CONSULTAZIONE CON IL MERCATO SISTEMI PER LA GARA (ID 17APB006) PER TOMOGRAFO CT/PET

(rif.: avviso prot. 0032631 dd. 04.12.2017)

ESTRATTO DEL CAPITOLATO PER L'AFFIDAMENTO DELLA FORNITURA E INSTALLAZIONE DI SISTEMI PER CT/PET E RELATIVE OPERE PROPEDEUTICHE PER GLI ENTI DEL S.S.R. FVG

1. Premessa

Oggetto della gara:

fornitura e installazione di complessive:

n. 1 sistema CT/PET ASUIUD

n. 1 sistema CT/PET ASUITS

2. Requisiti di partecipazione

A titolo esemplificativo e non esaustivo, le apparecchiature e i dispositivi opzionali forniti dovranno rispettare:

- marcatura CE secondo direttiva 93/42/CEE e s.m.i.;
- Iscrizione nel Repertorio dei Dispositivi Medici come previsto dal D.M. 20 febbraio 2007
- norme nazionali CEI 62.5, CEI 62.51 e CEI CT 62 di pertinenza
- conformità alle vigenti disposizioni in materia di sicurezza stabilite nel D.Lgs. 9 aprile 2008, n. 81 e s.m.i.;
- conformità alle vigenti disposizioni in materia di radioprotezione dei Pazienti e dei lavoratori
- conformità alle "Normative di buona preparazione dei radiofarmaci in Medicina Nucleare" (Decr.Min.Salute del 30/03/05 – pubblicato nella GU n°168 del 21/07/05)

3. Caratteristiche principali della fornitura

Le apparecchiature dovranno essere, nuove di fabbrica, in produzione, di ultima generazione e in versione aggiornata al momento della consegna.

La Ditta aggiudicataria dovrà provvedere alla effettuazione delle opere propedeutiche e alla consegna dell'attrezzatura e accessori, installazione, collaudo, istruzione del personale, oltre a fornire una garanzia di almeno 24 mesi su quanto oggetto di fornitura ed un servizio di assistenza tecnica "full risk" per il periodo di garanzia, indicando nell'offerta anche gli oneri per la sicurezza (interferenziali e specifici).

La ditta può presentare il modello della propria gamma che ritiene più idoneo in relazione alla configurazione e destinazione d'uso prevista. Si intende sempre e comunque che deve essere offerto un solo modello: non è quindi ammessa la formulazione di offerte alternative, parziali, equivoche e/o condizionate.

Si considera che ulteriori/diverse specifiche tecnico-funzionali rispetto ai requisiti richiesti sono ammessi purché la ditta ne dimostri l'equivalenza o il miglioramento.
In tale caso, ai sensi dell'art. 68 del D.Lgs. 50/2016, l'offerta tecnica dovrà essere corredata, a pena di esclusione, da una relazione tecnica che, evidenziando la non conformità, motivi l'equivalenza funzionale, nonché dall'eventuale documentazione scientifica a supporto di quanto dichiarato.

La fornitura dovrà essere comprensiva di:

A. **LAVORI**
B. **CONSEGNA E COLLAUDO**
C. **SERVIZI ACCESSORI**

A. LAVORI

Per ciascun sito di installazione i lavori compresi in fornitura dovranno includere qualsiasi intervento necessario per la corretta installazione e utilizzo in sicurezza dell'apparecchiatura offerta. Sono quindi da comprendere lavori, implementazioni, modifiche edili, impiantistiche, protezionistiche, di sicurezza necessarie per adeguare gli spazi esistenti all'installazione dell'apparecchiatura, nulla escluso.

In sede di sopralluogo, come specificato nell'Avviso pubblicato in data 04.12.2017 presso i 2 siti di installazione, saranno consegnati la relazione dell'Esperto Qualificato, gli elaborati grafici delle strutture edilizie ed impianti (piante dei locali, sezioni, distribuzioni impiantistiche, quadri elettrici e la relazione di calcolo strutturale) dei locali interessati riprodotti su supporto magnetico.

Resta inteso che la documentazione tecnica, da produrre in fase di gara distintamente per ogni sito di installazione, dovrà comprendere una RELAZIONE TECNICO-ILLUSTRATIVA che si completerà con una stima economica parametrica (da inserire esclusivamente nella busta economica) da redigere secondo uno schema di offerta indicato dalla Stazione appaltante così come indicato all'art. 216 comma 4 del D.LGS. 50/2016. Solo l'aggiudicatario dovrà produrre il progetto esecutivo delle opere da realizzare propedeuticamente all'installazione delle apparecchiature oggetto di fornitura. Il progetto esecutivo, distinto per ogni sito di installazione, dovrà essere consegnato entro 35 giorni lavorativi dalla data di stipula del contratto pena l'applicazione delle penali. Eventuali lavorazioni non previste nella "RELAZIONE TECNICO-ILLUSTRATIVA" che emergessero in fasi successive all'offerta e che comportassero maggiori oneri per l'aggiudicatario non potranno essere imputate alla stazione appaltante, mantenendo quindi costante il prezzo offerto in fase di gara.

B. CONSEGNA E COLLAUDO

Al momento della consegna delle apparecchiature, la ditta aggiudicataria sarà tenuta a fornire tutta la documentazione tecnica come indicato nel capitolato di gara.
La fatturazione è vincolata all'esito positivo del collaudo. Qualora si verificassero contestazioni, il termine di pagamento rimarrà sospeso e riprenderà con la definizione della pendenza.

C. SERVIZI ACCESSORI

Garanzia

Per ciascuna apparecchiatura e dispositivo/apparecchiatura accessoria offerta, è inclusa la garanzia per vizi e difetti di funzionamento (art. 1490 c.c.), per mancanza di qualità promesse o essenziali all'uso cui la cosa è destinata (art. 1497 c.c.), nonché la garanzia per buon funzionamento (art. 1512 c.c.) per 24 (ventiquattro) mesi a partire dalla data di collaudo positivo.

Durante il periodo di garanzia il Fornitore dovrà fornire i servizi di assistenza e manutenzione tecnica di tipo full risk per l'apparecchiatura e per gli eventuali dispositivi, apparecchiature, accessori ordinati.

Manutenzione FULL RISK

Il Fornitore per i primi 24 (ventiquattro) mesi a partire dalla data del collaudo positivo dovrà fornire i servizi di assistenza e manutenzione full risk sull'apparecchiatura e gli eventuali dispositivi, apparecchiature, accessori ordinati, secondo quanto di seguito specificato.

Il costo dei servizi di assistenza e manutenzione full risk per il primo periodo di 24 (ventiquattro) mesi decorrenti dalla data del collaudo positivo dei beni e incluso nel prezzo unitario di acquisto delle apparecchiature e dei dispositivi accessori.

Sono comprese nel servizio la riparazione e la sostituzione dell'apparecchiatura in tutte le sue componenti comprensiva degli accessori (tubo radiogeno, rivelatori, adattatori, ecc.), dei materiali di consumo soggetti ad usura (gas/liquidi per raffreddamento, lubrificanti, filtri, sensori, sorgenti interne o esterne, ecc), con la sola esclusione del materiale di consumo necessario all'ordinario utilizzo (es: materiale monouso e monopaziente, se presente).

L'assistenza verrà effettuata con personale specializzato del Fornitore e comprenderà:

1. Manutenzione preventiva;

2. Manutenzione correttiva;
3. Fornitura parti di ricambio;
4. Aggiornamento hardware e software

Tali attività saranno espletate secondo quanto di seguito previsto. Resta inteso che, qualora gli interventi di assistenza e manutenzione full risk dovessero comportare una interruzione dell'utilizzo clinico delle apparecchiature e/o dei dispositivi accessori, gli interventi stessi dovranno essere effettuati dal Fornitore in orario non lavorativo per l'Amministrazione, salvo diverse indicazioni dell'Amministrazione medesima.

In particolare il Fornitore dovrà garantire la fornitura di qualsiasi parte necessaria a mantenere in perfetta efficienza le apparecchiature e i dispositivi accessori tanto sotto l'aspetto infortunistico, di sicurezza e di rispondenza alle norme quanto sotto l'aspetto della rispondenza ai parametri tipici delle apparecchiature e al loro corretto utilizzo, garantendo un servizio tecnico di assistenza e manutenzione sia delle apparecchiature fornite sia delle singole componenti per i difetti di costruzione e per i guasti dovuti all'utilizzo e/o ad eventi accidentali non riconducibili a dolo.

Inoltre, il Fornitore deve garantire per tutta la durata del contratto il medesimo livello qualitativo delle apparecchiature come accertato all'atto del collaudo; in caso di decadimento delle prestazioni di uno o più componenti, esplicitato dall'utilizzatore, non risolvibile con normali interventi di manutenzione, il Fornitore provvederà a sostituire tali componenti con attrezzature nuove identiche o migliori rispetto a quelle della fornitura originale.

Resta inteso che per qualsiasi congegno, parte o elemento meccanico, elettrico e elettronico che presenti rotture o logorii o che comunque diminuisca il rendimento delle apparecchiature, il Fornitore dovrà eseguire le dovute riparazioni e/o sostituzioni con materiali di ricambio originali e nuovi di fabbrica e di caratteristiche tecniche identiche o superiori a quelli sostituiti. Le parti sostituite verranno ritirate dal Fornitore che ne assicurerà il trattamento in conformità alle norme vigenti, senza alcun onere aggiuntivo per il Committente.

Il Fornitore si impegna a garantire la disponibilità delle parti di ricambio per 10 (dieci) anni a decorrere dalla data di accettazione della fornitura.

1. Manutenzione preventiva

La manutenzione preventiva comprende le procedure periodiche di verifica, controllo, messa a punto, sostituzione parti di ricambio e parti soggette ad usura o decadimento (sorgenti interne o esterne) ed eventuale adeguamento e/o riconduzione delle apparecchiature risultanti non conformi, come previsto dai manuali d'uso forniti in dotazione.

Tale manutenzione sarà effettuata nel rispetto delle modalità, frequenza e condizioni stabilite nel manuale relativo all'apparecchiatura e/o dispositivo accessorio acquistato.

La manutenzione preventiva comprende, inoltre, le verifiche e i controlli dei parametri di funzionamento (verifiche funzionali) comprensive del relativo materiale di consumo, le regolazioni e i controlli di qualità, nel numero e nei termini previsti dai manuali dei produttori; si intendono anche comprese le verifiche di rispondenza alle norme per la sicurezza elettrica, generali e particolari, da eseguirsi a seguito degli interventi di manutenzione preventiva/correttiva e comunque almeno una volta all'anno e gli eventuali interventi di rimessa a norma.

A titolo esemplificativo e non esaustivo, la manutenzione preventiva potrà includere: verifiche e controlli dei parametri di funzionamento delle apparecchiature e dei dispositivi accessori, tarature e controlli di qualità di funzionamento.

Le date del piano di manutenzione preventiva saranno concordate con il referente di ASUIUD. prima del collaudo definitivo.

Il Fornitore è tenuto al rispetto del calendario redatto, pena l'applicazione delle penali.

Al positivo completamento delle attività di manutenzione preventiva, verrà redatto un apposito "Verbale di manutenzione preventiva", da consegnare al Servizio di Ingegneria Clinica (SIC), il quale dovrà riportare almeno le

informazioni relative alle attività svolte, alla data in cui e stata svolta l'attività di manutenzione, al numero di ore nelle quali l'apparecchiatura e rimasta in stato di fermo e all'elenco delle componenti eventualmente sostituite.

2. Manutenzione correttiva

La manutenzione correttiva su chiamata comprende la riparazione e/o la sostituzione di tutte le sue parti, componenti, accessori e di quant'altro componga il bene nella configurazione fornita con la sola esclusione del materiale di consumo necessario all'ordinario utilizzo (es: materiale monouso e monopaziente), che subiscano guasti dovuti a difetti o deficienze del bene o per usura naturale o per danno accidentale, esclusi danni da eventi atmosferici e naturali.

La manutenzione correttiva consiste nell'accertamento della presenza del guasto o malfunzionamento, nell'individuazione delle cause che lo hanno determinato, nella rimozione delle suddette cause e nel ripristino delle originali funzionalità, con verifica dell'integrità e delle prestazioni dell'apparecchiatura. 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.

La manutenzione correttiva comprende un'assistenza da remoto per tutte le apparecchiature collegate in rete e per le quali dovrà essere organizzata e garantita una gestione dei guasti da remoto.

La manutenzione correttiva sarà effettuata con le seguenti modalità:

- Illimitato numero interventi su chiamata/segnalazione;
- intervento per guasto bloccante (macchina non utilizzabile) entro 4 (quattro) ore lavorative, (esclusi sabato, domenica, festivi) dalla chiamata, pena l'applicazione delle penali;
- intervento per guasto non bloccante (macchina utilizzabile) entro 16 (sedici) ore lavorative, (esclusi sabato, domenica, festivi) dalla chiamata, pena l'applicazione delle penali;
- ripristino funzionalità dell'apparecchiatura/dispositivo guasta (bloccante e non bloccante) entro 4 (quattro) giorni lavorativi dalla data di ricezione della chiamata, pena l'applicazione delle penali;
- In caso di guasto bloccante, fornitura di un sistema sostitutivo, eventualmente anche con ricorso a noleggio di sistemi mobili su camion di caratteristiche simili a quella in uso, entro 5 (cinque) giorni lavorativi dalla chiamata, pena l'applicazione delle penali;

Per ogni intervento dovrà essere redatto un apposito "verbale di manutenzione correttiva", da consegnare al SIC, il quale dovrà riportare almeno le informazioni relative alle attività svolte, alla data in cui e stata svolta l'attività di manutenzione, al numero di ore nelle quali l'apparecchiatura e rimasta in stato di fermo e all'elenco delle componenti eventualmente sostituite.

Una copia del verbale è destinata al Fornitore e una copia della stessa resta all'Amministrazione.

Il Fornitore dovrà assicurare un servizio per la ricezione delle richieste di intervento e delle chiamate che dovrà essere attivo tutti i giorni dell'anno, esclusi sabato, domenica e festivi, per almeno 8 (otto) ore in una fascia oraria che va dalle ore 8:00 alle ore 19:00.

Le richieste di intervento di assistenza e/o manutenzione inoltrate il sabato o la domenica o i festivi, si intenderanno ricevute all'inizio dell'orario di lavoro del giorno lavorativo successivo.

Le richieste inoltrate dopo le 8 (otto) ore di lavoro del centralino del Fornitore si intenderanno come ricevute all'inizio dell'orario di lavoro del giorno lavorativo seguente.

3. Fornitura parti di ricambio

Tutte le parti di ricambio dovranno essere originali. Il Fornitore deve garantire all'Amministrazione la loro reperibilità e fornitura per un periodo non inferiore a 10 (dieci) anni a decorrere dalla data di accettazione della fornitura.

4. Aggiornamento hardware e software

Il Fornitore si impegna a fornire gratuitamente per tutta la durata della vita utile dell'apparecchiatura ogni aggiornamento hardware e software inteso ad aumentare la sicurezza, l'affidabilità del sistema, nonché le prestazioni delle funzionalità già presenti. L'aggiudicatario dovrà fornire annualmente una relazione riportante tutti gli aggiornamenti sviluppati nell'anno in corso su tutti i software presenti nella configurazione offerta in modo da programmare, annualmente, l'aggiornamento da comprendere nel contratto di manutenzione full risk.
L'aggiornamento gratuito comprende quindi, a titolo esemplificativo ma non esaustivo, circuiti elettronici, sostituzione di PC e server, aggiornamento di sistemi operativi e software in genere, sostituzione di parti del sistema e tutto il necessario per garantire quanto sopra indicato.

Qualora invece gli aggiornamenti riguardino nuove funzionalità, questi dovranno essere proposti all'acquirente entro 60 giorni dal loro rilascio con quotazione economica scontata del 50% sul prezzo di listino.

4. Caratteristiche e configurazione minima richiesta della CT/PET e accessori opzionali obbligatori

Le caratteristiche tecniche e funzionali minime richieste pena l'esclusione sono le seguenti:

1. **Gantry CT-PET e lettino porta paziente**
   - CT-PET
     - Diametro utile del vano paziente ≥ a 70 cm
   - Lettino porta paziente
     - Movimento controllato da consolle e da lettino/gantry
     - Dotazione standard di accessori/cinghie per un corretto e sicuro posizionamento del paziente
     - In fibra di carbonio o altro materiale a basso coefficiente di attenuazione e dotato di sistemi di sicurezza anti collisione e di sistemi di sblocco manuale.
   - Accessori per trattamenti radioterapici
     - N. 3 Laser esterni "mobili" (uno sagittale e due laterali) installati a parete
     - Table Top per centrature radioterapiche in fibra di carbonio o altro materiale a basso coefficiente di attenuazione per la simulazione di trattamenti radioterapici, compatibile con i modelli di Acceleratori Lineari in dotazione alle 2 Aziende destinatarie della fornitura (seguirà dettaglio in CSA, comunque modelli Elekta per ASUITS e modelli Varian per ASUIUD).
   - Accessori a corredo
     - Interfono per la comunicazione con il paziente e quant'altro necessario per la corretta esecuzione dell'esame, compresi presidi di sicurezza (es: impianto di segnalazione RX, funghi di arresto, videocamere, altro).
     - Catena televisiva a circuito chiuso con 2 telecamere dotate di zoom e brandeggio e relativi 2 monitor;

2. **Sottosistema PET**
   - Materiale dei cristalli di scintillazione con drogaggio al Lutezio (LYSO o LSO o LBS o altro acronimi)
   - Matrice di cristalli con dimensioni, per ogni singolo cristallo, ≤ a 4,2x6.3 mm
   - Spessore del cristallo scintillatore di almeno 20 mm
   - Risoluzione temporale ≤ 600 psec
   - Ricostruzione dell'immagine PET con tecnologia TOF
   - FOV assiale ≥ a 15,5 cm
   - FOV transassiale ≥ a 55 cm

3. **Sottosistema CT**
   - Generatore RX:
     - Potenza utile ≥ a 50 kW
     - Tensione massima ≥ a 130 kV
   - Tubo radiogeno:
     - Elevata capacità termica anodica: ≥ a 5.000.000 HU
     - Elevata dissipazione termica anodica: ≥ 800.000 HU/min
   - CT:
     - Numero di file di detettori fisicamente presenti ≥ a 64
     - Spessore di strato minimo inferiore a 1 mm
     - Tempo di scansione minimo su 360° indicativamente non superiore a 0,5 sec.
     - FOV transassiale ≥ a 48 cm
     - Dimensioni della matrice di acquisizione più elevate possibile; (almeno 512x512 e visualizzazione di almeno 1024x1024 pixels.)
     - Utilizzabile anche in modalità stand-alone.
     - Dispositivo e/o software dedicato alla riduzione della dose

4. **Software di acquisizione, elaborazione e refertazione**
   - Per diagnostica CT PET:
     - Acquisizione PET: statica, dinamica, whole body, gated respiratorio (opzione), gated cardiaca (opzione) e neurologico (opzione)
     - Acquisizione CT: scout, assiale e spirale
     - Software clinico completo per l'analisi ed il follow-up di pazienti oncologici e per la valutazione del trattamento chemio/radioterapico
     - Software/algoritmo clinico per la valutazione semi-quantitativa delle immagini (SUV)
     - Protocolli di acquisizione pre-programmate per scansioni CT-PET
     - Software/algoritmo per la riduzione dell'artefatto da protesi metallica
     - Software/algoritmo di ricostruzione iterativa (IR) e FBP
     - Software/algoritmo di ricostruzione basato sul "tempo di volo" (TOF)

- Software/algoritmo che permetta l'importazione e la fusione con immagini da altra modalità di acquisizione (PET/SPECT/RM/TC)
- Software/algoritmo clinico di ricostruzione multiplanare PET, CT e PET-CT.
- Software/algoritmo di rendering volumetrico per immagini PET e CT.

- Controllo della dose e controlli di qualità:
  - Software/indicatore che informi il medico specialista, prima della procedura ed al suo termine, dei parametri pertinenti alla dose del paziente, e capacità di trasferire queste informazioni nella registrazione dell'esame.
  - Software/algoritmo per l'esecuzione dei controlli di qualità giornalieri (se previsti) e periodici e relativi fantocci
- Per piani di trattamento radioterapici:
  - Software di simulazione virtuale per trattamenti radioterapici e per l'export DICOM-RT

5. Consolle di controllo ed elaborazione immagini

- Consolle di comando:
  - Hardware, con caratteristiche tecniche adeguate a garantire prestazioni allo stato dell'arte, completo di ;
    - N. 1 monitor LCD a colori ad alta risoluzione, di grado medicale, di dimensioni non inferiori a 19";
    - N. 1 monitor LCD a colori di grado medicale e ad uso diagnostico, di dimensioni non inferiori a 21" e con una risoluzione non inferiore a 2MP;
  - In grado eseguire tutte le operazioni di acquisizione e ricostruzione del sistema integrato CT PET e per il controllo dei LASER per acquisizioni RT
  - Piattaforma software unica per la gestione del sistema PET e CT.
- Stazioni di elaborazione: vedere allegato 1
- Integrazione, connessione e trasmissioni dati:
  - Integrazione ai sistemi PACS, HIS per il controllo delle funzioni di visualizzazione, archiviazione e networking delle immagini PET, CT e di fusione CT-PET. Integrazione anche con i sistemi in dotazione alla Struttura di Fisica Sanitaria/Radioterapia esistenti per l'elaborazione dei piani di trattamento radioterapico. Le specifiche d'integrazione per i sistemi PACS E HIS sono riportate nell'allegato 2. Gli allegati 3 e4 riportano invece le caratteristiche dei SI delle 2 aziende destinatarie della fornitura

6. Calibrazioni e controlli qualità

- Fantoccio per acquisizione dei controlli di qualità giornalieri per il sistema CT;
- Set completo di sorgenti sigillate per la calibrazione e i controlli di qualità giornalieri. I controlli di qualità giornalieri (se previsti) e periodici dovranno essere veloci e il più possibile automatizzati per limitare al minimo il fermo macchina e l'esposizione a radiazioni ionizzanti dell'operatore. Resta inteso che rientra tra gli oneri del fornitore garantire la disponibilità delle sorgenti in questione nel periodo di garanzia e

successivamente attraverso il contratto di Full Risk che verrà eventualmente sottoscritto.

7. Accessori opzionali richiesti, non inclusi in configurazione, ma la cui disponibilità deve essere obbligatoriamente garantita pena l'esclusione:

A. Licenza/software/algoritmo clinico completo per elaborazioni CT PET cerebrali
B. Soluzione (hardware e/o software) per applicazioni avanzate di gating cardiologico sia PET che CT
C. Soluzione (hardware e/o software) per applicazioni avanzate di gating respiratorio sia PET che CT (in particolare per applicazioni di radioterapia)
D. Iniettore di mezzo di contrasto a doppia siringa con relativa consolle di comando, completo di software dedicato e pienamente interfacciato con il sistema offerto;
E. Soluzioni tecnologiche differenziate per ASUITS e ASUIUD per il frazionamento ed infusione di radiofarmaco:

a. <u>Per ASUIUD</u>:

- Sistema per frazionamento ed iniezioni di FDG con calibratore integrato dell'attività conforme alle "Normative di buona preparazione dei radiofarmaci in Medicina Nucleare"
- Accuratezza della dose misurata < del 2%
- Adeguata schermatura per limitare l'esposizione degli operatori
- Carrello con movimento motorizzato su ruote
- Display touch screen per la gestione semplice e rapida del processo di frazionamento e di iniezione
- Sistema di calcolo automatico della dose in base al peso del paziente
- Sistemi di sicurezza per il paziente come filtri particellari e sensori di aria con disattivazione automatica della somministrazione
- Completo di stampante per etichette con report personalizzabile
- Collegamento wifi ed ethernet per assistenza/manutenzione da remoto
- Interfaccia DICOM per lo scarico della worklist
- Completo di due contenitori porta vials.

b. <u>Per ASUITS</u>:

- N. 1 Isolatore schermato, in Classe "A" a flusso laminare su tutta l'area di lavoro, dotato di adeguato sistema di filtraggio, adatto alla manipolazione e calibrazione di radiofarmaci gamma e beta emittenti in ambito asettico e in accordo a quanto previsto dalle "Norme di Buona Preparazione dei Radiofarmaci in Medicina Nucleare" per la manipolazione di preparazioni sia ottenute per mezzo di kit sia estemporanee e dotato delle seguenti caratteristiche:
  - Tutte le operazioni di routine (ingresso materiali, uscita materiali e preparati, inserimento contenitori schermati, estrazione rifiuti, etc.) dovranno avvenire attraverso precamere ventilate in classe "B".
  - Sistema di sicurezza G.M che consenta l'interdizione all'apertura delle porte dell'isolatore in caso di attività all'interno superiore ad una soglia reimpostata;

- Pannello operatore di controllo esterno di tipo touch-screen, con possibilità di esportazione dei dati su supporto USB;
- Accesso all'area di lavoro tramite un portello frontale, dotato di visiva, con vetro anti X di almeno 50 mm Pb Eq; le due flange per guanti devono essere fissate su pannello in materiale plastico trasparente, chiudibile ed a tenuta, in modo da garantire le operazioni "a freddo" (portello in piombo aperto) ma in condizioni di tenuta d'aria (pannello trasparente chiuso);
- Dotato di calibratore di attività con memorizzati gli isotopi normalmente utilizzati in Medicina Nucleare, PET e Terapia Radiometabolica, e con la possibilità di inserirne di nuovi; accuratezza: ± 2% su tutto il range di misura.
- Dotato di programmi per il controllo di qualità;

o Frazionatore automatico, alloggiato all'interno dell'area di lavoro dell' isolatore, per effettuare il riempimento di siringhe in attività e in volume da un flacone principale di, per radiofarmaci PET e SPECT e dotato delle seguenti caratteristiche:
- Possibilità di dispensare, in caso di emergenza, il radiofarmaco manualmente mantenendo integre tutte le condizioni di sterilità e radioprotezione;
- Il sistema di frazionamento deve essere dotato di un calibratore di attività idoneo e di interfaccia software su PC touch screen, con sistema di calcolo automatico del decadimento e dei volumi delle soluzioni da preparare, database informatico degli eventi e delle dosi preparate, reportistica e stampa di etichette per l'identificazione delle siringhe;
- Il sistema di controllo del dispensatore deve essere interfacciabile al sistema RIS ospedaliero mediante protocollo Dicom.

o N. 1 Iniettore Automatico di Radiofarmaci adatto per radiofarmaci gamma e beta emittenti, di dimensioni ridotte e di semplice utilizzo; classificato come dispositivo medico di classe I, tramite una pompa di infusione dovrà consentire l'esecuzione di iniezioni endovenose automatiche utilizzando kit sterili monouso e contenendo al minimo l'esposizione alle radiazioni ionizzanti dell'operatore durante la fase di iniezione.

5. Valore presunto di fornitura

Il valore presunto della fornitura dovrà considerare una base d'asta non superabile, pena esclusione, articolata come segue:

CT/PET fornitura per ASUIUD e ASUITS

1. $P_{CT\text{-}PET}$: il prezzo a base d'asta per ciascuna apparecchiatura è di **€ 1.393.000 IVA esclusa** ed è comprensiva di:
   - valore dell'apparecchiatura e di tutti gli accessori richiesti inclusi i costi della consegna, il trasporto, l'imballo, lo scarico
   - montaggio, installazione, collaudo, prove funzionali, controlli qualità e relativi viaggi e trasferte;
   - formazione del personale sanitario e tecnico;
   - garanzia di almeno 24 mesi, inclusa la manutenzione full risk sull'intero oggetto della fornitura

- spese per la salute e sicurezza dei lavoratori per il rischio specifico valutati dal datore di lavoro e oneri della sicurezza relativi ai rischi interferenziali valutati dalla stazione appaltante pari a 2.000 €

2. **P_{LAvori}:** il prezzo a base d'asta, per ciascuna Azienda interessata, per la parte opere edili, impiantistiche e protezionistiche e quant'altro necessario è di **€ 82.000,00 € IVA esclusa;**
3. **$P_{Opzioni}$:**il prezzo a base d'asta per le opzioni obbligatorie per ciascuna Azienda interessata, elencate all'articolo precedente, è di € **295.000 € IVA esclusa.**

   Tutti i prezzi per gli opzionali sono comprensivi di:
   - i costi della consegna, il trasporto, l'imballo, lo scarico;
   - montaggio, installazione, collaudo, prove funzionali, controlli qualità e relativi viaggi e trasferte;
   - formazione del personale sanitario e tecnico;
   - garanzia di almeno 24 mesi, inclusa la manutenzione full risk sull'intero oggetto della fornitura.
   - spese per la salute e sicurezza dei lavoratori per il rischio specifico valutati dal datore di lavoro e oneri della sicurezza relativi ai rischi interferenziali valutati dalla stazione appaltante.
4. **P_{FR}**: la base d'asta per la manutenzione annua FULL RISK, per il periodo di post garanzia, per il tomografo CT PET nella configurazione richiesta è di **140.000 € IVA esclusa**. Tale voce è di interesse sia di ASUIUD che di ASUITS.
5. **$P_{FR\text{-}2°liv}$**: la base d'asta per la manutenzione annua FULL RISK di 2° livello, per il periodo di post garanzia, per il tomografo CT PET nella configurazione richiesta da ASUITS è di **112.000 € IVA esclusa.** Tale voce è di interesse di ASUITS.
6. **$P_{FRcarrello}$**: la base d'asta per la manutenzione FULL RISK post garanzia per il carrello frazionatore-infusore**.** Tale voce è di interesse presumibilmente solo di ASUIUD.
7. **$P_{FRcella+iniettore}$**: la base d'asta per la manutenzione FULL RISK post garanzia per la cella+frazionatore+infusore**.** Tale voce è di interesse presumibilmente solo di ASUITS.

Ai fini della valutazione di tutti i possibili elementi che concorrono a determinare il prezzo di gestione e utilizzo di un sistema CT/PET, quale quello richiesto in fornitura, si chiede alle ditte di indicare in occasione dell'incontro già fissato per l'indagine conoscitiva del mercato, la necessità di utilizzare del materiale d'uso dedicato ed esclusivo, mono paziente oppure no, avendo cura anche di fornire un dettaglio completo di tali materiali.
Inoltre, l'incontro conoscitivo sarà anche l'occasione per fornire elementi informativi in merito ad ulteriori funzionalità o moduli accessori disponibili rispetto a quanto richiesto.

6. Griglia di valutazione

Punteggio massimo attribuibile 70 punti con soglia di sbarramento fissata a XX.

CARATTERISTICHE TECNICHE	PUNTEGGIO MAX
1. Gantry CT-PET e Lettino porta paziente	

2. Sottosistema PET	
3. Sottosistema CT	
4. Consolle di controllo ed elaborazione immagini	
5. Calibrazioni e controlli qualità	
PROVA PRATICA	**PUNTEGGIO MAX**
1. …	

7. Criterio di aggiudicazione per la parte economica

L'offerta economicamente più vantaggiosa sarà individuata sulla base del miglior rapporto qualità/prezzo considerando le seguenti voci economiche:

1. **$P_{CT\text{-}PET}$** per ASUITS
2. **$P_{CT\text{-}PET}$** per ASUIUD
3. **P_{LAvori}** per ASUITS
4. **P_{LAvori}** per ASUIUD
5. **$P_{Opzioni}$** per le opzioni obbligatorie per ASUIUD
6. **$P_{Opzioni}$** per le opzioni obbligatorie per ASUITS
7. **P_{FR}** per la manutenzione annua FULL RISK, per il periodo di post garanzia, per il tomografo CT PET nella configurazione richiesta. Tale voce è di interesse sia di ASUIUD che di ASUITS.
8. **$P_{FR\text{-}2°liv}$** per la manutenzione annua FULL RISK di 2° livello, per il periodo di post garanzia, per il tomografo CT PET. Tale voce è di interesse di ASUITS.
9. **$P_{FRcarrello}$** per la manutenzione FULL RISK post garanzia per il carrello frazionatore-infusore. Tale voce è di interesse presumibilmente solo di ASUIUD.
10. **$P_{FRcella+iniettore}$** per la manutenzione FULL RISK post garanzia per la cella+frazionatore+infusore. Tale voce è di interesse presumibilmente solo di ASUITS.
11. Se del caso, il prezzo per il materiale di consumo dedicato ed esclusivo.

8. Strategia di gara

Gli elementi essenziali della strategia di gara consistono in:

- Convenzione della durata di 36 mesi
- Lotto Unico
- Modalità di aggiudicazione: offerta economicamente più vantaggiosa 70 punti qualità (con soglia minima di sbarramento pari a XX) - 30 punti prezzo
- Gara svolta tramite piattaforma informatica.

ALLEGATO 1

SISTEMA DI ELABORAZIONE

Il sistema di elaborazione si intende complementare, ovvero con funzionalità aggiuntive, rispetto a quanto già fornito nelle Aziende del SISR in maniera capillare agli operatori attraverso il sistema PACS.

L'architettura hardware e software del sistema di elaborazione deve essere compatibile con tale accezione come di seguito specificato.

A livello di architettura software, il sistema di elaborazione deve preferibilmente implementare tecnologie che minimizzano l'impatto sui client aziendali ovvero le tecnologia *web* e/o *thin-client* e in particolare:

- Essere eseguibile a livello client, come via browser (destinazione web) o come applicativo software, sui PC aziendali o sulle Workstation PACS delle Aziende
  (*L'aggiudicatario dovrà esplicitamente validare le stesse installazioni, a valle della condivisione delle specifiche per l'installazione con le Aziende, comunque obbligatorie e anticipate nel relativo Allegato* "SPECIFICHE IT" (all. 3 e 4).
- Essere dotato di almeno 2 licenze software *flottanti, comprendenti tutte le funzionalità di elaborazione offerte, fruibili su un numero di postazioni illimitate*.

L'architettura proposta sarà oggetto di valutazione tecnica.

In tutte le soluzioni che lo prevedono, l'applicativo server sarà preferibilmente:

- virtualizzabile nell'infrastruttura informatica Aziendale.
  (*L'aggiudicatario dovrà esplicitamente validare le stesse installazioni, a valle della condivisione delle specifiche per l'installazione con le Aziende, comunque obbligatorie e anticipate nel relativo Allegato* "SPECIFICHE IT" (all. 3 e 4)).

Nel caso il sistema necessiti di hardware fisico, sempre incluso in fornitura, il sistema si intende:

- dotato di hardware server con caratteristiche tecniche adeguate, in generale fornito di tutto quanto necessario a garantire:
  - la sicurezza e ridondanza del dato;
  - prestazioni allo stato dell'arte considerando una crescita di attività di almeno il 50% nei prossimi anni;
  - conforme alle specifiche dettagliate nello specifico Allegato "SPECIFICHE IT" (all. 3 e 4).

In assenza di documentate limitazioni tecniche che devono essere dettagliate in offerta, l'hardware server fornito dovrà essere inoltre:

- installato in un armadio rack standard 19'' da 42U (oggetto di fornitura e dotato di: serratura su tutti i pannelli estraibili, apribile su 4 lati, con fondo rimovibile, ventole di raffreddamento per estrazione forzata a soffitto, passacavi verticali, 2 prese multiple da rack 19'' da almeno 6 posizioni tipo schuko ciascuna con connettore CEE IP44 interbloccato tripolare certificato);
- una macchina server modulare da rack standard 19''
- dotata di doppia scheda di rete 10/100/1000 Base-T, con preferibilmente implementazione del protocollo LACP o link aggregation;
- dotata di doppio modulo di alimentatore tipo hot-plug;
- dotata di dischi rigidi tipo hot-plug;
- dotata di sistema di backup dei sistemi (sistema operativo e applicativo server) e dei database rispondente a quanto riportato nell'Allegato "SPECIFICHE IT" (all. 3 e 4) e tale per cui in ogni caso

non sia necessario, nell'uso ordinario, l'intervento di un operatore sul server fisico (che verrà collocato in un locale tecnico/datacenter ovvero senza permanenza di personale).

Infine, qualora l'offerta preveda anche la fornitura a livello client di hardware dedicato per la gestione del sistema di elaborazione, l'hardware offerto dovrà avere le seguenti caratteristiche:

- display medicale a colori di tipo LCD di dimensione non inferiori a 19" e con risoluzione almeno 2MP;
- dotazione hardware di tipo workstation tale da garantire prestazioni allo stato dell'arte considerando una crescita di attività di almeno il 50% nei prossimi anni;

In ogni caso, il sistema, a livello di funzionalità applicative, dovrà in particolare:

- integrazione con i sistemi informatici in dotazione e uso alle strutture di Medicina Nucleare;
- integrazione con i sistemi informatici in dotazione e uso alle strutture di Radioterapia e Fisica Sanitaria;
- avere la possibilità di esportazione su CD o DVD in formato DICOM di tutta gli oggetti prodotti;
- essere interfacciato con la rete aziendali e il SIO a livello applicativo per la gestione delle immagini prodotte secondo le specifiche contenute all'allegato 6 "Specifiche per l'integrazione delle apparecchiature con il Sistema Informativo Ospedaliero e con il sistema PACS";
- implementare un'interfaccia utente omogenea con la consolle principale;
- costituire un ambiente operativo che ottimizzi e faciliti la gestione delle immagini;
- implementare programmi di elaborazione che consentano una completa gestione delle immagini e dei dati ottenuti con le sequenze e le tecniche precedentemente elencate, e consentire la gestione delle immagini provenienti da altre modalità (Es: TC e RM);
- consentire l'apertura contestualizzata del software specialistico offerto da applicativo PACS con esplicitazione delle interfacce da utilizzare.

In ogni caso l'integrazione con l'infrastruttura sistemistica aziendale di tutti i sistemi informatici offerti, server e client, dovrà avvenire secondo quanto previsto all'ALLEGATO "SPECIFICHE IT" (all. 3 e 4).

ALLEGATO 2

SPECIFICHE PER L'INTEGRAZIONE DELLE APPARECCHIATURE CON IL SISTEMA INFORMATIVO OSPEDALIERO E CON IL SISTEMA PACS

Il sistema offerto **dovrà garantire** l'integrazione con il Sistema Informativo Ospedaliero e il sistema di archiviazione delle immagini PACS in uso presso le Aziende.

Per integrazione con il Sistema Informativo Ospedaliero si intende la possibilità di gestire le anagrafiche, gli ID paziente, le liste di lavoro e lo stato di avanzamento dell'esame, dati gestiti dagli applicativi prodotti da Insiel S.p.A. costituenti il Sistema Informatico Ospedaliero (SIO).

Per integrazione con il sistema di archiviazione e gestione dell'immagini si intende l'integrazione col sistema PACS FVG in uso nelle Aziende, prodotto da Esaote S.p.A, Business Unit Ebit AET.

Tali interfacciamenti devono essere realizzati in rispondenza allo standard DICOM 3 e ad una logica IHE **al massimo livello di implementazione disponibile**, secondo i documenti Integration Statement IHE pubblicati ufficialmente.

Al sistema offerto sarà pertanto richiesta la conformità ai seguenti profili per le seguenti transazioni e attori:

Profili IHE	Attori IHE	Transazioni IHE
SWF	**Acquisition Modality**	**Tutte**
REM	**Acquisition Modality**	**Tutte**
Consistent Time	**Time Client**	**Tutte**

I sistemi offerti dovranno, inoltre, includere in offerta la classe DICOM RT verso i sistemi TPS, in dotazione alle Aziende, per il trattamento radioterapico.

Sarà inoltre positivamente valutata la conformità al profilo IHE Audit Trail e Node Authentication (ATNA), concernente la comunicazione criptata in DICOM e l'audit dell'accesso ai dati, come da Technical Framework IHE ITI, e la possibilità di utilizzare credenziali di dominio per accedere ai sistemi offerti con funzionalità di cache logon.

La mappatura degli attributi tra worklist e studi prodotti deve essere eseguita almeno secondo profilo IHE e comunque esplicitata e concordata in fase di installazione con il personale tecnico delle Aziende.

Le modalità dovranno essere configurate per fornire a livello di trasferimento in rete le massime performance possibili, e pertanto andranno attivate tutte le funzioni standard di compressione e/o classi DICOM più moderne (ad esempio Enhanced MR e Enhanced CT).

Se disponibile, si intende inclusa nella fornitura anche la funzionalità e l'adeguata messaggistica standard per la gestione di più Scheduled Procedure Step o più protocolli di acquisizione da parte della modalità all'interno di un singolo studio DICOM.

Le configurazioni IHE/DICOM disponibili dovranno essere dettagliatamente dichiarate dalla ditta offerente tramite la documentazione richiesta e descritte nell'allegato "*Specifiche per l'integrazione delle apparecchiature con il Sistema Informativo Ospedaliero e con il sistema PACS*".

Per quanto non riguarda l'imaging, la modalità offerta dovrà preferibilmente poter catturare e salvare sul sistema PACS come oggetto DICOM, SR o non, e/o come classe Secondary Capture e/o DICOM Encapsulated PDF, gestita secondo il profilo IHE SWF, una raccolta delle evidenze prodotte, possibilmente selezionabile e presentata come documento, i cui dettagli saranno concordati in fase di installazione con le Aziende.

Per ogni software fornito, incluso ogni software di post-processing ovvero con funzioni di elaborazione sui dati acquisiti, questo **dovrà** poter salvare in formato standard (DICOM ove applicabile) tutti i dati necessari alla fase di post elaborazione.

Il sistema pertanto dovrà permettere il seguente caso d'uso: l'utente dovrà poter archiviare tutti i dati prodotti sul sistema PACS aziendale, cancellare i dati dall'archivio locale del sistema, e poter comunque eseguire tutte le funzioni di elaborazione proprie del sistema PACS Aziendale.

Nel caso limiti tecnici ostacolino tale funzionalità, tali limiti dovranno essere dettagliatamente esplicitati in sede di offerta.

L'intento è evitare la produzione di backup specifici dei dati, sfruttare le doti di sicurezza del dato fornite dall'architettura aziendale e permettere la fruizione a più operatori delle funzionalità di elaborazione. A tal fine dovranno essere evidenziate in sede di offerta anche tutte le classi proprietarie eventualmente utilizzate, al fine di utilizzare il PACS come unico archivio delle elaborazioni specialistiche.

Ogni software fornito dovrà essere dispositivo medico secondo la direttiva 2007/47/CE.

Il software dovrà, ove possibile, prevedere la possibilità di individuare e scaricare/visualizzare - nel caso possa interfacciarsi con un archivio DICOM, attraverso la procedura di DICOM Query/Retrieve solo gli studi prodotti dalla macchina di acquisizione oggetto di offerta.

Se applicabile, dovrà essere possibile discernere anche tra il tipo di esami prodotti (in funzione del richiedente o del protocollo utilizzato).

L'offerente dovrà esplicitare la soluzione tecnico/procedurale offerta e più adatta al proprio tipo di software.

L'offerente dovrà esplicitare tutte le possibili integrazioni configurabili sull'applicativo offerto, ovvero tutte le specifiche che permettono ad un applicativo di terze parti di scatenare

l'esecuzione dell'applicativo offerto e l'apertura di un determinato studio con determinate credenziali (di dominio).

La commissione giudicatrice valuterà la rispondenza ai suddetti requisiti (quale fonte ufficiale di consultazione per la verifica di corrispondenza sarà utilizzato il sito di IHE Europe e i relativi link ivi registrati).

Al momento del collaudo, sarà attuata la contestualizzazione e il test degli stessi in ambito PACS e G2 l'accertamento dell'effettiva funzionalità degli interfacciamenti.

Un esito negativo di tali verifiche porterà alla sospensione delle procedure di collaudo (e relativo pagamento) fino alla loro completa soddisfazione.

Resta altresì inteso che le Aziende, destinatarie della fornitura, dovendo fornire un servizio pubblico, si riservano il diritto di utilizzare le attrezzature anche in assenza di un collaudo formale completo.

In tal caso si procederà alla redazione di un "*collaudo funzionale*" atto a certificare l'utilizzabilità della fornitura in sicurezza ed entro i limiti dovuti alle carenze, ma non darà diritto ad alcun pagamento per il fornitore.

Infine, l'offerente dovrà comunque includere in offerta la formazione specialistica all'uso di tutti i software offerti – *con esclusione del software di acquisizione* - e alla loro reinstallazione (con attestato di partecipazione) anche per i tecnici delle Aziende.

L'offerente dovrà inoltre includere tutto quanto necessario alla reinstallazione del software.

Resta infine inteso che, anche dopo il collaudo funzionale, la disponibilità da parte della ditta aggiudicataria di sviluppare, preferibilmente senza alcun onere a carico delle Aziende della fornitura in oggetto, delle soluzioni migliorative dei profili di integrazione tra la modalità oggetto di fornitura e il sistema PACS/G2.

ALLEGATO 3

SPECIFICHE IT per ASUITS

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare relativamente ad aspetti della sfera dell'IT (Information Technology).

Il sistema nel suo complesso dovrà essere coerente con le politiche di sicurezza e di privacy dell'ASUITS e più in generale dovrà funzionare nel rispetto delle norme di buona tecnica, delle "best practice", dei regolamenti, delle norme tecniche e della legislazione vigente, in particolar modo in materia di sicurezza e privacy.

Il sistema nel suo complesso dovrà rispondere a quanto previsto dal codice in materia di protezione dei dati personali (D. Lgs. 196/2003, cosiddetto codice privacy) e – dal maggio del 2018 – dal regolamento europeo sulla protezione dei dati, nonché le prescrizioni della Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

Inoltre, l'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'ASUITS è chiamata a redigere in ottemperanza alla suddetta circolare AGID.

Il collaudo dell'intero sistema sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un accordo di responsabilità (responsibility agreement) redatto secondo i dettami della norma IEC 80001. Tale documento farà esplicito riferimento all'installazione ASUITS, nei modi e nei termini definiti dal presente documento e che verranno a presentarsi all'atto pratico dell'installazione e della manutenzione del sistema nel tempo. Il responsibility agreement conterrà espliciti riferimenti alla "marcatura CE" dei sistemi offerti ed al fatto che i requisiti essenziali di sicurezza non verranno inficiati nella particolare installazione ASUITS, così come intesa sopra.

Specifiche di integrazione con l'infrastruttura IT

I sistemi oggetto di fornitura dovranno essere integrati ed interfacciati con l'infrastruttura informatica di rete e sistemistica dell'ASUITS, secondo quanto riportato nel seguito.

I dispositivi dotati di connettività di rete (host) che necessitano di collegamento alla rete dati per svolgere le funzioni richieste, potranno essere inseriti nella LAN ASUITS seguendo uno dei due scenari, mutuamente esclusivi, descritti nel seguito.

Scenario 1

Nel primo scenario, agli host oggetto di fornitura verrà assegnata una specifica classe di indirizzi IP statici coerente con il piano di indirizzamenti ASUITS. Tali dispositivi verranno

inseriti in una VLAN dedicata, assegnata dall'ASUITS, dalla quale potranno effettuare solo il traffico necessario per svolgere le funzioni richieste e traffico relativo all'assistenza remota da parte del fornitore. La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall, per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso.

È attivo sulla LAN ASUITS un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x e realizzato per mezzo di tecnologia Microsoft NPS. Tutti gli host forniti e collegati alla LAN ASUITS dovranno essere tali da consentire l'autenticazione di rete tramite MAC address (cosiddetta MAC authentication).

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUITS, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'ASUITS. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali; nel caso in cui l'aggiudicatario non fosse in condizione di garantire tale configurazione, sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza sulla base della quale l'ASUITS si riserverà di attivare connessioni di tipo site-to-site. Nel presente scenario, a valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza potrà avvenire con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi e della loro configurazione da parte dell'ASUITS.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, nel presente scenario, lo strumento messo a disposizione dall'ASUITS è il proxy di navigazione autenticata, gestito da Insiel e basato su tecnologia Blue Coat: gli host forniti dovranno essere tali da consentire la configurazione del proxy internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici. Verranno effettuate specifiche eccezioni all'autenticazione basate su IP sorgente che consentiranno il traffico solo sulle porte necessarie e solo verso gli IP necessari. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'ASUITS per la definizione delle suddette eccezioni.

Nel presente scenario l'aggiudicatario sarà responsabile in toto delle prescrizioni di ambito sicurezza informatica e privacy, secondo quanto previsto dal quadro legislativo e normativo

vigente, nonché dal presente documento; in particolare per quanto riguarda le politiche: di autenticazione, autorizzazione e accounting (AAA), di backup e disaster recovery, sugli aggiornamenti di sicurezza di tutti i software installati sugli host oggetto di assistenza, di protezione antivirus e da altre tipologie di cyber attacco.

Si specifica infine che, qualora l'aggiudicatario aderisca al presente scenario, sono da intendersi oggetto di fornitura eventuali PC client ed eventuali server fisici che si rendessero necessari, nonché tutto l'hardware di tipo IT necessario al corretto e sicuro funzionamento dei sistemi oggetto di fornitura.

Gli eventuali server forniti dovranno, inoltre, essere del tipo da installazione da rack standard 19" con una occupazione massima di 2 rack unit e dotati di doppio modulo di alimentazione integrato.

Inoltre tali server non dovranno/potranno per alcun motivo essere utilizzati dagli operatori come stazioni di lavoro.

Scenario 2

Nel secondo scenario, in alternativa, l'aggiudicatario potrà integrare i sistemi oggetto di fornitura con l'infrastruttura sistemistica dell'ASUITS. Di seguito vengono riportate, in prima istanza, alcune caratteristiche peculiari dell'infrastruttura informatica dell'ASUITS; successivamente vengono definite le specifiche di interfacciamento all'infrastruttura ASUITS che i sistemi oggetto di fornitura dovranno avere in caso di adesione al presente scenario. L'architettura generale e le caratteristiche dei singoli elementi dei sistemi forniti dovranno in ogni caso essere pienamente coerenti e allineati con le logiche di seguito descritte.

L'ASUITS è dotata di un dominio Active Directory (AD) 2008 R2 (aouts.it), che presto verrà migrato alla versione 2012. In ciascuno dei due principali siti AD (Ospedale di Cattinara e Ospedale Maggiore) è presente almeno un domain controller global catalog ed un file server. Ogni account del directory service aziendale è associato ad almeno un gruppo di dominio (gruppi locali al dominio, domain local) corrispondente alla struttura amministrativa ASUITS di appartenenza.

La default domain policy impone l'utilizzo di password complesse di almeno 12 caratteri, con password history a 24 e cambio password obbligatorio ogni 90 giorni. Gli aggiornamenti di sistema per i client e per i server vengono distribuiti tramite il servizio Microsoft WSUS, su base mensile e appena rilasciati da Microsoft.

Le postazioni di lavoro ASUITS (PC) sono inserite nel dominio aouts.it. Esse sono dotate di sistema operativo Microsoft Windows XP Professional Italiano SP3 o Microsoft Windows 7 Professional Italiano e di browser Microsoft Internet Explorer 8 (nel seguito anche IE8) e Google Chrome ultima versione; l'hardware di tali postazioni è eterogeneo e varia, nelle prestazioni e caratteristiche di base, da

- CPU Intel Core Due Duo 1,8 GHz o equivalente
- memoria RAM DDR2 1 GB
- hard disk da 250 GB

a

- CPU Intel Pentium G3420 3,2 GHz o equivalente
- memoria DDR3 4 GB
- 2 hard disk da 500 GB

Tutte le postazioni di lavoro ASUITS sono dotate di connettività di rete Gigabit Ethernet (secondo quanto definito dagli standard IEEE 802.3). Tutti gli operatori aziendali accedono, nell'operatività quotidiana, alle postazioni di lavoro (PC) tramite account e relative credenziali personali con bassi privilegi; su tutte le postazioni è attivo il servizio Microsoft DEP (Data Execution Prevention).

Il protocollo di rete utilizzato è IPv4. La risoluzione dei nomi è basata esclusivamente sul servizio DNS (Domain Name Service), integrato in AD, che accetta solo registrazioni sicure. I server Microsoft aziendali appartengono a due subnet IP dedicate – una per ciascun sito AD – e sono virtualizzati tramite due sistemi VMware vSphere v5.x, uno installato presso l'Ospedale di Cattinara ed uno presso l'Ospedale Maggiore. L'architettura di rete ASUITS è realizzata in modo che tutti i servizi sono raggruppati nel datacenter (CED) ASUITS del sito di pertinenza; in particolare i server virtualizzati appartengono ad una VLAN dedicata.

In generale la LAN ASUITS è una rete layer 2-3 (pila ISO/OSI) a due livelli (core e periferia): per ciascun presidio, gli apparati di periferia sono collegati in layer 2 agli apparati di core; il data center è collegato direttamente agli apparati di core in layer 3. Il traffico è suddiviso in VLAN separate, a cui corrispondono specifiche sottoreti IP, sulla base della tipologia di host e del traffico dati che effettuano, ovvero nell'intento di isolare il traffico dati stesso sulla base dei servizi e dei domini di competenza degli amministratori degli host. Il traffico dati tra apparati di periferia appartenenti a differenti VLAN non è in generale consentito, in quanto i flussi funzionali sono sempre dal data center (CED) ASUITS alla periferia e viceversa.

È attivo sulla LAN ASUITS un servizio DHCP (Dynamic Host Configuration Protocol) che in generale rilascia gli indirizzi IP a tutti gli host in rete, ad esclusione dei server (per i quali sono previste specifiche configurazioni) e degli host con IP statico.

Come precedentemente riportato, è attivo sulla LAN ASUITS un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x e su tecnologia Microsoft NPS. L'autenticazione è basata, a seconda delle caratteristiche dell'host, su uno dei seguenti criteri (ordinati per livello di sicurezza e quindi per preferenza di implementazione):

- account macchina Microsoft Active Directory, se l'host è dotato di client AD;
- nome utente e password, se l'host non è dotato di client AD ma è dotato di client IEEE 802.1x;
- MAC address, solo se l'host non è dotato di client IEEE 802.1x.

La struttura di backup ASUITS è basata su due tape library: una Sun Storage Tek SL500 posta nel data center dell'Ospedale di Cattinara ed una Sun Storage Tek SL48 posta nel data center dell'Ospedale Maggiore. Tramite il software Symantec Backup Exec 10d, le tape library effettuano – con periodicità variabile a seconda dei casi – le copie di sicurezza: dei sistemi operativi di tutti i server ASUITS, della configurazione dei DB ASUITS, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi.

In ciascuno dei due presidi ospedalieri (Cattinara e Maggiore) è presente un server Microsoft SQL 2008 R2 64 bit; tutti i database delle applicazioni aziendali basati su tale tecnologia vengono ivi istanziati. Tali server supportano solo l'autenticazione nativa (Native Mode o Windows Integrated) e l'istanza di default non viene utilizzata.

L'applicativo antivirus (AV) aziendale è l'ESET NOD32 v4.x distribuito su tutti i client e aggiornato automaticamente ogni tre ore.

Su tutti i client aziendali è presente l'agente CA IT Client Manager v14.x, che consente l'accesso interattivo alle sessioni utente per fini di assistenza tecnica.

Nel presente scenario, gli eventuali server forniti dovranno essere virtualizzati nel sistema ASUITS VMware vSphere v5.x del sito che verrà indicato dall'ASUITS (Cattinara o Maggiore) e seguirne le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, di backup e di disaster recovery. Potranno essere create una o più macchine virtuali a seconda delle necessità e dell'architettura proposte dall'aggiudicatario, ma in ogni caso tali macchine dovranno essere compatibili almeno con il sistema operativo Windows Server 2008 R2 Standard/Enterprise/Datacenter Edition ENG e inserite nel dominio aouts.it e conseguentemente nel sistema WSUS ASUITS.

Tutte le licenze Windows Server necessarie al funzionamento del sistema, non sono da intendersi a carico del fornitore e non saranno in alcun caso di tipo OEM, bensì licenze Retail intestate all'ASUITS e comunque in ogni caso compatibili con l'ambiente di virtualizzazione dell'ASUITS descritto precedentemente.

Allo scopo di uniformare i sistemi forniti agli standard ASUITS, compresi quelli di sicurezza e autorizzazione (authorization), tali macchine server verranno inserite in una Organizational Unit (OU) generica dedicata ai server ASUITS oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l'ASUITS; la default domain policy verrà applicata in ogni caso su tutte le OU.

Ai server verrà in ogni caso assegnata una opportuna classe di indirizzi IP fissi.

Nel presente scenario, i dati acquisiti e generati dal sistema e/o i loro riferimenti, nonché tutti quelli direttamente o indirettamente necessari al funzionamento degli applicativi forniti, dovranno essere organizzati in uno o più RDBMS, che potranno essere istanziati sui server Microsoft SQL ASUITS a discrezione dell'aggiudicatario; in tal caso dovranno seguirne le politiche di gestione, comprese quelle di backup e disaster recovery. In particolare potranno essere dedicati ai sistemi forniti una o più istanze oppure uno o più database in accordo con l'ASUITS.

In base alla specifiche scelte progettuali e di infrastruttura, l'aggiudicatario dovrà usufruire della struttura di backup ASUITS per i sistemi operativi di tutti i server e per la configurazione dei database. Dovrà essere fornito all'ASUITS supporto per il loro inserimento nel sistema di backup dell'ASUITS, nonché per la redazione delle procedure di backup e disaster recovery.

Nel presente scenario, lato utente, ovvero lato postazione ASUITS (PC client), gli applicativi eventualmente forniti potranno essere basati su tecnologia client/server o web.

Gli eventuali applicativi client forniti nell'ambito della presente fornitura, necessari all'espletamento di una o più funzionalità dei sistemi forniti, verranno installati sulle postazioni ASUITS – senza limitazioni in termini di numero di postazioni – e dovranno essere adeguati alle caratteristiche software e hardware delle postazioni stesse, in particolare alle policy del dominio aouts.it e conseguentemente a quelle del sistema WSUS ASUITS. La distribuzione sulle postazioni di lavoro ASUITS di tali applicativi, nonché degli aggiornamenti, verrà eseguita per mezzo del sistema di software distribution di Microsoft AD, cioè tramite pacchetti MSI (Microsoft Installer), in alternativa l'installazione verrà effettuata – con analoghe caratteristiche qualitative e di risultato – da parte dell'aggiudicatario.

Gli eventuali applicativi web forniti nell'ambito della presente fornitura, dovranno essere compatibili con i browser web IE8 e Google Chrome ultima versione, attualmente installati sulle postazioni ASUITS.

Eventuali PC oggetto di fornitura potranno essere inseriti nel dominio aouts.it a condizione di seguire le policy e caratteristiche dei PC ASUITS, così come descritte nel presente documento.

Nel presente scenario, tutte le funzionalità dei sistemi forniti dovranno essere garantite con il sistema di indirizzamento IP dinamico (DHCP) attivo sulle postazioni ASUITS. Nel caso in cui l'architettura e le caratteristiche tecniche dei sistemi forniti impedissero tale configurazione, l'aggiudicatario sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza e sulla base della quale l'ASUITS si riserva di create sul servizio DHCP opportune e specifiche configurazioni (reservation).

Nel presente scenario, tutte le funzionalità dei sistemi fornito dovranno essere garantite con il client antivirus aziendale ESET NOD32 v4.x di cui ogni postazione ASUITS è dotata, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'ASUITS, a meno di eccezioni concordate con l'ASUITS. Inoltre, tutte le

funzionalità dei sistemi forniti dovranno essere garantite con l'agente CA IT Client Manager v14.x di cui ogni postazione ASUITS è dotata.

Nel presente scenario, eventuali host (di tipologia non server) oggetto di fornitura che non siano dotati di client AD e che necessitano di connettività con la rete dati ASUITS, verranno connessi alla stessa con una specifica classe di indirizzi IP statici assegnata dall'ASUITS. Tali dispositivi verranno inseriti in una VLAN dedicata, assegnata dall'ASUITS, dalla quale potranno solo effettuare traffico specifico da e verso gli eventuali applicativi server forniti e installati nella virtualizzazione ASUITS e traffico relativo all'assistenza remota da parte del fornitore. La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico. In ogni caso, gli host non dotati di client AD non avranno visibilità di rete sugli applicativi client/web installati sulle postazioni ASUITS. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sul firewall, per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso.

Nel presente scenario, in generale, sia lato server che lato client, se non diversamente comunicato dall'aggiudicatario, verranno installate tutte le patch rilasciate da Microsoft. Potranno essere segnalate all'ASUITS patch contrassegnate come "non applicabili", solo se di natura non critica; per tali patch "non applicabili" verranno generate dall'ASUITS delle eccezioni in WSUS, che avranno una durata limitata di 6 mesi entro cui l'aggiudicatario dovrà provvedere alla risoluzione del problema di compatibilità.

Nel presente scenario, tutti i dispositivi forniti collegati alla LAN ASUITS dovranno autenticarsi in rete secondo il protocollo 802.1x, con uno dei tre criteri sopra esposti. In particolare:

- tutti i client tramite account macchina;
- tutti gli host non dotati di client AD, dovranno autenticarsi per mezzo di nome utente e password o di MAC address.

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUITS, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'ASUITS. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali; nel caso in cui l'aggiudicatario non fosse in condizione di garantire tale configurazione, sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza sulla base della quale l'ASUITS si riserverà di attivare

connessioni di tipo site-to-site. Nel presente scenario, a valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza: dovrà avvenire esclusivamente con gli strumenti aziendali ASUITS CA IT Client Manager v14.x e Microsoft Windows RDP, nel caso di host dotati di client AD; potrà avvenire con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi e della loro configurazione da parte dell'ASUITS, nel caso di host non dotati di client AD.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, nel presente scenario, lo strumento messo a disposizione dall'ASUITS è il proxy di navigazione autenticata, gestito da Insiel e basato su tecnologia Blue Coat: gli host forniti dovranno essere tali da consentire la configurazione del proxy internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici.

È in uso presso l'ASUITS una soluzione di single sign-on (SSO) per l'autenticazione (authentication) ed il conseguente accesso alle risorse informatiche. Di seguito vengono riportate, in prima istanza, le caratteristiche peculiari del SSO ASUITS e successivamente vengono definite le specifiche dei sistemi da fornire in tal senso, nell'ambito del presente scenario.

Il SSO ASUITS permette al singolo account di autenticarsi una sola volta e di essere successivamente autenticato automaticamente – ovvero in maniera trasparente e senza dover reinserire le proprie credenziali – ogni volta che tenta di accedere ad una risorsa di rete di rete a cui è abilitato. Gli account possono essere associati sia a credenziali personali (ad uso esclusivo di una persona fisica, ovvero di un operatore) che impersonali (ad uso non esclusivo di una sola persona fisica, ovvero di un operatore), nonché account digitali (a titolo di esempio non esaustivo, un'applicazione che deve autenticarsi verso un'altra applicazione, un servizio, ecc.). Per risorsa di rete si intende un qualsiasi servizio erogato su qualsiasi sistema operativo (a titolo di esempio non esaustivo, l'accesso: ad un applicativo web o client/server, interattivo ssh, a file, a stampanti, ecc.).

La soluzione SSO ASUITS prevede un repository centrale realizzato attraverso il protocollo Lightweight Directory Access Protocol (LDAP), che contiene gli account e la configurazione delle macchine e dei servizi correlati; tale repository è il directory service aziendale Microsoft AD 2008 R2 (aouts.it) e non accetta bind anonimi. Per quanto riguarda l'autenticazione degli account, questa si basa sul protocollo kerberos versione 5 (in seguito anche v.5) e viene effettuata dal dominio aouts.it. Il SSO ASUITS ricalca quanto trova nome in letteratura come "Windows Integrated Single Sign-On" o "Windows Integrated Authentication". Le credenziali utilizzate sono ad oggi "nome utente" e "password", e seguono le politiche descritte precedentemente; in futuro verranno adottati sistemi basati su certificati digitali.

I sistemi forniti dovranno essere coerenti ed integrati con la soluzione di SSO ASUITS. Le modalità operative di accesso agli applicativi ed ai sistemi forniti da parte degli operatori dovranno essere personali, avverranno cioè per mezzo di credenziali informatiche personali; a queste potranno inoltre essere associati uno o più ruoli.

Come suddetto, l'unico repository di account ASUITS (personali e impersonali) è il directory service Active Directory e a ciascun account di dominio sono associate le rispettive credenziali informatiche. In tal senso tutte le credenziali personali, previste negli applicativi e nei sistemi forniti, dovranno essere quelle del dominio aouts.it; gli account associati a credenziali personali si autenticheranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi, in base al proprio livello di autorizzazione (definito in base al ruolo) e a seguito dell'accesso alla sessione di lavoro. Tutte le credenziali impersonali, eventualmente presenti negli applicativi e nei sistemi forniti, dovranno essere opportunamente create e configurate nel dominio aouts.it; gli account AD associati a credenziali impersonali si autenticheranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi in base al proprio livello di autorizzazione minimo necessario e a seguito di auto log-on (in ogni caso senza l'immissione delle credenziali impersonali da parte degli operatori).

In ogni caso l'autenticazione degli account personali e impersonali dovrà avvenire tramite protocollo kerberos v.5. Ciò significa in particolare che, nell'architettura kerberos, i domain controller del dominio aouts.it svolgeranno il ruolo di KDC (Key Distribution Center), mentre gli applicativi/sistemi forniti assolveranno i ruoli di Client e SS (Service Server); a titolo di esempio non esaustivo, i Service Server forniti dovranno essere in grado di interpretare e validare correttamente i Service Ticket inviati dai Client, nonché instaurare successivamente le Client/Server Session (sia in caso di architetture fornite tipo client/server che web).

L'autorizzazione (authorization) è intesa in questo contesto come profilatura dell'account e gestione dei ruoli e delle abilitazioni ad esso associati. In particolare gli applicativi/servizi forniti dovranno importare gli account da abilitare dal repository LDAP ASUITS (dominio aouts.it), sulla base di un Gruppo AD specifico che verrà realizzato ad hoc, e circoscrivere la profilatura e l'attribuzione dei ruoli all'interno degli applicativi/servizi stessi solo per gli account appartenenti a quello specifico gruppo. In via propedeutica al collaudo dei sistemi forniti, l'aggiudicatario dovrà installare la consolle amministrativa su un client ASUITS afferente alla SC Informatica e Telecomunicazioni e dovrà formare una risorsa ASUITS alla profilatura degli account nei sistemi forniti, in modo da rendere l'ASUITS autonoma nelle procedure di abilitazione e successiva reinstallazione della consolle amministrativa.

Non dovrà essere possibile creare, configurare e profilare altri account non appartenenti ad AD, ad eccezione di specifiche situazioni opportunamente motivate ed in ogni caso concordate con l'ASUITS. La profilatura e l'attribuzione dei ruoli degli applicativi/servizi forniti dovrà essere tale da garantire il massimo livello di dettaglio di configurazione, ed in ogni caso dovrà garantire tutto quanto descritto nel presente documento.

Altre soluzioni di SSO, autenticazione e account/identity management non saranno consentiti.

Specifiche tecniche sicurezza informatica

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare, sia nello Scenario 1 che nello Scenario 2, relativamente ad aspetti generali della sfera dell'IT (Information Technology) con particolare riferimento alla sicurezza informatica (security).

Vale in ogni caso il principio generale per cui la sicurezza informatica è un fattore intrinseco dell'architettura dei sistemi oggetto della presente fornitura e delle caratteristiche tecniche degli elementi che li compongono; perciò l'aggiudicatario dovrà garantire che, sia l'architettura che gli elementi, siano progettati, implementati e manutenuti nel tempo in modo da minimizzare il rischio informatico residuo (sia di "attacchi ai sistemi" che di "attacchi dai sistemi").

Inoltre i sistemi forniti dovranno rispettare le seguenti prescrizioni.

In generale, tutti gli elementi forniti non dovranno essere in alcun caso fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo definitivo dei sistemi.

In generale, tutti i software forniti dovranno essere:

- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
- dotati di labeling (GUI) in Italiano e tali che le impostazioni internazionali di Microsoft Windows (se presente) siano sempre IT standard, comprese le tastiere;
- stabili, in particolare che siano in grado di gestire le eccezioni;
- sicuri, sia dal punto di vista della sicurezza informatica che della qualità delle funzioni svolte;
- ottimizzati, in termini di rapporto tra uso delle risorse e prestazioni;
- sviluppati tenendo conto dei principi del "ciclo di vita del software" e dell'"analisi del rischio", secondo le norme tecniche (o principi e metodologie almeno equivalenti) e le best practice internazionali; in ogni caso non dovranno utilizzare librerie deprecate e/o obsolete, né dovranno essere scritti e sviluppati con versioni del linguaggio di programmazione fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo definitivo dei sistemi;
- pensati, progettati e realizzati nel rispetto del quadro legislativo vigente, nonché in modo da non mettere in alcun caso gli operatori in condizione di violare il quadro legislativo stesso nell'espletamento del normale utilizzo dei sistemi;

- installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità, nello specifico contesto dell'ASUITS, così come descritto nel presente documento;
- manutenuti e gestiti in modo da conservare e mantenere stabili nel tempo tutte le caratteristiche possedute al momento del collaudo definitivo.

In particolare, tutti i software forniti che verranno installati su dispositivi collegati alla LAN ASUITS e inseriti nel dominio aouts.it, dovranno essere eseguiti sempre:

- in un contesto user space per i client,
- come servizio per tutti i server,
- come servizio per i client se non è richiesta interazione con l'operatore,

ed in ogni caso non dovranno essere modificati in alcun modo i permessi di default del file system e del registro di sistema Microsoft (ove presente).

In particolare, per quanto concerne le configurazioni:

- quelle degli applicativi server dovranno risiedere in database e comunque mai sui dischi locali dei PC client;
- quelle globali degli applicativi client (ovvero non riferite alle personalizzazioni dei singoli account) dovranno risiedere in un file nella cartella di installazione dell'applicativo (a cui quindi avranno accesso solo gli utenti con ruolo Amministratore) oppure nel registro di sistema (ove presente) nella sottochiave appositamente creata in fase di installazione in HKEY_LOCAL_MACHINE\SOFTWARE, ed in ogni caso informazioni critiche in termini di sicurezza e funzionalità (a titolo di esempio non esaustivo: le stringhe di connessione ai database, le credenziali necessarie per instaurare eventuali altre connessioni client/server, ecc.) dovranno essere cifrate almeno con algoritmo AES256;
- quelle personali degli applicativi client (ovvero riferite alle personalizzazioni dei singoli account) dovranno risiedere nel profilo dell'account a cui si riferiscono (ove presente).

Ovvero, in ogni caso non dovranno risiedere configurazioni globali degli applicativi client nei profili degli account, né altresì configurazioni personali degli applicativi client fuori dai profili degli account.

In particolare, in tutti i software forniti che si configurano come "strumenti elettronici" che effettuano trattamento di dati personali, così come definito nel D.Lgs. 196/03 "Codice in materia di trattamento dei dati personali" e s.m.i., dovranno essere adottate:

- le "misure minime di sicurezza" previste dal suddetto codice e dal relativo disciplinare tecnico (Allegato B, D.Lgs. 196/03);
- le "idonee e preventive misure di sicurezza" previste dal medesimo codice all'art. 31 nell'ambito degli obblighi di sicurezza.

Dovranno essere rispettati tali obblighi in particolare in termini di:

- adozione di un "sistema di autenticazione informatica", comunque nel rispetto di quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
- adozione di un "sistema di autorizzazione", comunque nel rispetto di quanto riportato nel presente documento relativamente alle modalità di autorizzazione (authorization) degli account personali;
- "protezione degli strumenti elettronici e dei dati", comunque nel rispetto di quanto riportato nel presente documento relativamente alla sicurezza informatica;
- "copie di sicurezza" e di "ripristino della disponibilità dei dati e dei sistemi", comunque nel rispetto di quanto riportato nel presente documento relativamente alle politiche di backup e di disaster recovery.

L'aggiudicatario dovrà individuare, all'interno della sua organizzazione, un "Responsabile per la privacy". Questi verrà in tal senso nominato dal titolare del trattamento dei dati personali ASUITS e dovrà inviare, nel rispetto delle procedure ASUITS, le richieste di abilitazione degli incaricati e degli amministratori afferenti all'aggiudicatario (anche quelle necessarie per lo svolgimento delle attività di assistenza remota). I relativi account e le relative autorizzazioni verranno sempre erogate dall'ASUITS e a livello personale, secondo le proprie procedure ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

Per quanto concerne gli "account amministrativi" (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), questi:

- potranno, nel caso di account amministrativi locali di default (a titolo di esempio non esaustivo: "admin", "administrator", "root", ecc.), essere impersonali e dovranno essere tutti comunicati all'ASUITS, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi locali ulteriori rispetto a quelli di default;
- dovranno, nel caso di account amministrativi non locali che consentano l'accesso interattivo a macchine/sistemi/applicativi collegati alla LAN ASUITS, essere sempre personali e rispettare quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
- potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN ASUITS, essere impersonali e dovranno essere tutti comunicati all'ASUITS, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi in numero maggiore dello stretto necessario;
- potranno, nel caso di account digitali amministrativi, essere configurati dall'aggiudicatario solo in accordo con l'ASUITS e dovranno essere impersonali, dovranno essere tutti comunicati all'ASUITS, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza;

- non dovranno, nel caso di account amministrativi impersonali, essere in alcun caso presenti.

Per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel presente documento, questi non dovranno in alcun caso permettere:

- di modificare le configurazioni, impostazioni e settaggi di macchine/sistemi/applicativi;
- di visualizzare, modificare o cancellare dati personali diversi da quelli eventualmente trattati contestualmente all'uso dell'account stesso.

Eventuali dati personali salvati in ulteriori archivi, diversi da quelli descritti nel presente documento, saranno ammessi solo con funzioni di "archivi provvisori", ovvero di passaggio intermedio dei dati prima dell'invio agli archivi definitivi. I dati personali devono permanere negli archivi provvisori il minor tempo possibile, ovvero per un tempo massimo che sia configurabile e che in ogni caso non superi le 24 ore naturali, con l'implementazione di opportune procedure di cancellazione automatica che non consentano il recupero locale dei dati.

In ogni caso l'accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo da parte degli account personali e degli account digitali autorizzati, sulla base di opportuni permessi settati in modo che il livello dei privilegi di accesso sia il più basso possibile e preferibilmente che l'accesso ai dati avvenga sempre per tramite dell'applicativo e non direttamente da parte dell'account.

Non è consentita l'archiviazione, anche temporanea ed anche in forma anonima, dei dati su macchine situate esternamente rispetto alla rete dati dell'ASUITS, salvo esplicita autorizzazione da parte dell'ASUITS.

ALLEGATO 4

SPECIFICHE IT per ASUIUD

Documento in fase di redazione.