ALLEGATO 5 - CAPITOLATO TECNICO

Sommario

1. DEFINIZIONI ED ACRONIMI

Nel presente documento vengono riportate le definizioni univoche di alcuni termini che ricorrono all'interno della documentazione di gara. Inoltre, per agevolare la lettura, si fornisce un elenco degli acronimi più frequentemente utilizzati con il relativo significato.

Tabella 1 – Termini e Definizioni	
Ambito	L'insieme di risorse che possono essere raggiunte da pacchetti IP su una VPN. Il SPC prevede 3 ambiti: Intranet, Infranet e Internet.
Amministrazione/i	Le Amministrazioni centrali dello Stato nonché le Amministrazioni locali e gli altri enti che hanno la facoltà di avvalersi dei servizi del SPC.
Application Service Provider (ASP)	Ente che fornisce server e software applicativo all'utente.
Autonomous System (AS)	Insieme di router sottoposti a una sola autorità amministrativa.
Border Gateway Protocol (BGP)	Protocollo che realizza la connessione fra router di Autonomous System (AS) diversi.
Border Router (BR)	Router che realizza la connessione fra Autonomous System (AS) diversi; può essere considerato come il punto di ingresso e di uscita verso altri AS.
Border Router della QXN (BRQXN)	Router della QXN collegato con i BR dei fornitori per realizzare la connessione con la

	QXN a livello IP.
Classe di servizio (CdS)	Caratterizzazione dei pacchetti secondo parametri di priorità.
Comitato di Direzione Tecnica	Comitato composto dai rappresentanti dell'AgID, della CONSIP e dai rappresentanti di tutti i fornitori assegnatari, che assume le determinazioni relative al funzionamento complessivo dei servizi
Comitato Tecnico della QXN	Comitato composto dal direttore tecnico della società di gestione della QXN, da un rappresentante dell'AgID che supporta la definizione delle caratteristiche tecniche della QXN e la definizione di regole tecniche per l'interoperabilità del SPC
Differentiated Services Code Point	Codice contenuto nell'header di un pacchetto IP che consente l'assegnazione del pacchetto ad una classe di servizio DiffServ.
Domain Name System (DNS)	Applicazione client/server in grado di tradurre i nomi mnemonici utilizzati dagli utenti per identificare un sito, nei relativi indirizzi IP.
Dominio di interconnessione SPC	Complesso delle risorse informatiche ed infrastrutture telematiche che realizzano il SPC e la QXN.
Dominio di una PA	Complesso delle risorse informatiche e delle infrastrutture che realizzano il Sistema Informativo della Pubblica Amministrazione; raccoglie i flussi dati di tutte le sedi dell'Amministrazione.
Dominio VoIP	Insieme di postazioni IP native ed i relativi elementi sede della logica di controllo delle

	chiamate
Fornitore Aggiudicatario	La società che risulta aggiudicataria secondo le procedure della gara.
Fornitore Assegnatario	Una delle Società a cui è stata assegnata una delle parti, successive alla prima, della fornitura pervista dalle procedure di gara.
Fornitore	Fornitore Aggiudicatario o Assegnatario
Host Intrusion Detection System (HIDS)	Sistema che rileva accessi non consentiti o potenziali attacchi a un sistema informatico per mezzo di sorgenti d'informazioni disponibili sul sistema.
Infranet	L'ambito SPC che permette il trasferimento di informazioni tra sedi di diverse Amministrazioni
Internet Service Provider (ISP)	Ente che fornisce all'utente l'accesso ad Internet.
Infranet	L'ambito SPC che permette il trasferimento di informazioni tra sedi di diverse Amministrazioni
Network Address Translation (NAT)	Funzionalità di mapping tra indirizzi interni ad una rete (privati) ed indirizzi esterni (pubblici ovvero univoci in ambito Internet).
Network Intrusion Detection System (NIDS)	Sistema che rileva accessi non consentiti o potenziali attacchi a un sistema informatico per mezzo di sorgenti d'informazioni disponibili sulla rete.
Network Operation Center (NOC)	Centro di controllo delle funzionalità della rete.

Network Time Protocol (NTP)	Protocollo che consente ai computer su Internet di sincronizzare i loro orologi con un tempo di riferimento.
Offerta Economica	Il Documento redatto dalla Società Concorrente che partecipa alla Gara Multifornitore. L'Offerta Economica dovrà contenere la quotazione economica di dettaglio di tutti i servizi e delle prestazioni Oggetto della Fornitura.
Open Systems Interconnection (OSI)	Standard internazionale dell'ISO (documento ISO 7498) per un modello di riferimento per l'interconnessione di sistemi.
Gestore delle IC-SPC	Soggetto individuato dall'AgID per la gestione delle Infrastrutture Condivise in relazione, tra l'altro, ai Servizi di Interoperabilità delle reti ed ai Servizi di Governance.
Punto di Accesso ai Servizi	Punto fisico del Dominio che permette l'accesso ad ognuno dei servizi e che funge da riferimento per le misure
Security Operating Center (SOC)	Centro di controllo delle funzionalità di sicurezza della rete.
Service Level Agreement (SLA)	Contratto fra utente e gestore di un servizio in cui vengono specificati i parametri gestionali e prestazionali minimi da garantire per il servizio stesso.
Simple Mail Transfer Protocol	Standard protocollare che regola la trasmissione dei messaggi e-mail.
Società Concorrente/Partecipante	L'Impresa, il Raggruppamento Temporaneo di Imprese (RTI) ovvero il Consorzio che partecipa alla Gara Multifornitore.

Virtual Private Network (VPN)	Ambiente comunicativo in cui l'accesso alle risorse della rete è controllato in modo da permettere la comunicazione tramite connessioni paritarie solo all'interno di una ben definita comunità di interesse nonostante tali connessioni possano essere realizzate utilizzando un'infrastruttura di rete pubblica e condivisa, quale ad esempio internet.

Tabella 2 – Acronimi e abbreviazioni

AAA	Autenticazione, Autorizzazione e Accounting
AgID	Agenzia per l'Italia Digitale
AS	Autonomous System
ATI	Associazione Temporanea d'Impresa
BGA	Banda Garantita in Accesso
BGETE	Banda Garantita End To End
BGP	Border Gateway Protocol
BMA	Banda Massima in Accesso
BR	Border Router
BRQXN	BR della QXN collegato con i BR dei fornitori per realizzare la connessione con la QXN a livello IP ed Ethernet.
CC-SPC	Commissione di Coordinamento del Sistema Pubblico di Connettività
CdA	Componente di Accesso per i servizi di trasporto
CdT	Componente di Trasferimento per i servizi di trasporto

CERT	Computer Emergency Response Team
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione.
CdS	Classe di Servizio
CTT	Componente di Terminazione del traffico
DNS	Domain Name System
DSCP	Differentiated Services Code Point
HIDS	Host Intrusion Detection System
ISP	Internet Service Provider
NAP	Neutral Access Point
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NOC	Network Operation Centre
NOC-QXN	Network Operation Centre della QXN
NTP	Network Time Protocol
OOB	Out Of Band
OPA	Offerta per le Amministrazioni
OPO	Offerta per gli altri Operatori
OSI	Open System Interconnection
OWD	One Way Delay
PA	Pubblica Amministrazione (centrale o locale)
PAC	Pubblica Amministrazione Centrale
PAL	Pubblica Amministrazione Locale
PAS	Punto di Accesso al Servizio
PBX	Private Branch eXchange
PKI	Internal Key Infrastructure

PLMN	Internal Land Mobile Network
pps	Pacchetti per secondo
PSTN	Internal Switched Telephone Network
QXN	Qualified eXchange Network
RTD	Round Trip Delay
RTI	Raggruppamento Temporaneo d'Impresa
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOC	Security Operating Center
SPC	Sistema Pubblico di Connettività
SSP	Security Service Provider
TdR	Terminazione di Rete
TT	Trouble Ticket
VoIP	Voice Over IP
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

2. PRESCRIZIONI GENERALI

[R.1] 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 o dalle mutazioni dei processi e delle esigenze delle Amministrazioni.

[R.2] I servizi descritti 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 come richiesto dal capitolato. Salvo quanto espressamente previsto nei listini, nessun onere derivante da queste attività e da quelle derivanti dalle misure tecnico-organizzative adottate per il monitoraggio e la rendicontazione dei livelli di servizio può essere richiesto dal Fornitore.

[R.3] I servizi sono caratterizzati da opportuni livelli di servizio (SLA) che ne prescrivono la qualità. I livelli di servizio richiesti sono descritti nell'Allegato 5 bis - Livelli di servizio e penali.

[R.4] 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 non esiste un punto di frontiera diretto tra infrastruttura per il servizio e quella dell'Amministrazione.

[R.5] Tutti i servizi nel presente capitolato includono attività di gestione e manutenzione (meglio descritte nel § 7) erogate all'interno della finestra temporale Lunedì-Venerdì, 08.00-20.00 e Sabato 08.00-14.00, festivi esclusi (finestra standard), salvo contrattualizzazione dell'opzione di "finestra di erogazione estesa" (cfr. [R.6]).

[R.6] Per ogni servizio è disponibile l'opzione **finestra di erogazione estesa,** che prevede l'adozione di una finestra di erogazione H24, in sostituzione della finestra di erogazione standard (lun. ven. 8:00 – 20:00, sab. 8:00 – 14:00) inclusa nel servizio base.

[R.7] 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.

[R.8] L'installazione dei sistemi necessari per la fornitura dei servizi deve essere eseguita in conformità alle norme CEI attualmente in vigore, alle norme per la sicurezza degli impianti ed alle altre norme vigenti in materia.

3. SERVIZI DI TRASPORTO DATI

I servizi di trasporto dati sono dedicati alla trasmissione di qualunque tipo di dato (inclusi immagini e fonia) basati su protocollo IP.

I servizi di trasporto si articolano in:

- Servizi Wired:
- Servizi di trasporto dati su portante elettrica (STDE);
- Servizi di trasporto dati su portante ottica (STDO);
- Servizi Wireless:
- Servizi di trasporto dati satellitari (STDS).

[R.9] 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.10] 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, ecc.).

[R.11] Le interfacce per la fruizione dei servizi devono essere conformi ai relativi standard de jure e de facto, come richiesto all'interno delle specifiche relative ad ogni servizio oggetto di fornitura.

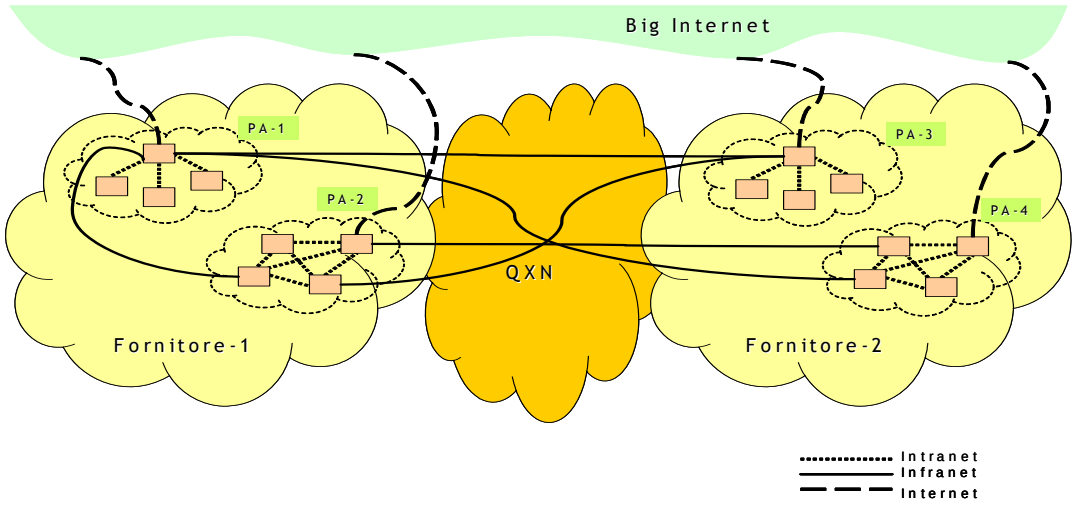
[R.12] Relativamente al trasporto del traffico IP sono definiti sul SPC i seguenti ambiti:

- Intranet: un ambito costituito dal dominio interno alla singola Amministrazione che connette tutte le sedi (o un sottoinsieme delle stesse) della stessa;

- Infranet: un ambito di interconnessione che connette tra loro le singole Amministrazioni attestate sul medesimo Q-ISP, o su Q-ISP differenti attraverso la QXN (Qualified eXchange Network) secondo le modalità definite nel 8;
- Internet: un ambito di interazione tra le singole Amministrazioni e soggetti non afferenti al SPC, attraverso la rete Internet.

[R.13] Il Fornitore deve garantire, su accessi configurati per gestire più ambiti, la segregazione del traffico appartenente a ciascun ambito.

Nella figura seguente è rappresentato uno schema del sistema.



[R.14] Tutti i servizi di trasporto dati definiti nel presente capitolato includono nel servizio base l'ambito Intranet.

[R.15] Ogni Amministrazione dovrà dotarsi di almeno un collegamento in ambito Infranet.

[R.16] La connettività verso tutti gli ambiti deve essere fornita senza limitazioni temporali e di accesso ai contenuti (network neutrality), anche da parte dei subfornitori e fino ai backbone internazionali; il Fornitore non può autonomamente limitare il trasporto di alcun protocollo dell'intera suite di protocolli Internet.

[R.17] Gli apparati di accesso forniti con i servizi di trasporto, ove previsti, devono essere gestiti e configurati dal Fornitore come componenti integranti del servizio, devono pertanto:

- essere ricompresi nel prezzo offerto;

- 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.18] 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.19] I parametri che caratterizzano i servizi di trasporto dati sono:

- **BNA (Banda Nominale in Accesso)**: definita come la banda fisica configurata sull'interfaccia geografica del servizio in oggetto. Relativamente ai soli servizi STDE e STDS, la BNA prevede una differenziazione in termini di banda nominale in uplink (BNAU) e di banda nominale in downlink (BNAD).
- **BGA (Banda Garantita in Accesso)**: definita come la larghezza di banda IP (comprensiva dell'overhead di protocollo) simmetrica in uplink e downlink garantita dal Fornitore. La BGA costituisce quindi il massimo valore di throughput per il quale il Fornitore è obbligato alla garanzia dei parametri di performance indicati per ciascuna tipologia di servizio (cfr. Allegato 5 bis).

[R.20] I servizi di trasporto dati di base, privi quindi della sottoscrizione di opzioni aggiuntive, devono comprendere:

- l'apparato di accesso al servizio;
- il circuito che permette all'Amministrazione il collegamento alla rete del Fornitore;
- l'abilitazione all'ambito Intranet (disattivabile su richiesta);
- la garanzia del trasporto di flussi di traffico fino al raggiungimento della BGA (se prevista dallo specifico servizio);
- il trasporto in modalità *best effort*, fino al raggiungimento della BNA;
- il rispetto dei livelli di assurance nella "finestra di erogazione standard".

[R.21] 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.22] Per consentire la comunicazione tra le reti, il Fornitore deve connettersi alla QXN nelle modalità previste al § 8.

[R.23] 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.24] 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.25] La componente DNS Internet deve annunciare le zone di propria competenza sulla sola rete Internet.

[R.26] 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.27] 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.28] Il Fornitore deve garantire altresì la gestione dei change dei nomi a dominio su richiesta dell'Amministrazione.

[R.29] 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.30] Il sistema DNS deve implementare meccanismi di cache per la risoluzione dei nomi, e meccanismi di forwarding selettivo su base dominio.

[R.31] Il piano di indirizzamento adottato nell'ambito del SPC deve garantire l'univocità degli indirizzi IPv4 e/o IPv6 attribuiti ai singoli sistemi che, connessi tramite QXN, scambieranno traffico tra loro.

[R.32] 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 SPC.

[R.33] 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 SPC wired e wireless secondo quanto indicato nella tabella successiva.

Numero di 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

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

3.1. SERVIZI DI TRASPORTO DATI WIRED

[R.34] I servizi di trasporto di tipo wired sono caratterizzati da collegamenti fisici permanenti tra le sedi delle Amministrazioni e la rete del Fornitore.

[R.35] I servizi di traporto di tipo wired richiesti al Fornitore sono di due tipi:

- **Servizi di Trasporto Dati su Portante Elettrica (STDE)**: di tipo always-on, in cui il rilegamento fisico utilizzato per il circuito di accesso è costituito da uno o più doppini in rame. E' ammessa la realizzazione dei medesimi servizi anche tramite collegamenti in fibra ottica.
- **Servizi di Trasporto Dati su Portante Ottica (STDO)**: di tipo always-on, in cui il rilegamento fisico utilizzato per il circuito di accesso è realizzato in fibra ottica.

[R.36] Per ciascun servizio, il Fornitore deve mettere a disposizione dell'Amministrazione uno o più apparati di accesso, con 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).

[R.37] La capacità totale delle interfacce lato utente non può essere inferiore alla BNA contrattualizzata sull'accesso (in caso di accesso asimmetrico della maggiore tra BNAU e BNAD).

[R.38] Gli apparati di accesso forniti con i servizi devono garantire una capacità di commutazione in termini di pacchetti al secondo (CCP) pari a quella indicata per ciascun profilo di servizio secondo quanto riportato in [R.41] per STDE e in [R.49] per STDO.

[R.39] Sul medesimo apparato di accesso fornito con i servizi di trasporto dati wired, su richiesta dell'Amministrazione, possono essere configurati uno o più ambiti.

[R.40] Sui servizi di trasporto dati wired, oltre l'ambito Intranet, incluso di default e disattivabile su richiesta, è prevista un'**opzione Multiambito** che permette l'abilitazione del traffico dati sugli ambiti Infranet ed Internet. Ognuno degli

ambiti, su richiesta dell'Amministrazione, deve poter essere disabilitato separatamente, tenuto conto del requisito [R.15].

3.1.1. Servizi di Trasporto Dati su Portante Elettrica (STDE)

[R.41] I servizi STDE prevedono la fornitura di servizi di trasporto dati su protocollo IP (IPv4 e/o IPv6) con le caratteristiche indicate nella seguente tabella:

Profilo	BNA Down/Uplink		BGA		CCP (Kpps)
STDE-A1	640/128	Kbps	64	Kbps	-
STDE-A2	1024/128	Kbps	64	Kbps	-
STDE-A3	1024/256	Kbps	128	Kbps	-
STDE-A4	2048/256	Kbps	128	Kbps	-
STDE-A5	2048/512	Kbps	256	Kbps	-
STDE-A6	4096/512	Kbps	256	Kbps	-
STDE-A7	10240/1024	Kbps	512	Kbps	1
STDE-A8	20480/1024	Kbps	512	Kbps	1
STDE-A9	30/3	Mbps	512	Kbps	1
STDE-A10	30/3	Mbps	1.024	Kbps	8
STDE-S1	2048/2048	Kbps	256	Kbps	0,5
STDE-S2	2048/2048	Kbps	384	Kbps	0,75
STDE-S3	2048/2048	Kbps	512	Kbps	1
STDE-S4	2048/2048	Kbps	1024	Kbps	2
STDE-S5	4096/4096	Kbps	2048	Kbps	4

STDE-S6	8192/8192	Kbps	4096	Kbps	8

[R.42] Il servizio STDE prevede accessi:

- asimmetrici (profili da STDE-A1 a STDE-A10), caratterizzati cioè da BNAU<BNAD;
- simmetrici (profili da STDE-S1 a STDE-S6), caratterizzati cioè da BNA=BNAU=BNAD.

[R.43] I servizi di trasporto di tipo STDE

- asimmetrici a bassa velocità (profili da STDE-A1 a STDE-A8), devono essere erogati con copertura geografica almeno coincidente con quella del servizio Wholesale Bitstream ADSL dell'operatore notificato per servizi con identica BNA, aggiornando la disponibilità dei servizi nel caso in cui l'offerta Wholesale Bitstream venga estesa durante la durata del contratto. Nel caso in cui, durante la durata del contratto AGCOM non ritenesse giustificata un'offerta Wholesale Bitstream in aree servite attraverso l'offerta di accesso disaggregato alla rete in rame (ULL), l'obbligo di fornitura includerà anche le aree coperte solo dalla succitata offerta di accesso disaggregato;
- asimmetrici ad alta velocità (profili da STDE-A9 a STDE-A10), devono essere erogati con copertura geografica almeno coincidente con quella del servizio Wholesale Bitstream NGA in modalità FTTCab dell'operatore notificato;
- simmetrici (profili da STDE-S1 a STDE-S6), devono essere erogati con copertura geografica almeno coincidente con quella del servizio Wholesale Bitstream SHDSL dell'operatore notificato per servizi con identica BNA, aggiornando la disponibilità dei servizi nel caso in cui l'offerta Wholesale Bitstream venga estesa durante la durata del contratto. Nel caso in cui, durante la durata del contratto AGCOM non ritenesse giustificata un'offerta Wholesale Bitstream in aree servite attraverso l'offerta di accesso disaggregato alla rete in rame (ULL), l'obbligo di

fornitura includerà anche le aree coperte solo dalla succitata offerta di accesso disaggregato.

3.1.1.1. Opzioni dei servizi STDE

[R.44] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDE:

- **Affidabilità elevata** (cfr. [R.45]);
- **Multiambito Internet / Infranet** (cfr. [R.40]);
- **Estensione apparato Wi-Fi** (cfr. [R.46]);
- **Backup tramite rete ISDN o radiomobile** (cfr. § 3.1.4);
- **Finestra di erogazione estesa** (cfr. [R.6]).
- **Servizi di Banda Riservata (SBRI)** (cfr. § 3.1.3);
- Inoltre ai soli servizi STDE si può associare il servizio di sicurezza centralizzata (cfr. [R.153])

[R.45] L'opzione **Affidabilità elevata** prevede che il servizio sia realizzato ridondando completamente la soluzione tecnologica caratterizzante il servizio base in modo da garantire, in caso di guasto singolo, funzionalità e prestazioni equivalenti. La soluzione consiste in un accesso secondario equivalente all'accesso primario (quello incluso con il servizio base di cui al [R.20] con i profili di cui al [R.41]) con realizzazione del collegamento tale da minimizzare i singoli punti di guasto. Sugli apparati di accesso, devono essere implementati meccanismi di tipo active-standby, pertanto solo in caso di indisponibilità dell'accesso primario, il traffico è instradato sull'accesso secondario. L'opzione 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. Gli SLA del servizio per quanto riguarda i parametri di assurance sono differenziati rispetto al servizio base (cfr. Allegato 5 bis).

[R.46] L'**opzione Estensione apparato Wi-Fi** prevede l'attivazione di una funzionalità di accesso senza fili in ambito privato (indoor). La funzionalità deve essere attivata su un apparato di accesso del servizio di trasporto co-

locato presso la sede dell'Amministrazione e deve supportare almeno i seguenti standard:

- IEEE 802.11b/g/n;
- IEEE 802.11i (WPA2).

3.1.1.2. Precondizioni e vincoli per la sottoscrizione dei servizi STDE

[R.47] L'opzione **Multiambito** richiede obbligatoriamente garanzie di sicurezza, pertanto per l'attivazione di tale opzione deve essere assicurata, sull'accesso per il quale viene richiesta, almeno una delle seguenti condizioni:

- sottoscrizione dell'opzione "sicurezza centralizzata" dei Servizi di Trasporto STDE (di cui al § 3.1.1);
- sottoscrizione di almeno un Servizio di Sicurezza Perimetrale Unificata (di cui al § 4.1.1);
- implementazione di sistemi di sicurezza propri in grado di garantire almeno le seguenti funzionalità di sicurezza:
  - firewalling;
  - intrusion detection;
  - monitoraggio e registrazione degli eventi di sicurezza.

[R.48] In quest'ultimo caso il Fornitore contestualmente alla richiesta dell'Amministrazione deve far compilare alla medesima un documento di dichiarazione che attesti detta implementazione da parte dell'Amministrazione.

3.1.2. Servizi di Trasporto Dati su Portante Ottica (STDO)

[R.49] Il servizio di trasporto di tipo STDO prevede la fornitura di servizi di trasporto dati su protocollo IP (IPv4 e/o IPv6) con le caratteristiche indicate nella seguente tabella:

Profilo	BNA	BGA	CCP (Kpps)

STDO-1	10	Mbps	10	Mbps	15
STDO-2	20	Mbps	20	Mbps	30
STDO-3	40	Mbps	40	Mbps	60
STDO-4	100	Mbps	100	Mbps	150
STDO-5	200	Mbps	200	Mbps	300
STDO-6	300	Mbps	300	Mbps	450
STDO-7	600	Mbps	600	Mbps	900
STDO-8	1	Gbps	1	Gbps	1500
STDO-9	2,5	Gbps	2,5	Gbps	3000
STDO-10	5	Gbps	5	Gbps	5000
STDO-11	10	Gbps	10	Gbps	6000

[R.50] Il servizio di trasporto di tipo STDO prevede accessi simmetrici, caratterizzati cioè da BGA=BGAU=BGAD.

[R.51] I servizi di trasporto di tipo STDO:

- con BNA da 10 Mbps fino a 100 Mbps (profili da STDO-1 a STDO-4) devono essere erogati almeno all'interno dei comuni capoluogo di regione, inclusi i comuni sede di provincia autonoma di Trento e Bolzano, e in tutti i punti del territorio in cui è disponibile l'offerta Wholesale Bitstream NGA in modalità FTTH dell'operatore notificato;
- con BNA superiore a 100 Mbps (profili da STDO-5 a STDO-11) devono essere erogati almeno all'interno dei comuni di Roma e Milano.

3.1.2.1. Opzioni dei servizi STDO

[R.52] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDO:

- **Affidabilità elevata** (cfr.[R.53]);
- **Multiambito** (cfr.[R.40]);
- **Backup tramite rete ISDN o radiomobile** (cfr. § 3.1.4);
- **Finestra di erogazione estesa** (cfr. [R.6]).
- **Servizi di Banda Riservata (SBRI)** (cfr. § 3.1.3);

[R.53] L'opzione **Affidabilità elevata** prevede che il servizio sia realizzato ridondando completamente la soluzione tecnologica caratterizzante il servizio base in modo da garantire, in caso di guasto singolo, funzionalità e prestazioni equivalenti. La soluzione consiste in un accesso secondario equivalente all'accesso primario (quello incluso con il servizio base di cui al [R.20] e i profili di cui al [R.49]), ma con instradamento fisico differente, in modo da minimizzare i singoli punti di guasto. L'opzione affidabilità elevata per i servizi STDO prevede il **load balancing**, consistente nell'implementazione di politiche di bilanciamento di carico fra i due distinti apparati di accesso contrattualizzati con l'adesione all'opzione. La soluzione deve essere comprensiva degli ulteriori apparati necessari all'implementazione delle politiche di load balancing non già previsti dalla soluzione base. L'opzione deve garantire nella centrale del Fornitore l'attestazione dei circuiti di accesso su apparati differenti o laddove disponibile, per accessi con BNA ≥ 100 Mbps, **il dual-homing** (attestazione dei circuiti di accesso su PoP distinti del Fornitore). Entrambe le componenti del servizio devono essere monitorate e gestite. Gli SLA del servizio per quanto riguarda i parametri di assurance sono differenziati rispetto al servizio base (cfr. Allegato 5 bis).

3.1.2.2. Precondizioni e vincoli per la sottoscrizione dei servizi STDO

[R.54] L'opzione **Multiambito** richiede obbligatoriamente garanzie di sicurezza, pertanto per l'attivazione di tale opzione deve essere assicurata,

sull'accesso per il quale viene richiesta, almeno una delle seguenti condizioni:

- sottoscrizione di almeno un Servizio di Sicurezza Perimetrale Unificata (di cui al § 4.1.1);
- implementazione di sistemi di sicurezza propri in grado di garantire almeno le seguenti funzionalità di sicurezza:
  - firewalling;
  - intrusion detection;
  - monitoraggio e registrazione degli eventi di sicurezza.
- In quest'ultimo caso il Fornitore contestualmente alla richiesta dell'Amministrazione deve far compilare alla medesima un documento di dichiarazione che attesti detta implementazione da parte dell'Amministrazione.

3.1.3. Opzione dei servizi STDE e STDO: Servizio di Banda Riservata (SBRI)

[R.55] La componente opzionale **Servizio di Banda Riservata (SBRI)**, garantisce parametri qualitativi differenziati a seconda della tipologia di traffico in transito su un servizio di trasporto dati wired. I parametri qualitativi di cui è garantito il rispetto sono i seguenti:

- *Round Trip Delay (RTD)*: tempo di percorrenza necessario ad un pacchetto per percorrere la tratta origine-destinazione-origine;
- *Packet Loss (PL)*: tasso di perdita dei pacchetti, rapporto espresso in percentuale tra il numero di pacchetti non consegnati e numero di pacchetti trasmessi in una tratta origine-destinazione;
- *Packet Delay Variation (PDV)*: variazione in valore assoluto del ritardo tra due pacchetti consecutivi.
- La componente opzionale SBRI prevede 5 profili definiti nella seguente tabella. I profili SBRI-1, SBRI-2, SBRI-3 e SBRI-4, fanno riferimento a modalità di trasmissione di tipo Unicast, mentre il

profilo SBRI-5 fa riferimento a modalità di trasmissione di tipo Multicast:

Profilo	Classe di Servizio
SBRI-1	Real Time
SBRI-2	Mission Critical
SBRI-3	Streaming
SBRI-4	Multimedia
SBRI-5	Multicast

[R.56] La componente opzionale SBRI è sottoscrivibile unicamente per i servizi STDE ed STDO.

[R.57] In funzione delle applicazioni trasportate, sono definite le seguenti Classi di Servizio (CdS) con i corrispondenti valori minimi accettabili per ciascuna caratteristica di qualità:

CdS	RTD	PL	JI
Real Time (RT)	< 65 ms	< 0,1%	<10 ms
Mission Critical (MC)	< 100 ms	< 0,1%	-
Streaming (ST)	< 400 ms	< 0,5%	<250 ms
Multimedia (MM)	< 500 ms	< 5%	-
Multicast	-	< 0,5%	-

[R.58] La componente opzionale SBRI, deve essere in grado di assegnare una delle cinque possibili classi di servizio a ciascun pacchetto in transito (esclusi i pacchetti relativi all'ambito Internet e quelli di tipo best effort), secondo politiche basate su:

- indirizzo IP di origine;

- indirizzo IP di destinazione;
- protocollo applicativo utilizzato;
- una combinazione delle precedenti.

[R.59] La somma delle componenti SBRI associate ad un servizio non può eccedere la BGA propria dello specifico servizio, cioè:

$$\sum_{i=1}^{5} SBRIi \leq BGA$$

[R.60] La componente SBRI di tipo Real Time contrattualizzabile non può essere superiore al 35% della BGA (in blocchi di 64 Kbps). Pertanto, per quanto riguarda il trasporto del traffico Real Time di cui alla componente SBRI:

- per profili asimmetrici STDE da A1 a A4 non è possibile contrattualizzare la componente SBRI di banda riservata Real Time;
- per i profili STDE A5, A6 e A9 è possibile contrattualizzare una sola componente SBRI di banda riservata Real Time composta da un unico blocco da 64 Kbps;
- per gli altri servizi STDE e per tutti i servizi STDO è possibile contrattualizzare più di una componente SBRI e più blocchi di banda riservata Real Time fino al 35% della BGA.

[R.61] L'apparato d'accesso fornito con i servizi di trasporto dati per i quali è stata sottoscritta la componente opzionale SBRI1, deve essere in grado di gestire il traffico attraverso un meccanismo di accodamento prioritario che, in caso di saturazione della banda associata alla suddetta componente, deve prevedere lo scarto dei pacchetti in eccesso; il traffico delle componenti SBRI-2, SBRI-3 e SBRI-4, deve essere gestito equamente, e in caso di saturazione delle bande associate alle suddette componenti, essere declassato a traffico Best Effort.

[R.62] Le componenti SBRI che prevedono una modalità di trasmissione di tipo Multicast possono essere utilizzate dalle Amministrazioni che hanno necessità di inviare flussi di informazione da una o più sorgenti verso un gruppo di più riceventi, per il solo ambito Intranet.

[R.63] L'architettura del servizio utilizzata dal fornitore dovrà essere in grado di supportare il multicast secondo gli standard Protocol Indipendent Multicast –

Sparse Mode (PIM SM) e IGMP (Internet Group Management Protocol) almeno versioni v2 e v3. Nel caso di utilizzo del protocollo IPv6 il fornitore dovrà utilizzare il protocollo Multicast Listener Discovery (MLD) v1 e v2 descritto nelle RFC 3810 e 4604.

[R.64] Il fornitore dovrà realizzare un servizio di multicast all'interno della propria rete in grado di trasferire informazioni da sorgenti di flussi multicast di proprietà dell'Amministrazione a più destinatari posti sull'intranet dell'Amministrazione.

[R.65] Il fornitore dovrà gestire l'indirizzamento multicast IPv4 e/o IPv6 della rete necessario per fornire il servizio alle Amministrazioni.

3.1.3.1. Precondizioni e vincoli per la sottoscrizione dell'opzione SBRI

[R.66] L'opzione SBRI può essere attivata solo in relazione ad un accesso di tipo STDE o STDO.

3.1.4. Servizi accessori dei servizi STDE e STDO: Backup tramite ISDN o radiomobile

[R.67] Il servizio accessorio di **Backup tramite ISDN o radiomobile** offre una funzionalità di ridondanza basata su tecnologia differente rispetto a quella caratterizzante il servizio base. Il servizio accessorio prevede l'utilizzo di due possibili tecnologie:

- *backup ISDN*: il servizio di backup è implementato tramite un accesso BRI (2 canali a 64 kbps) per ciascun singolo servizio di accesso STDE/STDO contrattualizzato. Il servizio si intende comprensivo di tutte le dotazioni tecnologiche necessarie alla soluzione, dei canoni e dell'eventuale traffico associati alla linea ISDN;
- *backup Radiomobile*: il servizio di backup è implementato tramite apparati che consentono il trasporto di dati su rete radiomobile. Il servizio prevede la fornitura e l'utilizzo di SIM (Subscriber Identification Module) in grado di gestire traffico EDGE/UMTS/HSDPA/LTE (o evoluzioni). Il servizio si intende comprensivo di tutte le dotazioni tecnologiche necessarie alla soluzione, dei canoni e dell'eventuale traffico associati alla SIM radiomobile.

[R.68] Il servizio accessorio **Backup tramite ISDN o radiomobile** prevede attività di monitoraggio e gestione tali da rilevare eventuali malfunzionamenti anche in condizioni di normale operatività dell'accesso primario ed è comprensiva di tutte le funzionalità/apparati necessari al re-indirizzamento del traffico sul link di backup in caso di indisponibilità del collegamento primario o, nel caso di servizi in alta affidabilità, in condizioni di indisponibilità sia del collegamento primario che del secondario. Il servizio accessorio deve prevedere anche tutte le funzionalità necessarie al re-indirizzamento del traffico sul link primario non appena questo venga correttamente ripristinato. Considerando che il collegamento di backup deve essere inattivo in caso di disponibilità del servizio primario, il servizio accessorio non prevede l'implementazione di politiche di load balancing.

[R.69] Il PAS del servizio accessorio **Backup tramite ISDN o radiomobile** coincide con il PAS del servizio STDE o STDO associato.

3.1.4.1. Opzioni del servizio accessorio Backup tramite ISDN o radiomobile

[R.70] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio accessorio Backup tramite ISDN o radiomobile:

- **Finestra di erogazione estesa** (cfr. [R.6]), col vincolo che la finestra di erogazione del servizio accessorio Backup tramite ISDN o radiomobile coincida con quella del servizio STDE o STDO associato.

3.1.4.2. Precondizioni e vincoli per la sottoscrizione del servizio accessorio Backup tramite ISDN o radiomobile

[R.71] I servizi accessori Backup tramite ISDN o radiomobile possono essere acquistati esclusivamente in abbinamento ad un accesso di tipo STDE o STDO.

3.2. SERVIZI DI TRASPORTO DATI WIRELESS

[R.72] I servizi di trasporto di tipo wireless sono caratterizzati da collegamenti radio tra sedi delle Amministrazioni e la rete del Fornitore.

[R.73] I servizi di trasporto di tipo wireless che devono essere erogati dal Fornitore sono:

- **Servizi di Trasporto Dati Satellitari (STDS)**: di tipo always-on, consentono il collegamento alla sola rete dell'Amministrazione attraverso un canale satellitare.

3.2.1. Servizi di Trasporto Dati Satellitare (STDS)

[R.74] I servizi STDS prevedono la fornitura di servizi di trasporto dati su protocollo IP attraverso collegamenti satellitari bidirezionali costituiti da profili asimmetrici, con le caratteristiche BNA in Downlink e in Uplink indicate nella seguente tabella:

Profilo	BNA (Down/Uplink)	
STDS-1	6 Mbpsec	1 Mbpsec
STDS-2	8 Mbpsec	2 Mbpsec
STDS-3	10 Mbpsec	4 Mbpsec

[R.75] I servizi di trasporto di tipo STDS erogati in tecnologia satellitare sono comprensivi:

- del collegamento fra il satellite e l'Amministrazione;
- del collegamento fra il satellite e la rete del Fornitore;
- delle parabole e dei cablaggi necessari per la fruizione del servizio fino ad un massimo di 50 metri (l'Amministrazione richiedente deve rendere disponibile, per ciascuna sede su cui è

richiesto il servizio, appositi spazi per l'installazione delle parabole che assicurino la visibilità del satellite ed eventuali autorizzazioni necessarie per i cablaggi);

- dell'apparato di attestazione in sede dell'Amministrazione;
- dell'abilitazione all'ambito Intranet;
- della componente di traffico in modalità Best Effort, con throughput fino all'intero valore di BNA definito per il singolo accesso e per un volume di traffico incluso nel canone mensile pari a quanto indicato in [R.82] in termini di GByte/mese.

[R.76] L'apparato di attestazione deve essere in grado di interfacciarsi con la LAN o singoli PC almeno attraverso interfacce Fast Ethernet (10/100 Autosensing).

[R.77] I servizi STDS non sono caratterizzati da alcuna limitazione in termini di copertura geografica sul territorio nazionale.

[R.78] Per i servizi STDS non è previsto il Servizio di Banda Riservata (SBRI) e l'intera banda viene pertanto trattata esclusivamente in modalità Best Effort. Pacchetti appartenenti a diverse CdS devono comunque essere trasportati ma a questi non sono applicati degli SLA prestazionali differenziati.

[R.79] I servizi STDS prevedono l'abilitazione al solo ambito Intranet.

[R.80] Il Fornitore deve installare nella singola sede dell'Amministrazione sistemi trasmissivi che garantiscano una velocità almeno pari alla BNA definita per ciascun profilo in Upload (trasmissione) e in Download (ricezione).

[R.81] Il Fornitore deve garantire che, almeno in alcuni momenti, sia possibile l'utilizzo dell'intera BNA.

[R.82] Al fine di considerare il servizio disponibile, la banda messa a disposizione per ogni singolo accesso non deve essere mai inferiore a 16 Kbps. Il Fornitore può adottare politiche di limitazione della banda di tipo "Fair Access Policy", in funzione della soglia di traffico (in trasmissione o ricezione) oraria, settimanale e mensile raggiunta.

- Al superamento di una soglia di traffico in trasmissione e ricezione su base oraria la banda disponibile può essere ridotta al valore di banda limite $BL_{oraria.}$ L'intera disponibilità della BNA

deve essere ripristinata al termine del periodo orario di riferimento.

- Al superamento di una soglia di traffico in trasmissione e ricezione su base settimanale la banda disponibile può essere ridotta al valore $BL_{settimanale}$. L'intera disponibilità della BNA deve essere ripristinata al termine del periodo settimanale di riferimento.
- Al superamento di una soglia di traffico in trasmissione e ricezione su base mensile la banda disponibile può essere ridotta al valore $BL_{mensile}$. L'intera disponibilità della BNA deve essere ripristinata al termine del periodo mensile di riferimento.

[R.83] Per ciascuna tipologia di profilo i valori di riferimento per le soglie e le BL sono indicate in tabella:

Profilo	BNA		Soglia traffico oraria in GByte/ora	BL_{oraria}		Soglia traffico settimanale in GByte/settimana	$BL_{settimanale}$		Soglia traffico mensile in GByte/mese	$BL_{mensile}$	
	(Down/Uplink in Mbps)			(Down/Uplink in Kbps)			(Down/Uplink in Kbps)			(Down/Uplink in Kbps)	
STDS-1	6	1	0,5	1024	256	2	256	64	4	16	16
STDS-2	8	2	1	248	512	4	256	64	8	16	16
STDS-3	10	4	-	no	no	-	no	no	40	16	16

[R.84] Il Fornitore ha la possibilità, previa autorizzazione dell'Amministrazione, di limitare o bloccare alcune tipologie di traffico anomalo non collegate ad applicazioni di interesse dell'Amministrazione stessa.

3.2.1.1. Opzioni dei servizi STDS

[R.85] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDS:

- **Estensione apparato Wi-Fi** (cfr. [R.86]);

- **Finestra di erogazione estesa** (cfr. [R.6]).

[R.86] L'opzione **Estensione apparato Wi-Fi**, prevede l'attivazione di una funzionalità di accesso senza fili in ambito privato (indoor). La funzionalità deve essere attivata su un apparato di accesso del servizio di trasporto co-locato presso la sede dell'Amministrazione e deve supportare almeno i seguenti standard:

- interfaccia Wi-Fi 802.11b/g/n con autenticazione IEEE 802.11i (WPA2).

4. SERVIZI DI SICUREZZA

Il Fornitore deve erogare i Servizi di Sicurezza descritti dal presente capitolato in modo da:

- proteggere il sistema informativo e la relativa infrastruttura tecnologica sotto il dominio amministrativo delle Amministrazioni;
- proteggere le infrastrutture telematiche interconnesse con tali servizi.

I servizi di sicurezza richiesti dal presente capitolato si caratterizzano come servizi di sicurezza perimetrale, volti a fornire prestazioni per il controllo di sicurezza del traffico relativo agli accessi SPC e alle reti della PA ad esso collegate. Tali servizi si articolano in:

- Servizi di sicurezza perimetrale unificata (SPUN) cfr. § 4.1.1;
- Servizi di sicurezza Centralizzata (SCEN) cfr. § [R.153];

[R.87] Le soluzioni e i servizi proposti dal Fornitore devono essere:

- aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato;
- conformi alle normative e agli standard di riferimento applicabili;
- adeguati in modo continuativo alle normative che la Comunità Europea o l'Italia rilasceranno in merito a servizi analoghi a quelli descritti nel presente Documento senza oneri aggiuntivi per le Amministrazioni.

[R.88] I servizi descritti nel presente capitolato si intendono comprensivi di tutte le componenti HW e SW necessarie ai fini dell'erogazione degli stessi.

[R.89] Il Fornitore deve erogare i servizi di sicurezza utilizzando apparati che si raccordino con i sistemi dell'Amministrazione attraverso interfacce conformi agli standard IEEE Fast-Ethernet 10/100 Autosensing, Gigabit-Ethernet o 10 Gigabit Ethernet. È facoltà dell'Amministrazione scegliere fra le interfacce indicate sopra.

[R.90] Il Fornitore ha la completa responsabilità della configurazione, gestione, monitoraggio e manutenzione delle componenti che realizzano i servizi di sicurezza perimetrale. L'Amministrazione ha comunque la responsabilità di esprimere al Fornitore tutti i requisiti necessari per la corretta installazione e configurazione dei servizi e fornire tutte le informazioni di propria competenza.

[R.91] Tutti i servizi di sicurezza devono essere erogati dal Fornitore in modalità di "outsourcing completo", mediante l'attivazione di un Centro di Gestione per la Sicurezza (SOC – Security Operating Center), non necessariamente dedicato ai servizi SPC, che ha il compito di gestire le risorse utilizzate per erogare i servizi di sicurezza.

[R.92] Gli apparati collocati presso sedi delle Amministrazioni ed utilizzati per erogare i servizi di sicurezza perimetrale devono essere dotati di funzionalità di gestione remota tramite protocolli cifrati.

[R.93] Tutti i dispositivi utilizzati per l'erogazione dei servizi di sicurezza devono implementare meccanismi di Identificazione, Autenticazione, Autorizzazione e Accounting (IAAA) attraverso i quali sia possibile l'accesso logico da console e da remoto per attività di gestione e/o di Amministrazione.

[R.94] 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).

Il Fornitore può proporre in alternativa un diverso schema di autenticazione, che deve essere approvato in fase di collaudo del servizio, purché la comunicazione tra la stazione di gestione e l'apparato gestito sia protetta dall'uso di un adeguato algoritmo crittografico.

[R.95] I sistemi adottati devono rilevare e registrare i tentativi di accesso non autorizzato al sistema stesso.

[R.96] 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.97] I dati registrati dal sistema di sicurezza devono essere disponibili per l'uso da parte degli utenti abilitati.

[R.98] I file di log devono essere protetti da modifiche o cancellazioni non autorizzate, in conformità alla normativa vigente.

[R.99] I dispositivi utilizzati devono garantire la piena compatibilità IPv6 e il supporto di base dual stack Firewall (IPv4 e IPv6) e dei protocolli IPv4 e IPv6 subordinati.

[R.100] I sistemi adottati devono essere in grado di risolvere problematiche di NAT/Firewall traversal per i protocolli VoIP.

4.1. SERVIZI DI SICUREZZA PERIMETRALE

4.1.1. Servizio di Sicurezza Perimetrale Unificata (SPUN)

[R.101] Il servizio di Sicurezza Perimetrale Unificata deve prevedere elementi architetturali atti a implementare le seguenti funzionalità di base:

- Firewall;
- VPN IPsec Site-to-Site;
- Intrusion Detection & Prevention System (IDS/IPS).

[R.102] I servizi SPUN sono disponibili in sei distinte modalità di erogazione del servizio (differenti profili di servizio contrattualizzabili dall'Amministrazione). Tali profili si differenziano in base a:

- **coppia di parametri Firewall e IPS Throughput:** rappresentano il throughput minimo che deve essere rispettivamente gestito dalle due prestazioni del servizio;
- **massimo numero di Tunnel VPN IPsec S2S simultanei:** rappresenta il numero massimo di tunnel VPN IPsec Site-to-Site simultanei che l'apparato di sicurezza è in grado di gestire;
- **numero di operazioni (per anno solare) di modifiche/aggiornamento policy/regole di sicurezza soggette a SLA** (cfr. [R.104]).

[R.103] I diversi profili previsti per il servizio SPUN sono caratterizzati dai requisiti riportati nella presente tabella:

Profilo	Firewall Throughput (Mbps)	IPS Throughput (Mbps)	Tunnel VPN IPsec S2S simultanei	Change management (interventi annuali)
SPUN-1	100	40	10	20
SPUN-2	200	100	20	25
SPUN-3	450	200	50	30
SPUN-4	1500	650	100	35

SPUN-5	4000	2000	500	40
SPUN-6	20000	8000	1000	45

[R.104] Il Fornitore, quando è chiamato a modificare e/o aggiornare le politiche di sicurezza (operazioni di Change Management) sulla base di esigenze espresse dall'Amministrazione, è tenuto a eseguire le richieste pervenute per un numero illimitato di volte. Tuttavia:

- sono soggette a SLA solo le operazioni che rientrano nel limite fissato dallo specifico profilo associato al servizio SPUN (cfr.[R.102] e [R.103]);
- oltre tale limite, le operazioni non saranno più soggette a SLA ma devono essere garantite dal Fornitore e gestite in modalità Best Effort.

[R.105] Le funzionalità del servizio base indicate in [R.101], e le eventuali funzionalità opzionali acquistate dalle Amministrazioni (cfr. 4.1.1.4 e specificamente [R.130]), devono essere erogate attraverso l'utilizzo di un unico dispositivo HW, configurato in modo tale da rispettare le caratteristiche tecniche e prestazionali descritte nel presente Capitolato ed i livelli di servizio definiti nell'Allegato 5 bis.

[R.106] Gli apparati devono essere dotati di almeno n° 3 interfacce di tipo Fast-Ethernet 10/100 Autosensing, Gigabit-Ethernet o 10 Gigabit Ethernet. Per ciascun servizio SPUN la somma della capacità delle interfacce non deve essere inferiore al Firewall Throughput indicato nella tabella del [R.103] per lo SPUN corrispondente.

[R.107] Alcune delle funzionalità offerte dal servizio di sicurezza si basano su "*signature*", che devono essere aggiornate entro, e non oltre, 1 giorno dal momento in cui sono rese disponibili dal vendor che fornisce i sistemi utilizzati dal Fornitore per l'erogazione del servizio di sicurezza.

[R.108] Il Punto di accesso al servizio (PAS) per i servizi SPUN è definito come l'insieme delle interfacce messe a disposizione sul dispositivo HW di cui al [R.105].

4.1.1.1. Funzionalità SPUN: Firewall

[R.109] Il servizio deve essere dotato di una funzionalità di firewalling che permetta di analizzare il traffico, bloccando i pacchetti di rete che appartengono a collegamenti non autorizzati tramite funzionalità "stateful inspection", secondo le regole configurate dal Fornitore sulla base delle esigenze espresse dall'Amministrazione.

[R.110] Il sistema di firewalling su cui è basato il servizio deve supportare tutti i protocolli specificati nello standard TCP/IP.

[R.111] La funzionalità di firewalling deve implementare le seguenti caratteristiche di base:

- filtraggio di traffico IP che consente di proteggere una rete IP da accessi indesiderati bloccando indirizzi, porte o protocolli;
- auditing e logging che consente l'analisi del traffico che attraversa il firewall;
- modulo di ispezione che effettua l'ispezione dei datagrammi IP e realizza il filtraggio sulla base delle regole implementate. Deve essere implementata almeno la metodologia "stateful inspection" escludendo l'impiego di dispositivi di firewalling di tipo Packet Filtering Stateless;
- modulo di gestione che consente di configurare e monitorare il comportamento del sistema firewall;
- meccanismi antispoofing;
- meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service;
- Network Address Translation (NAT) secondo la specifica RFC 3022, sia di tipo statico (uno a uno), sia di tipo dinamico (n a uno) e Port Address Translation (PAT);
- URL filtering che consente solo a determinate postazioni di abilitare la navigazione Web attraverso il firewall, di controllare le statistiche sulla navigazione e di bloccare l'accesso a particolari siti Internet/Intranet.

4.1.1.2. Funzionalità SPUN: VPN IPsec Site to Site

[R.112] 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).

[R.113] La funzionalità di VPN IPsec Site to Site deve implementare le seguenti caratteristiche:

- 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.

[R.114] Il servizio deve prevedere il supporto per IPsec "Tunnel mode" e "Transport mode" come definiti nella specifica pubblica RFC 4301.

[R.115] Nell'implementazione e nella gestione delle reti private virtuali, il Fornitore deve erogare il servizio secondo una delle seguenti modalità:

- **Autonoma**: il Fornitore deve provvedere alla realizzazione e gestione di entrambe le terminazioni dei tunnel che realizzano la VPN dell'Amministrazione;
- **Cooperativa**: il Fornitore deve interagire con altri Fornitori per la realizzazione e gestione dei tunnel che realizzano la VPN. Quest'ultimo caso si riferisce a tutti quegli scenari secondo i quali il dispositivo che realizza un'estremità di un tunnel risulta sotto il dominio amministrativo di un Fornitore diverso da quello che amministra l'altra estremità;
- **Predefinita**: ai fini di semplificare la gestione cooperativa nei casi in cui differenze tecnologiche e gestionali tra Fornitori diversi non garantiscano una completa interoperabilità, è

possibile che la scelta del Fornitore sia dettata dall'Amministrazione che eroga i servizi applicativi. Le altre Amministrazioni, per poter usufruire dei servizi su VPN IPsec, devono richiedere tale servizio allo stesso Fornitore. È pertanto responsabilità del Fornitore la progettazione e la fornitura del servizio.

[R.116] Il Fornitore è completamente responsabile dell'erogazione dei servizi in modalità autonoma o predefinita, mentre il servizio, erogato in modalità cooperativa, richiede l'implementazione e la gestione dell'estremità dei tunnel sotto il dominio amministrativo del Fornitore, oltre a tutte le attività necessarie per attivare il tunnel con Fornitori terzi che gestiscono l'altra estremità. La modalità cooperativa richiede che il Fornitore impieghi sistemi interoperabili con terminazioni di tunnel diverse, gestite da Fornitori terzi.

[R.117] 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/IES 9594-8 (X.509v3).

[R.118] In particolare, l'impiego dei certificati digitali è obbligatorio qualora il servizio sia erogato in modalità cooperativa.

[R.119] Il Fornitore si impegna ad erogare il servizio VPN IPsec utilizzando certificati digitali X.509v3 emessi esclusivamente da una Certification Authority di rete situata sul territorio italiano.

[R.120] Il formato per le richieste dei certificati deve essere conforme allo standard PKCS#10.

[R.121] Il servizio deve prevedere l'adozione di adeguati meccanismi di protezione della chiave privata e delle chiavi di sessione memorizzate nei dispositivi utilizzati.

[R.122] Prima dell'apertura di un nuovo tunnel crittografico, deve essere verificato lo stato di validità del certificato con l'ausilio delle Certification Revocation List (CRL) o, in alternativa e preferibilmente, direttamente online con il supporto del protocollo OCSP.

4.1.1.3. Funzionalità SPUN: Intrusion Detection & Prevention System (IDS/IPS)

[R.123] Il servizio prevede la funzionalità di rilevamento e prevenzione delle intrusioni che consenta di identificare (IDS) e, laddove possibile, interrompere (IPS) azioni aventi come obiettivo la violazione o la compromissione del funzionamento di un sistema, di un apparato o di una rete.

[R.124] Per il riconoscimento dei potenziali attacchi, il servizio erogato dal Fornitore deve utilizzare informazioni presenti in una banca dati centrale costantemente aggiornata e compatibile con le Common Vulnerabilities and Exposures (CVE-compatible).

[R.125] Il sistema deve prevedere una raccolta e conservazione delle tracce tipiche di un determinato attacco, allo scopo di favorire l'individuazione degli autori dell'attacco.

[R.126] Il sistema deve prevedere meccanismi di notifica a fronte dell'identificazione di un evento di attacco.

[R.127] Il servizio di Intrusion Detection & Prevention deve prevedere almeno le seguenti tecniche di rilevazione degli attacchi:

- Anomalia di traffico/protocollo: analisi dei flussi di traffico ed individuazione di anomalie nei protocolli comunemente utilizzati nell'ambito delle reti IP;
- "*Signature analysis*": analisi basata su *signature* che consente di riconoscere le serie di pacchetti (o i dati contenuti in essi), selezionate preventivamente in fase di configurazione al fine di riconoscere un tipico pattern rappresentativo di un attacco.

[R.128] 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.129] In caso di rilevamento di un attacco, il sistema deve essere in grado di impedirne l'esecuzione per mezzo delle seguenti tecniche di prevenzione:

- Drop packet/session, ossia scarto del pacchetto/sessione;

- Close client/server, ossia invio di un segnale di chiusura (reset) lato client e/o server.

4.1.1.4. Opzioni del servizio SPUN

[R.130] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio di Sicurezza Perimetrale Unificata:

- **Affidabilità elevata** (cfr. [R.132]);
- **Antivirus/Antispyware Content filtering** (cfr. da [R.133] a [R.141]);
- **Application filtering and monitoring** (cfr. da [R.142] a [R.146]);
- **Accesso remoto sicuro (VPN Client-to-site)** (cfr. da [R.147] a [R.152]);
- **Finestra di erogazione estesa** (cfr. [R.6]).

[R.131] Le funzionalità incluse in questa opzione possono essere implementate utilizzando gli stessi dispositivi utilizzati per l'erogazione del servizio SPUN.

[R.132] L'opzione **Affidabilità elevata** prevede, a fronte della corresponsione di un canone aggiuntivo, la duplicazione dell'apparato o degli apparati forniti per l'erogazione dei servizi di sicurezza, gestiti e manutenuti dal Fornitore. Gli apparati aggiuntivi devono essere installati nel medesimo locale tecnico ove sono installati gli apparati primari. Il servizio prevede la configurazione in "hot-standby" degli apparati primari e secondari, e quindi la possibilità di mantenimento trasparente delle funzioni di sicurezza in caso di guasto. Gli apparati forniti devono essere bi-attestati agli apparati di rete utilizzati per lo scambio del traffico tra la rete da proteggere e l'esterno. Gli SLA del servizio per quanto riguarda i parametri di assurance sono differenziati rispetto al servizio base (cfr. Allegato 5 bis).

[R.133] L'opzione **Antivirus/Antispyware & Content Filtering** deve attivare funzionalità in grado di proteggere il Sistema Informativo delle Amministrazioni da spamming, da attacchi veicolati tramite il protocollo HTTP e da codice eseguibile (Virus, Spyware, Worm, Cavallo di Troia, ecc.).

[R.134] Il Fornitore deve garantire le seguenti caratteristiche per tali funzionalità:

- Antivirus/Antispyware Gateway (AVG) per la protezione da codice dannoso che può propagarsi tramite lo scambio di posta elettronica;
- HTTP Gateway (HTTPG) per la protezione da codice dannoso che può propagarsi per il tramite della navigazione WEB e per la protezione da attacchi informatici veicolati tramite il protocollo http;
- FTP Gateway (FTPG) per la protezione da codice dannoso che può propagarsi per il tramite del trasferimento di file mediante FTP;

[R.135] La soluzione proposta deve garantire la rilevazione dei *virus* e degli *spyware* noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal formato di trasmissione.

[R.136] La soluzione proposta deve garantire la capacità di scansione dei pacchetti IP in tempo reale.

[R.137] La soluzione proposta deve garantire piena interoperabilità e/o trasparenza tra client e server.

[R.138] La soluzione proposta deve prevedere il supporto di file in formati compressi per il controllo della presenza di codice dannoso.

[R.139] La soluzione proposta deve prevedere il supporto dei protocolli standard tipici del servizio (SMTP, POP v.3/v.4, IMAP v.4, HTTP, FTP, IM protocol).

[R.140] Per quanto riguarda le caratteristiche di AVG, HTTPG e FTPG il servizio fornito dal Fornitore deve garantire il supporto dei filtri di esclusione sul tipo di file trasferito (vbs, exe, pif, bat, ecc.).

[R.141] Per quanto riguarda le caratteristiche di AVG, il Fornitore deve garantire le seguenti ulteriori funzionalità:

- capacità di riparare file e/o messaggi infetti, nel caso di virus per i quali esiste la possibilità di recupero;
- supporto di blacklist (liste contenenti domini di mail o indirizzi di mail indesiderati);
- configurazioni antispamming che consentano il blocco di messaggi di posta elettronica che transitano per il gateway

basati su blacklist e riconoscimento di porzioni del contenuto del messaggio di posta elettronica personalizzabili;

- verifica sintattica e semantica sull'header dei messaggi.

[R.142] L'opzione **Application Filtering & Monitoring** deve fornire una funzionalità che permetta di effettuare un'analisi delle applicazioni che generano traffico sulla rete, assieme alla possibilità di controllare tali applicazioni, indipendentemente dalla porta e dal protocollo utilizzati dall'applicazione stessa.

[R.143] La funzionalità deve utilizzare un processo per l'analisi del traffico basato su identificativi delle applicazioni e *signature*.

[R.144] Per le applicazioni che non possono essere identificate attraverso analisi del protocollo e l'adozione delle *signature*, devono essere previsti meccanismi basati su euristiche e analisi comportamentale.

[R.145] La funzionalità deve essere in grado 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.146] In particolare, il sistema deve 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.

[R.147] L'opzione **Accesso remoto sicuro (VPN Client-to-site IPsec/SSL)** deve prevedere una funzionalità che consenta, al personale delle Amministrazioni, di accedere da remoto alla Intranet attraverso l'utilizzo di postazioni di lavoro mobili (PC, laptop, smartphone, ecc.) in modalità VPN client-to-site IPsec e/o SSL.

[R.148] L'opzione deve operare creando un tunnel tra il nodo interessato e un gateway della rete, utilizzando il protocollo IPsec o in alternativa il protocollo SSL, in base alle esigenze delle Amministrazioni.

[R.149] Nel caso di utilizzo del protocollo IPsec, il sistema deve operare secondo la modalità "tunnel mode" come definita nella specifica pubblica RFC 4301. In tal caso la parte client deve essere fornita almeno per le seguenti piattaforme: Windows, Linux, Mac.

[R.150] Nel caso dell'utilizzo del protocollo IPsec, devono essere rispettate le specifiche indicate dal [R.117] fino al [R.122].

[R.151] Nel caso di utilizzo del protocollo SSL, il sistema deve operare seguendo la specifica pubblica RFC 6101, in modalità *clientless*. In tal caso, gli utenti accedono alla Intranet attraverso un portale web accessibile a valle di un'autenticazione dell'utente. Tale portale web deve quindi fungere da *proxy* verso un set di applicazioni prestabilito.

[R.152] Il sistema deve essere in grado di supportare un numero di collegamenti in contemporanea a seconda del profilo SPUN di base come riportato nella seguente tabella:

Profilo	Numero massimo di tunnel IPsec simultanei (Client to Site)	Numero massimo di tunnel SSL simultanei (Client to Site)
SPUN-1	10	5
SPUN-2	20	10
SPUN-3	50	25
SPUN-4	100	50
SPUN-5	500	100
SPUN-6	1000	100

4.1.1.5. Precondizioni e vincoli per la sottoscrizione del servizio SPUN

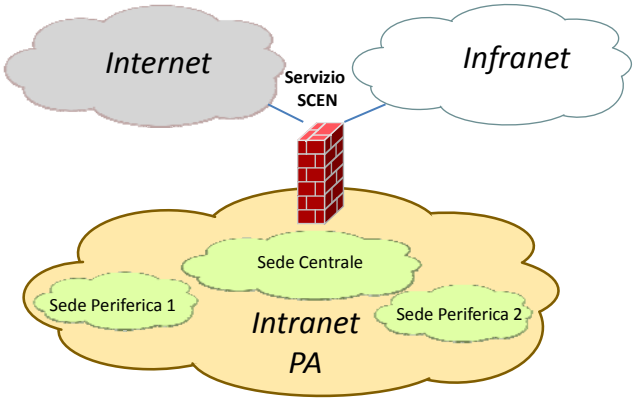
[R.153] Solo le Amministrazioni che hanno sottoscritto, in ambito SPC, servizi di trasporto (STDE o STDO) possono richiedere i servizi SPUN qui descritti e limitatamente alle sedi collegate coi suddetti servizi.

4.1.2. Servizio di Sicurezza Centralizzata (SCEN)

[R.154] Il servizio di **Sicurezza Centralizzata (SCEN)** prevede l'erogazione di servizi di sicurezza perimetrali (firewall, antivirus, Intrusion Detection/Prevention System) in modalità centralizzata su specifici accessi STDE

dell'Amministrazione. Il servizio di sicurezza centralizzato è erogato da un centro servizi del Fornitore locato presso siti del Fornitore medesimo, e deve essere adeguatamente dimensionato per far fronte al carico complessivo generato da tutti i servizi contrattualizzati da tutte le Amministrazioni nel perimetro di competenza del Fornitore.

[R.155] Il servizio SCEN deve essere collocato alla frontiera tra il dominio Intranet ed i domini Infranet ed Internet, e quindi eventualmente esposto su indirizzi privati dell'Amministrazione, secondo quanto riportato nella figura seguente:



[R.156] Il servizio SCEN comprende una componente di network firewall in grado di offrire protezione per il tramite di analisi e filtro di tutto il traffico in transito tra le reti tra cui è interposto, con le seguenti caratteristiche:

- supporto di tutti i protocolli specificati nello standard TCP/IP;
- filtraggio di traffico IP che consente di proteggere la rete dell'Amministrazione da accessi indesiderati bloccando indirizzi, porte o protocolli;
- auditing e logging che consente l'analisi del traffico che attraversa il servizio;
- modulo di ispezione che effettua l'ispezione dei datagrammi IP e realizza il filtraggio sulla base delle regole implementate;
- Traffic Filtering, che consenta di abilitare la navigazione web (ambito Internet) solo a determinate postazioni (intese come

indirizzi IP di provenienza), e di bloccare l'accesso a particolari siti;

- Network Address Translation (NAT) secondo la specifica RFC 3022, sia di tipo statico (uno a uno), sia di tipo dinamico (n a uno) e Port Address Translation (PAT).

[R.157] Il servizio SCEN comprende una componente di Antivirus Filtering in grado di garantire protezione agli accessi dell'Amministrazione nei confronti di spamming, attacchi veicolati tramite il protocollo HTTP e da qualsiasi tipologia di codice software eseguibile (Virus, Worm, Cavallo di Troia, ecc.) che possa provocare danni al Sistema Informativo dell'Amministrazione. Tale servizio di gestione centralizzata delle funzionalità antivirus deve offrire protezione da codice dannoso che può propagarsi per il tramite:

- dello scambio di posta elettronica;
- della navigazione web tramite il protocollo HTTP;
- del trasferimento di file mediante protocollo FTP.

[R.158] Il servizio SCEN comprende una componente di Intrusion Detection System (IDS) in grado di effettuare un rilevamento delle intrusioni tale da consentire l'identificazione di tutte le sequenze di eventi, condotti da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o di una rete. Il servizio deve in particolare:

- garantire analisi predeterminate degli eventi rilevati attraverso l'utilizzo di "*signature analysis*" che consentano di riconoscere le serie di pacchetti (o i dati contenuti in essi), selezionate preventivamente in fase di configurazione, al fine di riconoscere un tipico pattern rappresentativo di un attacco;
- garantire notifiche specifiche a fronte dell'identificazione di un evento di attacco;
- garantire notifiche all'Amministrazione in merito ad eventuali situazioni che necessitino di interventi/decisioni da parte dell'Amministrazione stessa;
- essere customizzabile in termini di definizione di regole personalizzate, registrazione delle attività sulla rete che

rispondano a determinate condizioni, attivazione delle notifiche a fronte di particolari sequenze di eventi sulla rete, ecc.

[R.159] Il servizio SCEN comprende una componente di Intrusion Prevention System (IPS) in grado di svolgere azioni per bloccare selettivamente il traffico in caso di identificazione positiva di tutte le sequenze di eventi, condotte da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o di una rete. Tale caratteristica di IPS deve in particolare garantire funzionalità di:

- analisi di protocollo, al fine di valutare le diverse parti di un protocollo alla ricerca di comportamenti anomali;
- ricerca all'interno dei pacchetti di sequenze uniche per rilevare e prevenire attacchi noti come Worm;
- prevenzione da attacchi di tipo DoS (Denial of Service) e DDoS (Distributed DoS).

[R.160] Alcune delle funzionalità offerte dal servizio di sicurezza si basano su "*signature*", che devono essere aggiornate entro, e non oltre, 1 giorno dal momento in cui sono rese disponibili dal vendor che fornisce i sistemi utilizzati dal Fornitore per l'erogazione del servizio di sicurezza.

[R.161] Il servizio SCEN deve essere configurato dal Fornitore in modo da garantire che in caso di malfunzionamento della funzionalità di sicurezza, venga inibita completamente la capacità di trasmissione/ricezione del traffico fra l'accesso STDE dell'Amministrazione e gli ambienti Internet e Infranet, mantenendo comunque attiva la comunicazione in ambito Intranet.

[R.162] Il servizio SCEN non è caratterizzato da PAS.

4.1.2.1. Opzioni del servizio SCEN

[R.163] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio SCEN:

- **Finestra di erogazione estesa** (cfr. [R.6]), col vincolo che la finestra di erogazione del servizio SCEN coincida con quella del servizio STDE associato.

4.1.2.2. Precondizioni e vincoli per la sottoscrizione del servizio SCEN

[R.164] Un servizio SCEN può essere attivato solo in relazione ad un accesso di tipo STDE con opzione Multiambito.

5. SERVIZI DI COMUNICAZIONE EVOLUTA

I Servizi di Comunicazione Evoluta sono dedicati a consentire alle Amministrazioni di effettuare comunicazioni voce o audio/video utilizzando il medesimo accesso attraverso il quale viene approvvigionata la connettività IP (servizi di trasporto).

I Servizi di Comunicazione Evoluta si articolano in

- **Servizi VoIP (VOIP):** devono consentire alle Amministrazioni contraenti di effettuare conversazioni telefoniche su protocollo IP;
- **Servizi di Telepresenza (TELP):** devono consentire alle Amministrazioni la comunicazione tra utenti remoti attraverso strumenti di acquisizione/riproduzione audio/video di alta qualità.

[R.165] Le soluzioni e i servizi proposti devono essere:

- conformi a direttiva 1999/5/CE (D.Lgs. 9 maggio 2001, n. 269), direttiva 2009/125/CE (D.Lgs. 15 febbraio 2011, n.15), direttiva 2002/95/CE (D. Lgs. 151/2005) e, in generale, completamente conformi alla normativa vigente e agli standard di riferimento applicabili;
- adeguati in modo continuativo alle normative che la Comunità Europea o l'Italia rilasceranno in merito a servizi analoghi a quelli descritti nel presente Documento senza oneri aggiuntivi per le Amministrazioni;
- aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato.

[R.166] Il servizio deve essere garantito nelle modalità di protocollo IPv4, IPv6 o dual stack.

[R.167] Tutti i dispositivi devono supportare il protocollo SNMP per consentire monitoring in tempo reale e trouble-shoooting.

5.1. SERVIZI VOIP

[R.168] I servizi VoIP, comprendono:

- Servizi di Centralino IP (CEIP)
- Servizi di Resilienza Periferici (RESI)
- Servizi di Gateway (GWTD e GWIP)
- Servizi di Gestione degli Endpoint (ENIP)

[R.169] I servizi VoIP nel seguito descritti devono:

- garantire il rispetto delle disposizioni regolamentari in merito alla interconnessione IP e interoperabilità per la fornitura di servizi VoIP (delibera AGCOM n. 128/11/CIR e smi), in particolare per la definizione di un insieme comune di standard, dei protocolli di segnalazione, dei codec (audio e fax) e funzionalità del VoIP;
- consentire l'invio e la ricezione di fax (con supporto del protocollo T.38);

[R.170] Il Fornitore si impegna a porre in essere tutte le azioni necessarie ad interconnettersi ad un eventuale punto di peering per il Voip (NIV2) che dovesse essere realizzato per la veicolazione di servizi VOIP tra le Pubbliche Amministrazioni aderenti ad SPC. Inoltre, in tale contesto, su indicazione dell'Agenzia per l'Italia Digitale ed in conformità con le procedure previste dall'art. 18 dello schema di Contratto Quadro allegato alla lettera di invito, si impegna ad integrare l'offerta dei servizi SPC con ulteriori servizi VoIP che verranno individuati per tale specifica esigenza.

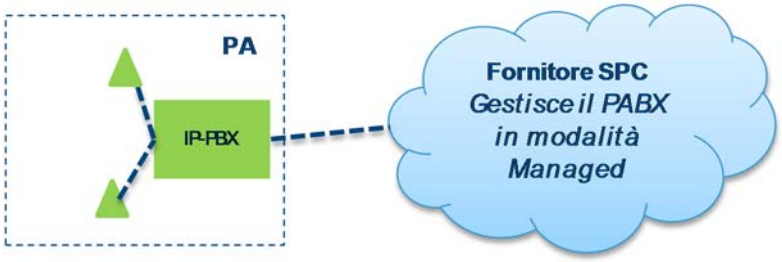
5.1.1. Servizi di Centralino IP (CEIP)

[R.171] I servizi CEIP costituiscono il substrato di servizi VoIP disponibile nel listino SPC e rappresentano in tal senso la componente obbligatoria e propedeutica per l'acquisto dei restanti servizi VoIP presenti nel suddetto listino.

[R.172] Il Punto di accesso al servizio (PAS) per i servizi CEIP è definito come l'insieme delle interfacce verso la LAN dell'Amministrazione (e, se

disponibili, verso la RTG) sugli apparati che erogano il servizio in sede della Amministrazione.

[R.173] I servizi CEIP sono rivolti a quelle Amministrazioni che non dispongono di infrastrutture di proprietà e consistono nella fornitura, messa in opera, gestione in modalità Managed (on-site) e manutenzione di un'infrastruttura IP-based; prevedono pertanto un apparato IP-PBX presso una sede dell'Amministrazione. Presso le altre sedi dell'Amministrazione il servizio di base non prevede ulteriori apparati; i terminali possono essere acquistati nell'ambito del servizio ENIP di cui al § 5.1.4



[R.174] I servizi devono integrarsi completamente rispetto alle infrastrutture preesistenti, con riferimento alle reti locali delle Amministrazioni e al piano di numerazione dei derivati telefonici che, a richiesta dell'Amministrazione, deve poter essere mantenuto. Quindi all'Amministrazione deve essere garantita la possibilità di:

- riutilizzare numerazioni interne già in uso;
- utilizzare nuove estensioni;
- disporre di un piano di numerazione ex-novo utilizzando una diversa radice.

[R.175] Devono essere erogate funzionalità di gestione della segnalazione per il controllo dei vari stati di una chiamata. Tali funzionalità possono in particolare essere declinate in:

- Incoming Call Gateway: funzione deputata alla gestione della segnalazione al fine del corretto instradamento delle chiamate;
- Call Control Function: funzione deputata all'attivazione, rilascio e gestione/cambiamento degli stati della chiamata, nonché alla determinazione della necessità delle operazioni di transcodifica. Gestisce inoltre la registrazione delle differenti postazioni VoIP

ed è in grado di interfacciarsi con server esterni dedicati all'implementazione di servizi a valore aggiunto;

- Serving Profile Database: funzione deputata alla gestione e controllo dei profili delle utenze (es. autorizzazione, abilitazioni, ecc.);
- Address Handling: funzione deputata all'analisi, traduzione, eventuale modifica e risoluzione degli indirizzi da identificativo alfanumerico a indirizzo IP;

Il sistema utilizzato deve supportare il protocollo SIP.

[R.176] Nell'ambito del dominio di una singola Amministrazione (inteso come insieme delle utenze ad essa afferenti), devono essere garantiti almeno i servizi elencati in tabella:

Servizio
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

[R.177] I servizi CEIP devono prevedere funzionalità di trattamento del segnale audio (echo cancellation).

[R.178] I servizi CEIP devono garantire funzionalità di autenticazione e autorizzazione nei confronti degli utenti abilitati. Tali funzionalità devono essere implementate per il tramite di comunicazioni logiche IP sicure.

[R.179] I servizi CEIP devono prevedere funzionalità di *whitelist* e/o *blacklist* sulla base della coppia numero chiamante/numero chiamato.

[R.180] Come detto, l'elemento di gestione della logica di controllo deve essere installato dal Fornitore presso una sede a scelta dell'Amministrazione. Nelle restanti sedi non è prevista l'installazione di alcun apparato, fatta eccezione per gli Endpoint (cfr. § 5.1.4), o gli eventuali apparati previsti dai profili GWTD o GWIP per l'interconnessione a PBX/IP-PBX esistenti (cfr. § 5.1.2). Per quanto detto, in caso di architetture multisede, il prezzo viene sempre calcolato sulla somma di tutte le utenze afferenti alla totalità delle sedi dell'Amministrazione per le quali è stato attivato il servizio.

[R.181] I servizi CEIP sono raggruppati in fasce:

Profilo	Descrizione
CEIP-1	CEIP - 30 utenze
CEIP-2	CEIP - Da 31 a 100 utenze
CEIP-3	CEIP - Da 101 a 300 utenze
CEIP-4	CEIP - Oltre 300 utenze

5.1.1.1. Opzioni dei servizi CEIP

[R.182] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi CEIP:

- **Affidabilità elevata** (cfr. [R.183])
- **Segreteria telefonica** (cfr. [R.184] e [R.185])
- **Finestra di erogazione estesa** (cfr. [R.6])
- **Breakout** (cfr. [R.186], [R.187] e [R.188])

[R.183] L'opzione **Affidabilità elevata** prevede la duplicazione dell'apparato IP-PBX fornito, gestito e manutenuto dal Fornitore presso la sede dell'Amministrazione. Il secondo IP-PBX deve essere installato nel medesimo locale tecnico ove è installato l'IP-PBX primario. Il servizio prevede la configurazione in hot-standby dell'IP-PBX primario e dell'IP-PBX secondario, l'allineamento continuo e sincrono dei dati di configurazione e delle utenze/terminali gestiti consentendo quindi la possibilità di mantenimento trasparente della chiamata in corso in caso di guasto.

[R.184] L'opzione **Segreteria telefonica** prevede l'erogazione di un servizio di segreteria telefonica agli utenti abilitati; il servizio:

- consiste nella disponibilità di una casella vocale accessibile tramite numerazione ad hoc da un terminale attestato alla centrale telefonica e previa autenticazione;
- deve prevedere la consultazione via accesso remoto (da terminale non attestato alla centrale telefonica) previa autenticazione;

- deve prevedere l'indicazione della data, orario e numero chiamante di ogni chiamata registrata;
- deve garantire uno spazio per utente pari ad almeno 10 minuti di registrazione;
- deve consentire l'integrazione con il sistema di posta elettronica, in uso presso l'Amministrazione (e senza necessità di modifiche di configurazione del sistema mail stesso), per la ricezione di messaggi vocali come normale messaggio di posta con file audio allegato.

[R.185] L'opzione Segreteria telefonica può essere contrattualizzata per un numero di utenze minore o uguale al numero di utenze per le quali è stato contrattualizzato il servizio CEIP.

[R.186] L'opzione **Breakout** prevede l'erogazione di un servizio di interfacciamento con la rete telefonica pubblica (*breakout*) realizzato tramite schede o apparati gateway forniti, installati, gestiti e manutenuti dal Fornitore. Il servizio incontra le esigenze di quelle Amministrazioni che vogliono garantire affidabilità e continuità di servizio anche in assenza del collegamento dati principale. Il servizio è realizzato dotando il sistema IP-PBX di schede o apparati gateway che interfaccino la rete pubblica (a seconda delle esigenze BRI o PRI ISDN). L'Amministrazione che desidera implementare tale funzionalità deve contrattualizzare l'opzione (per la sede in cui è attivo il servizio CEIP) indicando per ogni sede il numero di canali a 64 Kb/s necessari, secondo un corretto dimensionamento del traffico previsto, per l'interconnessione alla rete pubblica. Il servizio non è comprensivo delle linee di accesso alla RTG e del servizio di gestione del traffico.

[R.187] Il gateway alla base dell'opzione Breakout deve:

- essere dotato di interfacce ISDN BRI o PRI in numero tale da soddisfare i requisiti di traffico espressi dall'Amministrazione;
- includere funzionalità di encoding, echo cancellation, transcodifica.

[R.188] L'opzione Breakout si intende comprensiva di tutte le caratteristiche e funzionalità necessarie al mantenimento del piano di numerazione.

5.1.1.2. Precondizioni e vincoli per la sottoscrizione dei servizi CEIP

[R.189] I servizi CEIP comprendono la gestione del traffico VOIP nell'ambito Intranet di ciascuna Amministrazione e non sono comprensivi:

- della connettività IP necessaria al trasporto su SPC dei flussi informativi facenti parte del servizio CEIP. Ciascuna Amministrazione deve necessariamente dimensionare opportunamente i propri servizi di trasporto SPC in funzione delle risorse richieste dai servizi VoIP;
- del servizio di gestione del traffico RTG (commutazione del traffico su rete telefonica pubblica e relativo rilegamento trasmissivo);
- della fornitura dei terminali telefonici né di altre tipologie di apparati d'utente, che possono essere acquistati dalle Amministrazioni nell'ambito dei servizi di gestione degli Endpoint successivamente descritto (cfr. § 5.1.4).

5.1.2. Servizi di Gateway (GWTD e GWIP)

I servizi di Gateway si articolano in:

- Servizi di Gateway TDM (GWTD)
- Servizi di Gateway IP (GWIP)

[R.190] Il Punto di accesso al servizio (PAS) per i servizi Gateway è definito come l'insieme delle interfacce verso la LAN dell'Amministrazione sugli apparati che erogano il servizio in sede della Amministrazione.

[R.191] I servizi di Gateway TDM (GWTD) consistono nella fornitura, messa in opera, gestione e manutenzione di un'infrastruttura di IP Voice Gateway in grado di interconnettere il PABX TDM-based esistente presso una sede dell'Amministrazione con centrali IP di rete del Fornitore, trasformando il traffico voce in traffico IP; la soluzione prevede pertanto un apparato gateway presso l'Amministrazione connesso al PABX TDM-based di proprietà della stessa, che possa interagire con la sede dove è attivato un servizio CEIP. Si sottolinea che le attività di manutenzione e configurazione del PABX

TDM-based esistente presso la sede dell'Amministrazione non sono oggetto di fornitura e sono quindi da ritenersi a completo carico della medesima.

[R.192] I servizi di Gateway IP (GWIP) consistono nella fornitura, messa in opera, gestione e manutenzione di un'infrastruttura in grado di interfacciare il centralino IP-PBX di proprietà dell'Amministrazione (installata presso locali della stessa) con una centrale IP del Fornitore (installata presso locali nella sede dell'Amministrazione con profilo CEIP), consentendo in tal modo un collegamento ai servizi VoIP dell'infrastruttura di proprietà dell'Amministrazione. Si sottolinea che le attività di manutenzione e configurazione dell'IP-PBX esistente presso la sede dell'Amministrazione non sono oggetto di fornitura e sono quindi da ritenersi a completo carico della medesima.

[R.193] Deve essere garantita l'interoperabilità tra i differenti servizi di Gateway acquistati da diverse Amministrazioni afferenti al Fornitore.

[R.194] I servizi devono integrarsi completamente rispetto alle infrastrutture preesistenti, con riferimento alle reti locali delle Amministrazioni e al piano di numerazione dei derivati telefonici che, a richiesta dell'Amministrazione, deve poter essere mantenuto. Quindi all'Amministrazione deve essere garantita la possibilità di:

- riutilizzare numerazioni interne già in uso;
- utilizzare nuove estensioni;
- disporre di un piano di numerazione ex-novo utilizzando una diversa radice.

[R.195] Devono essere erogate funzionalità di gestione della segnalazione per il controllo dei vari stati di una chiamata. Tali funzionalità possono in particolare essere declinate in:

- Incoming Call Gateway: funzione deputata alla gestione della segnalazione al fine del corretto instradamento delle chiamate;
- Call Control Function: funzione deputata all'attivazione, rilascio e gestione/cambiamento degli stati della chiamata, nonché alla determinazione della necessità delle operazioni di transcodifica. Gestisce inoltre la registrazione delle differenti postazioni VoIP ed è in grado di interfacciarsi con server esterni dedicati all'implementazione di servizi a valore aggiunto;

- Serving Profile Database: funzione deputata alla gestione e controllo dei profili delle utenze (es. autorizzazione, abilitazioni, ecc.);
- Address Handling: funzione deputata all'analisi, traduzione, eventuale modifica e risoluzione degli indirizzi da identificativo alfanumerico a indirizzo IP.

Il sistema utilizzato deve supportare il protocollo SIP.

[R.196] Ferma restando la responsabilità delle Amministrazioni nella realizzazione, dimensionamento e gestione delle reti LAN interne, la configurazione degli apparati (Gateway) installati per la fornitura del servizio deve essere tale da minimizzare problemi di congestione di traffico della rete locale.

[R.197] I servizi di Gateway devono prevedere funzionalità di trattamento del segnale audio (echo cancellation).

[R.198] I servizi di Gateway devono garantire funzionalità di autenticazione e autorizzazione nei confronti degli utenti abilitati. Tali funzionalità devono essere implementate per il tramite di comunicazioni logiche IP sicure.

[R.199] Come detto, per quanto riguarda i servizi di Gateway l'apparato gateway deve essere installato dal Fornitore presso la sede indicata dall'Amministrazione. Per quanto detto, in caso di architetture multisede, il prezzo viene sempre calcolato sulla somma di tutte le utenze afferenti alla totalità delle sedi dell'Amministrazione per le quali è stato attivato il servizio.

[R.200] Il prezzo relativo alla prima fascia dei servizi di Gateway prevede l'acquisto di un numero minimo di 30 utenze.

5.1.2.1. Opzioni dei servizi di Gateway

[R.201] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di Gateway:

- **Finestra di erogazione estesa** (cfr. [R.6]).

5.1.2.2. Precondizioni e vincoli per la sottoscrizione dei servizi di Gateway

[R.202] I servizi di Gateway possono essere acquistati esclusivamente in abbinamento ai servizi CEIP.

5.1.3. Servizio di Resilienza Periferica (RESI)

[R.203] I servizi RESI offrono alle Amministrazioni la possibilità di aggiungere caratteristiche di affidabilità ai servizi CEIP che costituiscono la "piattaforma base di servizio" VoIP.

[R.204] I servizi RESI consistono nell'erogazione di un servizio di sopravvivenza locale della sede periferica di un'Amministrazione che ha contrattualizzato il servizio CEIP; RESI viene implementato tramite la fornitura, installazione, gestione e manutenzione di un apparato IP-PBX presso la sede periferica dell'Amministrazione. Tale apparato deve consentire la raccolta delle registrazioni dei terminali IP ivi presenti al fine di garantire il funzionamento locale della sede anche in caso di "mancata connessione" con la sede in cui è attivo CEIP. A seguito di contrattualizzazione del servizio RESI, in caso di mancato collegamento, per qualsiasi causa, con la sede in cui è attivo CEIP, i terminali della sede periferica possono comunicare fra loro e, attraverso l'opzione di breakout, collegarsi eventualmente con la RTG. Più specificatamente, il collegamento con la RTG tramite l'opzione di breakout deve essere disponibile anche quando sia disponibile la connessione con la sede in cui è attivo CEIP. In pratica, il gateway locale di sopravvivenza, in assenza del collegamento con il sistema master della sede principale, assume il ruolo di nuovo apparato master limitatamente a tutti gli apparati della sede periferica coinvolta. Una volta ripristinato il collegamento fra la sede principale e la sede periferica, in automatico deve essere garantito il ripristino delle normali condizioni operative registrando gli apparati della sede periferica sull'apparato master della sede principale. Se l'Amministrazione vuole implementare tale funzionalità su più sedi, deve contrattualizzare il servizio RESI per ciascuna singola sede, acquistandolo per "n" utenti, ove "n" è il numero degli utenti attestati sulla specifica sede.

[R.205] I servizi RESI si intendono comprensivi di tutte le caratteristiche e funzionalità necessarie al mantenimento del piano di numerazione.

5.1.3.1. Opzioni dei servizi RESI

[R.206] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi RESI:

- **Affidabilità elevata** (cfr. [R.207])
- **Finestra di erogazione estesa** (cfr. [R.6])
- **Breakout** (cfr.[R.208], [R.209] e [R.210])

[R.207] L'opzione **Affidabilità elevata** prevede, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto con riferimento al servizio RESI, la duplicazione dell'apparato fornito, gestito e mantenuto dal Fornitore presso la specifica sede dell'Amministrazione. Il secondo apparato è installato nel medesimo locale tecnico ove è installato l'apparato primario. Il servizio prevede la configurazione in hot-standby dei due apparati e quindi la possibilità di mantenimento trasparente della chiamata in corso in caso di guasto.

[R.208] L'opzione **Breakout** prevede, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto per il profilo RESI, l'erogazione di un servizio di interfacciamento con la rete telefonica pubblica (*breakout*) realizzato tramite schede o apparati gateway forniti, installati, gestiti e manutenuti dal Fornitore. Il servizio incontra le esigenze di quelle Amministrazioni che vogliono garantire affidabilità e continuità di servizio anche in assenza del collegamento dati principale. Il servizio è realizzato dotando il sistema IP-PBX con schede o apparati gateway che interfacciano la rete pubblica (a seconda delle esigenze BRI o PRI ISDN). L'Amministrazione che desidera implementare tale funzionalità deve contrattualizzare l'opzione (per la sede in cui è attivo il servizio RESI) indicando per ogni sede il numero di canali a 64 Kb/s necessari, secondo un corretto dimensionamento del traffico previsto, per l'interconnessione alla rete pubblica. Il servizio non è comprensivo delle linee di accesso alla RTG e del servizio di gestione del traffico.

[R.209] Il gateway alla base dell'opzione Breakout deve:

- essere dotato di interfacce ISDN BRI o PRI in numero tale da soddisfare i requisiti di traffico espressi dall'Amministrazione;
- includere funzionalità di encoding, echo cancellation, transcodifica.

[R.210] L'opzione Breakout si intende comprensiva di tutte le caratteristiche e funzionalità necessarie al mantenimento del piano di numerazione.

5.1.3.2. Precondizioni e vincoli per la sottoscrizione dei servizi RESI

[R.211] I servizi RESI possono essere acquistati esclusivamente in abbinamento ai servizi CEIP.

5.1.4. Servizio di gestione degli Endpoint (ENIP)

Come descritto in precedenza, i servizi CEIP non sono comprensivi della fornitura dei terminali. Il servizio di gestione degli Endpoint descritto nella presente sezione consiste pertanto in un completamento di tali profili CEIP in modo da offrire alle Amministrazioni un servizio VoIP completo.

[R.212] Il servizio di gestione degli Endpoint si intende comprensivo della fornitura del terminale e delle prestazioni di installazione, configurazione, gestione e manutenzione dello stesso. Per il servizio ENIP-1 le attività di installazione e configurazione si limitano alla messa a disposizione del software installabile con relative licenze ed al supporto remoto alla configurazione. Per i Servizi ENIP-2, ENIP-3, ENIP-4, ENIP-5 ed ENIP-9 le attività di installazione si limitano alla consegna degli endpoint presso la sede dell'Amministrazione ed al supporto remoto alla configurazione.

[R.213] Tutti i terminali devono essere compatibili con i servizi VoIP descritti nel presente Capitolato e con le funzionalità/opzioni richieste (cfr. § 5.1.1 e § 5.1.3).

[R.214] Gli apparati previsti dal listino sono:

- ENIP-1: soft-phone
- ENIP-2: telefono IP wired – Entry level model
- ENIP-3: telefono IP wired – Top level model

- ENIP-4: telefono IP wireless
- ENIP-5: postazione audio-conference
- ENIP-6: postazione operatore SW
- ENIP-7: postazione operatore ipovedente
- ENIP-8: postazione operatore non vedente
- ENIP-9: Analog Terminal Adapter (ATA)

[R.215] Il soft-phone (ENIP-1), tramite l'installazione su PC, notebook, ecc. di un client software fornito nell'ambito del servizio, consente all'utente di:

- effettuare/ricevere chiamate telefoniche;
- usufruire di funzionalità di:
  - Presence: indicazione grafica dello stato di presenza (o meno) degli utenti abilitati al servizio ENIP-1;
  - Instant Messaging: funzionalità di invio e ricezione di messaggi testo in tempo reale fra gli utenti abilitati al servizio ENIP-1;
  - File Transfer: scambio file fra utenti abilitati al servizio ENIP-1;
  - Document sharing: condivisione remota di documenti elettronici in tempo reale fra gli utenti abilitati al servizio ENIP-1 che condividono una sessione di lavoro (web collaboration);
  - Videochiamata, fra utenti abilitati al servizio ENIP-1.

[R.216] L'endpoint ENIP-1, nel rispetto delle funzionalità obbligatorie di cui al requisito precedente, deve essere dotato almeno delle seguenti caratteristiche:

- installabile ed eseguibile sui seguenti sistemi operativi: Microsoft Windows XP e successivi, Apple MacOS 10.6 e successive;
- compatibile con lo standard XMPP;
- supporto del protocollo SIP, implementazione della funzione di SIP User Agent e compatibilità con protocolli open di

messaggistica istantanea e presenza basati su XML (secondo la XMPP Standard Foundations);

- gestione della buddy list (o lista dei contatti) e funzionalità di tipo click-to-dial;
- supporto di funzionalità di composizione, risposta, trasferta, hold, mute.

[R.217] Il servizio ENIP-1 non è comprensivo della fornitura dei PC o di altro hardware su cui i soft-phone possono essere installati né di eventuali sistemi di interfacciamento con l'utente quali microfono, cuffie o cornette USB.

[R.218] Il telefono IP wired – Entry level model (ENIP-2) deve essere dotato almeno delle seguenti caratteristiche:

- switch interno con porte Ethernet 10/100 e rilevamento automatico della presenza di un PC connesso;
- supporto tele-alimentazione remota attraverso l'interfaccia Ethernet (IEEE 802.3af);
- supporto dello standard IEEE 802.1q;
- kit di alimentazione locale;
- supporto dello standard IETF RFC213 per l'assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP;
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- schermo monocromatico;
- display a 20 caratteri;
- tastiera alfanumerica;
- regolazione del volume del ricevitore;
- modalità di ascolto viva voce;
- servizio di guida in linea integrato per le operazioni di programmazione.

[R.219] Il telefono IP wired - Top model (ENIP-3) deve essere dotato almeno delle seguenti caratteristiche:

- switch interno con porte Ethernet 10/100 e rilevamento automatico della presenza di un PC connesso;
- supporto tele-alimentazione remota attraverso l'interfaccia Ethernet (IEEE 802.3af);
- supporto dello standard IEEE 802.1q;
- kit di alimentazione locale;
- supporto dello standard IETF RFC213 per l'assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP;
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- touch screen;
- display a colori 320 x 240 pixel;
- rubrica personale;
- slot per moduli aggiuntivi;
- regolazione del volume del ricevitore;
- modalità di ascolto viva voce;
- 10 tasti hardware o equivalenti software programmabili;
- messaggi di notifica su display multilingua (almeno italiano e inglese);
- servizio di guida in linea integrato per le operazioni di programmazione.

[R.220] Il telefono IP wireless (ENIP-4) non richiede un collegamento wired alla LAN dell'Amministrazione ma viene connesso a questa in modalità Wi-Fi tramite opportuni access point messi a disposizione dall'Amministrazione; il terminale deve essere dotato almeno delle 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;
- blocco tasti;
- regolazione del volume del ricevitore;
- 4 tasti programmabili;
- rubrica personale;
- autonomia: almeno 24 ore in stand-by e almeno 4 ore in conversazione;

[R.221] La postazione audio-conference (ENIP-5) consente a più utenti presenti nella stessa stanza (es. sala riunioni) di effettuare/ricevere chiamate telefoniche, con dispositivi privi di cornetta telefonica, in modalità esclusivamente vivavoce. L'apparato deve essere dotato almeno delle seguenti caratteristiche:

- collegamento alla rete IP tramite connessione Ethernet;
- supporto tele-alimentazione remota attraverso l'interfaccia Ethernet (IEEE 802.3af);
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- kit di alimentazione locale;
- modalità di ascolto viva voce;
- microfono con copertura a 360°;
- tecnologia full duplex;
- tasto mute.

[R.222] La postazione operatore SW (ENIP-6) consente all'utente tutte le operazioni inerenti la gestione delle chiamate entranti dal proprio PC. La postazione operatore SW è intesa come una applicazione software dotata almeno delle seguenti caratteristiche:

- installabile ed eseguibile almeno sui seguenti sistemi operativi: Microsoft Windows XP e successivi, Apple MacOS 10.6 e successivi;
- tutte le funzioni accessibili tramite l'utilizzo della tastiera del computer e/o del mouse;
- interfaccia grafica user friendly che consenta il rapido accesso a tutte le funzionalità disponibili;
- funzionalità di fonia disponibili analoghe a quelle di un soft-phone con l'utilizzo di un auricolare/microfono;
- visualizzazione del numero e della tipologia di chiamate in attesa;
- visualizzazione delle informazioni relative al chiamante, delle chiamate in attesa e dello stato di occupato degli utenti di tutta la rete;
- possibilità di risposta, inoltro e gestione (es. messa in attesa, ecc.) delle chiamate entranti.

[R.223] La postazione operatore SW (ENIP-6) costituisce inoltre la componente di base per i servizi ENIP-7 (postazione operatore ipovedente) e ENIP-8 (postazione operatore non vedente), nel senso che i servizi ENIP-7 e ENIP-8 si intendono comprensivi, oltre che delle caratteristiche specifiche descritte nel seguito, di quanto indicato al [R.222]. Quindi tutte le funzionalità di cui al predetto requisito precedente saranno a disposizione degli operatori non vedenti/ipovedenti per il tramite delle componenti speciali di cui ai requisiti specifici che seguono.

[R.224] La postazione operatore ipovedente (ENIP-7) deve essere dotata almeno delle seguenti componenti speciali aggiuntive rispetto alle caratteristiche/funzionalità descritte per la postazione operatore SW (cfr.[R.222]):

- funzionalità di sintetizzatore vocale, con lettura automatica del testo in italiano;
- software di tipo "screen magnifier" per ingrandimento dello schermo.

[R.225] La postazione operatore non vedente (ENIP-10) deve essere dotata almeno delle seguenti componenti speciali aggiuntive rispetto alle caratteristiche/funzionalità descritte per la postazione operatore SW (cfr.[R.222]):

- funzionalità di sintetizzatore vocale, con lettura automatica del testo in italiano;
- barra Braille piezoelettrica da 40 caratteri in grado di rappresentare tutte le combinazioni del codice ASCII.

[R.226] L'Analog Terminal Adapter (ENIP-9) consente l'utilizzo di terminali analogici (es. telefoni analogici, fax, ecc.) nell'ambito di un'infrastruttura Full-IP. L'adattatore deve essere dotato almeno delle seguenti caratteristiche:

- disponibilità di una porta Ethernet di connessione alla rete IP;
- disponibilità di due porte FXS;
- supporto del protocollo SIP;
- supporto del protocollo T.38.

[R.227] Il Punto di accesso al servizio (PAS) per i servizi ENIP è definito come l'interfaccia verso la LAN dell'Amministrazione sugli apparati che erogano il servizio in sede della Amministrazione (si esclude il caso dei soft-phone).

5.1.4.1. Opzioni del servizio ENIP

[R.228] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio ENIP:

- **Finestra di erogazione estesa** (cfr. [R.6]), col vincolo che la finestra di erogazione del servizio ENIP coincida con quella del servizio CEIP associato.

5.1.4.2. Precondizioni e vincoli per la sottoscrizione del servizio Endpoint

[R.229] I servizi di gestione degli Endpoint possono essere acquistati esclusivamente in abbinamento ai servizi CEIP (eventualmente in numero differente rispetto al numero di utenze abilitate ai servizi CEIP).

5.2. SERVIZI DI TELEPRESENZA

I servizi di Telepresenza, comprendono:

- Servizi di Gestione dell'Infrastruttura di Telepresenza (ITEP)
- Servizi di Gestione degli Endpoint di Telepresenza (ETEP)

[R.230] I servizi di Telepresenza si intendono autonomi rispetto ai servizi VoIP nel senso che, fermo il rispetto dei vincoli nel seguito specificati, non è richiesta alcuna integrazione fra le infrastrutture (es. apparati server centrali, ecc.) a supporto delle due tipologie di servizio.

5.2.1. Servizio di gestione dell'Infrastruttura di Telepresenza (ITEP)

I servizi ITEP sono riferiti alla componente centralizzata del servizio e come tali costituiscono il substrato dei servizi di Telepresenza, rappresentando in tal senso la componente obbligatoria e propedeutica per l'eventuale acquisto degli altri servizi (ETEP) presenti nel suddetto listino.

[R.231] I servizi di gestione dell'infrastruttura di telepresenza sono articolati in due distinte modalità di erogazione del servizio (differente profilo di servizio contrattualizzabile dall'Amministrazione):

- **Profilo ITEP-1**: consiste nella fornitura dei servizi di un'infrastruttura di Telepresenza, non necessariamente dedicata alla singola Amministrazione, in modalità Hosted e quindi attraverso sistemi locati presso la Server Farm del Fornitore SPC. Il servizio non prevede ulteriori apparati presso le sedi dell'Amministrazione; i terminali utente possono essere acquistati nell'ambito del servizio aggiuntivo ETEP, descritto successivamente;
- **Profilo ITEP-2**: consiste nella fornitura, messa in opera, gestione in modalità Managed (on-site) e manutenzione di un'infrastruttura di Telepresenza e prevede pertanto l'installazione degli apparati centrali presso una sede dell'Amministrazione; i terminali utente possono essere

acquistati nell'ambito del servizio aggiuntivo ETEP, descritto successivamente.

[R.232] I servizi devono essere comprensivi di funzionalità di *scheduling* che consentano la prenotazione centralizzata delle sessioni di telepresenza. La soluzione deve garantire inoltre funzionalità di convocazione automatica delle sessioni basata su e-mail.

[R.233] Il sistema deve consentire la piena interoperabilità tra postazioni in alta definizione (HD) e postazioni in definizione standard (SD).

[R.234] Deve 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.235] Il profilo ITEP-1 deve consentire ai partecipanti di collegarsi alle sessioni di telepresenza sia attraverso IP che attraverso connessioni multicanale ISDN. Il profilo ITEP-2 deve consentire ai partecipanti di collegarsi alle sessioni di telepresenza attraverso IP.

[R.236] Nel caso del profilo ITEP-1 l'infrastruttura Hosted che fornisce il servizio deve essere raggiungibile in IP dalle Amministrazioni mediante la connettività SPC attraverso Infranet. Per permettere la partecipazione di client esterni al SPC il servizio deve essere raggiungibile anche tramite Internet e attraverso linee ISDN RTG. La connettività ISDN dei client del sistema non è inclusa nei servizi ed è fornita a carico dell'Amministrazione. La configurazione del servizio non deve permettere la transizione di traffico diretto tra gli ambiti Internet ed Infranet.

[R.237] Il servizio deve garantire la conformità almeno ai seguenti standard:

- H.323 ITU-T Recommendations e SIP (Session Initiation Protocol – RFC 2543) 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;
- H.264 ITU-T Recommendations per quanto concerne la codifica video;

- G.711 e AAC-LD (Advanced Audio Coding with Low Delay) per quanto riguarda la codifica audio.

[R.238] Il servizio deve consentire funzionalità di trasferimento di file e di visualizzazione, condivisione e revisione di documenti fra i vari partecipanti alla sessione.

[R.239] La soluzione deve consentire funzionalità di invito e partecipazione degli utenti ad una sessione nonché funzionalità di moderazione della stessa.

[R.240] I servizi devono prevedere funzionalità di trattamento del segnale audio (echo cancellation).

[R.241] La soluzione deve consentire la memorizzazione, per almeno 6 mesi solari, delle informazioni elencate:

- utenti coinvolti e rispettive Amministrazioni di appartenenza,
- data e ora di inizio della sessione,
- data e ora di fine della sessione.

[R.242] Il servizio si intende comprensivo della disponibilità di una interfaccia verso servizi di "directory centralizzata" al fine di memorizzare e consultare una rubrica indirizzi.

[R.243] Il sistema messo a disposizione dell'Amministrazione per il servizio di profilo ITEP 2 deve avere le seguenti caratteristiche minime:

a. Interfaccia LAN 100 Mb/s Ethernet o superiore
b. Capacità di gestire contemporaneamente almeno 10 continuous presence ports a 1080p x 30 (risoluzione x fotogrammi al secondo)

5.2.1.1. Opzioni del servizio ITEP

[R.244] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi ITEP:

- **Affidabilità elevata** (cfr. [R.245]), applicabile esclusivamente al profilo di servizio ITEP-2;
- **Registrazione delle sessioni** (cfr. [R.246]), applicabile ad entrambi i profili ITEP-1 e ITEP-2;

- **Finestra di erogazione estesa** (cfr. [R.6]), applicabile ad entrambi i profili ITEP-1 e ITEP-2.

[R.245] L'opzione di **Affidabilità elevata** prevede, per il profilo di servizio ITEP-2, la completa ridondanza dell'infrastruttura di servizio.

[R.246] L'opzione di **Registrazione delle sessioni** prevede, per entrambi i profili ITEP-1 e ITEP-2:

- la memorizzazione di sessioni di video conferenza a cui si può accedere successivamente per rivedere la sessione registrata;
- la disponibilità delle seguenti informazioni:
  - utenti coinvolti e rispettive Amministrazioni di appartenenza;
  - data e ora di inizio della sessione;
  - data e ora di fine della sessione.

5.2.1.2. Precondizioni e vincoli per la sottoscrizione del servizio ITEP

[R.247] I servizi ITEP non sono comprensivi della connettività IP necessaria al trasporto su SPC dei flussi informativi facenti parte del servizio ITEP. Ciascuna Amministrazione deve necessariamente dimensionare opportunamente i propri servizi di trasporto SPC in funzione delle risorse richieste dai servizi ITEP.

5.2.2. Servizio di gestione degli ENDPOINT di telepresenza (ETEP)

[R.248] Come descritto in precedenza, i servizi ITEP non sono comprensivi della fornitura degli Endpoint. Il servizio ETEP consiste pertanto nella fornitura, installazione, configurazione e gestione di una serie di Endpoint, a completamento del servizio di Telepresenza, che prevedano modalità di connessione IP (non è richiesta connettività ISDN). Per i servizi ETEP-1 ed ETEP-2 le attività di installazione e configurazione si limitano alla messa a disposizione del software installabile con relative licenze ed al supporto remoto alla configurazione. Per i Servizi ETEP-3 le attività di installazione si

limitano alla consegna degli endpoint presso la sede dell'Amministrazione ed al supporto remoto alla configurazione.

[R.249] Tutti i terminali devono essere compatibili con i servizi ITEP descritti e con le funzionalità richieste nel [R.231].

[R.250] Gli apparati previsti dal listino sono:

- ETEP-1: client SW per PC;
- ETEP-2: client SW per dispositivi mobili;
- ETEP-3: postazione da tavolo;
- ETEP-4: postazione base;
- ETEP-5: postazione evoluta.

[R.251] Gli apparati previsti per i profili ETEP-3, ETEP-4 e ETEP-5 devono essere dotati di interfaccia Fast Ethernet o superiore.

[R.252] Il client SW per PC (ETEP-1) deve essere dotato almeno delle seguenti caratteristiche:

- fruizione del servizio a seguito di installazione su PC, notebook, ecc. di un client software fornito nell'ambito del servizio;
- installabile ed eseguibile almeno sui seguenti sistemi operativi: Microsoft Windows XP e successivi, Apple MacOS 10.6 e successivi.

[R.253] Il servizio ETEP-1 non è comprensivo della fornitura del PC o di altro hardware su cui i client SW possono essere installati né di eventuali sistemi di interfacciamento con l'utente quali microfono, cuffie, ecc.

[R.254] Il client SW per dispositivi mobili (ETEP-2) deve essere dotato almeno delle seguenti caratteristiche:

- fruizione del servizio a seguito di installazione su smartphone o tablet;
- installabile ed eseguibile almeno sui seguenti sistemi operativi per dispositivi mobili: Apple iOS 6 o successive release, Android 4.0 o successive release, Microsoft Windows 8 o successive release.

[R.255] La postazione da tavolo (ETEP-3) identifica un sistema di videoconferenza ad alta qualità per una postazione e deve essere dotata almeno delle seguenti caratteristiche:

- n° 1 schermo LCD 32", con qualità video High Definition – 720p;
- n° 1 telecamera con risoluzione HD;
- sistema audio con qualità CD full-duplex;
- microfono direzionale;
- telecomando;
- interfaccia utente con funzioni di Rubrica e menù multilingua.

[R.256] La postazione base (ETEP-4) deve essere dotata almeno delle seguenti caratteristiche:

- n° 1 schermo LCD 60", con qualità video High Definition – 720p;
- base di appoggio a terra o a parete;
- 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.257] La postazione evoluta (ETEP-5) deve essere dotata almeno delle seguenti caratteristiche:

- n° 2 schermi LCD 42", con qualità video High Definition – 720p;
- base di appoggio a terra o a parete;
- 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.

5.2.2.1. Opzioni del servizio ETEP

[R.258] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio ETEP:

- **Finestra di erogazione estesa** (cfr. [R.6])

5.2.2.2. Precondizioni e vincoli per la sottoscrizione del servizio ETEP

[R.259] I servizi ETEP possono essere acquistati esclusivamente in abbinamento ai servizi ITEP (eventualmente in numero differente rispetto al numero di utenze abilitate ai servizi ITEP).

6. SERVIZI DI SUPPORTO PROFESSIONALE (SSUP)

I Servizi di Supporto Professionale (SSUP) consistono in attività professionali erogate dal Fornitore alle Amministrazioni ad integrazione dei servizi già descritti nel presente Capitolato.

I Servizi di Supporto Professionale sono caratterizzati da un insieme di attività opzionali ad elevato valore aggiunto per l'identificazione di scenari di ottimizzazione dell'efficienza, della qualità intrinseca e percepita del servizio stesso, dell'utilizzo e di massimizzazione del valore per l'Amministrazione.

[R.260] I servizi di supporto non includono attività riconducibili al ciclo di vita del servizio acquistato dall'Amministrazione nell'ambito di SPC, il quale comprende:

- Definizione del servizio;
- Analisi dei requisiti;
- Progettazione della soluzione;
- Realizzazione della soluzione progettata;
- Collaudo;
- Documentazione relativa al servizio erogato;
- Messa in esercizio;
- Manutenzione, gestione e assistenza.

[R.261] Tutte queste attività sono da considerarsi incluse nella fornitura del servizio acquistato dall'Amministrazione, e non rientrano nel perimetro dei servizi di supporto.

[R.262] Viene definito un ciclo di vita per i servizi di supporto, complementare al ciclo di vita del servizio acquistato dall'Amministrazione (cfr. [R.260]). Il ciclo di vita per i servizi di supporto prevede tre fasi distinte:

- **Supporto alla definizione della strategia di servizio**: include attività utili a raccogliere informazioni sugli asset dell'Amministrazione, a valutare la fattibilità dell'introduzione di un servizio e a valutare i vantaggi ottenibili attraverso l'introduzione del servizio stesso;

- **Supporto all'introduzione del servizio**: include attività che consentono all'Amministrazione di pianificare l'introduzione del servizio e di introdurlo in maniera efficiente ed efficace;
- **Supporto all'operatività del servizio**: include attività che supportano l'Amministrazione nell'utilizzo ottimale del servizio e nell'acquisizione di eventuali certificazioni di conformità a standard e normative.

[R.263] Nell'ambito delle fasi "Supporto all'introduzione del servizio" e "Supporto all'operatività del servizio", possono essere erogati servizi di formazione del personale dell'Amministrazione.

[R.264] I servizi di supporto oggetto del presente Capitolato comprendono:

- Servizi di Supporto specialistico (SSUP)
- Servizi di Formazione (FORM)

[R.265] I servizi di supporto professionale non prevedono alcun PAS.

6.1. SERVIZI DI SUPPORTO SPECIALISTICO (SSUS)

I Servizi di Supporto Specialistico (SSUS) sono articolati in:

- Supporto al servizio di trasporto (STRA)
- Supporto al servizio di sicurezza (SSIC)
- Supporto al servizio di comunicazione evoluta (SSCE)

[R.266] Il servizio di supporto specialistico è erogato secondo il modello "accordo quadro a consumo". Il costo della prestazione professionale è quantificato in termini di giorni/uomo, differenziato in base al profilo professionale del professionista impiegato.

[R.267] Per tutti i SSUP sono previsti tre diversi profili professionali che possono essere impiegati per l'erogazione dei servizi di supporto specialistico:

- Team Leader;
- Specialista Senior;
- Specialista.

[R.268] Il ruolo principale del Team Leader consiste nel pianificare le attività da svolgere e coordinare lo svolgimento del progetto.

[R.269] Il ruolo principale dello Specialista Senior consiste nel fornire supporto specialistico durante l'esecuzione delle attività di progetto e nel coordinare e contribuire alla redazione della documentazione di progetto. Lo Specialista Senior è responsabile delle attività che gli vengono affidate.

[R.270] Il ruolo principale dello Specialista consiste nel fornire supporto specialistico e contribuire alla redazione della documentazione di progetto.

[R.271] Per ognuno dei singoli servizi di supporto, sono definiti più profili, come di seguito elencato:

- Supporto al servizio di trasporto (STRA-1);
- Supporto alla definizione di reti IPv6 (STRA-2);
- Supporto di base alla sicurezza (SSIC-1);
- Sistema di gestione della sicurezza delle informazioni (SSIC-2);
- Incident Management (SSIC-3);

- Business Continuity (SSIC-4);
- Supporto al servizio di comunicazione evoluta (SSCE-1);

[R.272] Ogni attività di supporto acquistata dall'Amministrazione, sia essa di supporto specialistico o di formazione, deve essere riconducibile ad una delle tipologie di servizio elencate in [R.271] e ad una delle fasi elencate in [R.262]. Di conseguenza, ogni attività di supporto, sia essa di supporto specialistico o di formazione, deve essere definita e documentata esplicitando:

- La tipologia di servizio di riferimento (cfr. [R.271]);
- La fase del ciclo di vita all'interno della quale l'attività si configura (cfr. [R.262]).

[R.273] A seconda della tipologia di servizio di supporto specialistico erogata, sono previsti differenti requisiti minimi inderogabili che caratterizzano i profili professionali di Team Leader, Specialista Senior e Specialista. Questi requisiti sono descritti in dettaglio nelle successive sezioni dedicate alle diverse tipologie di servizio di supporto specialistico.

[R.274] Per ognuna delle tre fasi definite in [R.262], sono definite le tipologie dei prodotti dell'attività di supporto specialistico e lo skill mix minimo che fissa delle percentuali minime di utilizzo delle diverse figure professionali definite in [R.267], come illustrato nella seguente tabella:

Fase	Prodotti della fase	Percentuali minime di utilizzo delle figure professionali
Supporto alla definizione della strategia di servizio	• Assessment degli asset dell'Amministrazione • Studio di fattibilità dell'introduzione di un servizio.	Team Leader: 10% Specialista Senior: 20% Specialista: 40%.
Supporto all'introduzione del servizio	• Piano di migrazione; • Pianificazione dell'introduzione del	Team Leader: 10% Specialista Senior: 20%

	servizio.	Specialista: 40%.
Supporto all'operatività del servizio	• Report dell'attività svolta; • Documentazione specifica relativa al servizio erogato	Team Leader: 10% Specialista Senior: 20% Specialista: 50%.

[R.275] Lo skill mix definito per ogni fase (cfr. [R.274]), deve essere applicato solo in caso di servizi di supporto di durata maggiore o uguale a 10 giornate uomo di lavoro. In caso di attività che richiedono un effort inferiore, non è previsto nessuno skill mix minimo.

6.1.1. Servizi di supporto al trasporto (STRA)

[R.276] Per il servizio di supporto al trasporto, le figure professionali da fornire devono essere caratterizzate dai requisiti minimi inderogabili riportati nella seguente tabella:

Profilo	Titolo di studio	Esperienze lavorative	Conoscenze
Team Leader	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 12 anni di cui almeno 6 nella specifica funzione. • Significative esperienze di direzione di progetti complessi nell'area delle telecomunicazioni in contesti	• Certificazione ITILv3 Foundation. • Certificazione di Project Management (ad esempio PMI-PMP, Prince2 Practitioner, Senior Project manager Level B-IPMA). • Modelli di

	.	multidisciplinari e multi servizi. • Stima di tempi e risorse necessari per la realizzazione di un progetto. • Responsabilità di gruppi di progetto.	acquisto e gestione di servizi tecnologici nel settore Pubblico. • Tecniche e metodi di project management. • Tecniche e metodi di quality management, norme ISO, modalità di certificazione. • Tecnologie e soluzioni per servizi di connettività (wired e wireless). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della

			lingua inglese.
Specialista Senior	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 8 anni di cui almeno 5 nella specifica funzione. • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni, in contesti multidisciplinari e multi servizi. • Esperienza nell'utilizzo di metodologie di project management. • Capacità di problem solving.	• Certificazione ITILv3 Foundation. • Se esistente, certificazione rilasciata dal vendor dei prodotti utilizzati dal Fornitore per l'erogazione del servizio di trasporto. • Mercato e tendenze evolutive delle telecomunicazioni. • Tecnologie e soluzioni per servizi di connettività (wired e wireless). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Buona conoscenza della

			lingua inglese.
Specialista	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 4 anni di cui almeno 2 nella specifica funzione. • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni	• Architetture di soluzioni di telecomunicazioni. • Reti di telecomunicazioni basati su protocolli standard.

[R.277] In aggiunta alle certificazioni previste per ogni profilo professionale ed elencate in [R.276], sono richieste ulteriori caratteristiche che dipendono dalla specifica tipologia di servizio di trasporto e dal profilo professionale considerato, come dettagliato nella seguente tabella:

Profilo servizio	Profilo professionale	Caratteristiche aggiuntive richieste
STRA-1	Team Leader	• N/A
	Specialista Senior	• Modelli di definizione e monitoraggio di Service Level Agreement.
	Specialista	• Principali metodiche di rilevazione dei livelli di servizio
STRA-2	Team Leader	• N/A
	Specialista Senior	• Conoscenza dei protocolli IPv6, piani di indirizzamento IPv6, tecniche di integrazione IPv4-IPv6, multicasting

		IPv6
	Specialista	• Conoscenza dei protocolli IPv6, tecniche di integrazione IPv4-IPv6

6.1.1.1. Precondizioni e vincoli per la sottoscrizione del servizio STRA

[R.278] Le Amministrazioni possono acquistare il servizio di supporto al trasporto se e solo se hanno acquistato almeno un servizio di trasporto.

[R.279] Se un'Amministrazione decide di avvalersi del servizio di supporto al trasporto, la spesa minima per tale attività è fissata pari a 2.000,00 Euro.

[R.280] La spesa massima per attività di supporto al trasporto (inclusi relativi servizi di formazione correlati), fermo restando il vincolo sulla spesa minima di cui al [R.279], è fissata:

- per i servizi STRA-1, al 5% della spesa totale sostenuta dall'Amministrazione per i servizi di trasporto,
- per i servizi STRA-2, al 10% della spesa totale sostenuta dall'Amministrazione per i servizi di trasporto.

6.1.2. Servizi di supporto alla sicurezza (SSIC)

[R.281] Il servizio di supporto alla sicurezza comprende quattro diversi profili di servizio di supporto:

- Supporto di base alla sicurezza (SSIC-1);
- Sistema di gestione della sicurezza delle informazioni (SSIC-2);
- Incident Management (SSIC-3);
- Business Continuity (SSIC-4).

[R.282] Per tutti i profili del servizio SSIC le figure professionali utilizzate devono essere caratterizzate dai seguenti requisiti minimi inderogabili:

Profilo	Titolo di studio	Esperienze lavorative	Conoscenze

Team Leader	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione). .	• Esperienza complessiva non inferiore a 12 anni di cui almeno 6 nella specifica funzione. • Significative esperienze di direzione di progetti complessi nell'area della sicurezza in contesti multidisciplinari e multi servizi. • Stima di tempi e risorse necessari per la realizzazione di un progetto. • Responsabilità di gruppi di progetto.	• Certificazione ITILv3 Foundation. • Certificazione di Project Management (ad esempio PMI-PMP, Prince2 Practitioner, Senior Project manager Level B-IPMA). • Modelli di acquisto e gestione di servizi tecnologici nel settore Pubblico. • Tecniche e metodi di project management. • Tecniche e metodi di quality management, norme ISO, modalità di certificazione. • Tecnologie e soluzioni per servizi di sicurezza. • Progettazione e realizzazione di soluzioni di sicurezza. • Procedure di

			monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista Senior	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 8 anni di cui almeno 5 nella specifica funzione. • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle sicurezza, in contesti multidisciplinari e multi servizi. • Esperienza nell'utilizzo di metodologie di project management. • Capacità di problem solving.	• Certificazione ITILv3 Foundation. • Se esistente, certificazione rilasciata dal vendor dei prodotti utilizzati dal Fornitore per l'erogazione del servizio di trasporto. • Mercato e tendenze evolutive della sicurezza. • Tecnologie e soluzioni per servizi di sicurezza. • Progettazione e realizzazione di soluzioni di sicurezza.

			• Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 4 anni di cui almeno 2 nella specifica funzione. • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni e della sicurezza	• Architetture di soluzioni di telecomunicazioni. • Reti di telecomunicazioni basati su protocolli standard. • Soluzioni di sicurezza • Principali metodiche di rilevazione dei livelli di servizio

[R.283] In aggiunta alle certificazioni previste per ogni profilo professionale ed elencate in [R.282], sono richieste ulteriori certificazioni che dipendono dalla specifica tipologia di servizio di sicurezza e dal profilo professionale considerato, come dettagliato nella seguente tabella:

Profilo servizio	Profilo professionale	Caratteristiche aggiuntive richieste

SSIC-1	Team Leader	• N/A
	Specialista Senior	• Certificazione di Project Management (ad esempio PMI-PMP, Prince2 Practitioner, Senior Project manager Level B-IPMA). • Certificazione di sicurezza (ad esempio ISACA CISA, ISACA CISM, (ISC)2 CISSP, (ISC)2 SSCP).
	Specialista	• N/A
SSIC-2	Team Leader	• Certificazione ISO/IEC 27001 Lead Auditor.
	Specialista Senior	• Certificazione ISO/IEC 27001 Lead Auditor.
	Specialista	• N/A
SSIC-3	Team Leader	• Certificazione ISO/IEC 20001:2005.
	Specialista Senior	• Certificazione ITILv3 Service Operation. • Certificazione ISO/IEC 20001:2005.
	Specialista	• N/A
SSIC-4	Team Leader	• Certificazione ISO/IEC 20001:2005.
	Specialista senior	• Certificazione ITILv3 Service Operation. • Certificazione ISO/IEC 20001:2005.
	Specialista	• N/A

6.1.2.1. Precondizioni e vincoli per la sottoscrizione del servizio SSIC

[R.284] Le Amministrazioni possono acquistare il servizio di supporto alla sicurezza se e solo se hanno acquistato almeno un servizio di sicurezza.

[R.285] Se un'Amministrazione decide di avvalersi del servizio di supporto alla sicurezza, la spesa minima per tale attività è fissata pari a 5.000,00 Euro.

[R.286] La spesa massima per attività di supporto alla sicurezza (inclusi relativi servizi di formazione correlati) è fissata pari al 20% della spesa totale sostenuta dall'Amministrazione per i servizi di sicurezza, fermo restando il vincolo minimo definito in [R.285].

6.1.3. Servizi di supporto alla Comunicazione evoluta (SSCE)

[R.287] Per il servizio di supporto alla comunicazione evoluta, le figure professionali da fornire devono essere caratterizzate dai requisiti minimi inderogabili riportati nella seguente tabella:

Profilo	Titolo di studio	Esperienze lavorative	Conoscenze
Team Leader	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione). .	• Esperienza complessiva non inferiore a 12 anni di cui almeno 6 nella specifica funzione. • Significative esperienze di direzione di progetti complessi nell'area delle telecomunicazioni in contesti multidisciplinari e multi servizi. • Stima di tempi e risorse necessari	• Certificazione ITILv3 Foundation. • Certificazione di Project Management (ad esempio PMI-PMP, Prince2 Practitioner, Senior Project manager Level B-IPMA). • Modelli di acquisto e gestione di servizi tecnologici nel settore Pubblico.

		per la realizzazione di un progetto. • Responsabilità di gruppi di progetto.	• Tecniche e metodi di project management. • Tecniche e metodi di quality management, norme ISO, modalità di certificazione. • Tecnologie e soluzioni per servizi di comunicazione evoluta (VoIP, Unified Communication e Telepresenza). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.

Specialista Senior	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 8 anni di cui almeno 5 nella specifica funzione. • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni, in contesti multidisciplinari e multi servizi. • Esperienza nell'utilizzo di metodologie di project management. • Capacità di problem solving.	• Certificazione ITILv3 Foundation. • Se esistente, certificazione rilasciata dal vendor dei prodotti utilizzati dal Fornitore per l'erogazione del servizio di trasporto. • Mercato e tendenze evolutive delle telecomunicazioni. • Tecnologie e soluzioni per servizi di comunicazione evoluta (VoIP, Unified Communication e Telepresenza). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e

			monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 4 anni di cui almeno 2 nella specifica funzione. • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni	• Architetture di soluzioni di telecomunicazioni. • Reti di telecomunicazioni basati su protocolli standard. • Architetture e standard relativi alle comunicazioni multimediali. • Principali metodiche di rilevazione dei livelli di servizio

6.1.3.1. Precondizioni e vincoli per la sottoscrizione del servizio SSCE

[R.288] Le Amministrazioni possono acquistare il servizio di supporto alla comunicazione evoluta se e solo se hanno acquistato almeno un servizio di comunicazione evoluta.

[R.289] Se un'Amministrazione decide di avvalersi del servizio di supporto alla comunicazione evoluta, la spesa minima per tale attività è fissata pari a 2.000,00 Euro.

[R.290] La spesa massima per attività di supporto alla comunicazione evoluta (inclusi relativi servizi di formazione correlati) è fissata pari al 5% della spesa totale sostenuta dall'Amministrazione per i servizi di comunicazione evoluta, fermo restando il vincolo minimo definito in [R.289].

6.2. SERVIZI DI FORMAZIONE (FORM)

[R.291] I Servizi di Formazione (FORM), si articolano in:

- Servizi di formazione in aula (FONS)
- Servizi di formazione remota (FREM)

[R.292] I servizi di formazione sono sottoposti a valutazione svolta attraverso un questionario i cui contenuti e modalità di somministrazione verranno concordati tra il fornitore assegnatario e l'amministrazione e che prevede sei livelli di valutazione: ottimo, buono, discreto, sufficiente, scarso, insufficiente.

[R.293] Il costo della formazione è quantificato in termini di costo di un giorno di formazione.

6.2.1. Servizi di Formazione in aula (FONS)

[R.294] I servizi di formazione in aula consistono nell'erogazione di un servizio di formazione da parte di un docente in presenza degli alunni.

[R.295] Il servizio di formazione in aula comprende una giornata di lezione (pari a 8 ore di lezione). In caso di necessità, l'Amministrazione può acquistare un numero maggiore di giornate di formazione in aula.

[R.296] Il servizio di formazione in aula comprende la preparazione del materiale didattico, consistente in un documento (di testo o presentazione con slide), che sarà rilasciato agli alunni iscritti al corso.

[R.297] Il servizio di formazione in aula è disponibile in tre diverse modalità di erogazione (differenti profili di servizio contrattualizzabili dall'Amministrazione):

- **Profilo FONS-1**: consiste nell'erogazione di 8 ore di formazione per un numero di alunni minore o pari a 30. L'aula dove si svolge l'attività di formazione è messa a disposizione dall'Amministrazione che acquista il servizio di formazione, e deve essere dotata almeno di un video proiettore. L'aula dove si

svolge la formazione si può trovare in qualsiasi comune sul territorio italiano.

- **Profilo FONS-2**: consiste nell'erogazione di 8 ore di formazione per un numero di alunni minore o pari a 30. L'aula dove si svolge l'attività di formazione è messa a disposizione dal Fornitore, e deve essere dotata almeno di un video proiettore e, su richiesta dell'Amministrazione, di una lavagna. L'aula dove si svolge la formazione deve essere situata in una città capoluogo di provincia (in territorio italiano) scelta dall'Amministrazione che acquista il servizio di formazione.
- **Profilo FONS-3**: questo profilo ha le stesse caratteristiche del profilo FONS-2. La differenza consiste nel fatto che, in questo caso, l'aula messa a disposizione dal Fornitore deve essere dotata, oltre che di un video proiettore anche di una postazione pc con connessione a Internet per ogni alunno.

[R.298] Il servizio di formazione in aula deve essere erogato da un docente che abbia almeno 5 anni di esperienza nell'attività formativa relativamente alla specifica tipologia di servizio di supporto trattata. In alternativa, il docente deve aver progettato/gestito almeno 3 interventi formativi nella tematica nei tre anni precedenti alla contrattualizzazione del servizio.

6.2.1.1. Precondizioni e vincoli per la sottoscrizione del servizio FONS

[R.299] Al momento dell'acquisto del servizio di formazione in aula, l'Amministrazione deve specificare a quale tipologia di servizio di supporto tale attività si riferisce (cfr. [R.271]).

[R.300] Le Amministrazioni possono acquistare il servizio di formazione in aula, relativamente ad una specifica tipologia di supporto, se e solo se hanno acquistato almeno un servizio rispetto al quale la formazione fa riferimento.

[R.301] Il costo del servizio di formazione in aula contribuisce al calcolo per la spesa totale massima sostenibile per i servizi di supporto, definita per ogni singola tipologia di servizio di supporto.

6.2.2.Servizi di Formazione remota (FREM)

[R.302] I servizi di formazione remota consistono nell'erogazione di un servizio di formazione attraverso una piattaforma accessibile dagli alunni via web. L'accesso a Internet e la postazione pc attraverso cui l'alunno accede al servizio di formazione remota non sono inclusi nel servizio.

[R.303] Il servizio di formazione remota comprende una giornata di lezione (pari a 8 ore). In caso di necessità, l'Amministrazione può acquistare un numero maggiore di giornate di formazione remota.

[R.304] Il servizio di formazione remota comprende la gestione della piattaforma accessibile via web e la preparazione del materiale didattico, consistente in un documento (di testo o presentazione con slide), che sarà rilasciato agli alunni iscritti al corso.

[R.305] Il servizio di formazione remota è disponibile in due diverse modalità di erogazione (differenti profili di servizio contrattualizzabili dall'Amministrazione):

- **Profilo FREM-1**: (formazione in telepresenza) consiste nell'erogazione di un servizio di formazione attraverso una piattaforma accessibile via web, per un numero di alunni minore o pari a 100. Questo profilo di servizio prevede l'erogazione di 8 ore di lezione in formato video in diretta. Un docente illustra la lezione e gli alunni, in real-time, seguono la lezione (audio e video) tramite una postazione pc. Il servizio comprende quindi la gestione della piattaforma, la docenza per 8 ore di lezione, la realizzazione del materiale didattico e un servizio di tutoraggio attraverso cui gli alunni possono richiedere informazioni o spiegazioni al docente via email per un periodo pari a sette giorni solari dall'erogazione del corso.
- **Profilo FREM-2**: (formazione in differita) consiste nell'erogazione di un servizio di formazione attraverso una piattaforma accessibile via web, per un numero di alunni minore o pari a 100. Questo profilo di servizio prevede l'erogazione di materiale didattico in formato di documento di testo o presentazione con slide per un self training stimato di 8 ore. Il servizio comprende quindi la gestione della piattaforma, la

realizzazione del materiale didattico e un servizio di tutoraggio attraverso cui gli alunni possono richiedere informazioni o spiegazioni al docente via email per un periodo pari a trenta giorni solari dal giorno in cui il materiale didattico è stato reso disponibile agli alunni.

[R.306] La docenza inclusa nel servizio di formazione remota FREM-1 e FREM-2 deve essere erogata da un docente che abbia almeno 5 anni di esperienza nell'attività formativa relativamente alla specifica tipologia di servizio di supporto trattata. In alternativa, il docente deve aver progettato/gestito almeno 3 interventi formativi nella tematica nei tre anni precedenti alla contrattualizzazione del servizio.

6.2.2.1. Precondizioni e vincoli per la sottoscrizione del servizio FREM

[R.307] Al momento dell'acquisto del servizio di formazione remota, l'Amministrazione deve specificare a quale tipologia di servizio di supporto tale attività si riferisce (cfr. [R.271]).

[R.308] Le Amministrazioni possono acquistare il servizio di formazione remota, relativamente ad una specifica tipologia di supporto, se e solo se hanno acquistato almeno un servizio rispetto al quale la formazione fa riferimento.

[R.309] Il costo del servizio di formazione remota contribuisce al calcolo per la spesa totale massima sostenibile per i servizi di supporto, definita per ogni singola tipologia di servizio di supporto.

7. GESTIONE E MANUTENZIONE

[R.310] Il Fornitore del servizio è responsabile della gestione e della manutenzione di tutte le componenti del servizio erogato fino alla frontiera di responsabilità definita dal punto di accesso al servizio (PAS).

[R.311] Il Fornitore deve provvedere come parte integrante del servizio alle seguenti attività:

- attivazione e cessazione di nuovi servizi e delle relative componenti;
- installazione e configurazione degli apparati: il Fornitore deve garantire l'effettiva installazione degli apparati per la fornitura dei servizi acquistati dall'Amministrazione. Il Fornitore deve consegnare all'Amministrazione un inventario degli apparati installati. L'Amministrazione è responsabile di mettere a disposizione del Fornitore adeguati spazi e sottoservizi (es. alimentazione elettrica, condizionamento, ecc.) secondo quanto indicato dal Fornitore nelle attività di site Preparation (cfr.§ 9.3);
- installazione del software: il Fornitore deve farsi carico delle attività di installazione del software sugli apparati, compreso il caricamento e l'attivazione di nuove release software su tutti i sistemi utilizzati e l'aggiornamento software degli apparati per l'allineamento con i rilasci software messi a disposizione dai fornitori della tecnologia, sia con finalità di *patching* che relativamente all'introduzione dei nuovi servizi;
- attuazione degli adeguamenti, riconfigurazioni o ristrutturazioni richiesti da attività di "*system tuning*";
- trasloco interno, inteso come lo spostamento, all'interno della medesima sede dell'Amministrazione, nel caso in cui le esigenze operative dell'Amministrazione stessa lo richiedano, delle componenti tecnologiche utilizzate per l'erogazione del servizio, fermo restando la responsabilità dell'Amministrazione di mettere a disposizione del fornitore ambienti ed infrastrutture

di supporto adeguate a quanto previsto nelle specifiche riguardanti la predisposizione dei siti ("Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi" allegato all'originale Progetto dei Fabbisogni).

[R.312] La realizzazione delle attività di Trasloco di un servizio tra due sedi dell'Amministrazione (Trasloco Esterno), saranno realizzate e contabilizzate in maniera analoga ad una attivazione del servizio presso la nuova sede (in particolare quindi con la corresponsione di una nuova Una Tantum, se prevista) e una disattivazione presso la vecchia sede, fermo restando l'obbligo del Fornitore a garantire la piena operatività dell'Amministrazione in tutte le fasi del Trasloco, ad esempio:

- Permettendo la sostituibilità dei due servizi (ad esempio garantendo il riutilizzo degli Indirizzi IP statici della sede cessante nella nuova sede)
- Mantenendo attivo il servizio cessante fino alla completa attivazione del servizio nella nuova sede;
- Garantendo con adeguate procedure la possibilità di eseguire un Roll back dei servizi se si verificassero problemi nella transizione tra le due sedi.

[R.313] Le attività di gestione e manutenzione devono essere erogate all'interno della finestra temporale contrattualizzata dall'Amministrazione, a scelta tra quella standard (definita nel requisito [R.5]) o quella estesa (definita nel requisito [R.6]).

[R.314] Fermo restando la necessità di ridurre al minimo le interruzioni o ostacoli all'operatività dell'Amministrazione, il Fornitore può concordare con l'Amministrazione intervalli di "Manutenzione Programmata" preventiva, (ad es. al fine di realizzare necessarie attività di test, aggiornamenti di release software, ecc.). Nell'intervallo concordato per tali attività, eventuali malfunzionamenti del servizio non incideranno sul calcolo di SLA e Penali, purché il servizio sia completamente e correttamente ripristinato al termine dell'intervallo programmato.

[R.315] Il Fornitore, limitatamente alla propria infrastruttura di rete, deve disporre di un sistema, non necessariamente dedicato ai servizi SPC, basato su architetture e tecnologie standard di tipo SNMP, dedicato alla gestione delle

risorse utilizzate per erogare i servizi SPC. Attraverso tale sistema il Fornitore deve verificare in modo continuativo le prestazioni della propria infrastruttura di rete al fine di:

- gestire la rete, con monitoraggio puntuale di ogni servizio;
- valutare il grado di occupazione delle risorse trasmissive;
- verificare il corretto dimensionamento complessivo del sistema;
- consentire una verifica dei livelli di servizio contrattualmente stabiliti ed il calcolo di statistiche.

[R.316] Il Fornitore deve rendere disponibile alle Amministrazioni un help desk di 2° livello, che riceva segnalazioni di malfunzionamento esclusivamente dai centri di gestione di 1° livello della singola Amministrazione; tale help desk deve essere raggiungibile, per la ricezione di segnalazioni ed apertura di ticket, almeno nei seguenti modi:

- via pagina web, con accesso 24X7 365 giorni l'anno;
- via fax, con accesso 24X7 365 giorni l'anno;
- via call center contattabile attraverso Numero Verde, disponibile per ciascuna Amministrazione nell'orario della finestra per cui è stato contrattualizzato il servizio (finestra standard o estesa).

[R.317] L'help desk deve dare riscontro alla presa in carico della segnalazione di un disservizio con l'apertura di un trouble ticket, fornendo all'Amministrazione interessata il numero del ticket aperto e una prima diagnosi.

[R.318] Il Fornitore deve interfacciarsi costantemente con l'Amministrazione interessata durante le fasi di lavorazione di un trouble ticket, aggiornando l'Amministrazione sull'avanzamento dei lavori necessari alla risoluzione del disservizio segnalato, concordando preventivamente eventuali interventi presso le sedi dell'Amministrazione, e formalizzando tempestivamente la proposta di chiusura del ticket.

[R.319] **Sito Web del Fornitore.** Il Fornitore, fino alla disponibilità dei servizi di Governance di cui al par. 8.2, deve rendere accessibili, da parte di Consip, di AgID e dell'Amministrazione (per la parte di propria competenza), mediante Web Browser, le informazioni relative a:

- servizi utilizzati e dettagli amministrativi sui servizi;

- misurazioni dei livelli di servizio che includano almeno i dati oggetto di tutti i report periodici previsti;
- trouble ticket gestiti dall'help desk;
- dati di riscontro relativi ai SLA.

[R.320] Il sistema deve consentire alle singole Amministrazioni le seguenti funzionalità:

- consultazione diretta della Base Dati relativa alla risorse di rete di propria competenza tramite interfaccia grafica che consenta la generazione guidata di report, grafici, e query complesse;
- funzionalità di esportazione dei dati, secondo formati standard, contenuti nella porzione di Base Dati relativa alla risorse di rete di propria competenza.

[R.321] Il Fornitore deve a tal fine fornire credenziali di accesso (username e password) per la consultazione della Base Dati.

8. INFRASTRUTTURE CONDIVISE SPC

[R.322] In coerenza con quanto previsto all'art. 86 del CAD, la Commissione di Coordinamento SPC, nel disegnare uno scenario evolutivo, attraverso il documento "GdL6 – Definizione dei requisiti tecnici per la transizione, l'evoluzione ed il funzionamento delle Infrastrutture Condivise" ha stabilito ruoli e modalità di governance delle infrastrutture nazionali condivise, necessarie all'interoperabilità del framework SPC. In particolare il modello di ripartizione dei costi proposto, prevede una suddivisione tra:

- Amministrazioni aderenti ai Contratti Quadro SPC;
- Fornitori SPC e Community Network interconnesse.

[R.323] La quota parte dei costi a carico del Fornitore, è ripartita in tre voci:

1. una-tantum e canone mensile, (in linea con il valore di mercato del servizio di interconnessione dei NAP commerciali), per i nuovi servizi infrastrutturali assimilabili agli attuali servizi QXN (Interconnessione OPA e, qualora sottoscritto – facoltativo solo nel caso di Fornitore Assegnatario -, Interconnessione OPO);
2. una-tantum e canone mensile per i nuovi servizi di interoperabilità delle reti, non assimilabili agli attuali servizi QXN;
3. una percentuale variabile del fatturato annuo dei servizi consuntivati da ciascun Fornitore.

[R.324] Il valore massimo annuale della percentuale di cui al precedente punto 3 del requisito [R.323] è prestabilito, per ciascun anno di contratto, dalla seguente tabella:

Anno 1	Anno 2	Anno 3	Anno 4	Anno 5	Anno 6	Anno 7
0,00%	0,20%	0,50%	0,50%	0,50%	0,50%	0,50%

[R.325] Ogni anno AgID verificherà l'ammontare totale dei contributi percepiti dai Q-ISP SPC, rispetto ai costi delle Infrastrutture Condivise. Nel caso in cui l'ammontare dei contributi superi i costi sostenuti per le infrastrutture, AgID

procederà ad una riduzione del valore della percentuale di cui al precedente punto 3 del requisito [R.323] relativa all'anno successivo.

[R.326] Il Fornitore è obbligato alla sottoscrizione dei servizi IC-SPC appartenenti alle seguenti categorie:

1. Servizi di Interconnessione QXN;
2. Servizi di Governance.

8.1. SERVIZI DI INTERCONNESSIONE QXN

In continuità con i servizi di interconnessione erogati dalla Società Consortile Per Azioni SCPA-QXN, permette l'interconnessione tra Q-ISP SPC e/o tra soggetti sussidiari dotati di Community Network.

[R.327] Il Fornitore è obbligato alla sottoscrizione del Servizio di Interconnessione QXN (IQXN).

[R.328] Il Servizio di Interconnessione QXN è costituito (su un singolo nodo geografico) dai seguenti profili di servizio:

- il profilo *"Interconnessione QXN OPA":* realizza la funzionalità di trasporto del traffico OPA (Offerta per Amministrazioni) in modalità IP routing (liv.3 della pila ISO/OSI);
- il *profilo "Interconnessione QXN OPO":* realizza la funzionalità di trasporto del traffico OPO (Offerta per Operatori) in modalità L2 switching con tecnologia Ethernet (liv.2 della pila ISO/OSI).

[R.329] Il Servizio di Interconnessione QXN garantisce sia la funzionalità di Domain Name System (DNS), per la gestione dei nomi di dominio delle Amministrazioni afferenti all'SPC, sia la funzionalità di sorgente del tempo ufficiale di rete SPC (tramite protocollo NTP), mediante server sincronizzati al segnale temporale generato dall'Istituto Elettrotecnico Nazionale "Galileo Ferraris".

[R.330] Per garantire la comunicazione via Infranet alle Amministrazioni aderenti a SPC, il Fornitore è obbligato a sottoscrivere con il Gestore delle IC-SPC almeno due profili di servizio di "Interconnessione QXN OPA" (uno relativo al nodo di Roma e uno relativo al nodo di Milano), assumendo gli obblighi di interconnessione specificati nel documento esecutivo "Regole di Interconnessione QXN" che sarà allegato al Contratto Esecutivo tra il Fornitore e il Gestore delle IC-SPC.

[R.331] Il Fornitore, per ogni profilo di servizio "Interconnessione QXN OPA" sottoscritto, è obbligato ad installare a suo carico una coppia di apparati (vedi art 17 comma 2 DPCM 1 Aprile 2008) con funzionalità di Border Router OPA (BRopa), su cui convogliare il traffico OPA proveniente da e diretto verso le Amministrazioni attestate sulla propria rete SPC.

[R.332] I BRopa del Fornitore devono operare a livello di routing (Livello 3 OSI) e comunicare con gli apparati della QXN mediante sessioni E-BGP.

[R.333] Il Fornitore Assegnatario, che abbia stipulato il contratto esecutivo OPO è obbligato:

- a sottoscrivere due profili di servizio "Interconnessione QXN OPO" (uno relativo al nodo di Roma e uno relativo al nodo di Milano);
- ad installare a suo carico, per ogni profilo di servizio "Interconnessione QXN OPO", almeno un apparato con funzionalità di Border Router OPO (BRopo) (l'apparato può coincidere con uno degli apparari BRopa, purché utilizzi interfacce fisicamente distinte da quelle previste per l'interconnessione OPA), su cui convogliare tutto il traffico OPO da e per il Fornitore Aggiudicatario.

[R.334] Il Fornitore Aggiudicatario, in ciascuno dei due nodi fisici (Roma e Milano), è obbligato ad installare a suo carico una coppia di apparati con funzionalità di Border Router OPO (BRopo) (gli apparati possono coincidere con i BRopa, purché utilizzino interfacce fisicamente distinte da quelle previste per l'interconnessione OPA), su cui convogliare tutto il traffico OPO da e per i Fornitori Assegnatari che intendono attingere all'offerta OPO di quest'ultimo.

[R.335] I collegamenti tra i BRopo dell'Assegnatario, QXN e BRopo dell'Aggiudicatario devono essere realizzati in modalità bridged (Livello 2 OSI) in configurazione trunk (IEEE 802.1q) su ciascuna porta di interconnessione.

[R.336] Ciascuna VLAN deve trasportare il traffico relativo ad una VPN di una PA, realizzata in modalità OPO in parte sulla rete dell'Assegnatario ed in parte su quella dell'aggiudicatario

[R.337] Il traffico OPA pertinente il Fornitore non deve attraversare QXN (anche limitatamente alle componenti LAN esterne all'AS della QXN, ma di sua competenza) nel caso sia:

- traffico Intranet o Infranet tra sedi collegate alla rete dello stesso Fornitore;
- traffico che coinvolge un'Amministrazione ed un soggetto non collegato al SPC;

- traffico tra soggetti non collegati ad SPC.

[R.338] Altresì il traffico OPA del Fornitore deve transitare sui nodi della QXN ogniqualvolta le Amministrazioni coinvolte nello scambio siano connesse alle reti di due Fornitori Assegnatari differenti.

[R.339] La gestione e manutenzione degli apparati BRopo e BRopa è a cura del Fornitore.

[R.340] Le seguenti funzionalità non sono in carico al Fornitore poiché comprese nel Servizio di Interconnessione QXN erogato da IC-SPC:

- housing per l'alloggiamento degli apparati sopracitati utilizzati dai Fornitori Assegnatari SPC (esclusivamente ai fini dell'interconnessione con i nodi QXN);
- porte GigabitEthernet per l'interconnessione degli apparati di accesso dei Fornitori Assegnatari SPC ai nodi QXN.

Il canone dovuto a fronte della sottoscrizione per ciascuno dei profili di servizio "Interconnessione QXN" (IQXN) è riportato nella seguente tabella:

Listino servizi IC-SPC rivolto ai Fornitori SPC			
Servizi di Interconnessione QXN		UT	CM
IQXN	Interconnessione QXN OPA	22.902,00 €	1.527,00 €
IQXN2	Interconnessione QXN OPO	22.902,00 €	1.527,00 €

8.2. SERVIZI DI GOVERNANCE

[R.341] Per garantire la corretta governance dei Servizi SPC alle Amministrazioni aderenti, il Fornitore è obbligato a sottoscrivere con il Gestore delle IC-SPC, tutti i Servizi di Governance erogati dalle IC-SPC assumendo gli obblighi di interconnessione specificati nel documento "Regole di Interconnessione per l'adesione ai servizi di Governance" che sarà allegato al Contratto Esecutivo tra il Fornitore e il Gestore delle IC-SPC.

[R.342] I servizi di Governance, erogati tramite una piattaforma informatica facente parte delle Infrastrutture Condivise, sono costituiti da:

- Servizio di Gestione Automatizzata dei Contratti (SGAC)
- Servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS)
- Servizio di Gestione delle Escalation (SGES)
- Servizio di Gestione del Portale Web (SGPW)

[R.343] Il canone dovuto a fronte della sottoscrizione dei servizi di Governance è riportato nella seguente tabella:

Listino servizi IC-SPC rivolto ai Fornitori SPC				
Servizi di Governance		UT	CA	CM
SGAC	Gestione Automatizzata dei Contratti	11.260,00 €	9.008,00 €	751,00 €
SGQS	Gestione dei Dati di Qualità e Sicurezza	11.260,00 €	9.008,00 €	751,00 €
SGPW	Gestione del Portale Web	5.526,00 €	4.421,00 €	368,00 €
SGES	Gestione delle Escalation	10.219,00 €	8.175,00 €	681,00 €

8.2.1. Sottoscrizione del Servizio di Gestione Automatizzata dei Contratti

[R.344] Il Servizio di Gestione Automatizzata dei Contratti (SGAC) consente la gestione automatizzata dei contratti SPC, conterrà tutti i dati normativi, contrattuali e tecnici di ciascun Contratto Quadro e dei relativi Contratti Esecutivi (inclusi eventuali allegati) stipulati dalle Amministrazioni. Il servizio permette sia la gestione dei contratti stipulati che di quelli in corso di stipula da parte del Fornitore.

[R.345] A fronte della sottoscrizione del servizio SGAC, il Fornitore è obbligato a sottoscrivere con il Gestore delle IC-SPC gli obblighi di interconnessione specificati nel documento "Regole di Interconnessione per l'adesione ai servizi di Governance" che sarà allegato al Contratto Esecutivo tra il Fornitore e il Gestore delle IC-SPC, contenenti le regole per l'interconnessione per l'adesione ai servizi SGAC.

[R.346] Il servizio SGAC è soggetto nel tempo a revisione e ottimizzazioni da parte dell'AgID.

[R.347] Il Fornitore è obbligato ad aderire al servizio SGAC e a utilizzare il sistema CRUD (*Create, Read, Update e Delete*) messo a disposizione dal Gestore delle IC-SPC come unico strumento per la corretta e formale modellazione dei Piani dei Fabbisogni (da parte delle Amministrazioni) e dei Progetti dei Fabbisogni (da parte dei Fornitori) attraverso:

- Web Application: attraverso il Servizio di Gestione del Portale Web di IC-SPC, mette a disposizione le opportune viste e web form;
- Web Service: accesso alle funzionalità della piattaforma tramite web service.

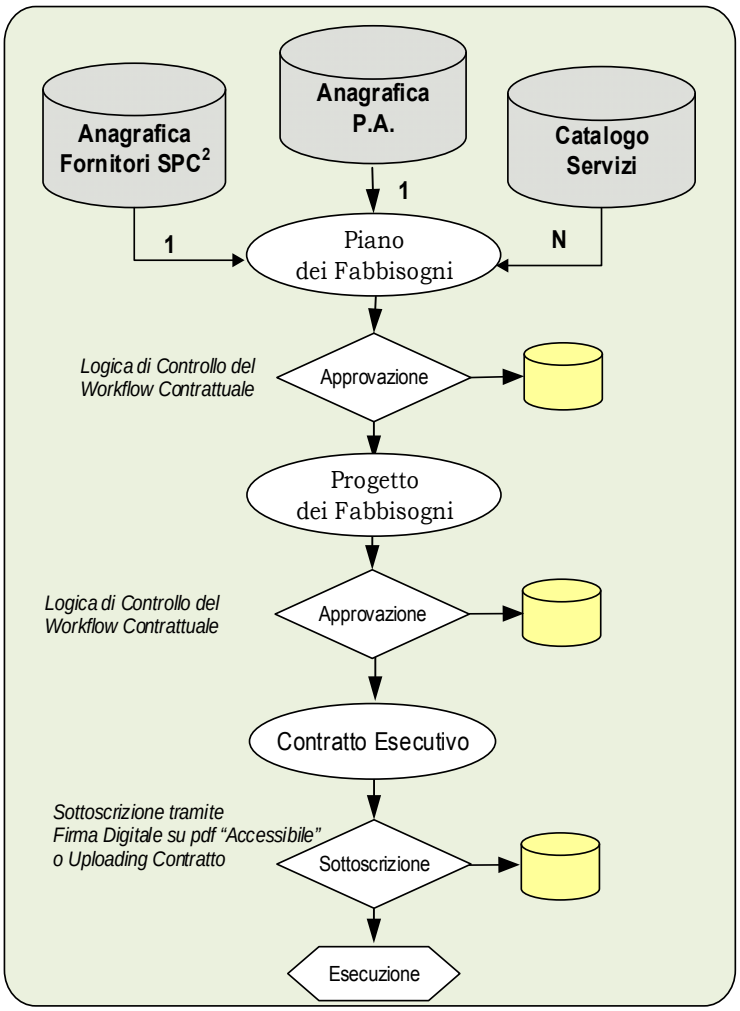
[R.348] Il Fornitore deve attenersi alle modalità di utilizzo di entrambe le interfacce secondo le regole descritte nel Manuale Operativo rilasciato dal Gestore delle IC-SPC.

[R.349] Il Servizio di Gestione Automatizzata dei Contratti consente l'interazione, attraverso interfaccia web, tra l'Amministrazione che ha aderito o intende aderire al SPC e il Fornitore, supportando tutte quelle funzionalità

necessarie alla realizzazione e sottoscrizione di un contratto esecutivo. In particolare il Fornitore deve:

- caricare sul sistema le informazioni relative alla propria anagrafica e a quella delle Pubbliche Amministrazioni con cui è sottoscritto un contratto esecutivo;
- compilare le webform relative al workflow di gestione "Piano dei Fabbisogni";
- compilare le webform relative al workflow di gestione dei "Progetto dei Fabbisogni", disponibili al Fornitore solo a valle dell'approvazione da parte dell'Amministrazione sul sistema stesso;
- gestire on line il Piano di Attuazione (sottoinsieme del Progetto dei Fabbisogni) e l'eventuale processo di migrazione dei servizi;
- sottoscrivere il contratto esecutivo tramite firma digitale o, in alternativa, effettuare l'upload del contratto sottoscritto dalle parti;
- gestire, con le opportune azioni correttive, gli allarmi generati su apposita dashboard dalla Logica di Controllo del Workflow Contrattuale (LWC) e generati dalle inconsistenze sui dati contrattuali inseriti.

[R.350] La seguente figura schematizza la sequenza logica che regola i legami tra le informazioni contenute nell'anagrafica degli utenti e fornitori, nei contratti esecutivi, piani e progetti dei fabbisogni:



8.2.2. Sottoscrizione del Servizio di Gestione dei Dati di Qualità e Sicurezza

[R.351] Il Fornitore è obbligato ad aderire al Servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS) al fine di garantire all'AgID il corretto monitoraggio della qualità e della sicurezza del SPC.

[R.352] A fronte della sottoscrizione del servizio SGQS, il Fornitore è obbligato a sottoscrivere con il Gestore delle IC-SPC gli obblighi di interconnessione specificati nel documento "Regole di Interconnessione per l'adesione ai servizi di Governance" che sarà allegato al Contratto Esecutivo tra il Fornitore e il Gestore delle IC-SPC, contenenti le regole per l'interconnessione per l'adesione ai servizi SGQS.

[R.353] La piattaforma informatica Dati di Qualità e Sicurezza (DQS) contiene i dati di qualità e sicurezza relativi ai *Key Performance Indicators* (KPI) di tutti i servizi erogati dai Fornitori SPC e i dati economici relativi ai KPI dei Fornitori SPC. Il Fornitore è obbligato ad utilizzare il sistema CMK (Caricamento Massivo dei KPI) per il caricamento massivo dei KPI sul DQS, attraverso:

- una interfaccia Secure File Transfer Protocol (SFTP);
- una interfaccia Web Service.

[R.354] Il Fornitore deve gestire, effettuando le opportune azioni correttive, gli allarmi inviati su apposita dashboard dalla Logica di Controllo della Corrispondenza dei KPI (LCCK) e generati dal non corretto caricamento dei dati sul DQS o dalla non conformità con quanto presente in AUC.

[R.355] Le strutture dati devono rispettare le specifiche ed il formato definiti all'interno del documento "Regole di Interconnessione per l'adesione ai servizi di Governance". A titolo di esempio si riporta il dettaglio di alcune strutture dati:

- KPI relativi ai singoli servizi SPC: data di inizio e data fine erogazione, quantità di componenti di servizio attive, disponibilità del servizio, Trouble Ticket associati e chiusi (con severità, causa disservizio e tempo di ripristino, ecc.);
- KPI economici relativi al Fornitore SPC: valore complessivo del contrattualizzato, valore complessivo delle penali su ciascun servizio, valore del fatturato annuale di ogni singolo contratto esecutivo, ecc.

8.2.3. Sottoscrizione del Servizio di Gestione delle Escalation

[R.356] Il Fornitore è obbligato ad aderire al Servizio di Gestione delle Escalation (SGES) al fine di permettere al Gestore delle IC-SPC di condurre le previste attività di escalation verso i soggetti SPC presso cui ha aperto un Trouble Ticket (TT) relativo ad un problema ancora insoluto.

[R.357] A fronte della sottoscrizione del servizio SGES, il Fornitore è obbligato a sottoscrivere con il Gestore delle IC-SPC gli obblighi di interconnessione specificati nel documento "Regole di Interconnessione per l'adesione ai

servizi di Governance" allegato al Contratto Esecutivo tra il Fornitore e il Gestore delle IC-SPC, contenenti le regole per l'interconnessione per l'adesione ai servizi SGES.

[R.358] L'infrastruttura informatica che realizza il servizio è integrata all'interno del Servizio di Gestione del Portale Web attraverso una web form e garantisce la registrazione e il tracciamento di tutti gli eventi di escalation relativi ai servizi di connettività e di sicurezza SPC.

[R.359] La piattaforma messa a disposizione del Prestatore delle IC-SPC permette la segnalazione da parte di un soggetto attestato alle IC-SPC di eventuali problematiche di connettività o di sicurezza che coinvolgono altri soggetti SPC attestati alle IC-SPC.

[R.360] La piattaforma garantisce la segnalazione, almeno tramite e-mail, ai soggetti interessati dall'evento di escalation.

8.2.4. Sottoscrizione del Servizio di Gestione del Portale Web

[R.361] Il Fornitore deve aderire al Servizio di Gestione del Portale Web (SGPW).

[R.362] A fronte della sottoscrizione del servizio SGPW, il Fornitore deve sottoscrivere con il Gestore delle IC-SPC gli obblighi di interconnessione specificati nel documento "Regole di Interconnessione per l'adesione ai servizi di Governance" allegato al Contratto Esecutivo tra il Fornitore e il Gestore delle IC-SPC, contenenti le regole per l'interconnessione per l'adesione ai servizi SGPW.

[R.363] L'infrastruttura informatica che realizza il Servizio SGPW è costituita da una piattaforma di Content Management System (CMS) in grado di gestire il ciclo di vita dei contenuti.

[R.364] L'infrastruttura gestisce le seguenti tipologie di utenze:

- *non autenticato*: utente generico del World Wide Web (WWW);
- *Fornitore SPC Connettività:* utente accreditato rappresentante un Fornitore SPC della presente gara;
- *Fornitore SPC Applicativi:* Fornitore SPC della gara Applicativa;
- *gestore PEC*: utente accreditato facente parte della struttura organizzativa di un gestore PEC;

- *Pubblica Amministrazione*: utente accreditato rappresentante una PA che ha aderito (o intende aderire) ai servizi SPC (soggetti di cui all'art. 75, comma 3-bis del d.lgs. 30 dicembre 2010 n.235);
- *soggetto sussidiario con Community Network:* utente accreditato facente parte della struttura organizzativa di una Regione o di qualsiasi altro soggetto sussidiario;
- *AgID*: utente accreditato rappresentante AgID;
- *CONSIP*: utente accreditato rappresentante CONSIP
- *CERT-SPC:* utente accreditato rappresentante la struttura organizzativa dell'AgID che ha la responsabilità del CERT-SPC.

[R.365] Il portale web è costituito almeno dalle seguenti aree di interesse per il Fornitore:

- *"Area informativa SPC":* contiene informazioni di carattere generale sul Sistema Pubblico di Connettività e Cooperazione (contesto normativo e tecnico, disposizioni della Commissione di Coordinamento, documentazione tecnico-operativa e contrattuale, ecc.); è visibile a tutte le tipologie di utenza, compresa quella non autenticata.
- *"Area Governance dei Servizi SPC per i Fornitori":* area accessibile dalle utenze di tipo "*Fornitore SPC Connettività*" e "*Fornitore SPC Applicativi"* contenente almeno: form per il caricamento dei documenti da pubblicare nell'Area Informativa SPC, form per la compilazione, variazione e la gestione dei Progetti dei Fabbisogni (configurazione di ciascun servizio e dettagli come indirizzo, data di attivazione, ecc.), form per la richiesta di approvazione dei Progetti dei Fabbisogni da parte della Pubblica Amministrazione contraente, informazioni sulle procedure di caricamento dati di qualità e sicurezza.
- *"Area Governance dei Servizi SPC per le PA"*: area accessibile alle utenze di tipo "*Pubblica Amministrazione"* contenente almeno: form per la compilazione e la variazione dei Piani dei Fabbisogni (solo quantitativa), form per l'approvazione o la richiesta di modifica dei Piani dei Fabbisogni, form per

l'approvazione dei Progetti dei Fabbisogni (attraverso l'inserimento della data di firma del contratto); l'elenco degli eventi di escalation tecniche e di sicurezza gestite tramite il Servizio di Gestione delle Escalation che riguardano i servizi della specifica PA; link per l'accesso ad altri servizi delle IC.

- *"Area Governance SPC"*: area accessibile dalle utenze di tipo "*AgID*" e *"Consip"* contenente almeno: la form per il caricamento dei documenti da pubblicare dell'Area Informativa SPC; form per l'approvazione o per la richiesta di modifica dei Progetti dei fabbisogni; reportistica personalizzata, cruscotti ed indicatori direzionali basati sui dati presenti nelle varie aree del sistema informativo di Governance; rappresentazione di dati storici e statistici (consistenza e caratteristiche tecniche dei servizi attivati, qualità del servizio, dati economici, ecc.).
- *"Area Reportistica dei Servizi SPC"*: area accessibile dalle utenze di tipo *"Fornitore SPC Connettività", "Fornitore SPC Applicativi", "Pubblica Amministrazione", "AgID", "Consip"* e *"CERT-SPC"*. Contiene almeno le seguenti informazioni: report statici e dinamici relativi ai dati della piattaforma "Anagrafica Unica dei Contratti"; report statici e dinamici relativi ai dati di qualità e sicurezza; reportistica delle penali dovute dai Fornitori SPC all'AgID, relative ai contratti quadro ed esecutivi; report statici e dinamici relativi ai valori economici dei contratti esecutivi sottoscritti da ogni singolo Fornitore SPC, con evidenza della capacità contrattuale residuale.
- *"Area Governance dei Servizi IC-SPC":* area accessibile dalle utenze di tipo *"Fornitore SPC Connettività", "Fornitore SPC Applicativi"* e *"soggetto sussidiario"*. Contiene le seguenti informazioni: form per il caricamento dei documenti da pubblicare nell'Area Informativa SPC; catalogo dei Servizi IC-SPC; form per la gestione automatica dei contratti sottoscritti tra il gestore dei servizi IC-SPC ed i Fornitori Assegnatari; form per la richiesta di intervento a IC-SPC per la risoluzione di escalation tecniche e di sicurezza attraverso il Servizio di Gestione delle Escalation.

- "Area Reportistica dei Servizi IC-SPC": area accessibile dalle utenze "Fornitore SPC Connettività", "Fornitore SPC Applicativi", "soggetto sussidiario", "AgID" e "CERT-SPC". Contiene report statici e dinamici su consistenza, utilizzo, qualità, sicurezza dei servizi IC-SPC erogati dal Prestatore delle IC-SPC ai Fornitori Assegnatari.
- *"Area Governance CERT-SPC"*: area accessibile unicamente al profilo *"Cert-SPC"*.

[R.366] Nella seguente tabella è riportato l'elenco delle Aree del portale web IC-SPC con le utenze che vi accedono.

	Utente non autenticato	**Fornitore SPC Connettività**	**Fornitore SPC Applicativi**	**PA**	**soggetto sussidiario**	**AgID**	**CONSIP**	**CERT-SPC**
Area informativa SPC	X	X	X	X	X	X	X	X
Area Governance dei Servizi SPC per i Fornitori		X	X					
Area Governance dei Servizi SPC per le PA				X				
Area Governance dei Servizi SPC						X	X	
Area Reportistica dei Servizi SPC		X	X	X		X	X	X
Area Governance dei Servizi IC SPC		X	X		X			
Area Reportistica dei Servizi IC SPC		X	X		X	X		X
Area Governance								X

CERT SPC								

9. MODALITÀ DI ATTIVAZIONE DEI SERVIZI

[R.367] Il Fornitore deve effettuare tutte le attività descritte nei paragrafi successivi sia nel caso di migrazione di un'Amministrazione da servizi preesistenti sia nel caso di realizzazioni ex novo.

[R.368] 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.

9.1. PIANO DEI FABBISOGNI

[R.369] 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.370] La redazione del "Piano dei fabbisogni" deve avvenire da parte dell'Amministrazione con l'eventuale ausilio del Fornitore, attraverso la compilazione delle webform relative al workflow di gestione dei "Piani dei Fabbisogni" messo a disposizione dai Servizi di Governance (cfr. § 8.2).

[R.371] Nelle eventuali more della realizzazione dei servizi di Governance, la consegna delle informazioni richieste al requisito precedente verrà realizzato tramite l'invio, mediante Posta Elettronica Certificata (PEC) ad una casella di PEC specifica del Fornitore. In questo caso sarà cura dell'Amministrazione con l'ausilio del Fornitore riportare le informazioni corrette all'interno dei webform succitati appena questi ultimi si rendano disponibili.

[R.372] Il Piano dei Fabbisogni riportato all'interno del SGAC (cfr. § 8.2) deve sempre mantenuto allineato con quanto richiesto dalle Amministrazioni. Tutte le eventuali variazioni devono essere riportate con quanto presente nel SGAC.

[R.373] 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.374] 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.

9.2. PROGETTO DEI FABBISOGNI

[R.375] Il Fornitore deve predisporre 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.376] Il “Progetto dei fabbisogni" deve contenere i seguenti allegati:

- “Progetto di Attuazione”: con il dettaglio, per ciascun servizio, di:
  - identificativo del servizio;
  - configurazione;
  - quantità (ove applicabile);
  - costi (una tantum e canone mensile come descritto nell’ Allegato 2);
  - indirizzo di dispiegamento (nel caso di servizi centralizzati riportare l’indirizzo della sede centrale);
  - data prevista di attivazione.
- “Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili”;
- “Piano di Attuazione”, articolato nei seguenti allegati:
  - “Piano operativo”;
  - “Documento programmatico di gestione della sicurezza dell’Amministrazione”;
  - “Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi”.

[R.377] La redazione del “Progetto di Attuazione” deve avvenire da parte del Fornitore attraverso la compilazione delle webform relative al workflow di gestione dei “Progetti di Attuazione” messo a disposizione dal SGAC (cfr. § 8.2).

[R.378] Ove l’Amministrazione esprima la necessità di tempi inferiori a quelli prescritti per la disponibilità dei servizi, Il Fornitore potrà offrire

all'Amministrazione servizi STDS nelle more della disponibilità dei servizi STDE o STDO richiesti. Di tale scelta dovrà essere data evidenza nel Progetto dei Fabbisogni. I servizi STDS saranno tariffati secondo quanto previsto all'Allegato 2.

[R.379] Nelle eventuali more della realizzazione dei servizi di Governance, la consegna delle informazioni richieste al requisito precedente verrà realizzato tramite l'invio, mediante Posta Elettronica Certificata (PEC) ad una casella di PEC specifica dell'Amministrazione. In questo caso sarà cura del fornitore riportare le informazioni corrette all'interno dei webform succitati appena questi ultimi si rendano disponibili.

[R.380] Il workflow per la gestione di uno specifico "Progetto di Attuazione" associato ad una specifica Amministrazione, è reso disponibile al Fornitore, solo a valle dell'approvazione da parte della stessa sul sistema messo a disposizione sul SGAC.

[R.381] Il "Piano di Attuazione" deve includere la descrizione dettagliata delle attività e procedure che il Prestatore metterà in atto nel processo di migrazione dei servizi, al fine di minimizzare l'impatto sull'operatività dei servizi erogati.

[R.382] Il "Progetto dei Fabbisogni" può essere modificato e/o aggiornato dall'Amministrazione ogni qualvolta questa lo ritenga necessario. In particolare, il processo di migrazione proposto deve essere concordato e sottoposto all'approvazione dell'Amministrazione oggetto di migrazione dei servizi.

[R.383] Il Fornitore deve inoltre fornire 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.384] L'Amministrazione approva il Progetto dei Fabbisogni mediante la stipula del Contratto Esecutivo OPA.

9.3. SITE PREPARATION

[R.385] Il Fornitore deve definire, all'interno del Progetto dei Fabbisogni (in particolare all'interno dell'allegato "Specifiche di dettaglio della realizzazione dei servizi AgID richiesti e specifiche di controllo della qualità degli stessi"), le specifiche riguardanti la predisposizione dei siti.

[R.386] Salvo ove specificamente definito, i servizi non comprendono attività di realizzazione e gestione delle infrastrutture di rete di proprietà dell'Amministrazione (cablaggio strutturato), LAN, fonia TDM e alimentazione presso i siti dell'Amministrazione.

[R.387] Su richiesta dell'Amministrazione, il Fornitore deve provvedere all'esecuzione di attività di posa in opera (cablaggi, apparati di condizionamento, ecc.) che si rendano necessarie per improcrastinabili esigenze realizzative, con un limite di spesa massimo di 5.000 € per sito, così come specificato all'interno del Contratto Quadro.

9.4. INSTALLAZIONE

[R.388] Il Fornitore deve definire, congiuntamente 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.389] Qualora un'operazione di installazione dovesse costituire causa di disservizio, il Fornitore deve adoperarsi per garantire un ripristino immediato della condizione preesistente.

[R.390] 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 (cfr. [R.377]). 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.

9.5. MIGRAZIONE

[R.391] 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.392] 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.393] 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.394] 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.395] 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 (SPC -2005) e di quelli forniti dal nuovo Fornitore dei Servizi di Connettività SPC. 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.396] 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 SPC ed Amministrazioni non ancora migrate, il Fornitore deve farsi carico della realizzazione dell'interconnessione tra la propria rete (SPC) e la QXN 2005.

[R.397] Per ciascuna sede oggetto di migrazione, il pagamento dei corrispettivi per la fornitura dei Servizi di Connettività SPC avrà decorrenza a partire dal 1° giorno del mese successivo alla data di collaudo positivo (verbale di collaudo) del servizio oggetto di migrazione.

10. COLLAUDI

Nel presente capitolo sono descritte tutte le procedure di collaudo che il Fornitore deve attuare ai fini della verifica della completa funzionalità dei servizi erogati.

10.1. PRESCRIZIONI GENERALI

[R.398] La fornitura dei servizi descritti nel presente capitolato tecnico deve essere soggetta alle seguenti procedure di collaudo:

- **Collaudo funzionale su piattaforma tecnica, test bed** (cfr. § 10.2): è svolto da CONSIP; il Contratto Quadro prevede delle prove mirate a verificare le modalità con le quali il Fornitore erogherà i servizi oggetto della presente gara.
- **Collaudo di configurazione** (cfr. § 10.3): è svolto dalla singola Amministrazione interessata; ogni contratto esecutivo stipulato tra il Fornitore e l'Amministrazione prevede delle prove mirate a verificare la corretta erogazione dei servizi acquisiti dall'Amministrazione attraverso la compilazione del "Piano dei fabbisogni dell'Amministrazione" (cfr. § [R.369]).

10.2. COLLAUDO FUNZIONALE SU PIATTAFORMA TECNICA (TEST BED)

[R.399] In seguito alla stipula del Contratto Quadro il Fornitore deve progettare e realizzare una piattaforma tecnica (Test Bed) al fine di consentire l'esecuzione di una prova di collaudo atta a verificare la conformità dei servizi erogati a quanto richiesto dal presente Capitolato Tecnico e ad eventuali modifiche concordate in corso d'opera nell'ambito del Comitato Operativo e/o del Comitato di Direzione Tecnica.

[R.400] Il Fornitore deve realizzare la piattaforma di test bed presso sedi individuate congiuntamente con CONSIP, strutturandola in modo tale da consentire l'esecuzione delle verifiche funzionali per tutti i servizi oggetto del Contratto Quadro. Il Fornitore deve fornire anche il personale necessario all'esecuzione delle prove.

[R.401] Il Fornitore deve consegnare a Consip un documento intitolato *"Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (test bed)"* contenente almeno:

- descrizione architetturale della piattaforma tecnica (test bed);
- elenco delle prove di collaudo, con particolare riferimento a:
  - servizi di trasporto;
  - servizi di sicurezza perimetrale;
  - servizi di comunicazione evoluta;
- sistema di misura dei livelli di servizio e di generazione della reportistica;
- funzionalità ed architettura del NOC/SOC del Fornitore;
- modalità di svolgimento delle prove di collaudo.

10.3. COLLAUDO DI CONFIGURAZIONE

[R.402] In seguito alla stipula del Contratto Esecutivo con la singola Amministrazione, il Fornitore deve supportare l'Amministrazione nell'esecuzione di una prova di collaudo "sul campo" atta a verificare la conformità delle caratteristiche di ogni singolo servizio contrattualizzato dall'Amministrazione:

- alle indicazioni contenute nel "Piano dei fabbisogni" redatto dalla singola Amministrazione (cfr. § [R.369]);
- al progetto del Fornitore descritto nel "Progetto dei fabbisogni" (cfr. § [R.375]);
- alle specifiche contenute nel presente Capitolato Tecnico;
- ai risultati delle verifiche su test bed (cfr. § 10.2).

[R.403] Il Fornitore deve consegnare all'Amministrazione un documento intitolato *"Specifiche di dettaglio delle prove di collaudo"* che descrive la tipologia delle prove di collaudo previste e la pianificazione temporale delle stesse.

[R.404] Le prove di collaudo devono verificare almeno:

- caratteristiche HW/SW e funzionalità dei sistemi installati;
- connettività end-to-end, se prevista dal servizio, e verifica della corretta implementazione delle CdS richieste nella sede;
- servizi di sicurezza implementati;
- rilevazioni sugli indicatori di qualità del servizio;
- procedure di fatturazione e rendicontazione.

[R.405] Il Fornitore deve altresì impegnarsi, qualora richiesto dall'Amministrazione, a svolgere ulteriori prove integrative. L'Amministrazione può procedere, a sua discrezione, ad un collaudo a campione.

11. DOCUMENTAZIONE DI RISCONTRO

Nel presente capitolo sono elencati i documenti che devono essere redatti e gestiti dal Fornitore.

[R.406] Il Fornitore deve inviare tutta la documentazione di seguito descritta in formato elettronico (almeno in formato .pdf). E' facoltà dei destinatari della documentazione richiedere l'invio della stessa anche in formato cartaceo.

[R.407] Tutta la documentazione tecnica relativa ai servizi di seguito descritta deve essere conforme alla norma UNI EN ISO 9004-2 ed in particolare deve 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:
  - 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.

11.1. DOCUMENTAZIONE RELATIVA AL CONTRATTO QUADRO OPA/OPO

[R.408] L'elenco della documentazione di riscontro che deve essere predisposta dal Fornitore in relazione alla propria struttura amministrativa e tecnica per l'erogazione dei servizi SPC è riportato nella tabella seguente con l'indicazione, per ciascun documento, dei contenuti di particolare interesse:

Documento di riscontro	Contenuto	Riferimento Capitolato Tecnico	Destinatario
Documento programmatico di gestione della sicurezza	• Descrizione delle misure organizzative (ruoli, responsabilità e procedure), tecniche (sistemi hw e sw impiegati) e fisiche adottate	N.A.	CONSIP e AgID
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.	CONSIP e AgID
Documentazione tecnica relativa all'erogazione dei Servizi di Trasporto Dati	• Caratteristiche degli apparati di terminazione dei servizi presso le sedi dell'Amministrazione: - Dimensioni di ingombro degli apparati e spazi complessivi necessari, comprese le aree di disimpegno per un'agevole ispezionabilità.	§ 3	CONSIP AgID e Amministrazioni che acquisiscono il servizio

	- Assorbimento di potenza misurato in kVA. - Caratteristiche del collegamento di terra necessario al corretto funzionamento dei sistemi. - Presenza eventuale del gruppo di continuità e di batterie e accumulatori. - Necessità o meno di condizionamento ambientale o di ventilazione forzata, indicando la dissipazione energetica. - Limiti di temperatura e di umidità relativa sopportati. - Modalità di interconnessione tra le parti, con indicazione di necessità o meno di pavimento sopraelevato. • Caratteristiche architetturali e tecnologiche degli accessi utilizzati (wired e wireless). • Descrizione dell'infrastruttura di rete utilizzata per l'erogazione dei servizi.		
Documentazione tecnica relativa alla funzionalità DNS	• Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio. • Tipologia e release del software utilizzato per erogare il servizio.	§ 3	CONSIP AgID e Amministrazioni che acquisiscono il servizio

Documentazione tecnica relativa ai Servizi di Sicurezza	• 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. • 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.	§ 4	CONSIP AgID e Amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa ai Servizi di Comunicazione Evoluta	• Descrizione delle soluzioni architetturali richieste. • Tipologia e caratteristiche tecniche dei sistemi hardware e software utilizzati per erogare il servizio. • Descrizione delle modalità di interfacciamento con la rete PSTN. • Protocolli utilizzati per la fornitura del servizio ed ulteriori protocolli supportati dalle apparecchiature.	§ 5	CONSIP AgID e Amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa a Gestione e Manutenzione	• Descrizione architetturale e funzionale del NOC/SOC. • 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	§ 7	CONSIP, AgID e Amministrazioni che acquisiscono il servizio

	servizio. • Caratteristiche architetturali, tecniche e funzionali del sito web, con descrizione della modalità con cui verrà gestito • Caratteristiche tecniche dei sistemi utilizzati per il call center, e criteri di dimensionamento delle risorse umane ad esso dedicate		
Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (test bed)	• Architettura del test-bed. • Elenco delle prove di collaudo.	§ 10.2	CONSIP

11.2. DOCUMENTAZIONE RELATIVA AL CONTRATTO ESECUTIVO OPA/OPO

Documento di riscontro	Contenuto	Riferimento Capitolato Tecnico	Destinatario
Progetto dei fabbisogni	• Descrizione della nuova rete della Amministrazione. • Piani di indirizzamento delle Amministrazioni. • Regole di traduzione di indirizzi (NAT) in rapporto con la QXN. • Dimensionamento dei servizi/accessi. • Modalità di attivazione dei servizi di connettività/sicurezza.	§ 9.2	Amministrazioni
Costi (parte integrante del Documento "Progetto dei fabbisogni")	• Dettaglio dei costi del progetto previsto dal Piano di Attuazione secondo quanto riportato nell'Allegato 2.	§ 9.2	Amministrazioni
Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili (parte integrante del Documento "Progetto dei fabbisogni")	• Formato degli Stati di Avanzamento o Servizi installati. o Esito dei collaudi effettuati. o Collaudi previsti nel mese successivo. o Varianti e modifiche emerse nel periodo. o Ritardi verificatisi nelle attivazioni rispetto alle	§ 9.2	Amministrazioni

	date previste nel Piano di Attuazione e cause. o Penali dovute per ritardi.		
Piano di Attuazione (parte integrante del Documento "Progetto dei fabbisogni")	• 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.	§ 9.2	Amministrazioni
Piano Operativo (parte integrante del Documento "Piano di Attuazione")	• Pianificazione temporale dettagliata (diagramma di Gantt delle singole attivazioni, schedulazione delle milestone principali, piano dei sopralluoghi, ecc.).	§ 9.2	Amministrazioni

Documento programmatico di gestione della sicurezza dell'Amministrazione (parte integrante del Documento "Piano di Attuazione")	• Descrizione delle misure organizzative (ruoli, responsabilità e procedure), tecniche (sistemi hw e sw impiegati) e fisiche adottate dal Fornitore in fase di erogazione dei servizi richiesti dall'Amministrazione.	§ 9.2	Amministrazioni
Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi (parte integrante del Documento "Piano di Attuazione")	• 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	§ 9.2	Amministrazioni

	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	• Tipologia di collaudo. • Elenco delle prove di collaudo. • Tempi dei collaudi.	§ 10.3	Amministrazioni