GARA A PROCEDURA APERTA AI SENSI DELL'ART 60 DEL D. LGS. N. 50/2016 PER LA STIPULA DI UNA CONVENZIONE PER L'AFFIDAMENTO DELLA FORNITURA IN FULL SERVICE DI SISTEMI PER L'ESECUZIONE DI TEST DIAGNOSTICI IN EMATOLOGIA PER UN PERIODO DI 60 MESI – ID.15REA015

PRECISAZIONE DEL 27/09/2016

DOMANDE:

1)

facendo riferimento al procedimento di gara "ID.15REA015 – Procedura aperta per la stipula di una convenzione per l'affidamento della fornitura in full service di sistemi per l'esecuzione di test diagnostici in ematologia", con la presente chiediamo di poter conoscere i quantitativi di CBC, reticolociti ecc. posti in gara per il Presidio Ospedaliero di Udine.

2) 1) Lotto 1 – Paragrafo "Caratteristiche Tecniche dei sistemi richieste" ASUI.TS-PRESIDIO OSPEDALIERO DI CATTINARA "….*In particolare si deve prevedere un sistema di visione che permetta la lettura degli strisci contemporaneamente ad almeno due laureati che operino in due sedi diverse*". Si chiede di confermare che le due sedi sono da intendersi Monfalcone e Ospedale Maggiore Trieste.

2) Lotto 1 - Paragrafo "Caratteristiche Tecniche dei sistemi richieste" ASUI.TS-PRESIDIO OSPEDALIERO OSPEDALE MAGGIORE - TRIESTE "….*In particolare si deve prevedere un sistema di visione che permetta la lettura degli strisci contemporaneamente ad almeno due laureati che operino in due sedi diverse*". Si chiede di confermare che le due sedi sono da intendersi Monfalcone e Cattinara.

3) Lotto 1 - Paragrafo "Caratteristiche Tecniche dei sistemi richieste" ASUI.TS-PRESIDIO OSPEDALIERO DI MONFALCONE "….*In particolare si deve prevedere un sistema di visione che permetta la lettura degli strisci contemporaneamente ad almeno due laureati che operino in due sedi diverse*". Si chiede di confermare che le due sedi sono da intendersi Cattinara e Ospedale Maggiore di Trieste.

4) Lotto 1 – Paragrafo "Caratteristiche tecniche minime richieste, pena di esclusione", A) STRUMENTAZIONE ANALITICA "*1. Determinazione e conteggio di eritroblasti, reticolociti con relative frazioni maturative*", si chiede di confermare che il parametro IRF (Frazione Immatura di Reticolociti) soddisfi il requisito relativo alle frazioni maturative dei reticolociti. Si evidenzia infatti che, come riportato dalla pubblicazione SIMeL "Linee guida per il referto ematologico – P. Cappelletti - GdSE-SIMeL", tale parametro viene annoverato tra quelli refertabili per il pannello dei rericolociti.

5) Lotto 1 – Paragrafo "Caratteristiche tecniche minime richieste, pena di esclusione", A) STRUMENTAZIONE ANALITICA "*7.Monitoraggio dei volumi dei reagenti a bordo*", si chiede di confermare che, alternativamente, il monitoraggio della % di reagente a bordo soddisfi la richiesta.

6) Per il Lotto 1 e Lotto 2, si chiede di fornire le planimetrie di tutti i presidi in formato AutoCAD (.dwg).

7) Lotto 2 – Paragrafo “Caratteristiche degli analizzatori ematologici (per le sedi CORELab, spoke, Dipartimento Immunotrasfusionale e Laboratorio della Clinica Ematologica)” al punto “*Consentire il monitoraggio dei volumi dei reagenti a bordo*”, si chiede di confermare che, alternativamente, il monitoraggio della % di reagente a bordo soddisfi la richiesta.
8) Lotto 2 – Paragrafo “Strisciatore/Coloratore” ai punti “*Dotato di lettura da barcode e stampa identificativo (nome e n richiesta) su vetrino* e *Acquisizione discrezionale dei vetrini da strisciare*”, si chiede di confermare che le due richieste sono da riferirsi al solo coloratore automatico per il laboratorio centrale di Udine.
9) Lotto2 – Paragrafo “Carichi di lavoro”, si chiede di indicare i carichi di lavoro annuali suddivisi per tipologia di esame (Emocromo, reticolociti , eritroblasti, Liquidi Biologici) relativi alla Sede di Udine (CORELab), al Dipartimento Immunotrasfusionale sede di Udine e alla Clinica Anestesiologica.
10) Lotto 2 – Paragrafo “Carichi di lavoro”, si chiede di indicare, per ciascun presidio ove necessari, il numero di vetrini annui.
11) Lotto 2 – Si chiede di confermare che i test per controlli giornalieri e calibrazioni siano già inclusi nei carichi di lavoro annuali.
12) Si chiede se la richiesta di produrre un elenco numerato dei documenti presenti all’interno della busta e che tali documenti dovranno essere numerati in ogni pagina con indicazione sulla prima pagina del numero di pagine complessivo di ogni documento sia riferita solamente alla busta n. 2 tecnica-qualitativa oppure sia riferita a tutte le n.3 buste.
13) BUSTA 1) Documenti di Partecipazione – ALLEGATO A punto l) Con riferimento all’attività di assistenza tecnica a carico dell’aggiudicatario, in considerazione della particolare specializzazione richiesta per l’esecuzione della predetta attività, dovuta ad una complessità tecnologica che connota la strumentazione tale da attribuirle un carattere di unicità, nell’ipotesi di affidamento in subappalto si chiede se sia possibile per il concorrente, ai sensi dell’art. 105 comma 6 del D.lgs. 50/2016, indicare solo la prestazione che intende affidare in subappalto.
14) DISCIPLINARE DI GARA – Art. 5 (Caratteristiche offerta economica) – Pagina 5 L’art. 5 inizia con la frase: “ L’offerta economica (Busta n. 2) dovrà essere redatta…”. Si chiede conferma che trattasi di refuso e che l’offerta economica dovrà essere contenuta nella busta n. 3.
15) BUSTA 3) OFFERTA ECONOMICA - Allegato E
- Si chiede la possibilità di offrire il materiale consumabile come calibratori, controlli, soluzioni di lavaggio e consumabili delle stampanti in sconto merce.
- Con riferimento alla richiesta di indicare “il prezzo unitario” di reagenti e materiali di consumo, si chiede se con tale richiesta s’intende il prezzo unitario per tipologia di esame. (esempio: prezzo unitario a emocromo, prezzo unitario a reticolociti ecc.).
- Si chiede conferma che la percentuale di sconto richiesta nell’ultima colonna della tabella nell’allegato E sia lo sconto medio applicato ai prodotti offerti.
16) BUSTA 2) OFFERTA TECNICA
In riferimento alla prescrizione di presentare la documentazione tecnica in formato cartaceo e su supporto informatico si chiede conferma che è sufficiente che il CD richiesto contenga in formato pdf la stessa documentazione trasmessa in forma cartacea con la sola differenza che la versione cartacea è firmata manualmente mentre la documentazione su CD non riporta detta firma.
A ciò si aggiunge la possibilità che su detto supporto elettronico, non riscrivibile, venga apposta la dichiarazione attestante che i documenti in esso contenuti sono identici a quelli trasmessi in forma cartacea, con l'unica eccezione della pagina finale del documento che non risulterà firmata.

3) Con riferimento a quanto in oggetto ed al fine di valutare al meglio la ns. proposta, inoltriamo la presente richiesta di chiarimenti:

GENERALI:
- Si chiede se è sufficiente effettuare nei laboratori analisi dei presidi ospedalieri di Udine e Trieste oppure devono essere effettuati i sopralluoghi di tutti i centri hub e spoke interessati dalla gara? nel caso fosse necessario effettuare il sopralluogo di tutti i centri è sufficiente fornire un modulo solo per il lotto 1 e d uno solo per il lotto 2?
- Si chiede la disponibilità che vengano messe a disposizione le piantine di tutti i centri interessati in formato digitale al fine di provvedere a realizzare una rappresentazione grafica del progetto proposto come richiesto da capitolato.
- In merito ai collegamenti delle strumentazioni per i singoli centri nelle precedenti gare era consuetudine che tale operazione venisse effettuata dalla software house proprietaria del LIS e le spese erano a carico dei singoli enti. Poiché all'interno del capitolato speciale ci sono versioni contrastanti siamo a chiedere se l'interfacciamento sia a carico degli enti come finora o se deve essere a carico delle aziende partecipanti.
- in merito alla base d'asta indicata, si nota una discrepanza fra la base d'asta indicata nel GUCE (con importo pari a euro 10.575.000,00) e l'importo indicato nel capitolato speciale che consta di un totale lotto 1+lotto 2 per 60 mesi (pari a 7.050.000,00 euro). Siamo a chiedere una precisazione in merito.
- L'offerta economica (Fac-simile Allegato E) va redatto con la suddivisione apparecchiature e prodotti per singolo presidio o complessivo per Lotto?

LOTTO 1:
- nel capitolato speciale, lotto 1, "caratteristiche della strumentazione" in riferimento alla aas 2 Osp. Di Monfalcone, colonna "strumenti" si richiede 1 microscopio e 1 telecamera. Nella pagina successiva, alla voce AAS 2 presidio Osp. di Monfalcone si chiede invece "[...]in particolare si deve prevedere una stazione automatizzata di lettura dei vetrini con invio immagini in remoto ed un ulteriore microscopio con telecamera per permettere la visione degli strisci ad almeno 2 operatori [...]". Con tale affermazione si deve intendere che devono essere forniti 2 sistemi per la lettura o 1 microscopio comprensivo di 2 punti di osservazione? oppure è un refuso ed è sufficiente un solo microscopio comprensivo di telecamera?

LOTTO 2:
- Si chiede di esplicitare posizione e numero delle stazioni di validazione per il corelab di Udine.
- in relazione al corelab di Udine si chiede di indicare il numero di emocromi complessivi all'anno che il centro andrà a processare. inoltre nella tabella riportante le routine degli altri centri manca il carico di lavoro annuale relativo al Dipartimento Immunotrasfusionale di Udine e della Clinica Anestesiologica. Infine si chiede di dichiarare la quantità di vetrini all'anno che verranno processati dai centri in cui è previsto lo strisciatore e coloratore.
- nelle caratteristiche relative al microscopio da prevedere nel lotto 2, alla settima voce dell'elenco, dove vengono richiesta stazione automatizzata di lettura dei vetrini più un microscopio ulteriore con telecamera per permettere la revisione contemporanea ad almeno due operatori è da intendere che i due operatori possono operare uno alla stazione automatizzata e uno al microscopio oppure il microscopio deve essere dotato di un doppio punto di osservazione? per i centri spoke si intende che il microscopio deve essere dotato di 1 telecamera e di 1 punto di osservazione?

4) Vi segnaliamo che i codici CIG della procedura in oggetto non sono ancora perfezionati ai fini del pagamento da pare degli operatori economici. L'errore che appare sul sito dell' ANAC è il seguente: *[50002] Il codice inserito è valido ma non è attualmente disponibile per il pagamento. È opportuno contattare la stazione appaltante.*

5) Vista la definizione degli "Indicatori del livello del servizio" contenuta nel disciplinare di gara, chiediamo: nei Criteri di valutazione qualità LOTTO N. 2 è sufficiente inserire gli obiettivi della proposta fatta all'ente?
QUESITO POI RIFORMULATO COME SEGUE: Si richiede di chiarire la definizione degli "Indicatori del livello del servizio" contenuta nel disciplinare di gara, nei Criteri di valutazione qualità LOTTO N. 2.

6)

1) Si chiede di confermare che per TAT si intende il tempo dall'entrata del campione nel settore ematologia alla generazione del dato analitico"

2) Documentazione tecnica Qualitativa , Punto 5 Relazione tecnica parte B8) è richiesto:*"La scheda riassuntiva compilata e firmata dovrà essere presentata per ogni apparecchiatura offerta. Tali informazioni dovranno consentire l'apposita commissione di valutare la qualità delle apparecchiature offerte, secondo i criteri del presente capitolato."*
Si chiede conferma che trattasi di una descrizione delle caratteristiche tecniche minime e preferenziali della strumentazione offerta. Oppure si chiede di specificare che tipo di documento è richiesto.

3) Capitolato Speciale Lotto 1 e Lotto 2: In merito alla richiesta " *La ditta dovrà comprendere un documento che indichi in modo chiaro ed inequivocabile dove, nella documentazione allegata, siano reperibili leinformazioni richieste (numero dell'allegato, pagina e rigo) in tutte le parti della presenta offerta"* si chiede di confermare che per documento si intenda la stessa relazione tecnica al punto 5 che deve riportare per ogni informazione richiesta numero dell'allegato, pagina e rigo dell'allegato a cui si fa riferimento.

RISPOSTE:

1) Si riporta nella seguente tabella il dettaglio richiesto in relazione ai quantitativi annui presunti per ASUI.UD:

	CORELab	Immunotrasfusionale	Clinica Anestesiologica
Emocromo	Circa 800.000	Circa 4.000	Presente in capitolato
reticolociti	Circa 12.000	nessuno	Presente in capitolato
eritroblasti	Circa 40.000	nessuno	Presente in capitolato
Liquidi Biologici	Circa 6.000	nessuno	Presente in capitolato

2)

PUNTI 1) 2) e 3) RISPOSTA UNICA: Viene richiesto un sistema composto da microscopio con telecamera e sistema di acquisizione di immagini in grado di consentire la lettura condivisa contemporaneamente ad almeno due laureati operanti in due sedi diverse, riferite ai Laboratori degli Ospedali: Maggiore di Trieste, Cattinara a Trieste e di Monfalcone.

4) La caratteristica riportata dal capitolato può essere soddisfatta da diverse soluzione tecnologiche. Si conferma che anche il parametro IRF soddisfa il requisito relativo alle frazioni maturative dei reticolo citi.

5) Si conferma che il monitoraggio della % di reagente a bordo è una modalità conforme alla richiesta del capitolato

6) Per il Lotto 1 ASUI.TS, le planimetrie da richiedere sono quelle riferite ai Laboratori dell'Ospedale Maggiore, Cattinara e Monfalcone. Per l'ottenimento delle stesse le aziende interessate devono rivolgersi alla Signora Favaretto Luisa, referente per il sopralluogo già indicata nel Capitolato Speciale (tel 040.3992454; luisa.favaretto@asuits.sanita.fvg.it).
Per il Lotto 2 ASUI.UD, per le piantine le Ditte devono rivolgersi al referente dei sopralluoghi già indicato nel Capitolato Speciale, il Dr Daniele Nigris. (daniele.nigris@asuiud.sanita.fvg.it - tel 0432.552323).

7) Si conferma.

8) Si conferma.

9) Si riporta nella seguente tabella il dettaglio richiesto in relazione ai quantitativi annui presunti per ASUI.UD:

	CORELab	Immunotrasfusionale	Clinica Anestesiologica
Emocromo	Circa 800.000	Circa 4.000	Presente in capitolato
reticolociti	Circa 12.000	nessuno	Presente in capitolato
eritroblasti	Circa 40.000	nessuno	Presente in capitolato
Liquidi Biologici	Circa 6.000	nessuno	Presente in capitolato

10) Si riporta il dettaglio richiesto in relazione ai quantitativi annui presunti di vetrini per ASUI.UD, per ciascun presidio ove necessari:

Udine	Circa 50.000 vetrini
San Daniele	Circa 2.000 vetrini
Palmanova	Circa 2.400 vetrini
Latisana	Circa 1.500 vetrini
Tolmezzo	Circa 2.500 vetrini

11) Si conferma che i test per controlli giornalieri e calibrazioni NON sono inclusi.

12) Si conferma che la richiesta è riferita a tutte le buste.

13) BUSTA 1) Documenti di Partecipazione – ALLEGATO A punto l): si evidenzia che non è possibile procedere come da Voi indicato e si conferma quanto già richiesto in merito nell'ALLEGATO A punto l).

14) Si conferma quanto già indicato nel Disciplinare di gara all'art. 2: **l'offerta economica è da inserirsi nella BUSTA n. 3** (e non quindi nella busta n. 2, come erroneamente riportato nell'art. 5 del Disciplinare di gara per mero errore di trascrizione).

15) BUSTA 3) OFFERTA ECONOMICA - Allegato E:
- si conferma che è possibile procedere come da Voi indicato (sconto merce).
- "prezzo unitario": si conferma che è possibile procedere come da Voi indicato.
- si conferma che si intende la percentuale di sconto praticata per la determinazione dei prezzi offerti sul prezzo del listino vigente.

16) BUSTA 2) OFFERTA TECNICA: si conferma che è possibile procedere come da Voi indicato.

3)

GENERALI:

- Per il Lotto 1 ASUI.TS è necessario un modulo di avvenuto sopralluogo per Trieste e uno per Monfalcone. E' richiesto il sopralluogo dei locali dei Laboratori dell'Ospedale Maggiore, Cattinara e Monfalcone prendendo appuntamento, per i primi due con la Signora Favaretto Luisa (tel 040.3992454), e per Monfalcone con la dottoressa Karneth Ulrike (tel. 0481.487647).
Per il Lotto 2 ASUI.UD i sopralluoghi vanno effettuati in tutti i centri hub e spoke. Si può soprassedere sulla Clinica Ematologica, sull'Istituto Immunotrasfusionale e sulla Clinica Anestesiologica, dov'e' previsto un solo analizzatore.
Gli attestati di sopralluogo vanno presentati con le modalità già indicate nel Disciplinare di gara e nel Capitolato Speciale.

- Per il Lotto 1 ASUI.TS, le planimetrie da richiedere sono quelle riferite ai Laboratori dell'Ospedale Maggiore, Cattinara e Monfalcone. Per l'ottenimento delle stesse le aziende interessate devono rivolgersi alla Signora Favaretto Luisa, referente per il sopralluogo già indicata nel Capitolato Speciale (tel 040.3992454; luisa.favaretto@asuits.sanita.fvg.it).
Per il Lotto 2 ASUI.UD, per le piantine le Ditte devono rivolgersi al referente dei sopralluoghi già indicato nel Capitolato Speciale, il Dr Daniele Nigris. (daniele.nigris@asuiud.sanita.fvg.it - tel 0432.552323).

- I collegamenti non sono a carico delle aziende partecipanti.

- L'importo corretto dei prezzi a base d'asta è quello già indicato nel Capitolato Speciale. Nel bando di gara (e nel Passoe) non viene indicato il prezzo a base d'asta ma il valore omnicomprensivo della gara, dato dal prezzo a base d'asta di ogni lotto più il valore delle opzioni contrattuali (estensione, rinnovo e proroga tecnica).

- L'offerta economica deve contenere le informazioni minime richieste nel fac-simile Allegato E): ciò premesso, le ditte concorrenti possono fornire all'interno dell'offerta economica stessa ogni ulteriore dettaglio ritenuto utile e pertanto risulta corretta una "suddivisione apparecchiature e prodotti per singolo presidio".

LOTTO N. 1:

- E' sufficiente la presenza di 1 microscopio con telecamera per l'acquisizione di immagini e non una stazione automatizzata di lettura dei vetrini, con analoga impostazione tecnologica prevista per il Laboratorio di Cattinara.

LOTTO N. 2:

- N. 3 stazioni di validazione in area ematologia (oltre ai collegamenti WEB su PC ASUI-UD in studi di dirigenti).
- Si riporta di seguito il dettaglio richiesto:

	CORELab	Immunotrasfusionale	Clinica Anestesiologica
Emocromo	Circa 800.000	Circa 4.000	Presente in capitolato
reticolociti	Circa 12.000	nessuno	Presente in capitolato
eritroblasti	Circa 40.000	nessuno	Presente in capitolato
Liquidi Biologici	Circa 6.000	nessuno	Presente in capitolato

Udine	Circa 50.000 vetrini
San Daniele	Circa 2.000 vetrini
Palmanova	Circa 2.400 vetrini
Latisana	Circa 1.500 vetrini
Tolmezzo	Circa 2.500 vetrini

- Si chiede UNA stazione automatizzata PIU' un ULTERIORE microscopio dotato di telecamera ad alta risoluzione e relativo monitor (maggiore definizione possibile; indicare le caratteristiche).
  Per i centri spoke deve essere un microscopio (con oculari) dotato ANCHE di telecamera.

4) Si riporta quanto già specificato in merito nel Capitolato speciale di gara: "*Il pagamento dei CIG (e l'ottenimento dei "PASSOE") potrà essere effettuato non prima di 15 giorni del termine ultimo per la ricezione delle offerte indicato dal bando di gara*".

5) Con riferimento agli "Indicatori del livello di qualità del servizio" inseriti nel Capitolato Speciale per quanto concerne il lotto n. 2, si precisa che per permettere l'attribuzione dei punti al corrispondente criterio di valutazione qualità, le ditte concorrenti devono presentare i dati storici reali delle prestazioni raggiunte – sulla base di tali indicatori – desunti dalle installazioni in Italia, che dovranno essere dichiarate nella documentazione tecnica.

6)

1) Si conferma.

2) Si conferma..

3) Si conferma.

SI PRECISA LA DESCRIZIONE DEL LOTTO N. 1 VIENE INTEGRATA CON LE SEGUENTI INFORMAZIONI RELATIVE AL SISTEMA INFORMATICO DI ASUI.TS:

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'AOUTS 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 collaudo dell'intero sistema sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un accordo di responsabilità (responsability agreement) redatto secondo i dettami della norma IEC 80001. Tale documento farà esplicito riferimento all'installazione AOUTS, 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 responsability 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 AOUTS, così come intesa sopra.

Specifiche di integrazione con il LIS

Il sistema dovrà colloquiare bidirezionalmente con il LIS (Laboratory Information System) Aziendale. Il LIS attualmente in uso (non oggetto di fornitura) – *DNLab* di NoemaLife S.p.A. fornito da INSIEL, gestito e manutenuto da Insiel in tutta la Regione Friuli Venezia Giulia – si interfaccia attualmente con la strumentazione analitica per mezzo dell'applicativo DNA della stessa NoemaLife gestito da Insiel.
È prevista a breve la migrazione da DNA al middleware HALIA della stessa NoemaLife gestito da Insiel.
L'aggiudicatario dovrà interfacciare gli analizzatori con il sistema in uso nel momento della consegna e, qualora questo sia DNA, si intende compreso nel prezzo di fornitura la successiva migrazione (secondo i tempi che verranno indicati) ad HALIA. Nessun onere dovrà ricadere su AOUTS per la messa a regime da DNA ad HALIA.

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'AOUTS, 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 AOUTS 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 AOUTS. Tali dispositivi verranno inseriti in una VLAN dedicata, assegnata dall'AOUTS, 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 AOUTS 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 AOUTS 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 AOUTS, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'AOUTS. La connessione VPN dovrà essere di tipo site-to-site; 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'AOUTS si riserverà di attivare connessioni di tipo client-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'AOUTS.

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.

Scenario 2

Nel secondo scenario, in alternativa, l'aggiudicatario potrà integrare i sistemi oggetto di fornitura con l'infrastruttura sistemistica dell'AOUTS. Di seguito vengono riportate, in prima istanza, alcune caratteristiche peculiari dell'infrastruttura informatica dell'AOUTS; successivamente vengono definite le specifiche di interfacciamento all'infrastruttura AOUTS 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'AOUTS 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 AOUTS 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 AOUTS (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); 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 AOUTS 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 AOUTS è realizzata in modo che tutti i servizi sono raggruppati nel datacenter (CED) AOUTS del sito di pertinenza; in particolare i server virtualizzati appartengono ad una VLAN dedicata.

In generale la LAN AOUTS 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) AOUTS alla periferia e viceversa.

È attivo sulla LAN AOUTS 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 AOUTS 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 AOUTS 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 AOUTS, della configurazione dei DB AOUTS, 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 Unicenter Remote Control v11.x, che consente l'accesso interattivo alle sessioni utente per fini di assistenza tecnica. E' inoltre installato su tutti i client l'agente Altiris Asset Managentent v6.x per la gestione dell'inventario e per l'interfacciamento con il software di gestione del servizio di help desk (cosiddetta "gestione dei ticket").

Nel presente scenario, gli eventuali server forniti dovranno essere virtualizzati nel sistema AOUTS VMware vSphere v5.x del sito che verrà indicato dall'AOUTS (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 AOUTS.

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'AOUTS e comunque in ogni caso compatibili con l'ambiente di virtualizzazione dell'AOUTS descritto precedentemente.

Allo scopo di uniformare i sistemi forniti agli standard AOUTS, compresi quelli di sicurezza e autorizzazione (authorization), tali macchine server verranno inserite in una Organizational Unit (OU) generica dedicata ai server AOUTS oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l'AOUTS; 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

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

Nel presente scenario, lato utente, ovvero lato postazione AOUTS (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 AOUTS – 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 AOUTS. La distribuzione sulle postazioni di lavoro AOUTS 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 il browser web IE8, attualmente installato sulle postazioni AOUTS.
Eventuali PC oggetto di fornitura potranno essere inseriti nel dominio aouts.it a condizione di seguire le policy e caratteristiche dei PC AOUTS, 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 AOUTS. 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'AOUTS 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 AOUTS è dotata, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'AOUTS, a meno di eccezioni concordate con l'AOUTS. Inoltre, tutte le funzionalità dei sistemi forniti dovranno essere garantite con l'agente CA Unicenter Remote Control v11.x e con l'agente Altiris Asset Managentent v6.x di cui ogni postazione AOUTS 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 AOUTS, verranno connessi alla stessa con una specifica classe di indirizzi IP statici assegnata dall'AOUTS. Tali dispositivi verranno inseriti in una VLAN dedicata, assegnata dall'AOUTS, dalla quale potranno solo effettuare traffico specifico da e verso gli eventuali applicativi server forniti e installati nella virtualizzazione AOUTS 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 AOUTS. 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'AOUTS patch contrassegnate come "non applicabili", solo se di natura non critica; per

tali patch “non applicabili” verranno generate dall’AOUTS 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 AOUTS 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 AOUTS, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all’AOUTS. La connessione VPN dovrà essere di tipo site-to-site; 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’AOUTS si riserverà di attivare connessioni di tipo client-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 AOUTS CA Unicenter Remote Control v11.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’AOUTS, nel caso di host non dotati di client AD.

È in uso presso l’AOUTS 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 AOUTS e successivamente vengono definite le specifiche dei sistemi da fornire in tal senso, nell’ambito del presente scenario.
Il SSO AOUTS 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 AOUTS 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 AOUTS 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 AOUTS. 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 AOUTS (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 AOUTS (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 AOUTS afferente alla SC Informatica e Telecomunicazioni e dovrà formare una risorsa AOUTS alla profilatura degli account nei sistemi forniti, in modo da rendere l'AOUTS 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'AOUTS. 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.

Altre specifiche
Sia nel caso dello scenario 1 che dello scenario 2 gli eventuali server forniti dovranno essere del tipo da installazione da rack standard 19" con una occupazione massima di 2 rack unit, a meno di casi particolari che andranno comunque opportunamente motivati e previamente ed esplicitamente approvati da AOUTS.
Inoltre tali server non dovranno/potranno per alcun motivo essere utilizzati dagli operatori come stazioni di lavoro.

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'AOUTS, 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 AOUTS 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 AOUTS e dovrà inviare, nel rispetto delle procedure AOUTS, 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’AOUTS 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’AOUTS, 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 AOUTS, 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 AOUTS, essere impersonali e dovranno essere tutti comunicati all’AOUTS, 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’AOUTS e dovranno essere impersonali, dovranno essere tutti comunicati all’AOUTS, 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'AOUTS, salvo esplicita autorizzazione da parte dell'AOUTS.

Luoghi di consegna:
Azienda Ospedaliero-Universitaria di Trieste – Ospedale Maggiore. ASS2 Ospedale di Monfalcone, entro 30 giorni dalla data della lettera di aggiudicazione. Il relativo collaudo dovrà essere eseguito alla presenza dei tecnici della Ditta aggiudicataria e del personale designato dall'Azienda Ospedaliero-Universitaria, entro 15 giorni consecutivi dalla data di avvenuta istallazione.