



Piano di Esecuzione dei Servizi

COMUNE DI COMO

Accordo Quadro

Servizi di Gestione e Manutenzione di sistemi IP e PdL

Edizione 1 – ID 2181 – Lotto 2

Richiesta Preliminare di Fornitura. N° 7125047

Indice

1.	PREMESSA	3
1.1	Glossario	3
1.2	Servizi richiesti dall'Amministrazione	3
2.	ASSESSMENT	5
3.	PIANO TECNICO ORGANIZZATIVO	6
3.1	Descrizione dei servizi erogati	6
3.2	Definizione tecnica dei servizi e delle modalità di erogazione	7
3.2.1	SERVIZI ON-SITE	7
3.2.2	SERVIZI EROGATI DA REMOTO	7
3.2.1	PUNTI DI CONTATTO	8
3.3	Personalizzazioni richieste dall'Amministrazione	9
3.4	Security By Design	9
3.5	Attività e tempistiche per l'avvio dei servizi	10
4.	PIANO ECONOMICO	11

Versioni del Documento

Versione	Resp. della Variazione	Data	Descrizione della modifica
1.0	Lorenzo Rossi	2 Marzo 2023	Prima versione

1. PREMESSA

Il presente documento contiene l'esatta definizione tecnica e gestionale dei servizi in risposta ai fabbisogni espressi dall'Amministrazione nella Richiesta Preliminare di Fornitura pervenuta in data 26/01/2023 nell'ambito dell'Accordo Quadro per i "Servizi di Gestione e Manutenzione di sistemi IP e PdL" stipulata tra la Consip S.p.A. e il Raggruppamento Temporaneo di Imprese costituito da

- Vodafone Italia S.p.A., mandataria;
- DXC Technology Enterprise Services Italia S.r.l., mandante;
- ITD Solutions S.p.A., mandante.

1.1 Glossario

Salva diversa esplicita indicazione, ai termini seguenti, riportati in ordine alfabetico, viene attribuito, ai fini del presente documento, il significato di seguito indicato.

TERMINE	DEFINIZIONE
PES	Piano di esecuzione dei servizi
AQ	Accordo Quadro
AS	Appalto Specifico
RTI	Raggruppamento Temporaneo di Imprese

1.2 Servizi richiesti dall'Amministrazione

In funzione delle informazioni fornite nella "Richiesta Preliminare di Fornitura" da codesta Amministrazione, nella tabella seguente è riportata una sintesi dei servizi oggetto del PES

Servizi	Centrale Telefonica	Rete Locale	Sicurezza	PdL	Server
Gestione	478	28	2	725	30
Manutenzione	478	28	2	725	
IMAC	-	-	-	80	-
Interventi sul Cablaggio	-	-	-	-	-
Presidio	1	-	-	2	-
Service Desk	25.500	-	-	62.200	-

Tabella 1 Servizi Oggetto del PES

Le sedi coinvolte nel progetto sono di seguito dettagliate:

Denominazione Sede	Indirizzo	Città
PALAZZO CERNEZZI	Via Vittorio Emanuele II 97	Como
COMANDO POLIZIA LOCALE	Viale Innocenzo	Como
SCUOLA MATERNA SANT'ELIA	Via Alciato	Como
ASILO AQUILONE	Via di Lora, 1	Como
ASILO BABYLANDIA	VIA PALESTRO 17	Como
ASILO FANTASIA	VIA ITALIA LIBERA 4	Como
ASILO GIROTONDO	VIA ZEZIO 27	Como
ASILO GIROTONDO	VIA PASSERI 2	Como
ASILO PANDA	VIA SEGANTINI 45	Como
ASILO PETER PAN	VIA LONGHENA 10	Como
BIBLIOTECA COMUNALE DI COMO	VIA PIAZZETTA VENOSTO LUCATI 1	Como
CENTRO DIURNO DISABILI	VIA DEL DOSS SNC	Como
CIMITERO MONUMENTALE MAGGIORE	VIA REGINA TEODOLINDA 74	Como
CIRCOSCRIZIONE 1-ALBATE	VIA SANTANTONINO 4	Como
CIRCOSCRIZIONE 4-CAMNAGO VOLTA	PIAZZA MARTIGNONI 2	Como
CIRCOSCRIZIONE 6-COMO BORGHI	VIA GRANDI 21	Como
CIRCOSCRIZIONE 7-COMO CENTRO	VIA COLLEGIO DEI DOTTORI 9	Como
CIRCOSCRIZIONE 8-MONTE OLIMPINO	VIA BELLINZONE 147	Como
CIRCOSCRIZIONE 8-SAGNINO	VIA SEGANTINI 2	Como
COMPLESSO DI VILLA OLMO	Via Simone Cantoni, 1	Como
INFORMAGIOVANI	VIA VITTORIO EMANUELE II 98	Como
MAGAZZINI VIA STAZZI	VIA STAZZI 3/5	Como
MUSEO CIVICO	PIAZZA MEDAGLIE D'ORO 1	Como
PINACOTECA-PALAZZO VOLPI	VIA DIAZ	Como
SCUOLA ELEMENTARE REBBIO	VIA GIUSSANI	Como
SEDE DISTACCATA POLIZIA LOCALE	VIA ODESCALCHI 13	Como

Tabella 2 Sedi Coinvolte nel Piano

I servizi definiti nel presente documento di PES hanno una durata di 48 mesi

2. ASSESSMENT

L'elenco completo delle consistenze come da Richiesta Preliminare di Fornitura e i dettagli degli apparati inclusi nel perimetro dei servizi sopra elencati è riportato nella tabella seguente

Ambito Tecnologico	Tipologia Apparato	Brand	Quantità
Rete Locale	Switch	Cisco	28
PdL	Desktop	Lenovo HP Dell Olivetti Altri Brand	585
	Laptop	ASUS Lenovo HP Toshiba ACER Altri brand	140
Centrali Telefoniche	Derivati telefonici	Cisco Yealink Panasonic Gigaset Samsung Sirio Snom	478
Server	Server Virtuali	VMware Microsoft Linux	30
Sicurezza	Firewall	Fortinet	2

Tabella 3 – Consistenze a perimetro del PES

3. PIANO TECNICO ORGANIZZATIVO

3.1 Descrizione dei servizi erogati

Il servizio di GESTIONE prevede:

- attività di gestione proattiva, ovvero rivolta alla prevenzione delle malfunzioni;
- attività di gestione reattiva, ovvero rivolta alla gestione ed alla risoluzione di tutte le malfunzioni che comportano interruzione o degrado nella fruizione del servizio, qualora non richiedano la sostituzione di parti guasti (intervento del servizio di manutenzione)
- identificazione della malfunzione, la sua documentazione, la gestione delle comunicazioni e dell'escalation e la risoluzione della malfunzione, anche attraverso l'attività di terze parti;
- l'analisi dei problemi ripetitivi. I risultati dell'analisi saranno inseriti in un database e sugli elementi interessati dovranno essere eseguiti controlli approfonditi atti ad individuare e risolvere problemi di tipo strutturale (processo di problem management);
- l'analisi delle informazioni derivanti dall'esecuzione delle attività di performance management nonché ricavate da serie storiche e in base a segnalazioni pervenute dai sistemi di gestione e di monitoraggio;
- la definizione, in base a valori stabiliti da norme tecniche, di valori di soglia oltre le quali sia necessario intervenire, da sottoporre all'approvazione dell'Amministrazione;
- l'effettuazione periodica di interventi di bonifica volti a salvaguardare il buon funzionamento di tutti i componenti oggetto del servizio e al recupero delle criticità evidenziate;
- supervisione e amministrazione della rete e gestione degli apparati, inclusiva di tutte le operazioni che servono per mantenere la rete di dati in operatività, quali ad esempio:
 - la supervisione dell'utilizzo delle risorse di rete e della loro assegnazione;
 - la gestione e configurazione degli apparati e dei servizi;
 - la distribuzione del software;
 - azioni e procedure orientate all'utilizzo ottimo delle risorse di rete;
- conduzione della rete, qualora non si renda necessaria la sostituzione di parti guaste (intervento del servizio di manutenzione), inclusiva di tutte le operazioni necessarie per gestire problemi e aggiornamenti quali ad esempio:
 - gestione dell'allarmistica e delle congestioni, inclusa la rilevazione e la risoluzione dei problemi;
 - supporto tecnico orientato alla risoluzione dei problemi tecnici degli apparati e degli upgrade di rete (patching di apparato, aggiunta/rimozioni di apparati, cambi di topologia) correttivi o preventivi che siano;
 - tutte le attività orientate alla attivazione, cessazione e modifica dei servizi e delle relative componenti;
- supervisione e amministrazione della sicurezza in rete, inclusiva delle azioni volte all'aggiornamento della rete e alla sua analisi, quali ad esempio:
 - analisi dei rischi di sicurezza;
 - controllo della robustezza delle procedure e delle soluzioni implementate;
 - aggiornamento e patching del software e degli apparati;
 - tutte le attività inerenti il costante aggiornamento delle componenti software/firmware dei sistemi/apparati all'ultima minor release disponibile sul mercato;
- logging e backup dei dati e delle configurazioni, inclusivi di attività quali ad esempio:
 - logging dei problemi e dei malfunzionamenti occorsi;
 - logging per l'auditing della sicurezza della rete e dei sistemi;
 - analisi delle prestazioni del servizio;
 - rendicontazione;
 - back-up dei dati di configurazione di tutti gli apparati di rete e salvataggio su area di memorizzazione predefinita con tempistica che non superi le 72 ore;

- gestione dell'indirizzamento IP secondo gli standard concordati con l'Amministrazione, la nomenclatura/indirizzamento dei server e dei posti di lavoro, nonché i parametri di configurazione e di QoS.
- è escluso il servizio di aggiornamento dei firmware alla major release.

Le attività di MANUTENZIONE possono riassumersi in:

- risoluzione della causa del guasto tramite:
 - intervento presso la sede per il quale è stato richiesto l'intervento;
 - sostituzione di parti finalizzate al recupero delle prestazioni iniziali dell'apparecchiatura;
 - ripristino del servizio sui livelli preesistenti al guasto/anomalia;
 - verifica dell'eliminazione della causa del guasto;
- aggiornamento della documentazione relativa;
- redazione del relativo "verbale di intervento".

Sono inclusi nel servizio anche gli interventi e gli oneri dovuti a guasti o malfunzionamenti causati da:

- sovratensione;
- sovracorrente;
- esaurimento batterie/accumulatori;
- sovratemperatura, anche dei locali.

mentre sono esclusi gli oneri dovuti a guasti o malfunzionamenti causati da:

- incendio per cause esterne e danneggiamenti da opere di spegnimento;
- allagamenti o inondazioni;
- furto;
- caduta di fulmini.

Come da accordi con l'Amministrazione gli interventi di manutenzione saranno eseguiti utilizzando parti hardware di ricambio messi a disposizione dall'Amministrazione stessa. Sono a carico dell'Amministrazione anche le licenze di supporto del vendor (es. licenze Forticare e FortiGuard su apparati a brand Fortinet, licensing server)

3.2 Definizione tecnica dei servizi e delle modalità di erogazione

3.2.1 SERVIZI ON-SITE

Il servizio proposto si basa prevalentemente su un presidio on-site presso le sedi dell'ente che verrà erogato nelle seguenti orari e modalità:

- 2 FTE in orario Base dal Lunedì al venerdì dalle 9 alle 18 (festivi esclusi)
- 1 FTE in orario Esteso dal Lunedì al venerdì dalle 8 alle 17, sabato dalle 8:30 alle 12:30 (festivi esclusi)

Il presidio avrà in carico tutte le attività on-site presso le sedi dell'Ente nonché i servizi di gestione di primo livello. Non è previsto intervento on-site da parte di personale diverso da quello di presidio. Al presidio si affiancheranno i servizi remoti descritti al paragrafo successivo.

Come da accordi rimangono a carico dell'Ente la fornitura di auto di servizio per spostamenti tra le sedi oggetti del Servizio e gli strumenti informatici (PC ed eventuale cellulare).

3.2.2 SERVIZI EROGATI DA REMOTO

SERVICE DESK

Il servizio in oggetto è raggiungibile telefonicamente mediante numero nero geografico da parte degli utenti finali dell'Ente (dipendenti o consulenti esterni dotati di PC o interno fisso) negli orari di copertura del servizio di presidio (dal lunedì al venerdì dalle 8 alle 18 e il sabato dalle 8:30 alle 12:30). Il servizio previsto eroga assistenza telefonica in ambito Postazioni di Lavoro e Centrali telefoniche come di seguito meglio dettagliato:

- Primo livello di supporto basato esclusivamente su FAQ. Non è previsto accesso diretto agli strumenti informatici dell'Ente ai fini di diagnostica e risoluzione del problema (es. accesso da remoto alla PdL o configurazione della centrale Telefonica), mentre dovrà essere a disposizione del Service Desk lo strumento di tracciamento dei Trouble Ticket.
- Supporto generale informatico ai dipendenti.
- Nel caso l'intervento del primo livello telefonico sia risolutivo, o la richiesta sia semplicemente di tipo informativo, l'operatore provvederà a tracciare e chiudere come "Risolto" la chiamata sul sistema di TT.
- Nel caso il primo livello basato su FAQ non sia risolutivo, il personale di Service Desk provvederà ad apertura di opportuno TT che sarà spacciato al personale di presidio o agli Amministratori IT dell'Ente (es. per richieste di autorizzazione all'accesso a sistemi informativi dell'Ente).

SUPPORTO SPECIALISTICO DI SECONDO LIVELLO IN AMBITO SERVER E SICUREZZA

Viene garantito un servizio di Supporto sistemistico remoto con copertura dal lunedì al venerdì dalle 8 alle 1, sabato dalle 8:30 alle 12:30 (festivi esclusi) da parte di personale specializzato nei seguenti ambiti:

- Sistemi operativi Linux
- Sistemi operativi Microsoft
- Servizi di gestione dell'infrastruttura informatica quali ad esempio, DNS, Active directory, file server
- Assistenza su programmazione di apparati di sicurezza Fortinet (Firewall e NAC)

Il servizio sarà ingaggiabile direttamente dai soli Amministratori IT dell'Ente o dal presidio. Per questo servizio si stimano 50 giornate di supporto annue.

Al fine della corretta esecuzione del servizio in oggetto, sarà cura dell'Amministrazione fornire adeguati strumenti di accesso da remoto alle infrastrutture interne oggetto del servizio (es. VPN) da parte dei tecnici di Vodafone Italia o dei propri subappaltatori (cfr. par. 3.4)

3.2.1 PUNTI DI CONTATTO

Il punto di contatto tra l'Amministrazione e il Centro di Gestione è il Contact Center/Service Desk, i cui riferimenti sono riportati nella tabella seguente, e avverrà tramite l'intermediazione dei Referenti Tecnici dell'Amministrazione mentre, per quanto concerne le attività inerenti alla gestione tramite Service Desk (se servizio acquistato), saranno direttamente gli utenti finali ad ingaggiare lo stesso.

Riferimenti Contact Center	
Contact Center Informativo	800810303 https://smconsip.service-now.com assistenzaqgm@vodafone.com
Contact Center Gestione e Manutenzione	800810303 SGM.assistentatecnica@vodafone.com
Service Desk utenti finali (cfr. par. 3.2.2)	Numero nero fornito in fase di avvio del servizio
Supporto remoto specialistico (cfr. par. 3.2.2)	Numero nero fornito in fase di avvio del servizio

Tabella 4 – Riferimenti Contact Center

3.3 Personalizzazioni richieste dall'Amministrazione

Vengono dettagliate di seguito le personalizzazioni ai servizi erogati.

Le risorse in presidio utilizzeranno gli strumenti di Trouble Ticketing, Service Management e CMDB indicati e messi a disposizione dall'Amministrazione

La reportistica periodica sarà prodotta attraverso i dati registrati e i tool messi a disposizione dall'Amministrazione.

Il servizio di presidio, in accordo con il cliente, potrà essere eventualmente erogato anche da remoto in modalità smart working.

Il servizio di presidio on-site si rende disponibile anche alla gestione del parco dispositivi mobili di proprietà dell'Ente in conformità alle indicazioni operative e agli strumenti informatici messi a disposizione dall'Amministrazione.

3.4 Security By Design

Vodafone Italia si caratterizza per un continuo orientamento all'innovazione, supportato da costanti investimenti, per creare servizi innovativi e competenze che integrano le nuove tecnologie di connettività, dalle soluzioni Cloud ed SD-WAN al 5G fino alle soluzioni di servizi gestiti, mantenendo sempre la Cybersecurity al centro di ogni evoluzione secondo un approccio di "Security by design".

Ai fini del presente progetto si evidenziano i seguenti principi fondamentali:

- Le persone di presidio opereranno su strumenti informatici messi a disposizione dell'ente
- Gli strumenti informatici di Trouble Ticketing saranno messi a disposizione dell'Ente
- Non si prevedono strumenti di accesso da remoto messi a disposizione di Vodafone. Eventuali accessi remoti verranno implementati dall'ente (es. VPN su vs. firewall)

Per tali ragioni i principi di sicurezza informatica applicati alla gestione del servizio saranno prevalentemente demandati alle policy previste e applicate dall'Amministrazione.

Ai fini del rispetto dei criteri di sicurezza informatica nell'ambito della gestione dei servizi oggetto di offerta Vodafone Italia (e i suoi subappaltatori) dichiara quanto segue:

- Si impegna ad adottare al proprio interno e a far adottare ai propri subappaltatori le procedure e politiche di sicurezza definite dall'amministrazione committente, con particolare riferimento alle modalità di accesso ai sistemi dell'amministrazione, all'hardening (esempio installazione di soluzioni di end point security) dei dispositivi utilizzati dal fornitore, alla gestione dei dati dell'amministrazione.
- Dichiara di essere certificata ISO/IEC 27001 e si impegna a mantenere tale certificazione per tutta la durata della fornitura.
- Si rende disponibile ad attività di auditing a carico dell'Amministrazione sui servizi a perimetro della presente offerta, secondo modalità concordate con Vodafone. Le risultanze di tali audit potranno essere comunicate all'Amministrazione.
- Si rende disponibile a verifiche da parte dell'Amministrazione direttamente o tramite terzi incaricati, in merito alla conformità della prestazione dei servizi rispetto a quanto stabilito nell'Accordo Quadro SGM e a quanto descritto nel presente Piano di Esecuzione.
- Dichiara che il personale che presterà il supporto operativo nell'ambito dei servizi di sicurezza possiede certificazioni su specifici aspetti della sicurezza.
- Dichiara di disporre di una struttura per la prevenzione e gestione degli incidenti informatici con il compito d'interfacciarsi con le analoghe strutture dell'amministrazione e con le strutture centrali a livello governativo.
- Si è dotata delle misure minime di sicurezza per limitare il rischio di attacchi informatici
- Garantisce il rispetto di quanto richiesto dalla normativa vigente in materia di sicurezza cibernetica, anche in riferimento ai contenuti del GDPR, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento come anche del rischio di varia

probabilità e gravità per i diritti e le libertà delle persone fisiche, e adottando procedure tecniche e organizzative volte alla gestione di eventuali violazioni di dati personali

- Si impegna ad usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati.
- Qualora subisca un attacco, in conseguenza del quale vengano compromessi sistemi del Committente da lui gestiti, si farà carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
- Si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE.
- Da' disponibilità a far parte di un Comitato di Direzione Tecnica, eventualmente aperto anche a soggetti terzi, che tratti il tema della sicurezza, sia nell'ottica di favorire la risoluzione di temi aperti sia per introdurre eventuali varianti al contratto per fronteggiare nuove minacce o altro.
- Condividerà le informazioni necessarie al fine di garantire il corretto monitoraggio della qualità e della sicurezza,
- Si impegna eventualmente a sottoscrivere una clausola di non divulgazione (NDA) sui dati e sulle informazioni dell'Amministrazione.
- Si impegna ad aggiornare le soluzioni e i servizi di sicurezza proposti dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato; che saranno conformi alle normative e agli standard di riferimento applicabili; e saranno adeguati nel corso del contratto, senza oneri aggiuntivi, alle normative che l'UE o l'Italia rilasceranno in merito a servizi analoghi.

3.5 Attività e tempistiche per l'avvio dei servizi

Di seguito si dettaglia la pianificazione prevista per le attività complessive – da remoto e on site - incluse nel Contratto di Fornitura che verrà attivato.

Per quanto non espressamente esplicitato in questo documento, si rimanda all'Accordo Quadro.

Come da accordi con l'Amministrazione l'avvio dei servizi è previsto entro 30 giorni solari, dalla disponibilità dei seguenti punti:

- Ordine di Fornitura su portale Consip
- Autorizzazione al subappalto da parte di CONSIP

4. PIANO ECONOMICO

I servizi del presente PES, erogati in accordo all'accordo Quadro in essere stipulata tra RTI e CONSIP, hanno un valore complessivo pari a **€ 273.787/anno**, per una durata univoca di **48 mesi**, per un totale di **€ 1.095.150 €** suddivisi tra Servizi a Canone e Servizi a Pacchetto. Il dettaglio e' riportato nel configuratore allegato al presente PES

Piano di Fatturazione

Per allineamento con la reportistica richiesta da Consip, la fatturazione avverrà con cadenza trimestrale seguendo il calendario solare (Gennaio, Aprile, Luglio, Ottobre). Si rimanda al piano di fatturazione di dettaglio che sarà concordato prima dell'avvio del servizio.

Ai fini della suddivisione dei servizi e degli importi fatturati nell'ambito del RTI, il 100% degli importi saranno fatturati all'Amministrazione da Vodafone Italia