DISCIPLINARE DI GARA PER L'AFFIDAMENTO DEI SERVIZI DI ASSISTENZA TECNICA E SUPPORTO SISTEMISTICO ALLE RISORSE DI RETE (FMSI)

ALLEGATO A _ CAPITOLATO TECNICO

1. Premessa

In considerazione del fatto che le attività operative federali sono svolte attraverso procedure informatizzate che prevedono l'uso quotidiano di un articolato insieme di risorse IT (apparati di rete, attrezzature hardware e specifici applicativi software), rivestono importanza strategica i servizi di supporto sistemistico e assistenza tecnica, ovverosia l'insieme delle attività tecniche erogate per la corretta ed efficiente gestione operativa del SIA (Sistema Informativo Aziendale) e per la manutenzione ordinaria degli apparati hardware che lo compongono.

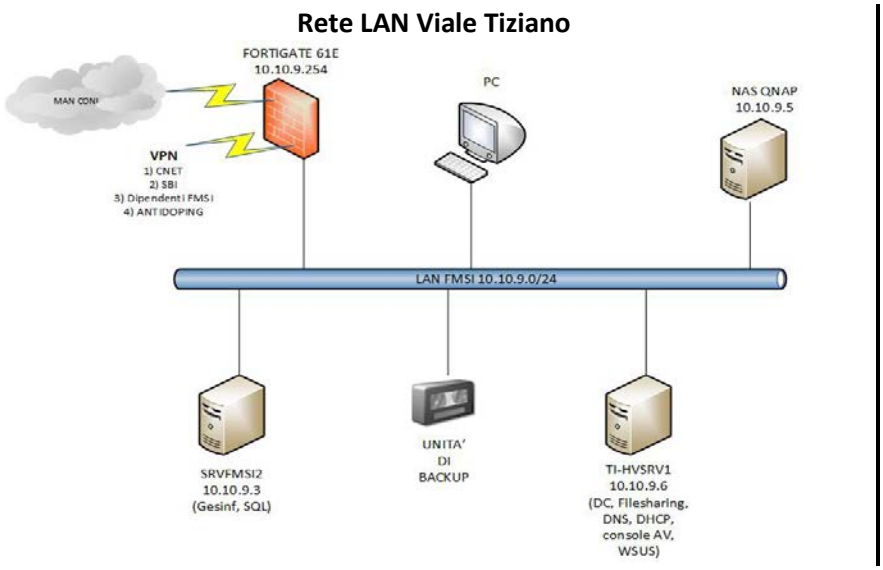
Parte fondamentale del servizio è l'assistenza e la manutenzione sistemistica per le configurazioni hardware e del software di base, al fine di conseguire i sotto indicati obiettivi:

- garanzia di elevate performance e maggiore continuità operativa agli utilizzatori finali dei sistemi informatici;
- rispetto di rigorosi standard di sicurezza e protezione dei dati;
- razionalizzazione dei costi di gestione.

2. Descrizione del sistema informativo federale

Il sistema informativo federale prevede le seguenti configurazioni hardware e del software di base:
. server (nr.2 server collocati nell'armadio rack sito negli Uffici FMSI del secondo piano del Palazzo FSN di Viale Tiziano 70);
. apparati di rete (firewall, switch, router);
. nas (nr.1 collocata nell'armadio rack sito negli Uffici FMSI del secondo piano del Palazzo FSN di Viale Tiziano 70);
. postazioni di lavoro e workstation (nr.17 PdL e nr.1 PC strumentale per la gestione del software di protocollazione e gestione informatica dei documenti).

Lo schema sottostante illustra il sistema LAN della FMSI, cui vanno aggiunte le postazioni di lavoro e le periferiche hardware, tutti posti sotto dominio.



Al riguardo occorre segnalare la peculiarità della Rete FMSI, che si configura come una Rete LAN "inglobata" nella più ampia Rete MAN del CONI, con la conseguente complessità della gestione dei flussi dei dati sia in uscita sia in entrata.

3. Elencazione dei servizi di assistenza tecnica e supporto sistemistico

È di seguito indicata un'esemplificazione dei servizi di supporto sistemistico e assistenza tecnica, distinti per specifica tipologia di intervento, richiesti dalla FMSI per assicurare il funzionamento corretto e senza soluzione di continuità delle risorse IT sopra descritte.

A. ASSISTENZA & SUPPORTO

Rientrano in questa area applicativa, a titolo esemplificativo, i seguenti servizi:

- Help desk, assistenza tecnica e supporto sistemistico per server, apparati di rete, postazioni di lavoro e workstation su piattaforme Microsoft, Apple e Linux
- Assistenza su reti wired e wireless, locali e geografiche, intranet, extranet e DMZ
- Attività sistemistiche per l'adeguamento dei requisiti minimi in materia di sicurezza e protezione dati
- Sostituzione, espansione, potenziamento di componenti hardware
- Aggiornamento di configurazione hardware/software e verifiche di compatibilità
- Implementazione di infrastrutture e soluzioni di protezione e salvataggio dati (storage & *disaster recovery*)
- Supporto per l'interfacciamento con i servizi di help desk per le applicazioni di terze parti

B. NETWORKING & CONNETTIVITÀ

Rientrano in questa area applicativa, a titolo esemplificativo, i seguenti servizi:

- Implementazione e gestione di firewall e network appliance
- Tunneling e VPN per l'interconnessione di sedi geografiche
- Accesso remoto verso la rete aziendale per collaboratori in mobilità e telelavoro
- Routing avanzato, source routing, bilanciamento del carico (NLB)
- Networking avanzato per la gestione delle priorità del traffico dati

C. SICUREZZA

Rientrano in questa area applicativa, a titolo esemplificativo, i seguenti servizi:

- Analisi delle non conformità e individuazione delle vulnerabilità, dello stato della sicurezza del sistema
- Implementazione di soluzioni per la sicurezza dell'architettura di rete e delle relative applicazioni, tra cui sistemi Anti Intrusione nelle reti informatiche (*Intrusion Detection System*)
- Implementazione di soluzioni per la sicurezza e protezione di ambiti di networking
- Verifica della validità delle procedure di backup e simulazione delle procedure di ripristino

D. INTERNET / INTRANET

Rientrano in questa area applicativa, a titolo esemplificativo, i seguenti servizi:

- Attivazione e gestione domini DNS
- Posta elettronica basata su Office365 con servizi AntiSpam e AntiVirus
- Networking e servizi di base con tecnologie basate DHCP, DNS e WINS
- Soluzioni e servizi stand-alone e centralizzati di sistemi antivirus e antispam
- Servizi di prossimità per risorse remote Server Proxy
- Gestione sistemi di distribuzione automatica degli aggiornamenti WSUS
- Autenticazione in ambiti di sicurezza misti Active Directory, LDAP, RADIUS

- Integrazione tra sistemi eterogenei in ambienti misti per i servizi di base e avanzati
- Gestione accounting, profili utente e Group Policies
- Accesso ad applicazioni remote, RDP, RemoteAPP, VNC
- Condivisione risorse documentali e di stampa
- Limitazione e gestione in quota degli archivi condivisi

E. MONITORAGGIO H.24 DEI PARAMETRI VITALI E FUNZIONALI

Rientrano in questa area applicativa, a titolo esemplificativo, i seguenti servizi:

- Monitoraggio remoto h24, con notifica automatica dello stato dei parametri vitali e funzionali, sia a livello hardware sia a livello software, di server e apparati di rete
- Sistemi automatici di notifica sullo stato di servizi e risorse *business critical*
- Sistemi automatici di notifica sullo stato di esecuzione dei backup
- Servizi centralizzati per l'automazione, la distribuzione e l'installazione degli aggiornamenti di sistema e degli applicativi software resi disponibili da parte dei produttori (*hotfixing*)
- Progettazione di procedure di *disaster recovery* e continuità operativa
- Assistenza di operatori specializzati in caso di recupero dei dati (attività straordinaria)

4. Elaborazione dell'offerta tecnica

Ai fini della valutazione della qualità e completezza dei servizi offerti, l'offerta deve essere redatta secondo la struttura di cui al precedente punto 3, con elencazione dettagliata dei servizi resi distinti per specifica area applicativa di intervento.

L'offerta tecnica deve, inoltre, indicare a) tipo di software antivirus e firewall consigliati, descrivendone feature principali e vantaggi tecnici; b) soluzioni di back-up & restore che si ipotizza di attuare, descrivendone modalità e articolazione.

L'offerta tecnica deve altresì specificare gli SLA (Service Level Agreement) ai fini dell'erogazione dei servizi precedentemente descritti e la conseguente risoluzione delle criticità segnalate da FMSI, distinguendo i seguenti SLA:

1) per interventi in teleassistenza:
o presa in carico della segnalazione in caso di problemi bloccanti;
o presa in carico della segnalazione in caso di problemi non bloccanti;
2) per interventi on site anche con richiesta di sostituzione di componenti hardware danneggiale:
o presa in carico della segnalazione.

Ai fini della valutazione della qualità e completezza del complesso dei profili proposti, l'offerta tecnica deve contenere una descrizione e relativo dimensionamento del team di supporto dedicato a svolgere i servizi richiesti, corredato dai Curricula Vitae (di seguito CV) anonimi dei profili professionali.

Al tal riguardo si segnala che, tenuto conto delle specificità dell'ambito in cui opera la FMSI e la conseguente riservatezza di alcune categorie di dati, la FMSI preferirà un team ristretto e skillato.

Ai fini della valutazione del livello di esperienza consolidata, l'offerta deve indicare, tra l'altro, le eventuali certificazioni attive (sia di struttura che sui profili individuali) e un portfolio di progetti realizzati.