CNAO
Centro Nazionale di Adroterapia Oncologica

Via Erminio Borloni, 1 27100 PAVIA
Tel. 0382 0781 – www.cnao.it

Numero	*Data*	*Rev.*	*Pagina*
DOC-IC-SB-GEN-00382	04/08/2026	0	1 di 13

Documento tipo / Document type

SPECIFICA TECNICA

Titolo / Title

TC – Manutenzione e servizio di assistenza tecnica

Autori (CNAO se non diversamente indicato) / Authors (CNAO if not differently indicated)

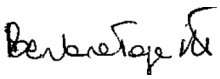
Referente / Contact person

Barbara Tagaste

Parole chiave / Keywords

Apparecchiature di diagnostica TC – ASSISTENZA TECNICA E MANUTENZIONE

Riassunto / Abstract

Emesso / Compiled	*Verificato / Controlled*	*Verificato / Controlled*	*Approvato / Approved*
Federico Bello	**Barbara Tagaste**	/	**Maria Rosaria Fiore**
		/	

LISTA DI DISTRIBUZIONE / DISTRIBUTION LIST			
#	*Data / Date*	*Nome / Name*	*Ditta / Society*

ELENCO DELLE VARIAZIONI / HISTORY OF CHANGES			
Ver.	*Data / Date*	*Pag.*	*Descrizione / Description*
0	04/08/2026	13	Prima emissione

INDICE

1 CONTESTO

Il Centro Nazionale di Adroterapia Oncologica (CNAO) di Pavia è una struttura sanitaria accreditata che eroga prestazioni di radioterapia con adroni per la cura delle patologie tumorali in regime di convenzionamento con il SSN e in regime privato.

Il Centro è di proprietà della Fondazione CNAO ed è situato in Via Erminio Borloni 1, 27100 a Pavia.

2 OGGETTO

Il presente Capitolato ha ad oggetto il servizio biennale (2 anni) di assistenza tecnica e manutenzione, come declinato al paragrafo 3, per l'apparecchiatura indicata nella tabella sottostante.

LOTTO	**Produttore**	**Data Collaudo**	**Modello Apparecchiatura**	**Componenti/ Accessori**
1	Siemens Healthcare srl	18/11/2009	n.1 **TOMOGRAFO COMPUTERIZZATO, SOMATOM Sensation Open**, comprensiva di accessori	Allegato 1, Allegato 2.

3 SERVIZIO DI ASSISTENZA TECNICA E MANUTENZIONE DEL SISTEMA CT SOMATOM SENSATION OPEN CON WORKSTATION (CONSOLE DI COMANDO) E SOFTWARE ESISTENTE.

L'apparecchiatura oggetto del servizio è dichiarata dal produttore EOS (*End of Support*) dal 1° Gennaio 2024.

L'Aggiudicatario dovrà assicurare tutti i servizi di assistenza tecnica necessari per la manutenzione ordinaria e straordinaria secondo la presente specifica tecnica e le eventuali modalità e condizioni migliorative indicate nell'offerta tecnica.
Durante tutta la durata del contratto, il Fornitore deve fare il possibile per garantire la fornitura di ogni parte di ricambio necessaria a mantenere tutte le apparecchiature funzionanti in modo efficiente e sicuro e nel rispetto delle norme di sicurezza, nonché certificare la piena corrispondenza ai parametri attesi dalle apparecchiature al fine di garantirne un uso idoneo e corretto.

La Ditta che risulterà aggiudicataria nello specifico dovrà:

- presentare la programmazione del piano manutentivo annuale, concordata con la Stazione Appaltante, mantenendo la periodicità in essere.
- per tutta la durata del contratto, erogare il servizio di assistenza tecnica, manutenzione ed aggiornamento volto a garantire il perfetto funzionamento delle apparecchiature e di tutti i pacchetti *software* di elaborazione presenti nelle stesse apparecchiature e *workstation*.
- mantenere in perfetta efficienza l'apparecchiatura tanto sotto l'aspetto infortunistico, di sicurezza e di rispondenza alle norme, quanto sotto l'aspetto della rispondenza ai parametri tipici dell'apparecchiatura stessa, al suo corretto utilizzo, garantendo un servizio di assistenza tecnica e manutenzione sia dell'apparecchiatura sia delle singole componenti per i guasti dovuti al normale utilizzo esclusi i danni derivanti da incuria e/o uso improprio.
- garantire che il personale, incaricato di eseguire le attività oggetto del presente bando di gara, sia competente e formato sulla base di un'istruzione adeguata, procedure, istruzioni di lavoro e materiale formativo di riferimento.
- fornire, a inizio appalto, e mantenere costantemente aggiornato in corso di esecuzione dell'appalto, l'elenco del personale autorizzato ad eseguire le attività oggetto del presente bando di gara.
- impiegare, nell'esecuzione del presente appalto, esclusivamente personale con esperienza di almeno 3 anni nell'esecuzione di attività analoghe a quelle oggetto del presente bando di gara.

- fornire una copia di schede e check-list utilizzate per l'espletamento delle manutenzioni ordinarie.
- conservare, per tutto il periodo contrattuale, le registrazioni delle attività di assistenza svolte e renderle disponibili a CNAO su richiesta in qualsiasi momento.
- assicurare che tutte le attività di manutenzione, ispezione assistenza e riparazione saranno effettuate secondo le istruzioni del fabbricante dell'apparecchiatura mantenendo la conformità alla Norma utilizzata per la progettazione dell'apparecchiatura stessa come richiesto dalla norma CEI EN 62353.
- seguire le procedure di manutenzione identificate dal fabbricante dell'apparecchiatura nella sua documentazione di accompagnamento come richiesto dalla IEC 60601-1.
- garantire il rispetto degli adempimenti previsti dal D.Lgs 101/20 e s.m.i. e in particolare:
  1) garantire il mantenimento della conformità della macchina e degli impianti agli aspetti di radioprotezione;
  2) predisporre la documentazione necessaria per l'accesso del proprio personale alle zone classificate del CNAO.

Lo svolgimento delle attività sarà vincolato al rispetto delle Norme Interne di Protezione e Sicurezza dalle radiazioni ionizzanti in vigore presso la Fondazione.

Il servizio dovrà comprendere:

- n.2 (due) interventi preventivi all'anno secondo i protocolli definiti dal costruttore comprensivi dei controlli di sicurezza secondo le Norme CEI e secondo la periodicità ed i protocolli indicati nel manuale delle apparecchiature;
- lubrificazione e pulizia delle parti meccaniche in movimento;
- pulizia periodica ed eventuale sostituzione di filtri, ventole, etc;
- verifica dei parametri di funzionamento delle sottoparti del Tomografo Computerizzato di simulazione (e.g. gantry, generatore, tavolo porta paziente, consolle di comando, cabinet, ricostruttore), ed eventuale calibrazione delle stesse secondo le indicazioni previste da Costruttore;
- sostituzione periodica di componenti giunti alla fine del loro ciclo vitale, prima che possano causare fermi del sistema;
- le Verifiche di Sicurezza Elettrica (VSE) annuali effettuate secondo le specifiche della casa costruttrice e le Norme CEI in vigore, per garantire la sicurezza d'esercizio sia meccanica che elettrica. La documentazione di riferimento dovrà riportare le misurazioni effettuate e i valori riscontrati;
- i controlli funzionali per mantenere i parametri di qualità immagine nei limiti definiti dal Costruttore, e pianificazione di eventuali interventi, tarature e calibrazioni atti al mantenimento degli stessi;
- un numero illimitato di interventi correttivi, nonché tutte le operazioni necessarie al ripristino del funzionamento dell'apparecchiatura (e.g. tarature, *check-up* sistema) a seguito di rotture avvenute durante il normale utilizzo. Qualora il guasto riscontrato possa incidere sulle condizioni di sicurezza dell'apparecchiatura, dovrà essere effettuata la Verifica di Sicurezza Elettrica e il controllo di funzionalità, conformemente a quanto previsto dalle norme CEI generali e particolari applicabili;
- interventi di configurazione di rete del sistema, inclusa la riconfigurazione dei nodi dicom, qualora intervengano modifiche nell'infrastruttura informatica aziendale;
- la manodopera e le spese di viaggio per diagnosi guasto e riparazione;
- gli aggiornamenti *hardware* e *software*, relativamente alle opzioni già installate sulla strumentazione, previsti dal produttore per mantenere o aumentare l'affidabilità e sicurezza del sistema;
- il monitoraggio in remoto sullo stato di funzionamento della macchina;

- l'esecuzione di tutte le azioni conseguenti ad eventuali avvisi di sicurezza e procedure di manutenzione in ambito di sicurezza e/o funzionalità emessi dal produttore;
- protezione dell'intero sistema e sottosistemi con pacchetto software antivirus;
- tutte le parti di ricambio che si rendesse necessario sostituire ed i materiali soggetti ad usura (es: tubo radiogeno, parti in vetro, sottovuoto, detettori digitali, filtri, batterie, lampade, parti non monouso, *kit* di manutenzione, cavi, eventuale materiale di calibrazione, cinghie, ecc.) ad esclusione del materiale di consumo (es: carta, supporti magnetici e/o ottici, ecc.). I ricambi, le parti soggette ad usura e i materiali di consumo utilizzati per le riparazioni e le manutenzioni devono essere originali o dichiarati compatibili dall'azienda produttrice dell'apparecchiatura su cui devono essere installati e nuovi salvo esplicita autorizzazione di CNAO. CNAO potrà autorizzare l'uso di materiale reperito dalla Ditta non originale, previo accertamento della compatibilità, nei seguenti casi:
  - parti di ricambio ricondizionate e certificate dalle imprese produttrici con garanzia totale di almeno 6 mesi;
  - per cause di forza maggiore quali:
    a. fallimento della ditta produttrice del dispositivo medico e/o della ditta produttrice della specifica parte di ricambio originale;
    b. dispositivo medico per cui la ditta produttrice non garantisca più la disponibilità dei ricambi perché fuori produzione.
- la spedizione dei materiali necessari all'intervento preventivo e/o correttivo;
- lo smaltimento degli imballaggi di tutti i materiali utilizzati e/o sostituiti durante gli interventi manutentivi.

Rimane inteso che ciascun intervento, di qualsiasi natura esso sia (e.g. manutenzione preventiva, controllo funzionale, aggiornamento, calibrazione), dovrà essere accompagnato da completi Rapporti di Intervento attestanti lo stato dell'apparecchiatura ed inclusivi di eventuali check-list compilate, tarature delle strumentazioni terze utilizzate durante gli interventi o qualsiasi altra documentazione specifica dello stesso.

Eventuali modifiche al calendario, preventivamente concordate, dovranno essere comunicate al Servizio di Ingegneria Clinica inviando il calendario aggiornato con l'indicazione delle modifiche e delle motivazioni relative alle stesse, con congruo anticipo (non inferiore a 3 giorni al fine delle autorizzazioni che vengono rilasciate dallo RSPP di CNAO all'intervento).

4 TEMPI DI RISPOSTA E DI INTERVENTO IN LOCO, DURATA DEL FERMO MACCHINA E RAPPORTI DI LAVORO DEL SERVIZIO DI ASSITENZA TECNICA E MANUTENZIONE

4.1 TEMPI DI RISPOSTA E DI INTERVENTO IN LOCO

L'impresa dovrà inviare, a seguito dell'aggiudicazione, la procedura per la richiesta di intervento tecnico, i riferimenti telefonici e di posta elettronica dedicati al servizio di assistenza straordinaria.

La Ditta aggiudicataria dovrà fornire un supporto telefonico e/o in teleassistenza disponibile tutti i giorni lavorativi del periodo contrattuale ad esclusione dei sabati, delle domeniche e dei festivi **dalle ore 8:00 alle ore 17:00**.

A seguito della ricezione della richiesta di intervento non programmato da parte della Fondazione CNAO, sia essa telefonica o via email, la Ditta dovrà assegnare un codice univoco di chiamata; il tecnico della Ditta dovrà contattare il personale del Servizio di Ingegneria Clinica (o altro contatto indicato nell'apertura di chiamata) per concordare data e ora dell'intervento. **Il tempo di risposta dovrà avvenire il prima possibile e comunque entro 1 ora dalla richiesta di intervento** da parte della Fondazione CNAO.

L'intervento in loco, se urgente e/o con guasto bloccante l'attività clinica, dovrà avvenire entro 8 ore lavorative dalla richiesta di intervento da parte della Fondazione CNAO. Per chiamate non urgenti e con eventi non bloccanti l'attività clinica, l'intervento in loco sarà concordato con il Servizio di Ingegneria Clinica.

Il tempo di risoluzione del guasto, una volta individuato e senza necessità di sostituzione di parti di ricambio, non dovrà essere superiore alle 8 ore lavorative.

Il tempo massimo entro cui l'operatore economico si impegna a risolvere il problema tecnico insorto, e a ripristinare l'operatività clinica dell'apparecchiatura, è fissato in 48 ore dalla chiamata.

4.2 DURATA DEL FERMO MACCHINA

Si definisce "tempo di fermo macchina" il periodo di tempo intercorrente tra il giorno successivo a quello di apertura chiamata, ricevuta entro le ore 17:00, ed il giorno del ripristino completo della funzionalità dell'apparecchiatura, incluse le sue parti e dispositivi accessori. La durata del periodo di fermo macchina ammissibile per ogni anno di funzionamento e per ogni parte ed accessorio della tecnologia è stabilito in 10 (dieci) giorni/anno, compresi quelli relativi ai fermi per manutenzione programmata. Saranno applicate le penali come indicato nello schema di contratto, cui si rinvia.

4.3 GENERAZIONE DI RAPPORTI DI LAVORO

I rapporti di lavoro relativi alle attività di manutenzione correttiva, preventiva, controllo funzionale e VSE dovranno essere consegnati al termine dell'intervento, firmati dal tecnico esecutore e controfirmati dal personale del Servizio di Ingegneria Clinica o da persona delegata dal SIC stesso; la documentazione in formato digitale dovrà essere inviata al seguente indirizzo di posta elettronica: ingegneriaclinica@cnao.it

La Ditta Aggiudicataria dovrà indicare dettagliatamente all'interno del rapporto di intervento, le modalità di esecuzione del servizio di assistenza tecnica ed in particolare:

- Ragione sociale della ditta esecutrice del servizio di manutenzione.
- Nome e Cognome del tecnico esecutore dell'intervento.
- Identificazione anagrafica dell'Apparecchiatura (N. Inventario e matricola, tipologia, ubicazione).

- Tipo di intervento effettuato (manutenzione preventiva, manutenzione correttiva, verifica di sicurezza).
- Descrizione dettagliata dell'intervento eseguito, in cui siano allegate opportune *check-list* per le attività programmate incluse nel servizio (e.g. manutenzione preventiva, verifiche di sicurezza elettrica, verifiche funzionali).
- Descrizione dettagliata dei Report di Quality Assurance (QA).
- Eventuale elenco di strumenti di misura utilizzati e loro certificazione di taratura con data di scadenza della stessa (se necessaria).
- Eventuale elenco del materiale utilizzato (parti di ricambio e/o consumabili).
- Data e ora chiamata (nel caso di manutenzione correttiva specificare data e ora della richiesta di intervento da parte del SIC o del reparto interessato).
- Data e ora inizio/fine intervento.
- Esito dell'intervento.
- Stato dell'intervento tecnico (concluso/non concluso/sospeso).

5 GOVERNANCE DELLA SICUREZZA CYBERSECURITY E CONNESSIONE REMOTA

Come indicato in premessa al presente documento, Fondazione CNAO è soggetto importante ai sensi della NIS e, in tale contesto, la descrizione della soluzione tecnologica e dei servizi di assistenza remota dovrà essere redatta dal concorrente in piena conformità ai parametri di sicurezza stabiliti dalla Direttiva (UE) 2022/2555 (NIS 2).

Le prescrizioni tecniche minime contenute nel presente documento, come di seguito meglio specificato, sono da intendersi quale livello minimo di sicurezza necessario e non derogabile per l'accettazione della fornitura.

Resta inteso che la conformità della soluzione proposta ai suddetti standard NIS 2 costituisce un requisito essenziale di esecuzione del contratto: l'operatore economico dovrà pertanto descrivere analiticamente le misure adottate, la cui verifica di conformità sarà effettuata in sede di collaudo e monitoraggio contrattuale, senza che tale descrizione sia oggetto di attribuzione di punteggio tecnico discrezionale nell'ambito dell'offerta economicamente più vantaggiosa.

5.1 MDS2 (MANUFACTURER DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY)

Al fine di consentire l'analisi del rischio aziendale, il Fornitore ha l'obbligo di fornire e mantenere aggiornato il modello **MDS2 (Manufacturer Disclosure Statement for Medical Device Security)**. Tale documento costituisce la base tecnica per validare la gestione delle vulnerabilità, la resilienza del sistema operativo e le capacità di auditing (logging) della fornitura.

5.2 STANDARD PER L'ACCESSO REMOTO E TELEDIAGNOSI TECNICA

Per le attività di monitoraggio e manutenzione, l'accesso remoto deve avvenire esclusivamente attraverso canali cifrati e tracciabili, seguendo la gerarchia di sicurezza stabilita dall'Amministrazione:

- **Standard Primario: Agente del Fornitore (Service Bridge/Gateway dedicato)** Implementazione di un gateway di comunicazione proprietario del costruttore che operi come unico punto di uscita verso i centri servizi del Fornitore. Il sistema deve garantire comunicazioni cifrate e permettere il monitoraggio proattivo dello stato del sistema.

- **Soluzione di Backup A: VPN Client su infrastruttura Sophos XGS** Accesso tramite tunnel VPN cifrato gestito dall'Amministrazione attraverso i propri firewall **Sophos XGS**. Il Fornitore dovrà utilizzare account nominali e autenticazione a due fattori (MFA) secondo le policy di sicurezza fornite dal reparto IT del CNAO.

- **Soluzione di Backup B: VPN Site-to-Site (Punto-Punto)** Instaurazione di un tunnel IPsec dedicato tra il firewall del Fornitore e l'infrastruttura **Sophos XGS** dell'Amministrazione, configurato per permettere il traffico esclusivamente verso gli indirizzi IP e le porte strettamente necessari all'erogazione del servizio.

5.3 DIVIETO DI STRUMENTI NON AUTORIZZATI

È fatto esplicito divieto di installare o utilizzare software di controllo remoto generalisti (es. TeamViewer, AnyDesk, VNC non cifrati). L'impiego di tali strumenti, non segregati e non autorizzati, è considerato una violazione dei protocolli di sicurezza e costituisce grave inadempienza contrattuale.

5.4 SICUREZZA DEL SOFTWARE E PATCHING

Il Fornitore è responsabile dell'installazione remota di tutti gli aggiornamenti di sicurezza relativi all'eventuale sistema operativo e all'applicativo forniti.

- **Vulnerabilità Critiche/Zero-Day:** Il Fornitore si impegna a fornire una prima analisi di impatto e un'eventuale strategia di mitigazione temporanea (es. modifiche configurazione firewall o procedure operative) entro 48 ore lavorative dalla notifica della vulnerabilità. L'installazione della patch definitiva dovrà avvenire nel minor tempo tecnico possibile, e comunque entro 15 giorni solari dal momento in cui la patch è stata validata e resa disponibile dalla casa madre per lo specifico modello di dispositivo medico offerto.

- **Patch Ordinarie:** Ogni attività di patching deve essere tracciata e comunicata preventivamente all'Amministrazione per coordinare eventuali fermi macchina. Le date di installazione di tali patch dovranno essere tassativamente concordate con il servizio di ingegneria clinica di CNAO.

5.5 RESPONSABILITÀ E GESTIONE DEGLI INCIDENTI (NIS2 COMPLIANCE)

Il Fornitore riconosce che la fornitura è parte integrante dell'infrastruttura di un **Soggetto Importante** ai sensi della Direttiva NIS2.

A. Garanzia di Manutenzione della Sicurezza: Il Fornitore garantisce che gli strumenti di accesso remoto utilizzati siano costantemente aggiornati e privi di vulnerabilità note. Il Fornitore si impegna a utilizzare esclusivamente endpoint (PC/Workstation dei propri tecnici) dotati di sistemi di protezione attivi (eventuali Antivirus/EDR) e conformi alle best practice internazionali di sicurezza.

B. Responsabilità per l'Infrastruttura: Qualora un incidente informatico (inclusi, a titolo esemplificativo, attacchi di tipo **Ransomware, Malware o esfiltrazione non autorizzata di dati**) che colpisca l'infrastruttura dell'Amministrazione sia riconducibile, in via diretta o indiretta, a una vulnerabilità del sistema di accesso remoto del Fornitore o a una negligenza del suo personale (es. compromissione delle credenziali VPN, utilizzo di software non autorizzati), il Fornitore sarà ritenuto integralmente responsabile.

C. Obblighi di Indennizzo: In caso di incidente informatico imputabile al Fornitore, quest'ultimo sarà tenuto a:

Manlevare e tenere indenne l'Amministrazione da ogni pretesa risarcitoria di terzi (inclusi i pazienti).

- Farsi carico dei costi di bonifica e ripristino dei sistemi e dei dati.
- Risarcire i danni derivanti dall'eventuale interruzione del servizio pubblico e delle attività cliniche.
- Corrispondere le eventuali sanzioni irrogate dal Garante per la Protezione dei Dati Personali ai sensi del GDPR, qualora l'incidente configuri un *Data Breach*.

D. Obbligo di Notifica e Cooperazione: In conformità a quanto previsto dalla Direttiva (UE) 2022/2555 (NIS2) e dal GDPR, il Fornitore si impegna a notificare all'Amministrazione qualsiasi incidente di sicurezza o violazione subita sui propri sistemi che possa avere un impatto, anche solo potenziale, sulla connessione remota, sulla riservatezza dei dati o sull'integrità dei sistemi dell'Ente.

- **Tempistiche**: La notifica dovrà avvenire senza indebito ritardo e comunque nel rispetto delle tempistiche stringenti previste dalla normativa vigente di settore per i fornitori di servizi critici e soggetti essenziali/importanti.

- **Contenuti**: La comunicazione dovrà essere accompagnata da una relazione preliminare sulle cause dell'evento, sulle potenziali conseguenze per l'Amministrazione e sulle misure di mitigazione già adottate o pianificate.

- **Cooperazione**: Il Fornitore si impegna a collaborare attivamente con il referente per la sicurezza informatica dell'Amministrazione (Incident Manager/Cyber Security Team) per fornire ogni informazione utile alla gestione dell'incidente e all'eventuale segnalazione alle Autorità competenti (ACN, Garante Privacy).

5.6 DISPOSIZIONI PER LA PROTEZIONE ANTIMALWARE ED ENDPOINT SECURITY

Considerata la natura segregata della rete aziendale (assenza di navigazione internet diretta della workstation), il Fornitore dovrà garantire l'aggiornamento costante delle definizioni dei virus e delle patch di sicurezza secondo la modalità di connessione prescelta tra quelle indicate al par. 5.2.

In particolare, l'erogazione degli aggiornamenti (firme antimalware e patch di sicurezza) dovrà avvenire inderogabilmente secondo uno dei seguenti scenari operativi:

- **Caso 1 – Se si utilizza l'Agente del Fornitore (Service Bridge):** Il gateway dedicato del Fornitore dovrà fungere da proxy di aggiornamento. Il Fornitore è responsabile della configurazione del sistema affinché la workstation riceva automaticamente le definizioni antimalware e le patch dal server centrale del produttore tramite il tunnel cifrato stabilito dall'agente.

- **Caso 2 – Se si utilizza la VPN Client su Sophos XGS:** Il Fornitore dovrà garantire che il tecnico, durante le sessioni di manutenzione remota pianificate, effettui manualmente o tramite script automatizzati il push degli aggiornamenti delle firme antimalware e delle patch di sicurezza, pre-scaricate su repository sicuri del Fornitore.

- **Caso 3 – Se si utilizza la VPN Site-to-Site:** Il Fornitore dovrà indicare all'Amministrazione gli indirizzi IP/FQDN dei propri server di update (Update Server/Console Centralizzata) per consentire al firewall **Sophos XGS** l'apertura delle rotte specifiche necessarie al download automatico delle sole firme antimalware da parte della workstation.

L'eventuale mancato aggiornamento dei sistemi di protezione, derivante da inadempienze nelle procedure sopra descritte, sarà considerato un **indebolimento volontario della postura di sicurezza** dell'Ente, con le responsabilità già descritte.

5.7 STANDARD DI PROTEZIONE ENDPOINT E INTEROPERABILITÀ (SOPHOS CENTRAL)

Il CNAO adotta come standard di sicurezza per la propria infrastruttura la piattaforma **Sophos Central**.

Al fine di garantire l'integrità del perimetro aziendale e la massima resilienza dei sistemi forniti, l'interoperabilità tra le soluzioni di protezione deve conformarsi alle seguenti prescrizioni:

INTEGRAZIONE DELLO STANDARD AZIENDALE

Nel caso in cui il fornitore desideri avvalersi dei sistemi CNAO, ove il sistema fornito sia certificato dal produttore per ospitare l'agente **Sophos Central**, ha l'obbligo di operare in stretta collaborazione con il reparto IT dell'Amministrazione per:

- **Installazione e Deploy:** Assicurare la corretta implementazione dell'agente sugli endpoint della fornitura.
- **Fine-Tuning Operativo:** Definire e configurare congiuntamente le **esclusioni dei processi critici** (es. flussi di acquisizione immagini, ricostruzioni DICOM, database locali), garantendo che la scansione in tempo reale non impatti sulla sicurezza del paziente o sulle performance cliniche.

UTILIZZO DI SOLUZIONI DI PROTEZIONE TERZE

Qualora il Fornitore prescriva l'utilizzo esclusivo di una propria soluzione antivirus/EDR pre-installata o proprietaria (es. Windows Defender for Endpoint, McAfee, ecc.), l'esercizio della stessa è soggetto alle seguenti condizioni:

- **Trasparenza Documentale:** Le specifiche e le capacità della soluzione devono essere dettagliate nel documento MDS2, con particolare riferimento alle modalità di monitoraggio e risposta agli incidenti.
- **Autonomia Manutentiva:** La gestione, il monitoraggio e l'aggiornamento costante della soluzione restano a totale ed esclusivo carico del Fornitore, che dovrà garantirne l'efficacia per tutta la durata del contratto senza oneri aggiuntivi (licenze, canoni o costi di intervento) per l'Amministrazione.
- **Salvaguardia delle Prestazioni**: Il Fornitore risponde direttamente della corretta configurazione della soluzione, assicurando che l'attività di protezione non generi latenze o malfunzionamenti nell'erogazione dei servizi clinici.

Se entrambe le soluzioni non sono percorribili dal Fornitore, qualora quindi il sistema offerto non preveda un software antimalware del fornitore e, contestualmente, lo stesso dichiari l'incompatibilità tecnica all'installazione dell'agente Sophos Central dell'Amministrazione, si applicheranno le seguenti disposizioni obbligatorie:

1. **Certificazione di Hardening:** Il Fornitore dovrà consegnare un documento tecnico che attesti le misure di "Hardening" (irrobustimento) applicate al sistema operativo. Tali misure devono includere, a titolo esemplificativo: disabilitazione di servizi non necessari, chiusura di porte logiche non utilizzate, restrizioni sulle esecuzioni automatiche (Autorun) e politiche di controllo degli accessi alle porte USB.
2. **Whitelist Applicativa:** In assenza di un antivirus basato su firme, il Fornitore dovrà configurare (o permettere all'Amministrazione di configurare) sistemi di *App-Locker* o *Whitelisting*, affinché sulla workstation possano essere eseguiti esclusivamente i processi autorizzati dal produttore.
3. **Assunzione di Responsabilità:** Il Fornitore dovrà rilasciare una dichiarazione formale in cui si assume la piena responsabilità della sicurezza del dispositivo. In caso di infezione virale che comprometta l'operatività del sistema o che si propaghi verso la rete aziendale a causa dell'assenza di protezione e della mancata compatibilità con i sistemi aziendali, il Fornitore sarà tenuto al ripristino del sistema e al risarcimento degli eventuali danni.
4. **Isolamento di Rete Supplementare:** L'Amministrazione si riserva il diritto di applicare, tramite i propri firewall **Sophos XGS**, restrizioni di rete ancora più stringenti (es. micro-

segmentazione estrema) per isolare il dispositivo privo di protezione attiva, senza che ciò possa essere invocato dal Fornitore come causa di malfunzionamento del servizio di assistenza remota.

5.8 CONFIGURAZIONE AVANZATA E SALVAGUARDIA DELLE PRESTAZIONI CLINICHE

Indipendentemente dall'architettura di protezione adottata (Sophos Central o soluzione proprietaria), il Fornitore ha l'obbligo di trasmettere all'Amministrazione un **Documento Tecnico di Configurazione** che dettagli le esclusioni necessarie (cartelle, estensioni di file, processi e chiavi di registro). Tale documento è finalizzato a:

- **Ottimizzazione Operativa:** Garantire che la scansione "real-time" non generi latenze, colli di bottiglia o blocchi critici durante le fasi di acquisizione, ricostruzione delle immagini o trasferimento dei dati verso i sistemi di archiviazione (PACS).
- **Sicurezza delle Esclusioni:** Il Fornitore deve attestare che le esclusioni richieste siano limitate allo stretto necessario per il funzionamento del software medico, assumendosi la responsabilità della protezione di tali percorsi attraverso misure di monitoraggio alternative o segregazione.
- **Aggiornamento Dinamico:** Il Fornitore si impegna ad aggiornare tempestivamente il suddetto documento a seguito di ogni aggiornamento software o cambio di versione dell'applicativo fornito.

5.9 GARANZIA DI EVOLUZIONE TECNOLOGICA, RESILIENZA CYBER E INTEROPERABILITÀ SOFTWARE

L'Appaltatore assicura che il sistema rimanga, per tutta la durata del servizio, pienamente conforme ai requisiti di sicurezza previsti dalla legislazione vigente. Tale obbligo include la fornitura gratuita e tempestiva di ogni aggiornamento (*update*) necessario alla conformità normativa (**NIS 2, GDPR, AI Act**) e alla massima resilienza cyber (patching e supporto ai sistemi operativi).

6 ALLEGATI

Allegato1, Componenti CT
Allegato2, Current History X-ray Tube