenza" richiesti dall'Amministrazione, ossia del numero di chiamate audio/video attivabili contemporaneamente da/verso la sede.

[R.202] Il servizio di Videoconferenza di qualità su IP dovrà essere erogato, garantendo la conformità ai seguenti standard:

- H.239 ITU-T Recommendations, per quanto riguarda la funzionalità dual- video, che abilita un doppio canale video all'interno della singola sessione;
- H.264 ITU-T Recommendations, sviluppato per video in alta definizione, per una velocità massima di rinnovo immagine di 30 frame al secondo.

[R.203] Il sistema dovrà consentire la piena interoperabilità tra postazioni in alta definizione (HD) e postazioni in definizione standard (SD).

[R.204] Il servizio fornito dal Fornitore dovrà garantire l'interoperabilità con eventuali sistemi di videoconferenza già presenti presso le Amministrazioni, anche nel caso di sessioni di videoconferenza multi-punto.

[R.205] Il sistema dovrà consentire la registrazione, l'archiviazione e lo streaming (fruizione di video registrati) di presentazioni video e multimediali.

[R.206] Il servizio fornito dal Fornitore dovrà prevedere il supporto dei codec audio G.711 e AAC-LD (Advanced Audio Coding with Low Delay).

[R.207] Il servizio fornito dal Fornitore dovrà garantire il rilevamento della portante audio principale ed il conseguente invio del video corrispondente a tutte le sale collegate in una sessione multi-punto.

[R.208] Il Fornitore dovrà prevedere la fruizione del servizio attraverso le seguenti tipologie di terminale (end-point):

- *Postazione Telepresence "Personal"*, identifica un sistema di videoconferenza ad alta qualità per 1 postazione, caratterizzato dai seguenti requisiti minimi:

- n° 1 schermo LCD 40", con qualità video High Definition – 720p;

- n° 1 telecamera con risoluzione HD;
- sistema audio con qualità CD full-duplex;
- microfono direzionale;
- telecomando per la navigazione dell'interfaccia utente con funzionalità di regolazione dell'inquadratura/zoom;
- interfaccia utente con funzioni di Rubrica e Menù multilingua.

▪ *Postazione Telepresence "Base", identifica un sistema di videoconferenza ad alta qualità per 2 postazioni, caratterizzato dai seguenti requisiti minimi:*

- n° 2 schermi LCD 42", con qualità video High Definition – 720p;
- n° 1 telecamera con risoluzione HD;
- sistema audio con qualità CD full-duplex;
- Strumenti di controllo audio (cancellatori di eco, riduzione automatica del rumore);
- microfono direzionale;
- telecomando;
- interfaccia utente con funzioni di Rubrica e Menù multilingua.

[R.209] Il terminale fornito dal Fornitore dovrà prevedere almeno le seguenti tipologie di interfacce:

▪ Interfaccia LAN/Ethernet (RJ-45);

▪ Interfaccia USB.

[R.210] Il sistema dovrà consentire la visualizzazione simultanea dei partecipanti.

[R.211] Il servizio di Videocomunicazione di qualità su IP sarà remunerato al Fornitore in base al numero e alla tipologia di postazioni installate. E' quindi richiesto al concorrente di indicare, in Offerta Economica, il canone mensile offerto per ciascuna tipologia di postazione prevista in gara, in Affidabilità Standard.

[R.212] Per il servizio di videocomunicazione di qualità su IP non è definito un PAS. I livelli di servizio di cui al par. 8 sono relativi ai tempi di ripristino a seguito dei disservizi di una qualunque delle componenti di servizio dell'infrastruttura sopra descritta, e alla risultante disponibilità, su base sede, dell'infrastruttura stessa.

5. SERVIZI DI SUPPORTO

Nell'ambito dei servizi oggetto della presente gara, il Fornitore dovrà erogare anche i relativi servizi di supporto, i quali comprenderanno tutte le attività di gestione della rete finalizzate a controllare ed intervenire a fronte di anomalie su tutte le componenti dei servizi offerti.
I servizi di supporto riguarderanno le seguenti attività:

- installazione, attivazione, cessazione e variazione dei servizi e delle relative componenti;
- supervisione della rete (network monitoring) e gestione degli apparati;
- adozione delle misure di sicurezza sulle infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato;
- supporto tecnico alla gestione dei malfunzionamenti (fault management);
- distribuzione del software di rete (inclusi eventuali aggiornamenti) e gestione centralizzata delle configurazioni;
- analisi delle prestazioni del servizio;
- rendicontazione;
- servizi professionali di supporto (sistemistico ed operativo) alle Amministrazioni nell'utilizzo dei servizi oggetto di gara.

Per l'espletamento di tali servizi il Fornitore dovrà dotarsi delle seguenti strutture di supporto:

- **Centro di Gestione di rete**, di seguito **NOC** (Network Operating Center);
- **Centro di Gestione della sicurezza**, di seguito **SOC** (Security Operating Center);
- **Call Center** integrato con le strutture del NOC e del SOC, in modo da assicurare, nel complesso, i livelli di servizio contrattualizzati (cfr. par. 8).

5.1 Network Operating Center (NOC)

[R.213] Il Fornitore dovrà realizzare e gestire un Centro di Gestione di rete (NOC), non necessariamente dedicato ai servizi S-RIPA, in grado di espletare le seguenti funzioni:

- gestione della rete, con monitoraggio *real-time* di ogni servizio;
- valutazione del grado di occupazione delle risorse trasmissive;
- verifica del corretto dimensionamento complessivo del sistema;
- monitoraggio dei livelli di servizio e calcolo statistiche;
- produzione di reportistica almeno per tutti i livelli di servizio definiti e per tutti i servizi contrattualizzati, nei piu comuni formati elettronici.

[R.214] Il sistema di gestione della rete dovrà essere basato su architetture di tipo SNMP, conformi agli standard applicabili.

[R.215] Il Fornitore, attraverso gli strumenti in dotazione al NOC, dovrà essere in grado di gestire, in modalità remota, tutti i servizi ed i sistemi di rete dispiegati in ciascuna Amministrazione contraente, provvedendo altresì a tutte le operazioni di configurazione remota degli apparati di rete contrattualmente previste.

[R.216] Il Fornitore dovrà mettere a punto un sistema di monitoraggio idoneo a dimostrare la conformità ai livelli di servizio definiti nel par. 8, per tutti i servizi contrattualizzati.

[R.217] Il sistema di monitoraggio dovrà includere una Base Dati contenente informazioni su:

- configurazione di rete e dei sistemi utilizzati;
- misurazioni dei livelli di servizio che includono almeno i dati oggetto di tutti i report periodici previsti;
- log dei trouble ticket gestiti dal call center (cfr. paragrafo 5.4);
- classificazione dei guasti a seconda dei livelli di servizio contrattualizzati.

[R.218] Il NOC dovrà acquisire, da una sorgente primaria riconosciuta a livello Internazionale, il Tempo Ufficiale di Rete e utilizzarlo come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble tickets, nonchè per tutte le altre funzioni di gestione della rete che richiedono un riferimento temporale.

[R.219] Il NOC dovrà avvalersi del supporto di un Call Center (cfr. paragrafo 5.4) quale punto di contatto con gli utenti delle Amministrazioni sia per i servizi di provisioning (attivazione servizi, modifica policy, ecc.) sia per la gestione dei problemi.

5.2 Security Operating Center (SOC)

[R.220] Il Fornitore dovrà realizzare e gestire un Centro di Gestione della sicurezza (SOC), non necessariamente dedicato ai servizi della Rete S-RIPA, dotato di una struttura di controllo centralizzata con funzionalità di:

- monitoraggio real-time degli eventi riguardanti la sicurezza;
- registrazione degli eventi;
- reportistica avanzata.

[R.221] Il Fornitore, attraverso gli strumenti in dotazione al SOC, dovrà essere in grado di gestire, in modalità remota, tutti i servizi ed i sistemi di sicurezza dispiegati in ciascuna Amministrazione contraente, provvedendo altresì a tutte le operazioni di configurazione remota degli apparati di sicurezza contrattualmente previste.

[R.222] Il trasferimento di dati sensibili, quali ad esempio configurazioni di sicurezza, tra apparati gestiti e sistema di gestione del Fornitore, dovrà essere adeguatamente protetto con opportuni meccanismi di sicurezza volti a preservare la confidenzialità delle informazioni (es. SSH, IPsec).

[R.223] Il SOC dovrà essere dotato di un sistema di supporto al monitoraggio e alla gestione delle informazioni e degli eventi di sicurezza (SIEM-Secuity Information and Event Management).

[R.224] Il Fornitore per l'erogazione del servizio di gestione della sicurezza attraverso il SOC dovrà prevedere l'utilizzo di un servizio di Threat Intelligence che fornisca tempestivamente le informazioni sulle nuove minacce informatiche al fine di migliorare e rendere sempre più efficace la protezione e la prevenzione dagli attacchi informatici.

[R.225] Il SOC dovrà essere realizzato attraverso infrastrutture che rispettino le normative vigenti in tema di sicurezza fisica e logica, oltre alla sicurezza di connessione in rete.

[R.226] Il Fornitore sarà tenuto ad accreditare presso il Cert PA il proprio SOC.

[R.227] L'infrastruttura tecnologica del Centro di Gestione della sicurezza dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza.

[R.228] Il Centro di Gestione della sicurezza dovrà garantire la continuità di servizio per ciascun servizio erogato in remoto, in coerenza con gli orari di servizio e con gli Indicatori di Qualità. In caso di eventi di disastro che rendono indisponibile l'intero sito preposto all'erogazione dei servizi remoti il fornitore dovrà invocare formalmente verso AGID/Consip tale evento e garantire la ripartenza di tutti i servizi, anche su un diverso sito.

[R.229] E' richiesto a tal fine al concorrente di **indicare, nell'offerta tecnica – foglio "Offerta Sicurezza e Supporto"**:

- **RTO – *Recovery Time Objective* (valore intero espresso in ore)**. Tale tempo è calcolato a partire dall'evento che causa l'interruzione del servizio SOC, fino al ripristino del servizio;

- **RPO – *Recovery Point Objective* (valore intero espresso in ore)**. E' il tempo massimo che deve intercorre tra la produzione di un dato e la sua messa in sicurezza, ed esprime la perdita di dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario in caso di disastro .

I valori offerti dal concorrente dovranno essere entrambi interi (numero di ore), compresi entro gli intervalli indicati nel modello di offerta tecnica, e concorreranno all'attribuzione del punteggio tecnico come definito nella lettera di invito.

[R.230] E' richiesto inoltre al concorrente di **indicare, nell'offerta tecnica – foglio "Offerta Sicurezza e Supporto"**, se offra o meno , quale caratteristica migliorativa che concorrerà all'attribuzione del punteggio tecnico come definito nella lettera di invito, il **possesso di almeno una certificazione tra Certified Information Security Manager (CISM) e/o Certified Information Systems Security Professional (CISSP) e/o Certified Etical Hacker (CEH) per almeno il 20%, arrotondato per eccesso, del personale impiegato nel SOC**.

[R.231] Il SOC dovrà espletare le seguenti attività:

- monitorare il funzionamento dei servizi di sicurezza al fine di determinare potenziali problemi e assicurare che vengano rispettati i livelli di servizio contrattualizzati (cfr. par. 8);
- gestire gli allarmi ed i malfunzionamenti delle componenti del servizio ed attivare le procedure di Incident Management;
- effettuare il *tuning* delle configurazioni dei servizi di sicurezza erogati;
- effettuare il capacity planning del servizio erogato a seguito di modifiche apportate ai sistemi.

[R.232] Il sistema di gestione della sicurezza, così come i dispositivi forniti alle Amministrazioni, dovranno essere basati sullo standard SNMP almeno v2.

[R.233] Il Fornitore dovrà prevedere la produzione mensile di report opportuni, tesi a documentare lo stato del servizio, in termini di servizi di sicurezza attivati, di incidenti eventualmente verificatisi, nonché delle relative operazioni di correzione effettuate. Tali report dovranno essere forniti sia in formato cartaceo che nei piu comuni formati elettronici.

[R.234] Il SOC dovrà includere una Base Dati contenente informazioni su:

- ubicazione, tipologia e configurazione dei sistemi utilizzati;
- policy configurate per ciascun sistema;
- misurazioni dei livelli di servizio che includono almeno i dati oggetto della reportistica definita nel par. 3;
- log delle richieste di intervento pervenute al Call Center;
- log dei trouble ticket;
- classificazione dei guasti a seconda dei livelli di servizio contrattualizzati;

- dati di riscontro della qualità.

[R.235] Il SOC dovrà acquisire, da una sorgente primaria riconosciuta a livello Internazionale, il Tempo Ufficiale di Rete e utilizzarlo come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble tickets, nonchè per tutte le altre funzioni di gestione che richiedono un riferimento temporale.

[R.236] Il SOC dovrà recepire ed aggiornare costantemente i propri sistemi con gli IoC (indicatori di compromissione) predisposti dal CERT-PA o inviati dall'Amministrazione.

[R.237] Il SOC dovrà avvalersi del supporto di un Call Center (cfr. par. 5.4) quale punto di contatto sia per i servizi di provisioning (attivazione servizi, modifica policy, ecc.) sia per la gestione dei problemi e degli eventi di sicurezza.

5.3 Sistema di supervisione e monitoraggio della qualità

[R.238] Il Fornitore dovrà realizzare ed attivare, dall'avvio dell'erogazione del primo servizio, un sistema di monitoraggio della qualità, accessibile in modalità di sola lettura, mediante Web Browser, da parte di ciascuna Amministrazione contrattualizzata.

[R.239] Il Fornitore dovrà fornire le credenziali di accesso Web (username e password secondo le policy definite per S-RIPA) al sistema di monitoraggio da parte delle singole Amministrazioni contrattualizzate, garantendo le seguenti funzionalità:

- monitoraggio, in tempo reale, dei servizi contrattualizzati attraverso opportuni quadri sinottici che consentano una tempestiva percezione dello stato dei servizi;
- verifica dei livelli di servizio (cfr. par. 8) e calcolo di statistiche, per tutti i servizi contrattualizzati;
- consultazione diretta delle Base Dati relative alle risorse di rete e di sicurezza di propria competenza, consentendo la generazione guidata di report, grafici, e query complesse;
- funzionalità di esportazione dei dati, secondo formati standard, contenuti nella porzione di Base Dati relativa alle risorse di rete e di sicurezza di propria competenza.

[R.240] Su richiesta dell'Amministrazione, limitatamente alle Amministrazioni che abbiano attivato almeno 30 sedi, il Fornitore dovrà fornire una stazione di supervisione con visibilità (in modalità read-only) limitata ai soli servizi contrattualizzati dalla stessa, che includa le sopracitate funzionalità.

[R.241] Il Fornitore dovrà provvedere alla fornitura, installazione e manutenzione di tutti i componenti hardware e software che costituiscono la stazione di supervisione sopracitata.

5.3.1 Servizi di Help Desk "on-site"

[R.242] Il Fornitore dovrà fornire, su richiesta dell'Amministrazione, un servizio di Help Desk "on-site" da erogare presso la sede centrale dell'Amministrazione. Tale servizio consentirà alle Amministrazioni contraenti di disporre in loco di risorse professionali in grado di fornire una risposta operativa tempestiva in caso di segnalazioni di malfunzionamento.

[R.243] Il servizio è vincolato alla disponibilità, da parte dell'Amministrazione, di almeno una stazione di supervisione sopra menzionata, che costituirà lo strumento con cui l'operatore di Help Desk potrà effettuare il monitoraggio real-time dei servizi di rete e di sicurezza.

[R.244] Il servizio dovrà garantire un presidio continuativo "on-site", ossia per 24 ore al giorno, 7 giorni alla settimana e 365 giorni l'anno, attraverso figure professionali del Fornitore.

[R.245] Si riportano di seguito i requisiti minimi previsti per le figure professionali utilizzate dal Fornitore per l'erogazione dei servizi in oggetto.

Operatore Help Desk "on-site"	
Anzianità professionale	Diplomato con esperienza lavorativa di più di 4 anni di cui almeno 3 nella specifica funzione.
Principali competenze	- Conoscenza dei flussi procedurali e degli standard di sicurezza; - Conoscenza dell'applicativo utilizzato per il servizio di supporto operativo ed in particolare delle funzionalità di Network & Security monitoring; - Analisi e gestione dei rischi, processi di recovery; - Conoscenza e applicazione di tecniche e metodi relativi alla comunicazione ed alla gestione del conflitto; - Competenze nell'uso di piattaforme di Trouble Ticketing.

5.4 Call Center

[R.246] Il Fornitore dovrà rendere disponibile un servizio di Call Center, integrato con le strutture di NOC e SOC (cfr. paragrafi 5.1 e 5.2) e raggiungibile, da parte di ciascuna Amministrazione, attraverso un numero unico gratuito predisposto dal Fornitore. Il servizio dovrà gestire tutte le problematiche connesse ai servizi contrattualizzati dalle Amministrazioni e attivati presso ciascuna sede.

[R.247] Il servizio di Call Center fornito dal Fornitore dovrà essere configurato come un help desk di 2° livello, che riceve segnalazioni di malfunzionamento esclusivamente dai centri di gestione 1° livello della singola Amministrazione. L'utente finale della singola Amministrazione potrà accedere direttamente al servizio di help desk di 1° livello (interno alla singola Amministrazione), il quale dirotterà la segnalazione al 2° livello solo se rileverà un problema di competenza del Fornitore.

[R.248] Il servizio di Call center dovrà ricevere segnalazioni di malfunzionamento almeno tramite chiamata telefonica e e-mail.

[R.249] È facoltà del Fornitore predisporre soluzioni aggiuntive di help desk basate su modalità Web. In ogni caso tale modalità non sarà considera sostitutiva della modalità telefonica e via e-mail.

[R.250] Per la ricezione delle chiamate dovrà essere istituito un apposito Numero Verde (la cui tariffazione omnicomprensiva sia a carico del Fornitore) e dovranno essere predisposte idonee attrezzature in termini d'apparati e linee al fine di garantire il livello di servizio specificato nel par. 8.

[R.251] Tutte le chiamate telefoniche dovranno essere gestite; nel caso di completa occupazione degli operatori dovrà attivarsi un sistema d'attesa che raccolga la segnalazione dell'utente da notificare al primo operatore libero.

[R.252] Il servizio dovrà essere disponibile per 24 ore al giorno, per 7 giorni alla settimana e per 365 giorni l'anno.

5.5 Misure di sicurezza dell'infrastruttura di rete

[R.253] In questa sezione sono definiti i requisiti minimi riguardanti le misure di sicurezza da applicare su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato.

[R.254] Tali requisiti costituiscono parte integrante della fornitura di qualsiasi tipologia di servizio prevista nel presente Capitolato.

[R.255] Il Fornitore dovrà specificare in dettaglio le politiche di sicurezza adottate e le soluzioni tecniche ed organizzative proposte in modo che, in fase di aggiudicazione si possa stabilire se tali soluzioni soddisfano i requisiti indicati.

[R.256] In conformità al D.P.C.M. del 1° Aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettivita" (G.U. n. 144 del 21 Giugno 2008), il SOC dovrà svolgere anche i compiti della Unità Locale di Sicurezza SPC per la gestione degli aspetti relativi alla sicurezza. Il Fornitore dovrà nominare all'interno del SOC un Responsabile Operativo della sicurezza che dovrà coordinare l'Unità Locale di Sicurezza SPC e fungere da punto di contatto prioritario per tutte le problematiche di sicurezza che interessano l'infrastruttura del Fornitore. Il Responsabile Operativo della sicurezza potrà avvalersi di sostituti i cui nominativi dovranno essere preventivamente comunicati all'Amministrazione.

5.5.1 Principi generali

[R.257] Il Fornitore dovrà garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato siano adottate le seguenti misure di carattere generale:

- attuazione delle misure minime organizzative e tecniche previste dalle normative in vigore in materia di protezione dei dati;
- disposizione di un'organizzazione per la gestione della sicurezza dell'infrastruttura, secondo il modello indicato dalla norma ISO 27001;
- disposizione, nei punti di ingresso alle proprie infrastrutture utilizzate per l'erogazione dei servizi di Rete Internazionale S-RIPA, di sistemi di prevenzione dalle minacce e rilevamento di attacchi informatici;
- implementazione sul dispositivo che realizza il PAS sotto il proprio dominio amministrativo, di tutte le funzionalità volte ad impedire attacchi di tipo IP spoofing provenienti/diretti verso le reti dell'Amministrazione;
- garanzia di tempestivo aggiornamento, con applicazione delle patch, del software/firmware degli apparati (router-switch) che trasportano il traffico destinato alle Amministrazioni;
- implementazione di un meccanismo di AAA centralizzato per l'autenticazione, l'autorizzazione e la tracciatura degli accessi sugli apparati di rete di propria competenza impiegati sulla Rete S-RIPA.

5.5.2 Misure di controllo e recupero

[R.258] Il Fornitore dovrà garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato siano adottate le seguenti misure di controllo e recupero:

- controllo costante dei propri apparati di rete e della rete fisica di trasporto con lo scopo di individuare eventuali anomalie che possano essere sintomo di problemi di sicurezza;
- analisi automatica del traffico di rete con l'obiettivo di riconoscere potenziali attacchi;

- attivazione delle funzioni di logging del traffico su tutti gli apparati di rete e sicurezza. I log dovranno essere conservati con modalità e tempi coerenti con le indicazioni della normativa sulla protezione dei dati. I log relativi agli apparati di sicurezza dovranno essere analizzati giornalmente;
- definizione ed implementazione delle procedure di gestione degli incidenti a valle di segnalazioni di eventi di sicurezza.

5.5.3 Misure organizzative

[R.259] Il Fornitore dovrà garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato siano adottate le seguenti misure organizzative:

- analisi dei rischi su base sistematica, almeno con cadenza annuale. Tale analisi dovrà inoltre essere ripetuta a seguito di attacchi o incidenti gravi di sicurezza o per variazioni significative dell'architettura;
- schedulazione di attività periodiche di revisione delle utenze e delle autorità di sicurezza ed immediata cancellazione delle utenze relative al personale che risolve il rapporto di lavoro;
- separazione delle responsabilità interne relative alla gestione della sicurezza ed alle verifiche;
- attivazione di un'organizzazione per la gestione dell'emergenza e dei problemi di sicurezza, volta ad assicurare la continuità del servizio nel caso di eventi eccezionali imprevedibili attraverso la stesura e la gestione dei piani per l'emergenza.

5.6 Servizi di Fault Management

[R.260] Il call center del Fornitore dovrà erogare un servizio di fault management che consiste nella rilevazione, diagnosi e risoluzione dei guasti occorrenti sui servizi erogati dal Fornitore stesso. In particolare, per i malfunzionamenti che coinvolgono gli apparati installati presso i siti dell'Amministrazione, il Fornitore dovrà intervenire secondo le seguenti modalità:

- gestione remota di tutti gli apparati installati presso i siti dell'Amministrazione dal proprio Centro di Gestione (NOC/SOC) per la risoluzione dei malfunzionamenti;
- manutenzione on-site, qualora il malfunzionamento non permetta una correzione attraverso il supporto remoto. Le attività di fault management che richiedano intervento diretto sul sito dovranno essere concordate con l'Amministrazione ed effettuate nella finestra di erogazione del servizio.

[R.261] Qualora una componente o parte di una componente del servizio installata presso i siti dell'Amministrazione presenti un malfunzionamento, il Fornitore dovrà provvedere alla sua sostituzione secondo i tempi di ripristino del servizio descritti nel par. 8, in funzione del tipo di impatto provocato dal malfunzionamento.

[R.262] L'Amministrazione, qualora lo ritenga opportuno, potrà mettere a disposizione del Fornitore, presso i propri siti, uno o più magazzini adatti allo spare-part management, secondo modalità che verranno concordate tra le Parti.

[R.263] Il Fornitore dovrà dotarsi di uno strumento di Trouble Ticketing per consentire la gestione ed il monitoraggio delle attività di fault management, fermo restando che la classificazione del livello di severity dei Trouble Ticket (TT) sarà cura dell'Amministrazione.

[R.264] Il Fornitore dovrà impegnarsi all'apertura proattiva di TT anche in mancanza di segnalazioni da parte dell'Amministrazione, in risposta a malfunzionamenti rilevati dai propri sistemi di gestione.

5.7 Servizi di Provisioning, Configuration e Change Management

[R.265] Il Fornitore dovrà provvedere alla fornitura, installazione, configurazione ed attivazione dei servizi oggetto del presente Capitolato, fornendo all'Amministrazione contrattualizzata un servizio "chiavi in mano".

[R.266] L'attivazione di ciascun servizio dovrà avvenire entro 3 mesi dall'approvazione del Progetto dei Fabbisogni in cui tale servizio è previsto, o entro il diverso tempo concordato nel Progetto dei Fabbisogni.

[R.267] Il Fornitore dovrà provvedere all'installazione e configurazione degli apparati per la fornitura dei servizi contrattualizzati dall'Amministrazione.

[R.268] Il Fornitore dovrà farsi carico delle attività di installazione del software sugli apparati utilizzati per l'erogazione dei servizi.

[R.269] A valle dell'installazione e configurazione, il Fornitore dovrà redigere e consegnare all'Amministrazione un inventario degli apparati installati.

[R.270] Il Fornitore dovrà provvedere all'aggiornamento software degli apparati utilizzati per mantenere l'allineamento con i rilasci software messi a disposizione dai fornitori della tecnologia sia con finalità di patching che per quanto riguarda l'introduzione dei nuovi servizi.

[R.271] Il Fornitore dovrà effettuare eventuali variazioni delle componenti dei servizi erogati e delle configurazioni di rete e di sicurezza adottate.

[R.272] Il Fornitore dovrà provvedere all'attuazione degli adeguamenti e/o riconfigurazioni richieste da attività di "system tuning".

[R.273] Il servizio dovrà prevedere la gestione remota degli apparati installati presso i siti dell'Amministrazione che permetta al Fornitore di intervenire dai propri NOC e SOC per attività operative.

[R.274] Il Fornitore dovrà gestire e controllare tutte le configurazioni hardware e software degli apparati utilizzati per l'erogazione dei servizi, mantenendo aggiornato un database delle configurazioni (integrato con le Base Dati di NOC e SOC descritte nei paragrafi precedenti) che consenta:

- l'inventario delle configurazioni hardware e software e delle personalizzazioni necessarie, in modo da facilitare le operazioni di ripartenza e riallineamento a fronte di un qualsiasi problema legato alle funzionalità dei sistemi gestiti;
- la produzione trimestrale di un report delle configurazioni;
- la pianificazione delle attività di gestione e di aggiornamento dei sistemi.

5.7.1 Servizio di trasloco delle sedi

[R.275] Il servizio di trasloco delle sedi delle Amministrazioni si compone di tutte le operazioni necessarie all'attivazione di un nuovo collegamento presso la sede in corso di attivazione dell'Amministrazione, al trasloco fisico degli apparati di rete, sicurezza, VoIP e Comunicazione evoluta, e alla cessazione dei servizi nella vecchia sede.

[R.276] In caso di trasloco di una sede, il Fornitore dovrà rendere disponibili tutti i servizi contrattualizzati presso il nuovo punto di attestazione indicato dall'Amministrazione.

[R.277] Il servizio di trasloco di ciascuna sede dell'Amministrazione potrà avvenire nelle seguenti modalità:

- trasloco esterno: il nuovo punto di attestazione dei servizi è situato in uno stabile differente dal precedente;
- trasloco interno: il nuovo punto di attestazione dei servizi è situato all'interno del medesimo stabile.

[R.278] Il Fornitore dovrà attivare il servizio nella nuova sede entro 3 mesi dall'approvazione del relativo Progetto dei Fabbisogni (o entro il diverso tempo concordato nel Progetto stesso)nel caso di trasloco esterno, ed entro 1 mese nel caso di trasloco interno.

[R.279] Nulla è dovuto dalle Amministrazioni per l'attivazione dei servizi nelle nuove sedi.

5.8 Servizi di Rendicontazione e Fatturazione

[R.280] I servizi di rendicontazione sono rivolti alle Amministrazioni, con lo scopo di rendere disponibili, attraverso apposita reportistica, i dati relativi all'erogazione e fruizione dei servizi oggetto del presente Capitolato e consentire il controllo e la verifica delle quantità da fatturare alla singola Amministrazione.

[R.281] Il servizio dovrà essere implementato per il tramite di una infrastruttura hardware e software che il Fornitore stesso provvederà a realizzare ed a mantenere in esercizio.

[R.282] Il Fornitore dovrà mettere a disposizione dell'Amministrazione opportuni strumenti che consentano la gestione e la consultazione, tramite interfaccia web, sia dei dati di rendicontazione che di fatturazione. Il servizio offerto dal Fornitore dovrà rispondere ai seguenti requisiti:

- rendere disponibile, tramite interfaccia web, la reportistica di rendicontazione e fatturazione per ciascun servizio contrattualizzato dall'Amministrazione;
- consentire, tramite interfaccia web, l'esportazione (download) della reportistica di rendicontazione e fatturazione relativa a ciascun servizio contrattualizzato dall'Amministrazione;
- consentire un accesso continuativo all'interfaccia web messa a disposizione dal Fornitore;
- aggiornare la reportistica di consuntivazione mensilmente, entro il giorno 15 del mese successivo a quello di riferimento;
- limitare la visibilità di ciascuna Amministrazione esclusivamente sui report di propria competenza.

[R.283] Il servizio fornito dal Fornitore, ai fini dell'accesso alla reportistica sull'utilizzo dei servizi, dovrà prevedere opportune modalità di identificazione degli utenti.

[R.284] Tutta la reportistica relativa ai servizi di rendicontazione e fatturazione dovrà essere archiviata e conservata in una base dati fornita dal Fornitore, per tutta la durata contrattuale.

[R.285] Il Fornitore dovrà essere disponibile, su richiesta delle Amministrazioni che ne facciano richiesta, a esportare ed inviare tramite posta elettronica le informazioni contenute nella base dati dei servizi di fatturazione e rendicontazione.

[R.286] In caso di specifiche esigenze da parte dell'Amministrazione in merito al formato dati, il Fornitore dovrà garantire la propria disponibilità a personalizzare il layout della documentazione.

[R.287] Il sistema di fatturazione dovrà fornire tutte le informazioni di dettaglio in merito alle sessioni tariffate, nel rispetto delle norme della privacy in vigore.

5.9 Servizi professionali di supporto operativo

[R.288] Il Fornitore dovrà erogare, su richiesta delle Amministrazioni contraenti, servizi professionali di supporto operativo volti a coadiuvare ed integrare il personale dell'Amministrazione.

[R.289] Il Fornitore dovrà erogare i servizi professionali di supporto attraverso figure professionali con comprovate competenze nel settore dell'ICT, al fine di coprire gli aspetti tecnologici ed organizzativi necessari alla realizzazione delle attività sistemistiche e/o operative descritte nel presente paragrafo. Si riportano di seguito i requisiti minimi previsti per le figure professionali utilizzate dal Fornitore per l'erogazione dei servizi in oggetto.

Profilo Senior	
Anzianità professional	Laureato con esperienza lavorativa di più di 6 anni, di cui almeno 4 nella specifica funzione
Principali competenze	- Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione di reti TLC e/o di soluzioni di sicurezza - Reti geografiche (WAN) e reti locali (LAN), basate su protocolli standard - Tecnologie/soluzioni per servizi di connettività e sicurezza. - Progettazione e realizzazione di reti TLC e/o di soluzioni di sicurezza - Utilizzo di tool avanzati di network monitoring - Utilizzo di tool per il monitoraggio di PdL, server, apparati attivi di rete - Gestione di processi di roll-out di reti TLC - Modelli di definizione e monitoraggio di SLA - Capacità di problem solving

Profilo Junior	
Anzianità professionale	Laureato con esperienza lavorativa di più di 4 anni di cui almeno 2 nella specifica funzione

Principali competenze	- Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione di reti TLC e/o di soluzioni di sicurezza - Architetture di TLC e sicurezza - Reti TLC basate su protocolli standard - Tecnologie/soluzioni per servizi di connettività e sicurezza - Conoscenza di tool di network monitoring - Esecuzione di test e collaudi - Principali metodiche di rilevazione dei livelli di servizio - Capacità di problem solving

[R.290] Relativamente all'erogazione del supporto operativo nell'ambito dei servizi di sicurezza, le figure professionali (Profilo Senior e Profilo Junior) messe a disposizione del Fornitore dovranno essere in grado di:

- contribuire alla definizione e implementazione delle policy di sicurezza;
- assicurare la sicurezza e l'uso appropriato delle risorse ICT;
- valutare rischi, minacce e conseguenze di un attacco in ambito sicurezza;
- verificare le vulnerabilità di sicurezza;
- proporre e implementare i necessari aggiornamenti di sicurezza;
- effettuare la validazione tecnica di tools di sicurezza;
- monitorare gli sviluppi di sicurezza per assicurare la sicurezza dei dati delle risorse ICT;
- formare e sensibilizzare il personale dell'Amministrazione sugli aspetti inerenti la sicurezza delle informazioni dell'organizzazione.

[R.291] E' richiesto inoltre al concorrente di **indicare, nell'offerta tecnica – foglio "Offerta Sicurezza e Supporto"**, se offra o meno , quale caratteristica migliorativa che concorrerà all'attribuzione del punteggio tecnico come definito nella lettera di invito, **l'impiego di figure professionali, nell'erogazione del supporto operativo nell'ambito dei servizi di sicurezza, in possesso di almeno una certificazione tra Certified Information Security Manager (CISM) e/o Certified Information Systems Security Professional (CISSP) e/o Certified Etical Hacker (CEH)**.

[R.292] Il Fornitore dovrà erogare alle Amministrazioni un supporto operativo volto a coadiuvare ed integrare le risorse professionali dell'Amministrazione nell'introduzione e nell'esercizio dei servizi oggetto del presente Capitolato durante le fasi di avvio e di conduzione dei servizi della Rete Internazionale S-RIPA.

[R.293] I servizi professionali a supporto potranno essere acquisiti solo in abbinamento ai servizi di connettività IP e/o sicurezza e/o VoIP e comunicazione evoluta, per un importo massimo pari al 20% del relativo valore contrattuale.

[R.294] Il servizio dovrà essere erogato presso le varie sedi indicate dall'Amministrazione per le quali sia richiesto il supporto operativo.

[R.295] E' richiesto al Concorrente di indicare in Offerta Economica il prezzo per giorno persona di una risorsa impiegata nelle attività. Si precisa che per "prezzo per giorno persona" si intende il corrispettivo per l'attività prestata in 8 ore lavorative, nell'ambito dell'orario dalle 9.00 alle 18.00, dal lunedì al venerdì, festivi esclusi.

5.10 Servizio di rendicontazione per l' Amministrazione aggiudicatrice

[R.296] Il Fornitore dovrà inviare a Consip report quadrimestrali delle "consistenze tecniche", in un formato da concordare, contenenti, per ciascuna Amministrazione contraente e per ciascuna sede, i servizi contrattualizzati, con tutte le relative caratteristiche e opzioni di servizio previste nel presente Capitolato.

[R.297] Annualmente, il Fornitore dovrà inviare a Consip una relazione consuntiva contenente, in un formato da concordare, l'ammontare dei corrispettivi fatturati a ciascuna Amministrazioni, distinto per tipologia di servizio, nonché delle penali applicate dalle Amministrazioni.

6. MODALITÀ DI ATTIVAZIONE DEI SERVIZI

[R.298] Il Fornitore deve effettuare tutte le attività di seguito descritte, sia nel caso di migrazione di un'Amministrazione da servizi preesistenti, sia nel caso di realizzazioni ex novo.

[R.299] Nel caso in cui l'Amministrazione fruisca di servizi preesistenti, il Fornitore deve esplicitamente prevedere, congiuntamente con l'Amministrazione contraente, le procedure di attivazione che permettano il mantenimento dell'operatività durante le fasi di migrazione.

6.1 Piano dei Fabbisogni

[R.300] Il Fornitore deve impegnarsi a supportare l'Amministrazione nella redazione di un documento intitolato "Piano dei Fabbisogni", contenente per ciascuna categoria di servizi, indicazioni di tipo quantitativo ed economico di ciascun servizio che la stessa intende sottoscrivere.

[R.301] La redazione del "Piano dei fabbisogni" deve avvenire da parte dell'Amministrazione con l'eventuale ausilio del Fornitore.

[R.302] L'Amministrazione invierà il Piano dei Fabbisogni, mediante Posta Elettronica Certificata (PEC), ad una casella di PEC specifica del Fornitore.

[R.303] Il Fornitore ha facoltà di condurre, con proprio personale tecnico o altro personale da lui stesso incaricato, e congiuntamente con i referenti dell'Amministrazione interessata, sopralluoghi sui siti, allo scopo di verificare gli impatti e le modalità dell'attivazione dei servizi nella sede in esame (secondo quanto richiesto dall'Amministrazione nel Piano dei fabbisogni).

[R.304] Il Fornitore deve approntare il calendario dei sopralluoghi necessari. Tale calendario deve indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal Prestatore per il sopralluogo, con gli estremi di un documento di riconoscimento e l'elenco delle verifiche da effettuare. Il calendario viene sottoposto all'approvazione dell'Amministrazione interessata.

6.2 Progetto dei Fabbisogni

[R.305] Il Fornitore deve predisporre ed inviare alla casella PEC indicata dall'Amministrazione, entro 45 giorni dalla ricezione del Piano dei Fabbisogni, un documento intitolato "Progetto dei fabbisogni", nel quale raccogliere e dettagliare le richieste dell'Amministrazione contenute nel Piano dei fabbisogni e formulare una proposta tecnico/economica (secondo le condizioni oggetto della presente gara).

[R.306] Il "Progetto dei fabbisogni" deve contenere i seguenti allegati:

- "Progetto di Attuazione": con il dettaglio, per ciascun servizio, di:
  - identificativo del servizio;
  - configurazione;
  - quantità;
  - costi;
  - indirizzo di dispiegamento;
  - data prevista di attivazione;
- "Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili":

- servizi installati;
- esito dei collaudi effettuati;
- collaudi previsti nel mese successivo;
- varianti e modifiche emerse nel periodo;
- ritardi verificatisi nelle attivazioni rispetto alle date previste nel piano di attuazione e cause.

- "Piano di Attuazione", contenente:
  - Descrizione della struttura funzionale ed organizzativa del Fornitore ai fini dell'erogazione dei servizi oggetto del Piano di Attuazione.
  - Descrizione delle procedure di attivazione dei servizi e piano di installazione.
  - Matrice compiti-responsabilità.
  - Risorse allocate.
  - Specifiche di realizzazione dei servizi.
  - Identificazione delle attività (procedure di provisioning delle linee TLC, apparati, ecc.) necessarie all'attivazione dei servizi.
  - Identificazione dei rischi e piano di recovery: fasi di verifica e riesame per l'individuazione di eventuali criticità insorte nonché riferimento alle procedure necessarie alla gestione/superamento delle stesse.

- "Piano operativo", contenente la pianificazione temporale dettagliata (diagramma di Gantt delle singole attivazioni, schedulazione delle milestone principali, piano dei sopralluoghi, ecc.).
- "Documento programmatico di gestione della sicurezza dell'Amministrazione", contenente la descrizione delle misure organizzative (ruoli, responsabilità, procedure), tecniche (sistemi hardware e software impiegati) e fisiche adottate dal Fornitore in fase di erogazione dei servizi richiesti.
- "Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi", contenente:
  - Specifiche dei servizi che descrivono in dettaglio le caratteristiche tecniche delle singole tipologie di servizio e le condizioni di accettabilità per ciascuna caratteristica.
  - Specifiche di realizzazione dei servizi, che descrivono le modalità di realizzazione ed erogazione del servizio e le risorse necessarie (modalità di provisioning, caratteristiche tecniche/dimensionali degli apparati utilizzati, requisiti elettrici, fisici ed ambientali che devono essere previsti nelle sedi dell'Amministrazione che ospita i servizi, nonché il modeling della rete).
  - Obiettivi di qualità, espressi in termini di livelli di servizio.
  - Metriche per la misura della qualità effettivamente fornita.
  - Identificazione dei controlli (test, reviews, verifiche, validazioni) che il Fornitore svolge per assicurare la qualità della fornitura ed i relativi piani di verifica.
  - Specifiche responsabilità riguardo ai controlli da svolgere e riguardo alla gestione dei problemi ed alla gestione delle non conformità.
  - Metodi, tecniche, strumenti, risorse, competenze previste dal Fornitore per assicurare la qualità della fornitura in corso d'opera.
  - Documenti prodotti dal sistema di assicurazione e controllo qualità.
  - Documenti di riferimento (guide, procedure, moduli, checklist, ecc.) utilizzati dal sistema di assicurazione e controllo qualità.

- "Specifiche di dettaglio delle prove di collaudo (configurazione degli accessi)", di cui al successivo par. 7.3:

- tipologia di collaudo;
- elenco delle prove di collaudo;
- tempi dei collaudi.

[R.307] L'Amministrazione potrà comunicare al Fornitore l'approvazione del Progetto dei Fabbisogni, ovvero richiedere eventuali modifiche e/o integrazioni ritenute necessarie al fine di rendere detto Progetto dei Fabbisogni compatibile con il Piano dei Fabbisogni precedentemente formulato. In tal caso, entro 15 giorni dal ricevimento della richiesta di modifica, il Fornitore dovrà inviare all'Amministrazione il Progetto dei Fabbisogni modificato secondo le indicazioni ricevute dall'Amministrazione.

[R.308] L'Amministrazione approva il Progetto dei Fabbisogni mediante la stipula del Contratto Esecutivo.

[R.309] Il Fornitore dovrà tenere costantemente aggiornato il Progetto dei Fabbisogni.

[R.310] Il Fornitore deve prestare un servizio di "project management" che consiste nella pianificazione, gestione e verifica delle attività mirate al completamento del progetto. La definizione delle attività è responsabilità di un gruppo di lavoro costituito almeno da:

- un responsabile del progetto presso la singola Amministrazione;
- un project manager del Fornitore.

[R.311] Nel corso di durata del Contratto Esecutivo, l'Amministrazione potrà variare (in aumento o in diminuzione) e/o aggiornare il Piano dei Fabbisogni ogni qualvolta lo ritenga necessario in ragione delle proprie esigenze ed al mutare delle stesse; il Fornitore dovrà di conseguenza aggiornare il Progetto dei Fabbisogni nei tempi e modi sopra previsti per il primo Progetto.

6.3 Installazione

[R.312] Il Fornitore deve definire, in accordo con l'Amministrazione contraente, il piano di installazione dei servizi che deve rispettare i seguenti requisiti minimi:

- gli interventi devono essere effettuati in intervalli orari definiti dall'Amministrazione coerentemente con le proprie esigenze di operatività;
- l'operatività del servizio deve essere garantita anche durante la fase intermedia di test e collaudo;
- l'impatto delle operazioni di roll-out e installazione sulla normale operatività delle sedi deve essere minimo.

[R.313] Qualora un'operazione di installazione dovesse costituire causa di disservizio, il Fornitore deve adoperarsi per garantire un ripristino immediato della condizione preesistente.

[R.314] A partire dalla data di decorrenza del contratto esecutivo, il Fornitore deve procedere all'installazione delle sedi secondo le modalità temporali previste dal Progetto di Attuazione. In fase di configurazione degli apparati di accesso per ogni sede individuata il Fornitore, congiuntamente con l'Amministrazione, deve:

- contattare il referente tecnico della sede;
- concordare le modalità ed i tempi di interventi on-site;
- effettuare una verifica del sito, se necessario;
- procedere all'attestazione del collegamento;
- partecipare alle attività di test ed emettere un verbale per collaudo eseguito con esito positivo.

6.4 Migrazione

[R.315] Il Fornitore deve considerare prioritaria, sia nella pianificazione che nell'esecuzione dell'attivazione, la salvaguardia dell'operatività delle Amministrazioni nel periodo di tempo durante il quale avviene la migrazione dei servizi.

[R.316] In particolare, nel caso in cui un'operazione di attivazione del servizio dovesse costituire causa di malfunzionamento, il Fornitore deve assicurare la possibilità di un ripristino immediato della condizione preesistente (procedura di roll-back).

[R.317] Tutti gli interventi eseguiti sulle piattaforme in esercizio devono essere effettuati al di fuori dell'orario di lavoro del personale delle Amministrazioni e, comunque, in intervalli orari definiti dall'Amministrazione coerentemente con le proprie esigenze di operatività.

[R.318] Pur nel rispetto della continuità del servizio, il piano di migrazione proposto dal Fornitore deve consentire il massimo parallelismo delle attività al fine di minimizzare i tempi di attivazione.

[R.319] Il processo di migrazione deve prevedere, ove applicabile, una fase di "parallelo operativo" che garantisca, in una determinata finestra temporale, la coesistenza dei servizi erogati dall'attuale Fornitore di Servizi di Connettività S-RIPA e di quelli forniti dal nuovo Fornitore dei Servizi S-RIPA. Il parallelo operativo deve essere tenuto attivo per il tempo necessario a completare le attività di migrazione e verificare la corretta operatività dei nuovi servizi.

[R.320] Nell'ambito del processo di migrazione, ove questo fosse possibile e necessario al fine di garantire la continuità nelle comunicazioni tra Amministrazioni migrate al nuovo contratto S-RIPA ed Amministrazioni non ancora migrate, il Fornitore deve farsi carico della realizzazione dell'interconnessione tra la propria rete e quella del Fornitore uscente.

[R.321] Per ciascuna sede oggetto di migrazione, il pagamento dei corrispettivi per la fornitura dei Servizi avrà decorrenza a partire dal 1° giorno del mese successivo alla data di collaudo positivo (verbale di collaudo) del servizio oggetto di migrazione.

7. VERIFICHE DI CONFORMITA' E COLLAUDI

7.1 Prescrizioni generali

[R.322] L'Accordo Quadro prevede una verifica di conformità e collaudo iniziale, volto a verificare le modalità con le quali il Fornitore erogherà i servizi oggetto della presente gara.

[R.323] Ogni Contratto Esecutivo stipulato tra il Fornitore e la singola Amministrazione prevede un collaudo della particolare configurazione di accessi, volto a verificare la corretta erogazione dei servizi acquisiti dall'Amministrazione.

7.2 Verifica di conformità e collaudo iniziale

[R.324] Entro 30 giorni dalla comunicazione di aggiudicazione, il Fornitore dovrà inviare all'Amministrazione Aggiudicatrice la documentazione di riscontro di cui al successivo par. 7.4. Tale documentazione sarà utilizzata da una Commissione nominata dalla Consip, al fine di verificare, a livello documentale, la conformità dei servizi a quanto previsto nel presente Capitolato e nell'Offerta Tecnica del Fornitore, come meglio precisato nello Schema di Accordo Quadro.

[R.325] L'Amministrazione Aggiudicatrice sottoporrà inoltre a collaudo, mediante nomina di una Commissione che potrà eventualmente coincidere con quella di cui al requisito precedente, come meglio precisato nello Schema di Accordo Quadro:

- Il sistema di misura per la rilevazione dei livelli di servizio e di generazione della reportistica di cui al par. 8;
- Il sistema preposto all'erogazione dei servizi di rendicontazione e fatturazione di cui al par. 5.8;
- La prestazione dei servizi erogati dal Centro di Gestione di rete (NOC), dal Centro di Gestione della sicurezza (SOC), nonché dal Sistema di Supervisione e monitoraggio della qualità;
- Il collegamento tra la S-RIPA e la QXN.

Il collaudo di tali sistemi verrà effettuato a seguito dell'approvazione, da parte della Commissione di cui al precedente [R.324], della relativa documentazione di riscontro. Nel caso di sistemi già in esercizio ed utilizzati dal Fornitore per erogare i propri servizi ad altri clienti, starà al Fornitore stesso predisporre un ambiente tale da consentire alla Commissione di verificare la conformità dei servizi che verranno erogati nell'ambito dell'Accordo Quadro, senza compromettere quelli già in esercizio. Nel caso di sistemi di nuova realizzazione, il Fornitore potrà scegliere se effettuare il collaudo in ambiente di prova (test bed), facendosi carico dei relativi oneri, o direttamente sugli stessi sistemi che, all'esito positivo del collaudo, entreranno in esercizio. In ogni caso, i sistemi dovranno essere pronti all'erogazione dei servizi entro 7 giorni dall'esito positivo del collaudo.

A tal fine, ciascuno dei sistemi dovrà essere realizzato secondo le specifiche approvate, e pronto al collaudo:

- entro 60 giorni solari dall'approvazione della documentazione di riscontro relativa al sistema, nel caso in cui tale approvazione intervenga successivamente alla stipula dell'Accordo Quadro

  o, in caso contrario:

- entro 60 giorni dalla stipula dell'Accordo Quadro.

Il Fornitore dovrà fornire il personale necessario per l'esecuzione delle prove di collaudo sui predetti sistemi.

7.3 Collaudo di configurazione degli accessi

[R.326] Ad ogni Contratto Esecutivo stipulato tra il Fornitore e la singola Amministrazione corrisponderà una procedura di collaudo "sul campo" atta a verificare la conformità delle caratteristiche di ogni singolo PAS rilasciato all'Amministrazione rispetto a:

- indicazioni contenute nel "Piano dei fabbisogni" redatto dalla singola Amministrazione;
- progetto del Fornitore descritto nel "Progetto dei fabbisogni";
- specifiche contenute nel presente Capitolato;
- risultati delle verifiche su test bed.

[R.327] Il Fornitore dovrà consegnare all'Amministrazione, nell'ambito del Progetto dei fabbisogni, un documento intitolato "Specifiche di dettaglio delle prove di collaudo (configurazione degli accessi)" che descrive la tipologia delle prove di collaudo previste e la pianificazione temporale delle stesse. Tali specifiche di dettaglio dovranno essere conformi alle "Specifiche delle prove di collaudo di configurazione degli accessi" contenute nella Documentazione di Riscontro, di cui al par. 7.4, approvata dall'Amministrazione Aggiudicatrice.

[R.328] Le prove di collaudo dovranno verificare:

- caratteristiche HW/SW e funzionalità dei sistemi installati;
- interfaccia rete interna (PAS);
- corretta implementazione della connettività;
- servizi di sicurezza implementati;
- rilevazioni sugli indicatori di qualità del servizio;
- procedure di fatturazione e rendicontazione.

[R.329] Il Fornitore dovrà altresì impegnarsi, qualora richiesto dall'Amministrazione, a svolgere ulteriori prove integrative.

[R.330] Le prove di collaudo relative ad un'Amministrazione saranno eseguite da personale del Fornitore in contraddittorio con il personale dell'Amministrazione.

7.4 Documentazione di riscontro

[R.331] La "Documentazione di riscontro", di seguito descritta, dovrà essere inizialmente predisposta nei tempi indicati al [R.324], e risulterà approvata all'esito positivo della verifica di conformità iniziale di cui al precedente par. 7.2.

[R.332] Il Fornitore dovrà aggiornare in corso d'opera (comunque, ad ogni cambiamento dei sistemi utilizzati) la Documentazione di riscontro. Tali aggiornamenti dovranno essere comunicati a Consip, che si riserva di accettarli o chiedere modifiche, che il Fornitore dovrà recepire e formalizzare in una nuova versione della documentazione entro 15 giorni dalla richiesta.

[R.333] Tutta la documentazione di seguito descritta e relativa ai servizi, dovrà essere conforme alla norma ISO 9004/2-91 ed in particolare dovrà contenere:

- le specifiche del servizio comprendenti:
  - una chiara descrizione delle caratteristiche del servizio soggette a valutazione del cliente;
  - le condizioni di accettabilità per ciascuna caratteristica del servizio.
- le specifiche di realizzazione del servizio, comprendenti:
  - una chiara descrizione delle caratteristiche di realizzazione del servizio che influenzano direttamente le prestazioni del servizio;
  - le condizioni di accettabilità per ciascuna caratteristica di realizzazione del servizio;
  - i requisiti delle risorse (hw, sw ed umane, in quest'ultimo caso la quantità ed il profilo professionale) utilizzate per svolgere il servizio.
- le specifiche di controllo qualità del servizio, comprendenti la definizione dei metodi di valutazione e controllo delle caratteristiche e della realizzazione dei servizi.

[R.334] L'elenco della Documentazione di Riscontro che dovrà essere predisposta dal Fornitore è riportato nella tabella seguente.

Documento di riscontro	***Contenuto***	***Riferimento Capitolato***
Documento programmatico di gestione della sicurezza	• Descrizione delle misure organizzative (ruoli, responsabilità e procedure), tecniche (sistemi hw e sw impiegati) e fisiche adottate per soddisfare i requisiti del capitolato.	n.a.

Piano generale per l'erogazione dei servizi	• Descrizione della struttura funzionale ed organizzativa del Fornitore ai fini dell'erogazione dei servizi oggetto della presente gara. • Matrice compiti-responsabilità. • Pianificazione delle macro attività necessarie per la realizzazione delle infrastrutture e l'erogazione dei servizi.	n.a.
Documentazione tecnica relativa all'erogazione dei servizi di connettività, sicurezza, VoIP e Comunicazione evoluta.	• Numero, tipologia e caratteristiche funzionali e di sistema dei sistemi, hardware e software, utilizzati per erogare il servizio, inclusi: ◦ Dimensioni degli apparati e assorbimento di potenza misurato in kVA. ◦ Presenza eventuale del gruppo di continuità e di batterie e accumulatori. ◦ Limiti di temperatura e di umidità relativa sopportati (necessità o meno di condizionamento ambientale, indicando la dissipazione energetica) ◦ Modalità di interconnessione tra le parti, con indicazione di necessità o meno di pavimento sopraelevato. • Caratteristiche architetturali e tecnologiche dei collegamenti IP. • Descrizione dell'infrastuttura di rete utilizzata per l'erogazione dei servizi. • Tipologia e release dei software utilizzati per erogare i servizi. • Protocolli utilizzati per l'erogazione dei servizi. • Descrizione delle modalità di interfacciamento con la rete PSTN (per il servizio VoIP). • Meccanismi/protocolli utilizzati per realizzare l'integrazione con altri strumenti di sicurezza forniti dal Fornitore o da terzi, la modalità e il livello di integrazione (per il servizio di sicurezza).	Par. 2, 3, 4.

Documentazione tecnica relativa ai servizi di supporto, rilevazione e reportistica sugli SLA	• Descrizione architetturale, funzionale e di sistema del NOC e SOC, comprensiva di:
	  • Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio.
	  • Tipologia e release del software utilizzato per erogare il servizio.
	  • Caratteristiche dei collegamenti tra la rete del Fornitore ed i sistemi utilizzati per erogare il servizio.
	• Specifiche di realizzazione:
	  • del sistema per la rilevazione dei livelli di servizio e di generazione della reportistica (rif. par. 8)
	  • del sistema preposto all'erogazione dei servizi di rendicontazione e fatturazione (rif. par. 5.8)
	  • del sistema di supervisione e monitoraggio della qualità (rif. 5.3)
	• Caratteristiche tecniche dei sistemi utilizzati per il call center, e criteri di dimensionamento delle risorse umane ad esso dedicate
		Par. 5, 8

Specifiche di dettaglio delle prove di collaudo iniziale	• Architettura dei sistemi utilizzati per il collaudo • Elenco delle prove di collaudo.	Paragrafo 7.2

Specifiche delle prove di collaudo di configurazione degli accessi	• elenco delle prove di collaudo cui saranno sottoposti cui saranno sottoposti, sul campo, i servizi contrattualizzati dalle Amministrazioni contraenti:
	  • servizi di connettività;
	  • servizi di sicurezza;
	  • servizi VoIP e servizi di Comunicazione Evoluta
		Paragrafo 6.2, 7.3

Documentazione di Comprova	Documentazione tecnica/schede tecniche/relazione sulle prove, come meglio descritto nel seguito	Paragrafo 7.4

Tabella 2**:** Documentazione di riscontro relativa al Contratto Quadro

[R.335] La documentazione di riscontro deve avere un dettaglio sufficiente a consentire la verifica della conformità dei servizi a tutte le prescrizioni tecniche del presente Capitolato, e alle caratteristiche definite nell'Offerta Tecnica del Fornitore.

[R.336] Relativamente agli apparati di accesso per i servizi di connettività IP (par. 2), e a tutti gli apparati per i servizi di sicurezza (par. 3), VoIP e Comunicazione Evoluta (par. 4) la Documentazione di Riscontro dovrà contenere la "Documentazione di Comprova". Quest'ultima dovrà provare che i predetti apparati rispettano tutte le caratteristiche tecniche definite nel presente Capitolato e nell'Offerta Tecnica del Fornitore.

Costituiscono mezzo appropriato per la predetta comprova:

- documentazione tecnica del produttore, sottoscritta da persona dotata di comprovati poteri del produttore, per la quale Consip S.p.A. si riserva di richiedere documentazione a comprova della sussistenza dei necessari poteri, in forma di:
    - dichiarazione del possesso degli apparati delle caratteristiche tecniche definite nel presente Capitolato e nell'Offerta Tecnica del Fornitore;

    e/o
    - documenti attestanti l'esecuzione di prove da parte del produttore che consentano di verificare il possesso degli apparati delle caratteristiche tecniche definite nel presente Capitolato e nell'Offerta Tecnica del Fornitore. La documentazione fornita dovrà descrivere l'ambiente in cui si è effettuata la prova, le modalità di verifica, gli esiti attesi e i risultati ottenuti;

  e/o
- scheda tecnica del prodotto che il concorrente dovrà produrre in copia conforme all'originale, ai sensi del D.P.R. n. 445/2000;

  e/o
- relazione sulle prove eseguite da un organismo riconosciuto (quali i laboratori di prova, di calibratura e gli organismi di ispezione e di certificazione conformi alle norme europee applicabili).

8. SLA e penali

8.1 Definizioni relative ai Livelli di servizio

Nella tabella seguente si riportano le definizioni adottate nella specifica dei livelli di servizio.

Orario di Erogazione dei Servizi	L'orario di erogazione dei servizi è 00:00 - 24:00, tutti i giorni dell'anno. Tale orario coincide con la viene utilizzato anche per il calcolo dei livelli di servizio
Periodo di osservazione contrattuale ($T_{oss-con}$)	Periodo per il calcolo dei livelli di servizio contrattuali ai quali sono associate le relative penali. ***Toss-con*** = 2 (due) mesi solari coincidenti con il bimestre di fatturazione
Punto di accesso al servizio (PAS)	È il punto di erogazione del servizio per il calcolo della disponibilità. I PAS sono definiti, per ciascuna tipologia di servizio, nella sezione corrispondente del presente Capitolato Tecnico.
Disponibilità unitaria	Percentuale di tempo durante il quale un singolo PAS è funzionante (ovvero non vi è interruzione di servizio) rispetto alla finestra temporale di erogazione del servizio stesso. È calcolata con la seguente formula: $D_i = \left(1 - \frac{\sum_{j=1}^{M_i} d_{ij}}{T_i}\right) \times 100$ dove: • D_i = disponibilità unitaria del PAS i-esimo espressa come valore percentuale; • d_{ij} = durata del disservizio j-esimo del PAS i-esimo; • M_i = numero totale di disservizi bloccanti (che comportano cioè l'indisponibilità del servizio, per interruzione dello stesso o per prestazioni decisamente degradate) del PAS i-esimo; • T_i = finestra temporale di misurazione della disponibilità del PAS i-esimo, pari al periodo di osservazione contrattuale ($T_{oss-con}$).

Tempo di Ripristino del servizio	Tempo intercorrente tra la segnalazione del disservizio e la chiusura dello stesso. La chiusura del disservizio viene catalogata dal Fornitore previa accettazione dell'Amministrazione, a conferma dell'avvenuto ripristino dell'operatività.
Livello di Disponibilità del PAS	Sono previsti due possibili livelli, in termini di disponibilità unitaria e di tempo di ripristino del servizio: • **AS (Affidabilità Standard)** • **AE (Affidabilità Elevata)**
Report Contrattuale ***(cadenza bimestrale)***	Report trasmesso alla singola Amministrazione contestualmentte alla fattura e, comunque, non oltre 20 (venti) giorni successivi al termine del bimestre di fatturazione, È il report che contiene le misurazioni dei livelli di servizio applicabili al calcolo delle penali, la cui approvazione, da parte dell'Amministrazione contraente, costituisce positiva verifica di conformità
Arrotondamenti	Ai fini del calcolo dello scostamento tra le percentuali misurate e quelle contrattuali le prime dovranno essere arrotondate nel modo seguente: • aumento o riduzione del 5%: si arrotonda allo 0% per scostamenti compresi tra lo 0,00% e 2,49% ed al 5% per scostamenti superiori; • aumento o riduzione dell'1%: si arrotonda allo 0% per scostamenti compresi tra lo 0,00 e lo 0,49 ed all'1% per scostamenti superiori; • aumento o riduzione del 0,5%: si arrotonda allo 0% per scostamenti compresi tra lo 0,000% e 0,249% ed al 0,5% per scostamenti superiori; • aumento o riduzione dello 0,1%: si arrotonda allo 0% per scostamenti compresi tra lo 0,000% e lo 0,049% ed allo 0,1% per scostamenti superiori; • aumento o riduzione del 0,05%: si arrotonda allo 0% per scostamenti compresi tra lo 0,0000% e 0,0249% ed al 0,05% per scostamenti superiori.
CToss (Corrispettivo per il periodo di osservazione contrattuale)	Importo alla base del calcolo delle penali. Per un dato servizio, CToss è pari ai corrispettivi complessivi contrattualmente previsti nel periodo di osservazione contrattuale, cioè 2 mesi. Ad esempio, nel caso in cui per il servizio sia previsto un canone mensile, il CToss è pari al canone mensile moltiplicato per 2.
Ctot (Corrispettivi totali)	Importo alla base del calcolo delle penali. E' l'importo contrattuale netto del contratto esecutivo, calcolato applicando i corrispettivi contrattualmente previsti alla totalità dei servizi attivati, per l'intera durata contrattuale. Per le penali basate su tale valore, l'Amministrazione applicherà una penale di importo basato sul Ctot risultante dai servizi già erogati dal Fornitore, e da quelli che erogherà in base all'ultimo Progetto dei Fabbisogni approvato. Nel caso in cui, successivamente all'applicazione della penale, vi siano variazioni del Progetto dei Fabbisogni e, quindi, del Ctot, si procederà a conguaglio dell'importo della penale già applicata.

8.2 Livello di servizio, penali contrattuali e reportistica per le Amministrazioni Contraenti

[R.337] Per la valutazione dei livelli di servizio, il Fornitore dovrà rilevare i parametri riportati nei paragrafi seguenti, compresi quelli non utilizzati direttamente per la valutazione delle penali.

[R.338] La valutazione dei livelli di servizio ai fini dell'applicazione delle penali contrattuali è fatta su base bimestrale, pertanto i parametri rilevati dovranno rimanere nei limiti indicati del bimestre di riferimento.

[R.339] In caso di mancato rispetto dei livelli di servizio, la singola Amministrazione applicherà le penali indicate nei successivi paragrafi. Il Fornitore dovrà rendere disponibili su supporto elettronico a Consip ed alle singole Amministrazioni, per la parte di propria competenza, i risultati delle misure effettuate, attraverso report bimestrali (*report contrattuali*), con la misurazione dei livelli di servizio e il calcolo delle penali.

[R.340] Tali report contrattuali dovranno essere trasmessi alla singola Amministrazione contestualmente alla fattura e, comunque, non oltre 20 (venti) giorni successivi al termine del bimestre di fatturazione.

8.2.1 Servizi di Connettività IP

Livelli di servizio e penali

Parametro	*Limite (SLA Target)*	*Penale*
Ritardo di trasferimento* ***(RTD)*** *(*) garantito per throughput entro la BGA*	Il 99% dei pacchetti entro: • 300 ms, nel caso di collegamenti con BGA pari o superiore a 2 Mbit/s • 400 ms, nel caso di collegamenti con BGA inferiore a 2 Mbit/s • 900 ms, per collegamenti satellitari	1% del CToss del collegamento fuori SLA Target, per ogni scostamento in diminuzione di 0,1% rispetto allo SLA Target
Tasso di perdita dei pacchetti	1% dei pacchetti (garantito per throughput entro la BGA)	1% del CToss del collegamento fuori SLA Target, per ogni scostamento in aumento di 0,1% rispetto allo SLA Target
Disponibilità unitaria	Valori offerti dal Fornitore per ciascuno specifico collegamento: - in Affidabilità Standard (AS) ed in Affidabilità Elevata (AE) per i collegamenti a Banda Garantita; - in Affidabilità Unica (AU) per i collegamenti Best Effort	Per AS e AU, 1% del CToss del collegamento fuori SLA Target, per ogni scostamento in diminuzione di 0,1% rispetto allo SLA Target Per AE, 0,1% del CToss del collegamento fuori SLA Target, per ogni scostamento in diminuzione di 0,01% rispetto allo SLA Target
Tempo di ripristino del servizio	Valori offerti dal Fornitore per ciascuno specifico collegamento: • in Affidabilità Standard (AS) ed in Affidabilità Elevata (AE) per i collegamenti a Banda Garantita; • in Affidabilità Unica (AU) per i collegamenti Best Effort	Per ogni evento fuori dello SLA Target, 0,015‰ dell'importo netto contrattuale Ctot, per ogni ora eccedente lo SLA Target. Per ogni ora eccedente il doppio dello SLA Target, la penale è pari allo 0,03‰ del Ctot

Report contrattuale

Disponibilità unitaria di ogni collegamento
Per ciascun collegamento, percentuale dei pacchetti con ritardo di trasferimento inferiore a: • *300 ms, nel caso di collegamenti con BGA pari o superiore a 2 Mbit/s* • *400 ms, nel caso di collegamenti con BGA inferiore a 2 Mbit/s* • *900 ms, per collegamenti satellitari*
Tasso di perdita dei pacchetti per ciascun collegamento

Elenco dei disservizi (trouble ticket), con indicazione, per ciascuno di essi: - *delle sedi e dei collegamenti interessati,* - *di data/ora di: apertura del guasto, segnalazione di ritorno, ripristino del servizio.* - *Tempo effettivo di ripristino, e SLA Target*
Riepiloghi statistici dei tempi di ripristino con indicazione dei valori minimi, medi e massimi
Calcolo analitico dell'importo delle eventuali penali dovute

8.2.2 Servizi di Sicurezza

Livelli di servizio e penali

Parametro	*Limite (SLA Target)*	*Penale*
Applicazione delle patch di sicurezza	Entro 2 giorni dal rilascio da parte del produttore del dispositivo	Per ogni evento fuori dello SLA Target, 0,3‰ dell'importo netto contrattuale Ctot, per ogni giorno di ritardo
Apertura del ticket di incidente di sicurezza	Livello 1 (gravità alta): entro 15 minuti dall'identificazione dell'evento Livello 2 (gravità media): entro 30 minuti dall'identificazione dell'evento Livello 1 (gravità alta): entro 60 minuti dall'identificazione dell'evento	Per ogni evento fuori dello SLA Target, 0,004‰ dell'importo netto contrattuale Ctot, per ogni 15 minuti eccedenti lo SLA Target
Report su incidente di sicurezza	Entro il giorno successivo a quello dell'evento	Per ogni evento fuori dello SLA Target, 0,3‰ dell'importo netto contrattuale Ctot, per ogni giorno di ritardo
Report riepilogativo giornaliero	Entro il giorno successivo a quello cui i dati si riferiscono	Per ogni evento fuori dello SLA Target, 0,3‰ dell'importo netto contrattuale Ctot, per ogni giorno di ritardo
Tempo di validazione della richiesta di una nuova regola/policy	Valore offerto dal Fornitore	Per ogni evento fuori dello SLA Target, 0,015‰ dell'importo netto contrattuale Ctot, per ogni ora eccedente lo SLA Target.
Tempo di implementazione della richiesta di una nuova regola/policy	Valore offerto dal Fornitore	Per ogni evento fuori dello SLA Target, 0,015‰ dell'importo netto contrattuale Ctot, per ogni ora eccedente lo SLA Target.
Verifica dell'attuazione delle policy di sicurezza	Invio trimestrale dell'esito delle verifiche	Per ogni evento fuori dello SLA Target, 0,3‰ dell'importo netto contrattuale Ctot, per ogni giorno di ritardo

Notifica degli incidenti di gravità elevata	Entro 30 minuti dall'identificazione dell'evento	Per ogni evento fuori dello SLA Target, 0,004‰ dell'importo netto contrattuale Ctot, per ogni 15 minuti eccedenti lo SLA Target
Invio dei log di sistema generati dai dispositivi di sicurezza	Entro il giorno successivo alla richiesta da parte dell'Amministrazione	Per ogni evento fuori dello SLA Target, 0,3‰ dell'importo netto contrattuale Ctot, Per ogni giorno di ritardo
Disponibilità unitaria	Valori offerti dal Fornitore: - in Affidabilità Standard (AS)per tutti i servizi di sicurezza	Per AS, 1% del CToss del PAS fuori SLA Target, per ogni scostamento in diminuzione di 0,1% rispetto allo SLA Target
	- in Affidabilità Elevata (AE) per il servizio di NGFW	Per AE, 0,1% del CToss del PAS fuori SLA Target, per ogni scostamento in diminuzione di 0,01% rispetto allo SLA Target
Tempo di ripristino del servizio	Valori offerti dal Fornitore: - in Affidabilità Standard (AS)per tutti i servizi di sicurezza - in Affidabilità Elevata (AE) per il servizio di NGFW	Per ogni evento "tempo di ripristino maggiore dello SLA Target", 0,015‰ dell'importo netto contrattuale Ctot, per ogni ora eccedente lo SLA Target. Per ogni ora eccedente il doppio dello SLA Target, la penale è pari allo 0,03‰ del Ctot

Report contrattuale

Disponibilità unitaria di ciascun PAS dei servizi di sicurezza
Elenco dei disservizi (trouble ticket), con indicazione, per ciascuno di essi: - *delle sedi e dei servizi interessati,* - *di data/ora di: apertura del guasto, segnalazione di ritorno, ripristino del servizio;* - *tempo effettivo di ripristino, e SLA Target.*
Elenco delle richieste di modifica delle regole/policy, con indicazione, per ciascuna di essa di data/ora di: richiesta, validazione, implementazione, SLA Target.
Elenco delle patch di sicurezza applicate, con indicazione, per ciascuna di esse, di data di: rilascio da parte del produttore del dispositivo, applicazione, SLA Target.
Elenco dei ticket di sicurezza, con indicazione, per ciascuno di essi: - *del livello di gravità associato* - *di data/ora di: identificazione dell'evento, apertura del ticket, SLA Target.* *Per gli eventi di gravità elevata, indicazione di data/ora della notifica all'Amministrazione, SLA Target.*
Report su incidenti di sicurezza e report riepilogativi giornalieri: elenco dei report inviati, con indicazione della data di invio, dell'evento/giorno cui si riferisce, e dello SLA Target

Elenco delle richieste formulate dall'Amministrazione relative ai log di sistema, con indicazione della data di richiesta, data invio log, SLA Target.
Calcolo analitico dell'importo delle eventuali penali dovute

8.2.3 Servizi VoIP e di Comunicazione Evoluta

Livelli di servizio e penali

Parametro	*Limite (SLA Target)*	*Penale*
Disponibilità unitaria della linea VoIP	Affidabilità Standard: 99% Affidabilità Elevata: 99,9%	Per AS, 1% del CToss del PAS fuori SLA Target, per ogni scostamento in diminuzione di 0,1% rispetto allo SLA Target Per AE, 0,1% del CToss del PAS fuori SLA Target, per ogni scostamento in diminuzione di 0,01% rispetto allo SLA Target
Tasso di chiamate su linea VoIP a buon fine	99% dei tentativi di chiamata	2% del CToss del PAS fuori SLA, per ogni scostamento in diminuzione di 0,1% rispetto allo SLA Target
Tempo di implementazione di una modifica di configurazione	12 ore dal ricevimento della richiesta	Per ogni evento fuori dello SLA Target, 0,015‰ dell'importo netto contrattuale Ctot, per ogni ora eccedente lo SLA Target
Disponibilità unitaria dei servizi IP Telephony, IP Trunking e videcomunicazione di qualità su IP	Affidabilità Standard: 99%, su base sede Affidabilità Elevata: 99,9%, su base sede	Per AS, 1% del CToss del servizio fuori SLA Target, su base sede, per ogni scostamento in diminuzione di 0,1% rispetto allo SLA Target Per AE, 0,1% del CToss del servizio fuori SLA Target, su base sede, per ogni scostamento in diminuzione di 0,01% rispetto allo SLA Target
Tempo di ripristino del servizio (tutti i servizi VoIP e Comunicazione Evoluta)	Affidabilità Standard: 72 ore Affidabilità Elevata: 8 ore	Per ogni evento "tempo di ripristino maggiore dello SLA Target", 0,015‰ dell'importo netto contrattuale Ctot, per ogni ora eccedente lo SLA Target. Per ogni ora eccedente il doppio dello SLA Target, la penale è pari allo 0,03‰ del Ctot

Report contrattuale

Disponibilità unitaria di ciascun PAS delle linee VoIP e, su base sede, dei servizi IP Telephony, IP Trunking e videocomunicazione di qualità su IP
Elenco dei disservizi (trouble ticket), con indicazione, per ciascuno di essi: - *delle sedi e dei servizi interessati,* - *di data/ora di: apertura del guasto, segnalazione di ritorno, ripristino del servizio;* - *tempo effettivo di ripristino, e SLA Target.*
Elenco delle richieste di modifica di configurazione, con indicazione, per ciascuna di essa di data/ora di: richiesta, implementazione, SLA Target.
Report dettagliato sulle chiamate originate, con indicazione del chiamante, del chiamato, della data/ora di inizio e fine della chiamata, della durata
Tasso di chiamate andate a buon fine e numero complessivo di tentativi di chiamata
Calcolo analitico dell'importo delle eventuali penali dovute

8.2.4 Servizi di supporto

Livelli di servizio e penali

Parametro da rilevare	***Limite (SLA Target)***	***Penale***
Tempo di attesa del servizio di call center	Tempo, misurato in secondi, che intercorre tra l'ingresso della chiamata nel sistema telefonico e la risposta da parte dell'operatore del Call Center (o la terminazione senza risposta della chiamata da parte dell'Amministrazione) ≤ 60 secondi	50 Euro per ogni evento di mancato rispetto del limite (SLA Target)
RTO	valore offerto dal Fornitore	Per ogni interruzione del servizio del SOC superiore allo SLA Target, 0,04‰ dell'importo netto contrattuale Ctot, per ogni ora di interruzione eccedente lo SLA Target

RPO	SLA Target = percentuale dei campioni di dati messi in sicurezza entro il valore di RPO offerto dal Fornitore = 99% Tale SLA Target è relativo ad un quadrimestre, con campionamento dei dati effettuato dal Fornitore almeno settimanalmente.	Per ogni punto percentuale di scostamento dalla soglia definita, verrà applicata una penale pari allo 0,3‰ dell'importo netto contrattuale Ctot

Report contrattuale

Chiamate ricevute dal call center: - *Numero totale* - *Numero di chiamate fuoriSLA Target;* - *Tempo medio di attesa*
Data ed ora di interruzione e ripristino del servizio del SOC
Campionamenti RPO: date di campionamento e, per ciascuna di esse, numero di campioni estratti e numero di campioni di dati messi in sicurezza entro il tempo di RPO offerto. Percentuale nel periodo di riferimento.
Calcolo analitico dell'importo delle eventuali penali dovute

8.2.5 Progetto dei Fabbisogni, Provisioning & Change Management, Reportistica

Parametro da rilevare	***Limite (SLA Target)***	***Penale***
Invio del Progetto dei Fabbisogni (primo Progetto, o aggiornamento a seguito di variazione/aggiornamento del Piano dei Fabbisogni)	Entro 45 giorni dalla ricezione del Piano dei Fabbisogni, o della variazione/aggiornamento del Piano dei Fabbisogni	Per ogni giorno di ritardo, 0,3‰ dell'importo netto contrattuale Ctot
Invio del Progetto dei Fabbisogni che recepisce le modifiche richieste dall'Amministrazione	Entro 15 giorni dalla ricezione delle richieste di modifica da parte dell'Amministrazione	Per ogni giorno di ritardo, 0,3‰ dell'importo netto contrattuale Ctot

Provisioning del servizio	Attivazione del servizio entro 3 mesi dall'approvazione del Progetto dei Fabbisogni in cui il servizio è previsto, o entro il diverso tempo concordato nel Progetto dei Fabbisogni	Per ogni giorno di ritardo, 0,3‰ dell'importo netto contrattuale Ctot. Per ciascun giorno di ritardo successivo al trentesimo, 0,6‰ dell'importo netto contrattuale Ctot
Trasloco esterno	Attivazione del servizio entro 3 mesi dall'approvazione del Progetto dei Fabbisogni in cui è previsto il trasloco del servizio	Per ogni giorno di ritardo, 0,3‰ dell'importo netto contrattuale Ctot. Per ciascun giorno di ritardo successivo al trentesimo, 0,6‰ dell'importo netto contrattuale Ctot
Trasloco interno	Attivazione del servizio entro 1 mese dall'approvazione del Progetto dei Fabbisogni in cui è previsto il trasloco del servizio	Per ogni giorno di ritardo, 0,3‰ dell'importo netto contrattuale Ctot. Per ciascun giorno di ritardo successivo al trentesimo, 0,6‰ dell'importo netto contrattuale Ctot
Frequenza dei report contrattuali	Contestuale alla fattura e, comunque, non oltre 20 (venti) giorni successivi al termine del bimestre di fatturazione	Per ogni giorno di ritardo, 0,3‰ dell'importo netto contrattuale Ctot

8.3 Livello di servizio, penali contrattuali e reportistica per l'Amministrazione Aggiudicatrice

Parametro	***Limite (SLA Target)***	***Penale***
Aggiornamento/adeguamento della documentazione di riscontro	Entro 15 giorni dal cambiamento dei sistemi utilizzati, o dalla richiesta di Consip	Euro 1.000,00 per ogni giorno di ritardo
Benchmark tecnico/economico dei servizi da ampliare/modificare (rif. par. 2.5)	Invio del Benchmark a Consip entro 30 giorni dalla richiesta	Euro 1.000,00 per ogni giorno di ritardo
Invio dei report quadrimestrali delle consistenze tecniche	Entro il giorno 20 dei mesi di gennaio, maggio e settembre con riferimento rispettivamente al terzo quadrimestre dell'anno precedente ed al primo e secondo quadrimestre dell'anno in corso.	Per ogni report inviato in ritardo, Euro 500,00 per ogni giorno di ritardo

Invio della relazione consuntiva annuale	Entro il giorno 20 del mese di gennaio, con riferimento rispettivamente all'anno precedente.	Per ogni relazione inviata in ritardo, Euro 500,00 per ogni giorno di ritardo