PR26INF020 | Lotto 1 - Procedura aperta sopra soglia comunitaria indetta su piattaforma telematica eAppaltiFVG, ai sensi dell'art. 71 D.lgs. n. 36/2023, per l'affidamento della fornitura in modalità "SaaS" del servizio Teamviewer One Advanced comprensivo di manutenzione e assistenza per la durata di 36 mesi per la manutenzione e le necessità di gestione della continuità operativa dei dispositivi desktop e mobile dell'Azienda Sanitaria Universitaria Friuli Centrale.

RDO TENDER: tender_87709- RdO: rfq_120970

CAPITOLATO TECNICO

Sommario

1. OGGETTO DEL CAPITOLATO

Il presente documento disciplina la fornitura in modalità "SaaS" per un periodo di 36 mesi eventualmente rinnovabile per un periodo di 24 mesi, della piattaforma denominata "TeamViewer One Advanced" per le esigenze di supporto remoto, assistenza tecnica e gestione dei dispositivi della SOC TICeAD dell'ASU FC.

2. OBIETTIVI

All'interno di un percorso di miglioramento e analisi dei processi aziendali ed in ottemperanza a direttive e normative nazionali ed europee in materia di cybersecurity, data protection e cloud migration, l'ASU FC mediante l'acquisizione della piattaforma oggetto di fornitura si pone l'obiettivo di garantire, attraverso l'utilizzo di un'unica piattaforma affidabile e scalabile, la gestione e l'assistenza remota di tutti i sistemi IT e OT, con tempi di intervento ridotti, tracciabilità completa e piena conformità alla Direttiva NIS2. A tal fine, la piattaforma deve garantire:

1. la piena integrazione con la piattaforma "ServiceNow" (in uso presso la SOC Tecnologie Informatiche della Comunicazione e Agenda Digitale di ASU FC quale CMDBS, sistema di ticketing, etc.) consentendo avvio delle sessioni remote dai ticket, registrazione automatica degli eventi nella scheda incidente, sincronizzazione dei log e utilizzo delle API TeamViewer;
2. l'integrazione nativa con l'ecosistema Microsoft Entra ID, supportando protocolli di autenticazione Single Sign-On (SSO) via SAML 2.0 o OpenID Connect. Deve inoltre permettere l'applicazione di policy di Conditional Access, supportare il provisioning automatico degli utenti tramite standard SCIM e assicurare la piena interoperabilità dei log di audit con i sistemi di monitoraggio e governance Microsoft.

3. STATO DELL'ARTE DEL SISTEMA ESISTENTE

Allo stato attuale in ASUFC trova impiego la soluzione denominata "ManageEngine Remote Access Plus" per l'assistenza remota delle postazioni di lavoro; detto sistema è installato su 2 server on-premise: uno dedicato al database e uno all'application che verrà dismesso quando la piattaforma oggetto della presente fornitura risulterà pienamente operativa.

4. CARATTERISTICHE DEL SISTEMA RICHIESTO

Il sistema richiesto consiste in una soluzione di connettività remota e monitoraggio degli endpoint di classe Enterprise (TeamViewer ONE Advanced), basata su architettura cloud SaaS (Software as a Service), progettata per garantire il supporto tecnico, l'amministrazione di sistema e il controllo degli asset IT in ambienti distribuiti di ASU FC e della SOC Tecnologie Informatiche della Comunicazione e Agenda Digitale (di seguito SOC TICeAD).

L'offerta deve coprire le seguenti necessità dell'ASUFC:

- **8500 dispositivi** con sistemi operativi Windows (incluso Windows Server), macOS,

Linux, Android e iOS, garantendo l'accesso "attended" (con autorizzazione utente) e "unattended" (accesso server/PC senza presidio) e almeno 100 tecnici che dovranno/potranno usare la piattaforma con varie tipologie di abilitazioni.

- **1 TeamViewer Integrations Addon Enterprise** che deve consentire l'interoperabilità nativa tra la piattaforma di controllo remoto e i sistemi di gestione aziendale in uso (es. ServiceNow), al fine di ottimizzare i flussi di lavoro del Service Desk e ridurre i tempi medi di risoluzione (MTTR) utilizzando queste caratteristiche:
    - Sessione Integrata:
        - One-Click Remote Support: Capacità di generare e avviare una sessione di supporto remoto direttamente dall'interno di un ticket di assistenza o da un'anagrafica cliente, senza necessità di inserire manualmente ID o password;
        - Sincronizzazione Automatica dei Log: Al termine di ogni sessione remota, il sistema può popolare automaticamente il ticket di riferimento con i dettagli della connessione (durata, operatore, note di sessione) per finalità di audit;
        - Notifiche In-App: Supporto per l'invio di inviti alla sessione tramite chat integrate o commenti nel ticket, migliorando l'esperienza dell'utente finale;
    - Sicurezza e Accesso:
        - Mantenimento della Crittografia: L'integrazione deve preservare i protocolli di sicurezza nativi (AES-256) e non deve richiedere l'apertura di porte supplementari sui firewall aziendali;
        - Single Sign-On (SSO): Coerenza delle credenziali tra la piattaforma ospite e TeamViewer per garantire un accesso fluido e sicuro agli operatori.
- **1 Conditional Access Standard Router** che deve fornire un livello di sicurezza "Zero Trust" per la rete aziendale, consentendo agli amministratori IT di definire, gestire e applicare regole di accesso granulari per tutte le connessioni remote, sia in entrata che in uscita con queste modalità:
    - Architettura di Controllo (Dedicated Router):
        - Isolamento del Traffico: La soluzione deve prevedere l'instradamento del traffico di controllo remoto attraverso router dedicati e certificati (Standard Router), garantendo che nessuna connessione possa bypassare le policy di sicurezza aziendali;
        - Firewall Logico: Capacità di bloccare preventivamente qualsiasi tentativo di connessione che non provenga da account o dispositivi esplicitamente autorizzati a livello di console centrale;
    - Gestione Granulare delle Policy:

      Il sistema deve permettere la creazione di regole basate su:
        - Account Utente/Gruppi: Autorizzare solo specifici tecnici o gruppi (es. Amministratori di Sistema) a connettersi a determinati asset;
        - ID Dispositivo: Restringere l'accesso solo a dispositivi aziendali censiti,

impedendo l'uso di computer privati o non autorizzati;
        - Indirizzi IP / Reti: Limitare le sessioni di controllo remoto a specifici range di indirizzi IP (es. solo dalla sottorete del Data Center o dalla VPN aziendale);
        - Tipo di Funzionalità: Possibilità di disabilitare specifiche funzioni (es. Trasferimento File, Stampa Remota, Appunti condivisi) per determinati profili di accesso;
    - Sicurezza e Conformità (Audit):
        - Prevenzione Accessi Non Autorizzati: Blocco totale di qualsiasi ID TeamViewer esterno all'organizzazione che tenti di collegarsi ai computer interni;
        - Reportistica Centralizzata: Registrazione di ogni tentativo di accesso (autorizzato o negato) con dettagli su mittente, destinatario, timestamp e policy applicata.
- **1 TeamViewer Mobile Device Support** che abilita le funzionalità di ricezione assistenza e controllo remoto per la flotta di dispositivi mobili aziendali (smartphone e tablet), garantendo il supporto tecnico centralizzato indipendentemente dalla localizzazione fisica del dispositivo che garantisce le seguenti specifiche:
    - Compatibilità Multi-Piattaforma:
        - Supporto Android: Capacità di controllo remoto completo (interazione con i tocchi e le app) per i principali produttori (es. Samsung, Google, Sony, LG) tramite l'installazione di Add-on specifici o l'integrazione con le API del produttore;
        - Supporto iOS (iPhone/iPad): Capacità di visualizzare lo schermo in tempo reale tramite la funzione "Screen Recording" nativa di iOS, permettendo al tecnico di guidare l'utente nelle configurazioni.

5. SERVIZI RICHIESTI

La fornitura dovrà comprende anche il servizio denominato "**TeamViewer Tier 3 Professional Services**" per il supporto specialistico di alto livello (Tier 3), erogato da Solution Engineer certificati, finalizzato alla progettazione, implementazione e ottimizzazione della piattaforma TeamViewer ONE Advanced all'interno dell'infrastruttura IT della SOC TICeAD.

6. CLASSIFICAZIONE DELLE PRIORITA' e SLA

Requisito minimo di disponibilità del sistema è del 99,9% su base mensile, per il calcolo dell'uptime si devono escludere le manutenzioni programmate, comunicate con almeno 48 ore di preavviso.

Presa in carico dei ticket "Critici" (es. console inaccessibile, o comunque bloccante per il lavoro di ASUFC) entro 2 ore naturali consecutive e risoluzione entro 4 ore naturali consecutive, per i restanti ticket entro 4 ore lavorative e risoluzione entro 48 ore naturali consecutive.

7. PIANO ESECUTIVO E CRONOPROGRAMMA

È richiesto all'operatore economico di produrre e presentare nella documentazione tecnica un cronoprogramma (diagramma di Gantt) con il dettaglio delle attività necessarie ad implementare, configurare, installare, testare, collaudare ed avviare il nuovo Sistema, "chiavi in mano" a beneficio dell'ASU FC e dell'ufficio competente.
Il cronoprogramma dovrà tener conto delle seguenti fasi:

- Progettazione (Design):
  - Architettura delle Policy: Definizione e configurazione guidata della struttura dei gruppi, delle gerarchie di permessi (RBAC) e delle policy di sicurezza centralizzate;
  - Configurazione Conditional Access: Supporto specialistico per l'implementazione del "Conditional Access", inclusa la configurazione dei router dedicati e l'integrazione con il firewall aziendale;
- Integrazione Sistemi:
  - Integrazione AD/SSO: Supporto alla configurazione del Single Sign-On (SAML 2.0) e alla sincronizzazione automatica degli utenti tramite Entra ID di Microsoft;
  - Workflow Custom: Consulenza per l'attivazione e il testing delle integrazioni con sistemi di terze parti (es. ServiceNow, Microsoft Intune) e l'utilizzo delle API per automazioni personalizzate;
- Deployment e Roll-out:
  - Strategia di Distribuzione: Supporto alla creazione di pacchetti MSI personalizzati (Host/Full Client) per l'installazione massiva tramite sistemi di distribuzione software (es. SCCM);
- Trasferimento di Conoscenza (Enablement):
  - Workshop Tecnico: Sessioni di approfondimento rivolte agli amministratori di sistema di ASU FC per il passaggio di consegne e la gestione autonoma della piattaforma;
  - Best Practices: Fornitura di linee guida per l'ottimizzazione delle performance e della sicurezza a lungo termine.

Si richiede che tutte le fasi sopraelencate vengano completate entro 30 giorni dal primo incontro tecnico che sarà oggetto di adeguata verbalizzazione.
Il numero totale di giorni necessari per l'espletamento delle suddette attività dovrà essere reso ben visibile nel documento che verrà allegato al fine di consentire la valutazione tecnica inerente le tempistiche del cronoprogramma.

8. COLLAUDO

L'Operatore economico Aggiudicatario acquisirà il diritto al pagamento del canone a partire dalla data di collaudo positivo della piattaforma oggetto di fornitura, e tale data segnerà l'inizio del periodo contrattuale di fruizione della piattaforma stessa.
In fase di collaudo del sistema verranno eseguite tutte le verifiche necessarie ad appurare che tutte le funzionalità richieste dal presente Capitolato tecnico (ad es. Remote Management, Mobile

Support) operino secondo i requisiti richiesti. Nel caso in cui le verifiche di cui sopra diano esito negativo l'Operatore economico Aggiudicatario sarà chiamato a risolvere tempestivamente, e senza alcun onere aggiunto per ASU FC, ogni mancato funzionamento e difformità rilevata e, solo dopo la completa e definitiva risoluzione di tutte le non conformità, il collaudo si intenderà concluso con esito positivo.

9. FORMAZIONE E AVVIAMENTO

L'Attività di formazione dovrà essere strutturata in sessioni distinte per profili utente, erogate da personale certificato dal produttore:

- Sessione Amministratori (IT Admin): Configurazione della Management Console, gestione del Single Sign-On (SSO), impostazione delle policy di sicurezza e permessi (condizionali), gestione della rubrica centralizzata e configurazione dei connettori API.
- Sessione Operatori (Service Desk): Gestione delle sessioni di controllo remoto, utilizzo della coda di assistenza (Service Queue), modalità di accesso non presidiato (Unattended Access) e utilizzo degli strumenti di collaborazione (chat, file transfer, registrazione sessioni).
- Reporting e Audit: Formazione specifica sull'estrazione dei log e sulla reportistica per la conformità normativa e il monitoraggio dei KPI di servizio.

Affiancamento e Avviamento

Il servizio di affiancamento (minimo 5 giorni) dovrà includere il supporto alla configurazione iniziale dell'ambiente (Setup & Provisioning), garantendo in particolare:

- Supporto al deployment massivo dei client sugli endpoint tramite pacchetti MSI/GPO.
- Configurazione dei criteri di sicurezza in linea con le policy dell'ASU FC.
- Assistenza diretta durante le prime sessioni di assistenza reale verso gli utenti finali per la risoluzione di eventuali criticità di connettività o permessi.

A completamento dell'attività, l'operatore economico dovrà fornire:

- Manuali operativi in lingua italiana in formato digitale.
- Eventuali registrazioni delle sessioni di formazione ad uso interno.
- Un piano di formazione aggiornato in caso di rilascio di major update per tutta la durata contrattuale.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: LADI DE CET
CODICE FISCALE: DCTLDA72M10D530W
DATA FIRMA: 24/04/2026 13:32:34
IMPRONTA: 1A63AF83B3080FEF90B04B46A3E16504B39DA4C73B535B237259C4F7DF83D414
B39DA4C73B535B237259C4F7DF83D414FEA237EF69DF9FB5E9BF82A98C105691
FEA237EF69DF9FB5E9BF82A98C1056912A14037109545BED5AD95628B51F3F02
2A14037109545BED5AD95628B51F3F022D7FE6280C2C9A1504A428897B376C40