Allegato A

DOCUMENTO TECNICO PER LA CONSULTAZIONE DI MERCATO

GARA PER LA FORNITURA IN SERVICE DI SISTEMI DI RACCOLTA E FRAZIONAMENTO DI SANGUE INTERO E DI PRODUZIONE DI EMOCOMPONENTI

ARCS (Azienda Regionale di Coordinamento per la Salute) pubblica la presente consultazione preliminare di mercato finalizzata alla raccolta di informazioni per la predisposizione della documentazione tecnica di gara in vista della prossima indizione della gara regionale per acquisire, mediante full service, quanto necessario, per la raccolta e frazionamento di sangue intero e di produzione di emocomponenti.

PREMESSA

Attualmente il sistema trasfusionale del Friuli-Venezia Giulia garantisce una diffusione capillare della raccolta del sangue con n.15 centri fissi e n.3 autoemoteche. Le sedi di raccolta fisse sono collocate nei Dipartimenti di Medicina Trasfusionale di Pordenone, Udine e Trieste e sono così divisi: n.5 centri nel Dipartimento di Pordenone, n.7 centri nel Dipartimento di Udine, n. 3 nel Dipartimento di Trieste. Le giornate di apertura settimanale dei centri fissi è variabile a seconda della sede e dell'organizzazione dipartimentale, ma definito e riportato nell'agenda unica regionale di prenotazione con un numero di accessi programmati e cadenzato nell'arco di apertura della seduta di raccolta. Le tre autoemoteche sono impegnate su tutto il territorio regionale secondo un calendario di programmazione annuale con una concentrazione delle attività di raccolta dal venerdì alla domenica.
Le unità di sangue intero raccolte ogni giorno in Regione vengono inviate al Centro Unico Regionale Produzione Emocomponenti (CURPE) presso l'Ospedale di Palmanova per la lavorazione e la qualificazione biologica. A seconda della sede di raccolta e dell'organizzazione dipartimentale le unità vengono inviate in uno o due momenti differenti in orari definiti e concordati con il CURPE. L'orario di consegna delle unità prelevate dalle autoemoteche può variare a seconda della distanza della sede di raccolta dal CURPE, mediante nel primo pomeriggio.
Tutte le sedi di raccolta dei Dipartimenti e le autoemoteche sono visionate dalla Regione ogni due anni per l'autorizzazione all'esercizio e l'accreditamento secondo la normativa vigente.

OBIETTIVI DELL'APPALTO

OBIETTIVO 1) Acquisire tutto ciò che è necessario per la raccolta e il frazionamento di sangue intero e produzione di emocomponenti, tenuto conto dei fabbisogni.

OBIETTIVO 2) Prevedere, al fine di migliorare l'efficienza produttiva, i flussi operativi e l'ergonomicità, soluzioni tecnologiche che prevedano la maggiore automazione possibile.

OBIETTIVO 3) Garantire la tracciabilità assoluta e la sicurezza del dato lungo l'intero ciclo di vita delle unità di emocomponenti raccolti/prodotti: dal prelievo, (n.15 centri di raccolta fissi e n. 3 sedi di raccolta mobile), al trasporto verso il Centro Unico Regionale Produzione Emocomponenti (CURPE) di Palmanova, sino alla distribuzione degli emocomponenti prodotti agli utilizzatori.

OBIETTIVO 4) Prevedere l'integrazione, mediante uno o più middleware, con il sistema Trasfusionale Emonet/Emolife. Prendere visione del documento "25REA010 - Specifiche ICT" allegato al presente documento, documento di specifiche tecniche approvato dalla Cabina di Regia dei Sistemi Informativi FVG,

che disciplina i requisiti generali di sicurezza informatica, privacy e integrazione con l'infrastruttura IT regionale.

La gara avrà una durata di 5 + 2 anni.

Gli operatori interessati alla presente consultazione sono, dunque, invitati a rispondere ai quesiti indicati nel documento Allegato B (questionario) per consentire all'amministrazione di approfondire le conoscenze delle soluzioni tecnologiche che il mercato di riferimento è in grado di proporre e quindi adottare la migliore soluzione volta al raggiungimento dei due obiettivi, pur nel rispetto della massima partecipazione del mercato alla gara.

DESCRIZIONE SINTETICA DELLE TECNOLOGIE OGGETTO DELLA PRESENTE FORNITURA

LOTTI		DESCRIZIONE SINTETICA
1		Bilance da prelievo – carelli porta bilance – saldatori portatili
2	Lotto unico o valutare se scorporare in più lotti	Tecnologie per la lavorazione del sangue intero e produzione di emocomponenti
		Stazione filtrante – connettori - stripper
		Sacche
3		Etichette plasticizzate
4		Tecnologia RFID

IMPORTO STIMATO

Non ancora definito

FABBISOGNI INDICATIVI

In un anno	DMT Pordenone	DMT Udine	DMT Trieste	Autoemoteche
N° totale di unità di sangue intero raccolte	14.000	21.000	12.000	10.000

SPECIFICHE TECNICHE INDICATIVE

LOTTO 1	
Descrizione sintetica	**BILANCE**
Specifiche tecniche di minime (indicative)	Interfacciamento della strumentazione al sistema informativo trasfusionale (Emonet/Emolife) → La bilancia deve essere in grado di ricevere dal sistema informativo trasfusionale la programmazione delle singole donazioni e di trasferire poi i dati relativi alla raccolta dell'unità di sangue (es. codice identificativo di unità, operatore, numero della bilancia, volume, tempo di prelievo, etc)
	Dotata di lettore barcode
	Alimentazione a rete e a batteria con possibilità di memorizzazione dei dati anche in

	caso di interruzione del collegamento
	Funzionamento in modalità off line con possibilità di scarico successivo (ethernet, wireless, usb, ecc.) senza perdita di dati
	Arresto automatico con chiusura clamp al raggiungimento del volume impostato di raccolta
	Possibilità di azzeramento automatico ad inizio procedura tenendo conto della tara al variare del tipo di sacca, programmabile per la pesatura di qualsiasi sacca presente sul mercato
	Possibilità di impostare manualmente il volume di sangue da raccogliere
	Trasmissione dei dati delle bilance al sistema informativo trasfusionale tramite rete cablata (LAN) o, in caso di blocco informatico, attraverso sistemi alternativi (ad es.: usb)
	Dispositivo per scrittura/lettura di tag RFID preferibilmente integrato nella bilancia
	Visualizzazione a display durante la procedura: del volume impostato e raccolto, del flusso istantaneo, della durata, dei messaggi di errore, della tipologia programma sacche.
	Presenza di allarmi visivi e acustici di flusso lento o troppo veloce, assenza di flusso, di fine donazione
	Arresto di emergenza in qualsiasi fase della donazione
	Deve permettere di tracciare, in modalità bidirezionale, al sistema informativo trasfusionale i codici operatore, donatore, numero di sacca (CDM o Codice Mondiale Donazione), campioni con relativi suffissi, esami di controllo del nuovo donatore, lotto e ref del dispositivo utilizzato per la raccolta, volume raccolto e tempo di donazione
	Azzeramento della tara all'atto dell'accensione
	Corretta miscelazione del sangue raccolto con l'anticoagulante
	Tipologia di taratura LAT a 1 o a 3 punti (manutenzione preventiva con strumentazione tarata LAT)
	Pinza saldante integrata alla bilancia

Requisiti preferenziali e oggetto di valutazione (indicativi)	Dimensioni delle bilance
	Lettura del numero di sacca (CDM o Codice Mondiale Donazione) e visualizzazione dati anagrafici del donatore al fine di aumentare la sicurezza nella corretta identificazione
	Visualizzazione degli allarmi tramite led luminoso con il fine di individuare la bilancia in allarme in maniera più immediata
	Display con maggiori dimensioni al fine di garantire una migliore visibilità delle informazioni
	Verifiche garantite per la corrispondenza tra anagrafica e numero dell'unità (Codice Mondiale di Donazione). Il fornitore descriva nel dettaglio le misure proposte per il soddisfacimento di questo requisito
	Fornitura di contenitore rigido per il trasporto della bilancia
Descrizione sintetica	**CARRELLI PER APPOGGIO BILANCIA E MATERIALE NECESSARIO ALLA VENIPUNTURA**
Specifiche tecniche di minime (indicative)	Carrello dotato di almeno 2 ripiani (1 portaoggetti + 1 per la bilancia)
	Carrello su ruote piroettanti a 360° con meccanismo di blocco ruote, dotato di ripiano porta oggetti di dimensioni adeguate all'appoggio di portaprovette e del necessario per venipuntura
Requisiti preferenziali e oggetto di valutazione (indicativi)	Sollevamento automatizzato per la regolazione dell'altezza del piano di appoggio della bilancia
	Ingombro minimo in termini di larghezza e profondità del carrello
Descrizione sintetica	**SALDATORI PORTATILI**
	Idoneo a prevenire il rischio di contaminazione microbica in fase di raccolta
	Omologato per saldature con ago in vena. Certificato per l'utilizzo con tubatismo collegato al donatore
	Controllo automatico della saldatura
	Saldatura di tubi di diversa tipologia e misura

	Funzionamento con batteria ricaricabile
	Garanzia di almeno 30 saldature consecutive
	Indicatore dello stato di carica della batteria, della saldatura in corso e del termine della saldatura

LOTTO 2	
LOTTO UNICO O VALUTARE SE SCORPORARE IN PIU LOTTI	
Descrizione sintetica	**TECNOLOGIE PER LA LAVORAZIONE DEL SANGUE INTERO E PRODUZIONE DI EMOCOMPONENTI**
Specifiche tecniche di minime (indicative)	Per la fase di lavorazione del sangue intero e produzione di emocomponenti, la Stazione Appaltante chiede di fornire apparecchiature per la centrifugazione (proporre soluzione anche centri HUB dei tre Dipartimenti per la lavorazione di secondo livello), la scomposizione del sangue intero, la filtrazione degli emocomponenti, la produzione di concentrati piastrinici da pool di buffy coat e la lavorazione di secondo livello (lavaggio emocomponenti e frazionamenti pediatrici) compresi saldatori e connettori sterili (per lavorazioni di secondo livello) necessarie per raggiungere gli obiettivi definiti al punto successivo. Il fornitore dovrà, relativamente alle tecnologie proposte, garantire la manutenzione strumentale ordinaria minima; istruzioni, manuale d'uso e di manutenzione in lingua italiana, strumentazione ed eventuali dispositivi dotati del marchio CE, conformità alle norme di sicurezza CEI vigenti o a equivalenti norme europee eventualmente applicabili, conformità alla normativa trasfusionale vigente.
	In base ai volumi e agli orari di attività e di risorse umane impiegate, la Stazione Appaltante chiede di fornire tecnologie congrue con le attività descritte in termini di numero e tipologia, privilegiando soluzioni che prevedano la maggior automazione possibile con il minor numero di passaggi manuali (sia per la produzione sia per la lettura dei barcode) ed il minor ingombro. La produzione di concentrati piastrinici da pool di buffy coat deve prevedere una linea di produzione dedica in maniera tale da non sovrapporsi alla lavorazione del sangue intero. Si tenga conto quanto di seguito riportato: *Ricezione e verifica conformità trasporto* - fascia oraria di arrivo dei messi (ad eccezione delle unità mobili, le quali, a seconda del luogo effettuano il servizio di raccolta, potrebbe prolungarsi fino alle 17:00): dalle 12:15 alle 15:00; - tempo medio messo per la ricezione delle unità e verifica conformità trasporto: 30 minuti. *Lavorazione* - orario di inizio lavorazione delle unità di sangue intero da lavorare: 14:00 (orario di

	arrivo messi per il trasporto ore 13:30); - orario termine verifica ultimi viaggio di trasporto sangue intero (ad esclusione delle unità mobili): ore 15:30. Termine attività di scomposizione delle unità: ore 18:15 Ora di avvio ultimo ciclo di abbattimento: ore 18:30 Termine attività di lavorazione (compresa filtrazione delle unità di emazie e stoccaggio in emoteca): ore 19:30 Produzione di concentrati piastrinici da pool di buffy coat: - orario di inizio ore 9.00/10.00 dopo la validazione delle unità - inizio distribuzione concentrati piastrinici ore 11:00 termine ore 14:00 *Risorse umane impiegate per le attività di lavorazione* - n. 1 Tecnico per la lavorazione (mattina) - n. 1,25 Tecnici per la lavorazione del sangue intero (pomeriggio) - n. 0,75 Tecnici che segue prima l'abbattimento del plasma poi termina la lavorazione del sangue intero (pomeriggio) - n. 1 Tecnico per la produzione di concentrati piastrinici da pool di buffy coat (mattina) *Dati di raccolta e produzione* Unità di sangue intero raccolte in 12 mesi: 57.000 unità - Unità mediano di sangue intero lavorate al giorno: 170 - Unità massime di sangue intero lavorate al giorno: 290 Concentrati piastrinici da pool doi buffy coat: Concentrati piastrinici prodotti in 12 mesi: 5200 - Numero mediano di concentrati piastrinici prodotti al giorno: 18 - Numero massimo di concentrati piastrinici prodotti al giorno: 30 - Numero di buffy coats utilizzati per 1 concentrato piastrinico: 5 <u>I dati di raccolta e produzione possono variare in base a richieste di variazione di produzione a livello regionale e/o ad aggiornamenti normativi (nota: verificare come scrivere)</u> Standard da rispettare sugli emocomponenti prodotti: A. Plasma da frazionamento: - almeno 220 millilitri (nota: verificare volume) prodotti di plasma da frazionamento ad unità di sangue intero - globuli bianchi residui ad unità: <0,1x10^9/Litro (EDQM edizione del 2024) - eritrociti residui ad unità: <6x10^9/Litro (EDQM edizione del 2024) - piastrine residue ad unità: <50x10^9/Litro (EDQM edizione del 2024) B. Emazie filtrate (con filtrazione post scomposizione): - volume medio ad unità attualmente prodotto pari a 267 millilitri Requisiti essenziali di qualità richiesti: - emoglobina: minimo di 40 grammi/Unità (EDQM edizione del 2024) - ematocrito: dal 50 al 70% - emoglobina libera: per valutare emolisi a fine conservazione: <0,8% della massa eritrocitaria (EDQM edizione del 2024) - Globuli bianchi residui: < 1x10^6 su unità C. Concentrati piastrinici da assemblaggio di singoli buffy coat: Requisiti essenziali di qualità richiesti:

	- Resa piastrinica: ≥ 2x10^11 su unità (EDQM edizione del 2024) - Globuli bianchi residui: < 1x10^6 su unità (EDQM edizione del 2024) - Ph a termine conservazione misurato ad una temperatura di +22°C: >6,4 (EDQM edizione del 2024)
Descrizione sintetica	**STAZIONE FILTRANTE**
Specifiche tecniche di minime (indicative)	Capacità non inferiore a 30 sacche
	Dotazione di ruote con freno
	Altezza dei ganci delle sacche regolabili (descrivere la modalità di alimentazione e di regolazione dell'altezza)
	Materiale di produzione in acciaio con superfici lisce e sanificabili
Descrizione sintetica	**CONNETTORI**
Specifiche tecniche di minime (indicative)	Tolleranza per le dimensioni dei tubi da saldare per quanto riguarda il diametro interno ed esterno
	Compatibilità con le caratteristiche chimico-fisiche dei tubi di connessione presenti in sistemi di raccolta, di pooling e di inattivazione microbiologica presenti sul mercato, nonché resistenza alla trazione dei segmenti saldati
	Capacità di effettuare un check di autodiagnosi all'accensione
	Hardware e software di facile uso per la gestione informatica dell'intero sistema e delle singole procedure
Descrizione sintetica	**STRIPPER**
Specifiche tecniche di minime (indicative)	Fornitura di stripper
Descrizione sintetica	**SACCHE**

SACCA QUADRUPLA CON FILTRO MORBIDO IN LINEA PER LA RACCOLTA DI SANGUE INTERO OMOLOGO	
Specifiche tecniche di minime (indicative)	Sacca quadrupla di raccolta di 450 ml ± 10% di sangue intero con filtro in linea morbido per leucodeplezione da concentrato eritrocitario che permetta la separazione in sacche satelliti di emazie concentrate e plasma conservando il buffy coat nella sacca madre
	Mini bag preassemblata per deviazione del primo volume di sangue e per il campionamento esami di legge di 40 ml di sangue, tramite sistema tipo Vacutainer, senza anticoagulante sulla linea di campionamento. Il sistema deve possedere camicia pre-assemblata compatibile con qualsiasi tipo di provetta
	Dotazione di valvola a frattura per apertura del reservoire e clamp di bloccaggio/chiusura linea di campionamento
	Ago da 16 G, taglio a becco di flauto dotato di copriago di sicurezza pre-assemblato onde evitare punture accidentali dopo il prelievo e munito di sistema di sicurezza "ago retrattile" per chiusura automatica all'estrazione a scopo di protezione dell'operatore
	Sistema di clamp per chiusura circuiti
	Soluzione conservante: ➢ Soluzione anticoagulante: CPD-A1 ➢ Soluzione additiva di conservazione per emazie fino a 42 gg: SAG-M
	Sacche in materiale conforme alla normativa vigente in materia di biocompatibilità, sacche Latex free, senza ftalati.
	Resistenza in centrifuga (fino a 5000 rcf) e alle basse temperature (fino a -80° C)
	Etichetta sacca a norma di legge con dati in chiaro almeno delle seguenti informazioni: produttore, data di produzione e data di scadenza, lotto e codice prodotto, dati in codice a barre almeno del codice prodotto e del lotto atto a garantire la massima tracciabilità del prodotto
	Sacca confezionata singolarmente, trasparente, apirogena, sterile con data di scadenza visibile
	A rilascio di nuovo lotto, invio di copia del certificato di qualità
	Completa compatibilità con i sistemi proposti per la scomposizione del sangue intero

	Tubi compatibili con i sistemi di connessione sterile, lunghi almeno 500mm
	Filtro per leucociti di tipo morbido per un semplice e sicuro alloggiamento nella centrifuga con indicato il lotto di produzione
	Filtro per leucociti con recupero di globuli rossi ≥ 90% e residuo di globuli bianchi < 1x10^6
	Presenza di codici di identificazione sui tubatismi della sacca dei GRC
SACCA PER LA RACCOLTA DI SANGUE INTERO ATTA ALLA PRODUZIONE DI SIERO COLLIRIO	
Specifiche tecniche di minime (indicative)	Sacca doppia senza anticoagulante idonea alla conservazione a +4 +/- 2°C, il fornitore indichi il volume massimo di raccolta
	Sacche in materiale conforme alla normativa vigente in materia di biocompatibilità, sacche Latex free, senza ftalati
	Sistema di campionamento preconnesso costituito da mini-sacca per il campionamento ematico. Il sistema deve possedere camicia preassemblata compatibile con qualsiasi tipo di provetta
	Assenza di anticoagulante lungo la linea di campionamento
	Dispositivo di protezione ago per consentire l'estrazione e la copertura dell'ago in un'unica operazione
	Tubatismi compatibili con i sistemi di connessione sterile
	Kit di manipolazione: connettori luer lock per il trasferimento del siero e diluizione in ambiente sterile
	A rilascio di nuovo lotto, invio di copia del certificato di qualità
	Etichetta sacca a norma di legge con dati in chiaro almeno delle seguenti informazioni: produttore, data di produzione e data di scadenza, lotto e codice prodotto, dati in codice a barre almeno del codice prodotto e del lotto atto a garantire la massima tracciabilità del prodotto

SACCA SINGOLA AUTODONAZIONE E SALASSI	
Specifiche tecniche di minime (indicative)	Sistema di raccolta (sacca singola) di 450 ml ± 10% di sangue intero autologo / sangue intero per salasso terapeutico
	Ago da 16 G, taglio a becco di flauto dotato di copriago di sicurezza pre-assemblato onde evitare punture accidentali dopo il prelievo e munito di sistema di sicurezza "ago retrattile" per chiusura automatica all'estrazione a scopo di protezione dell'operatore
	Mini bag preassemblata per deviazione del primo volume di sangue e per il campionamento esami di legge di 40 ml di sangue, tramite sistema tipo Vacutainer, senza anticoagulante sulla linea di campionamento. Il sistema deve possedere camicia pre-assemblata compatibile con qualsiasi tipo di provetta
	Tratto tra ago e sistema libero da anticoagulante garantito da blocco meccanico sulla linea della sacca
	Soluzione conservante CPDA -1
	Etichetta sacca a norma di legge con dati in chiaro almeno delle seguenti informazioni: produttore, data di produzione e data di scadenza, lotto e codice prodotto, dati in codice a barre almeno del codice prodotto e del lotto atto a garantire la massima tracciabilità del prodotto
	Sacche in materiale conforme alla normativa vigente in materia di biocompatibilità, sacche Latex free, senza ftalati
	Confezione singola, trasparente, apirogena, sterile munita di data di scadenza, resistente alle variazioni termiche e agli stress meccanici
	A rilascio di nuovo lotto invio di certificato di qualità
SACCHE PER ALIQUOTE PEDIATRICHE COMPRESA TRA 70 E 150 MILLILITRI	
Specifiche tecniche di minime (indicative)	Sacche in materiale conforme alla normativa vigente in materia di biocompatibilità, sacche Latex free, senza ftalati
	Sacche resistenti alle manipolazioni e di materiale idoneo al congelamento fino a -80°C ed alla conservazione a diverse temperature (+4°C +/- 2°C; +22°C +/-2°C)

	Sistema chiuso con sacche preconnesse
	Tubi compatibili con i sistemi di connessione sterile, lunghi almeno 30
	Etichetta sacca a norma di legge con dati in chiaro almeno delle seguenti informazioni: produttore, data di produzione e data di scadenza, lotto e codice prodotto, dati in codice a barre almeno del codice prodotto e del lotto atto a garantire la massima tracciabilità del prodotto
	A rilascio di nuovo lotto, invio di copia del certificato di qualità
SACCHE DI TRASFERIMENTO CON CAPACITA' DIFFERENTI: DI ALMENO 300ML; DI ALMENO 600ML; DI ALMENO 1000ML	
Specifiche tecniche di minime (indicative)	Sacche in materiale conforme alla normativa vigente in materia di biocompatibilità, sacche Latex free, senza ftalati
	Sacche resistenti alle manipolazioni e di materiale idoneo al congelamento fino a -80°C ed alla conservazione a diverse temperature (+4°C +/- 2°C; +22°C +/-2°C)
	Tubi compatibili con i sistemi di connessione sterile, lunghi almeno 30
	Etichetta sacca a norma di legge con dati in chiaro almeno delle seguenti informazioni: produttore, data di produzione e data di scadenza, lotto e codice prodotto, dati in codice a barre almeno del codice prodotto e del lotto atto a garantire la massima tracciabilità del prodotto
	A rilascio di nuovo lotto, invio di copia del certificato di qualità
SACCHE PER CRIOGENIA	
Specifiche tecniche di minime (indicative)	Sacche in materiale conforme alla normativa vigente in materia di biocompatibilità, sacche Latex free, senza ftalati.
	Sacche resistenti alle manipolazioni e di materiale idoneo al congelamento fino a -196°C successivo scongelamento a +37°C
	Componenti della sacca: • sedi perforabili • area di saldatura

	• tubo in EVA • tasca etichetta sacca esterna
	Componenti del tubo di riempimento: • sede per iniezione • tubo in PVC • roller clamp • connettore luer lock maschio • connettore luer lock femmina
Requisiti preferenziali e oggetto di valutazione (indicativi)	**Vedere la bozza di griglia di valutazione sottostante**

CRITERIO 1: CARATTERISTICHE TECNICHE				
Sub -criterio	**Descrizione**	**Riferimento documentale**	**C**	**PUNTI MAX**
STAZIONE FILTRANTE	Numero di ganci complessivi			
CONNETTORI	Lunghezza minima dei tubatismi da connettere			
	Modalità di connessione			
STRIPPER	Il 30 % della fornitura deve essere automatica			
SACCA QUADRUPLA CON FILTRO MORBIDO IN LINEA PER LA RACCOLTA DI SANGUE INTERO OMOLOGO	Presenza di una linea di raccordo per l'infusione di liquidi preconnessa in prossimità dell'ago			
	Due Port di ingresso separati e protetti singolarmente di spessore adeguato a consentire le operazioni di perforazione in sicurezza per le sacche destinate alla trasfusione			
SACCA SINGOLA AUTODONAZIONE E SALASSI	Presenza di una linea di raccordo per l'infusione di liquidi preconnessa in prossimità dell'ago			
SACCHE PER ALIQUOTE PEDIATRICHE COMPRESA TRA 70 E 150 MILLILITRI	Numero di sacche multiple preconnesse			
	Volume delle sacche multiple			
CRITERIO 2: PROGETTUALITÀ DELLA SOLUZIONE PROPOSTA				
Sub -criterio	**Descrizione**	**Riferimento documentale**	**C**	**PUNTI MAX**
LIVELLO DI AUTOMAZIONE DEL SISTEMA	Saranno premiate le soluzioni caratterizzate da sistemi chiusi e ad elevato grado di automazione, in grado di ridurre al minimo l'intervento diretto dell'operatore nelle fasi di lavorazione, produzione e controllo e di garantire una maggiore standardizzazione degli emocomponenti prodotti.			
RIDUZIONE DELLE OPERAZIONI MANUALI	Saranno valutate positivamente le soluzioni che prevedano il minor numero di passaggi manuali lungo l'intero processo operativo, compresa l'acquisizione, la gestione e la lettura dei barcode e delle informazioni identificative.			

EFFICIENZA DEI TEMPI DI LAVORAZIONE E PRODUZIONE	Saranno premiate le soluzioni che garantiscano tempi di lavorazione, produzione di concentrati piastrinici da pool di buffy coat e di completamento delle procedure inferiori, favorendo una maggiore produttività e rapidità operativa.			
INGOMBRO COMPLESSIVO DELLE APPARECCHIATURE	Saranno valutate positivamente le soluzioni caratterizzate da un ridotto ingombro fisico delle apparecchiature e dei relativi accessori, con ottimizzazione degli spazi disponibili.			
ERGONOMIA - ORGANIZZAZIONE DEGLI SPAZI E FLUSSI DI PROCESSO	Saranno premiate le soluzioni che presentino una disposizione funzionale delle tecnologie e delle apparecchiature all'interno degli spazi operativi, garantendo per la lavorazione del sangue intero e di produzione di emocomponenti.			
FUNZIONALITÀ E COMPLETEZZA DELLE INFORMAZIONI VISUALIZZATE	Sarà valutata la quantità, qualità e tipologia delle informazioni visualizzabili sui display dei sistemi, quali a titolo esemplificativo: peso degli emocomponenti, stato della procedura, tempi residui e/o trascorsi, allarmi, notifiche operative, parametri di lavorazione e informazioni di tracciabilità.			
CRITERIO 3: DIMOSTRAZIONE VIDEO				
Sub -criterio	**Descrizione**	**Riferimento documentale**	**C**	**PUNTI MAX**
USABILITÀ DEL MIDDLEWARE	Verranno valutate con maggior riguardo le proposte che presenteranno le migliori caratteristiche con riferimento a: facilità di utilizzo; intuitività; snellezza delle transazioni applicative.			
CRITERIO 4: SERVIZI				
Sub -criterio	**Descrizione**	**Riferimento documentale**	**C**	**PUNTI MAX**
FORMAZIONE	Verranno valutate le proposte che presenteranno condizioni migliorative rispetto a quelle minime richieste in capitolato			
MANUTENZIONE	Verranno valutate le proposte che presenteranno condizioni migliorative rispetto a quelle minime richieste in capitolato			
CRITERIO 5: ULTERIORI MIGLIORIE				
Sub -criterio	**Descrizione**	**Rif. questionario**	**C**	**PUNTI MAX**
MIGLIORIE PRESENTI NELLA CONFIGURAZIONE OFFERTA RISPETTO ALLA CONFIGURAZIONE BASE RICHIESTA IN TERMINI DI CARATTERISTICHE TECNICO/FUNZIONALI, DEI MODULI SW E DEI SERVIZI DI ASSISTENZA TECNICA	Verrà valutata la presenza nell'offerta di altre migliorie presenti rispetto alla configurazione base richiesta in termini di caratteristiche tecnico/funzionali, dei moduli SW. Saranno assegnati punti zero alle proposte che non presenteranno caratteristiche innovative rispetto ai requisiti minimi richiesti, che siano già state valutate in alcuni dei parametri di cui sopra o che non siano ritenute significative dalla commissione.			

LOTTO 3	
Descrizione sintetica	**ETICHETTE PLASTICIZZATE**
Specifiche tecniche di minime (indicative)	Plasticizzate (ad es., film di polipropilene espanso bianco, lucido, biassialmente allungato, con rivestimento di superficie – (stampa a trasferimento termico))
	La colla deve garantire adesività sulla superficie di unità conservate ad una temperatura compresa tra -40°C e -80°C
	Ben leggibili e con stampa di buona qualità
	Senza grinze e ghiaccio, non danneggiate
	Copertura dell'intera superficie con adesivo
	La colla deve essere in grado di resistere ad una temperatura di conservazione uguale o inferiore a -30°C per un periodo più lungo senza subire danni
	Assenza di altri codici a barre staccati
	Resistenti alla lacerazione, ma tali da poter essere tagliate con un coltello affilato senza che frammenti entrino nel plasma
	Possibilità di conservazione a temperatura ambiente per almeno 1 (un) anno senza deterioramento, ad es. danneggiamento o scolorimento
	Resistenti a: • Olio • Grasso • Plasma e sangue • Raggi ultravioletti • Acqua, umidità • Vapore ad una temperatura di +75 °C per un lasso di tempo di 2 (due) minuti • Fluttuazioni di temperatura • Formazione di ghiaccio durante il processo di congelamento • Conservazione a -30°C per lunghi periodi, umidità per brevi periodi durante il trasporto a temperatura ambiente (< 2 (due) ore) • Umidità per periodi più lunghi (da 10 a 30 ore) durante il processo di scongelamento. Questo può aver luogo da 0°C a +4°C o a temperatura ambiente
	Diametro anima interna del rotolo etichette

	Stampanti termiche e testine saldanti
	La ditta che intende partecipare alla gara dovrà fornire una campionatura completa di etichette affinché venga inviata alla ditta di plasmaderivazione per valutare le caratteristiche sopra indicate. Solo quelle che riceveranno l'approvazione dalla ditta di plasmaderivazione verranno prese in considerazione. Le dimensioni delle etichette per emocomponenti da 80 x 80 mm a 100 x 100 mm Le dimensioni delle etichette per provette 50 mm x 30 mm
Requisiti preferenziali e oggetto di valutazione (indicativi)	Numero e tipologia di formanti disponibili

LOTTO 4	
Descrizione sintetica	**TAG RFID**
La tecnologia proposta verrà utilizzata per la movimentazione degli emocomponenti all'interno del CURPE (per la tracciabilità delle fasi di lavorazione e conservazione) sia all'esterno (da e verso i centri raccolta e distribuzioni della Regione FVG).	
Specifiche tecniche di minime (indicative)	Tag passivo che consenta lettura e scrittura con tecnologia RFID.
	Adesivo idoneo all'etichettatura delle unità di sangue ed emocomponenti.
	Resistente agli stress fisici e meccanici previsti nelle fasi di preparazione e conservazione delle unità di sangue ed emocomponenti: • Plasticizzati; • Copertura dell'intera superficie con adesivo; • Il tag, etichetta, colla devono essere in grado di resistere ad una temperatura di conservazione uguale o inferiore a -30°C per un lungo periodo senza subire danni; • Resistenti alla lacerazione, ma tali da poter essere tagliate con un coltello affilato senza che frammenti entrino nel plasma; • Possibilità di conservazione a temperatura ambiente per almeno 1 (un) anno senza deterioramento, ad es. danneggiamento o scolorimento; • Resistenti a: olio, grasso, plasma e sangue, raggi ultravioletti, acqua, ghiaccio, fluttuazioni di temperatura; • Resistenti al vapore ad una temperatura di +75 °C per un lasso di tempo di 2 (due) minuti; • Resistenti all'umidità per periodi da 10 a 30 ore durante il processo di scongelamento. Questo può aver luogo da 0°C a +4°C o a temperatura ambiente.
	Codifica dei dati conforme a standard aperti e non proprietari.
	Capienza dei dati a parità di dimensioni dell'etichetta.
	Fornitura di una campionatura completa affinché venga inviata alla ditta di plasma derivazione per valutare le caratteristiche sopra indicate. Solo quelle che riceveranno l'approvazione dalla ditta di plasma derivazione verranno prese in considerazione.
Requisiti preferenziali e oggetto di valutazione (indicativi)	Conforme agli standard ISO 15693.
	Diverse soluzioni di fornitura delle etichette (rotolo, fogli A4).

	Diverse soluzioni in termini di dimensioni fisiche.
	Resistenza ad una temperatura di conservazione uguale a -80°C.
Descrizione sintetica	**TECNOLOGIA PER LA GESTIONE DELLA MOVINTAZIONE DEGLI EMOCOMPONENTI ALL'INTERNO DELLA STRUTTURA PER LA TRACCIBILITA' DELLA CONSERVAZIONE DEGLI EMOCOMPONENTI STESSI**
Soluzione che consenta la gestione/tracciabilità della movimentazione degli emocomponenti all'interno della struttura durante tutto il percorso di conservazione (dal termine della lavorazione al rilascio finale)	
Specifiche tecniche di minime (indicative)	Soluzione compatibile con le apparecchiature per la conservazione esistenti (ad es. frigoemoteche, congelatori, abbattitori di temperatura).
Requisiti preferenziali e oggetto di valutazione (indicativi)	Soluzione che preveda il minor numero di passaggi per gli operatori ed il minor ingombro fisico con attenzione all'ergonomia di utilizzo per gli operatori.
	Soluzione che preveda il minor impatto sull'infrastruttura tecnologica già esistente (impianti di rete, di alimentazione).
	Integrabile con le apparecchiature già esistenti (ad es. bilance di prelievo).
TUNNEL PER LETTURA/SCRITTURA E MOVIMENTAZIONE	
Specifiche tecniche di minime (indicative)	Possibilità di identificare i datalogger che lo attraversano per attivare (in partenza), disattivare e scaricare i dati di temperatura (in arrivo).
	Capacità di lettura/scrittura fino a 80 tag contemporaneamente attraverso l'utilizzo di un sistema di anticollisione.
	Tasso di errore in lettura/scrittura dei tag < 1%.
	Capacità di lettura/scrittura dei tag contenuti in contenitori terziari/scatole per stoccaggio emocomponenti di dimensioni: 478x288x178 mm, 348x288x178 mm, 430x430x290 mm, 480x480x290 mm.
	Dotato di piano di appoggio dei contenitori ad una altezza compresa tra i 50 e i 60 cm da terra (non inferiore a 50 cm), superficie liscia o a rulli per agevolare il passaggio del contenitore nel varco per la lettura dei tag RFID.
	Possibilità essere dotato di ruote per lo spostamento.

	Monitor integrato al tunnel a supporto dell'operatore.
Requisiti preferenziali e oggetto di valutazione (indicativi)	Soluzione che garantisca la maggiore ergonomia di utilizzo per l'operatore.
	Soluzione che preveda il minor impatto sull'infrastruttura tecnologica già esistente (impianti di rete, di alimentazione).
PLATE PER LETTURA/SCRITTURA E MOVIMENTAZIONE	
Specifiche tecniche di minime (indicative)	Possibilità di identificare i datalogger per attivare (in partenza), disattivare e scaricare i dati di temperatura in arrivo.
	Capacità di lettura/scrittura di più tag contemporaneamente (almeno 10) attraverso l'utilizzo di un sistema di anticollisione.
	Tasso di errore in lettura/scrittura dei tag < 1%.
	Soluzione che preveda dispositivi di dimensioni diverse.
Requisiti preferenziali e oggetto di valutazione (indicativi)	Soluzione che garantisca la maggiore ergonomia di utilizzo per l'operatore.
	Soluzione che preveda il minor impatto sull'infrastruttura tecnologica già esistente (impianti di rete, di alimentazione).
DATALOGGER	
Specifiche tecniche di minime (indicative)	Dimensionalmente idoneo all'inserimento nei contenitori per il trasporto di emocomponenti e provette.
	In grado di tracciare la temperatura e i tempi di trasporto.
	Possibilità di consentire la tracciabilità degli operatori che effettuano la programmazione ed avvio iniziale e lo stop a termine trasporto.
	Range di temperatura registrabile: da -40°C a +40°C.
	Possibilità di registrare la temperatura fino a 24 ore continuative.
	Frequenza di rilevazione programmabile.

	Possibilità di programmare soglie di allarme per temperature e per tempi di trasporto (per la valutazione dell'accettabilità degli emocomponenti/provette trasportati).
	Possibilità che i dati registrati vengano esportati o condivisi.
	Deve essere possibile visualizzare la vita residua della batteria o la segnalazione del prossimo esaurimento.
	Garantire servizio di verifica e taratura periodica dei datalogger in centro/laboratorio esterno di taratura accreditato Accredia.
	Possibilità di creare delle configurazioni di range di temperatura in base all'emocomponente movimentato da poter richiamare a necessità (in base al trasporto effettuato).
Requisiti preferenziali e oggetto di valutazione (indicativi)	Dimensioni ed aspetto del dispositivo a supporto di una migliore identificazione del dispositivo nel contenitore.
	Range di temperatura di registrazione garantito superiore a +40°c ed inferiore a -40°C.
PIATTAFORMA SOFTWARE NECESSARIA PER LA GESTIONE DELL'INTERO PROCESSO RFID	
Specifiche tecniche di minime (indicative)	Integrabile con applicativi o sistemi terzi.
	Conforme alla normativa vigente in materia di privacy e cyber security.
	Interfacciamento bidirezionale con il sistema informativo trasfusionale per lo scambio di informazioni (registrazione delle informazioni sia in fase di lettura dal tag al sistema informativo trasfusionale sia in fase di scrittura dal sistema informativo trasfusionale al tag).
	Accesso all'applicativo tramite utenti registrati con relativa profilazione.
	Supporto di sistemi di Single sign-on (SSO).
	Interfaccia ergonomica e di immediato utilizzo per l'operatore.
Requisiti preferenziali e oggetto di valutazione (indicativi)	Dotato di un sistema di reportistica interno.
	Possibilità di esportare i dati.

	Applicativo web (zero-footprint).

Allegato - Requisiti IT

Sommario

Allegato - Requisiti IT 1
Specifiche generali e responsabilità dell'aggiudicatario 2
Responsabilità nella gestione degli accessi 4
Specifiche di integrazione con l'infrastruttura IT 5
Caratteristiche delle applicazioni funzionali al servizio 5
Modalità di installazione dell'infrastruttura fornita necessaria al servizio 5
Modalità di autenticazione degli applicativi. 6
Segmentazione della rete dei client 6
Assistenza remota e telemonitoraggio 7
Prescrizioni in merito alla fornitura di postazioni di lavoro e server 8
Interoperabilità con gli applicativi del sistema informativo sanitario regionale 9
Specifiche tecniche di sicurezza informatica 9
Prescrizioni sulla posa in opera del cablaggio 12

Specifiche generali e responsabilità dell'aggiudicatario

Di seguito vengono definite le specifiche che i sistemi oggetto del servizio dovranno rispettare relativamente ad aspetti della sfera dell'IT (Information Technology). Qualunque elemento riportato in offerta tecnica dai partecipanti in contrasto o non in coerenza con i principi ed i contenuti di seguito riportati non avrà alcun valore contrattuale.

Il sistema nel suo complesso dovrà essere coerente con le politiche di sicurezza e di privacy della singola Azienda del SSR 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.

I sistemi oggetto del servizio dovranno permettere all'Azienda di rispondere, per lo specifico dei sistemi offerti, a tutte le prescrizioni del complesso quadro normativo vigente.

Dal punto di vista della sicurezza, in primis dovrà rispondere a quanto richiesto:

Dal punto di vista della sicurezza, in primis dovrà rispondere a quanto richiesto:

- Dal Regolamento Europeo sulla Protezione dei Dati – GDPR del 14.04.2016 e al D. Lgs. 196/2003 s.m.i., cosiddetto Codice Privacy, così come novellato dal D.Lgs. 101/2018; l'aggiudicatario verrà designato responsabile ex art. 28 del GDPR e dovrà produrre ed attuare tutto quanto richiesto, per quanto pertinente prima del collaudo e per tutta la durata del contratto. Il modulo fac simile di designazione è riportato in allegato ed è parte integrante della documentazione di gara.
- Dalla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", con livello ALTO; inoltre l'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'azienda è chiamata a redigere in ottemperanza alla suddetta circolare AGID.
- Dalla Determinazione AGID n. 220/2020 del 17/05/2020 "Adozione delle Linee Guida - La sicurezza nel procurement ICT" e dalle Linee Guida allegate.
- Dalle direttive UE NIS (Network and Information Security) e NIS2, nonché dai Decreti Legislativi di recepimento, come pure dalla Legge 90/2024.

Dovranno, inoltre, rispettare le indicazioni AgID inerenti lo sviluppo e l'acquisizione di software e, in particolare:

- il rispetto di quanto prescritto nelle "linee guida di sicurezza nello sviluppo delle applicazioni" AgID, anche dette "linee guida AgID per lo sviluppo sicuro del software";
- la conformità alle regole sull'interoperabilità prescritte dalle linee guida emanate in attuazione dell'articolo 73 del CAD;
- la possibilità di esportare l'intera base di dati (inclusi di ogni tipo di indice o metadato utilizzato per implementare le funzionalità del software stesso) in formato standard e aperto, per scongiurare la possibilità di lock-in, come meglio specificato nelle linee guida n.8 di ANAC.

Qualora i sistemi oggetto del servizio intendano essere collegati nella rete aziendale, essendo quest'ultima intrinsecamente una rete IT medicale secondo la norma IEC 80001-1, s'intende che 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 stessa norma.

Tale documento farà esplicito riferimento all'installazione dell'Azienda, 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, redatto dall'aggiudicatario e

revisionato/validato dall'Azienda, conterrà espliciti riferimenti alla "marcatura CE" dei sistemi offerti ed al fatto che i requisiti essenziali di sicurezza non verranno inficiati nella particolare installazione dell'Azienda e nel tempo, così come intesa sopra. Qualora i sistemi oggetto del servizio non s'intendano collegati in alcuna maniera alla rete dati, essi devono comunque rispondere ai requisiti dettati dalla normativa citata.

Se l'oggetto del servizio include dispositivi medici, il fornitore dovrà compilare, sottoscrivere e allegare all'offerta tecnica il modulo Manufacturer Disclosure Statement for Medical Device Security (MDS2) versione 2019 per ciascuno di essi, in maniera da permettere all'Azienda una più agevole valutazione delle eventuali criticità della messa in uso dei sistemi offerti anche secondo IEC/TR 80001-2-2. È comunque onere del fornitore verificare la versione più recente del modulo dal sito NEMA e compilare e fornire tale versione.

In caso di fornitura di dispositivi medici, inoltre, l'aggiudicatario con la partecipazione alla presente procedura di gara dichiara che le caratteristiche tecniche dell'infrastruttura IT descritte in capitolato e nel presente documento, sono adeguate ai dispositivi medici oggetto del servizio, nei termini previsti dal Regolamento Europeo 2017/745 con particolare riferimento all'Allegato I – par. 17.4 ("I fabbricanti indicano i requisiti minimi in materia di hardware, caratteristiche delle reti informatiche e misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato, necessari per far funzionare il software come previsto").

Inoltre, sempre nel caso in cui l'oggetto del servizio includa dispositivi medici, il sistema dovrà rispondere a quanto richiesto:

- dal IHE Patient Care Device (PCD) White Paper, "Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide";
- dalla linea guida "MDCG 2019-16 Guidance on Cybersecurity for medical devices".

In generale, l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e nel trattamento dei dati affidato nell'ambito di quanto richiesto dalla presente procedura, in particolare in merito all'integrità, disponibilità e riservatezza dei dati e dei sistemi. Pertanto, anche nei casi in cui la sicurezza dei dati gestiti dai sistemi oggetto del servizio possa essere legata agli effetti di altro hardware e software in gestione di altro soggetto, l'aggiudicatario rimane responsabile di monitorare tali elementi e segnalare in via formale qualora ritenga vi siano aspetti di inadeguatezza. In tale responsabilità ricade anche l'onere di richiedere gli strumenti per fare gli audit ed il monitoraggio, per eseguire le ricerche di anomalie, oltre alla comunicazione formale delle proposte percorribili per raggiungere gli obiettivi. Analogamente l'aggiudicatario accetta e collabora pienamente a qualsiasi attività di assessment e audit che l'Azienda o società da essa incaricate dovessero condurre sui sistemi oggetto del servizio.

In particolare, 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. Per quanto riguarda i sistemi operativi server, gli oneri di licenza e di qualunque altro tipo, diretti e indiretti, finalizzati al corretto e sicuro funzionamento del sistema oggetto di fornitura saranno completamente a carico dell'aggiudicatario, come pure l'onere della continua verifica nei dizionari di vulnerabilità internazionali (al minimo dovrà essere monitorato CVE - Common Vulnerabilities and

Exposures) dei sistemi operativi in uso e di qualunque altra componente software fornita od installata dall'aggiudicatario, nonché la sostituzione immediata ed incondizionata dei sistemi operativi stessi in caso di criticità contrassegnate con livello maggiore o uguale al range "6-7".

Responsabilità nella gestione degli accessi

Come indicato in premessa, l'aggiudicatario verrà designato responsabile ex art.28 del GDPR, ed in quest'ambito dovrà, tra l'altro, inviare, nel rispetto delle procedure aziendali, 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'Azienda e a livello personale, secondo le proprie procedure ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

Coerentemente con i contenuti della nomina, nel caso non sia presente un sistema di autenticazione delegata, configurato in accordo con l'Azienda, il fornitore è responsabile dell'intero ciclo di gestione, a norma, delle credenziali, in primis di incaricati e amministratori.

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'Azienda ove richiesti, 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; ove non richiesti da Aziende la gestione e responsabilità si intende a carico dell'aggiudicatario;
- dovranno, nel caso di account amministrativi non locali che consentano l'accesso interattivo a macchine/sistemi/applicativi collegati alla LAN, 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;
- non dovranno, nel caso di account amministrativi impersonali, essere in alcun caso presenti, se non del tipo gMSA;
- dovranno, nel caso di tutti gli account di sistemi non in LAN, essere gestiti a cura e responsabilità dell'aggiudicatario;
- potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN, essere impersonali e dovranno essere tutti comunicati all'Azienda ove richiesti, 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; ove non richiesti dalle Aziende la gestione e responsabilità si intende a carico dell'aggiudicatario;

  in tal caso, ovvero per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel punto precedente, 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.

Specifiche di integrazione con l'infrastruttura IT

Caratteristiche delle applicazioni funzionali al servizio

Tutte le applicazioni fornite o messe a disposizione dall'aggiudicatario per l'erogazione dei servizi devono essere del tipo "web zero footprint".

Il paradigma zero footprint può essere raggiunto anche mediante tecnologie di virtualizzazione applicative e distribuzione via web.

S'intendono incluse illimitate licenze d'uso degli applicativi e, nel caso dell'uso di strumenti funzionali alla realizzazione del paradigma zero foot print, tutti i costi degli strumenti, delle licenze, e degli eventuali costi per i singoli utilizzatori (es. CAL) si ritengono a totale onere dell'aggiudicatario e senza ulteriori oneri per gli enti appaltanti.

Le applicazioni dovranno essere fruibili dai web browser in uso presso le Aziende e senza alcun componente aggiuntivo sul browser stesso o sul client in generale; la sicurezza delle connessioni tra browser e servizi dovrà essere adeguata alla tipologia di dati scambiati, in ogni caso dovrà essere adottato il protocollo HTTPS (TLS 1.2 o superiore – in ogni caso non deprecato – con certificato pubblico in gestione e a carico dell'aggiudicatario; tale certificato dovrà essere riconosciuto come valido dai browser di cui sopra, senza specifiche configurazioni, ovvero non dovranno essere usati certificati di tipo self-signed) e in alcun caso verranno realizzate connessioni VPN o di altro tipo ad hoc, (es. sistemi di virtualizzazione applicativa o del desktop) per sopperire ad eventuali carenze architetturali in termini di sicurezza o funzionalità, ovvero i servizi dovranno sempre essere fruibili in maniera efficace e sicura.

Modalità di installazione dell'infrastruttura fornita necessaria al servizio

Gli elementi dell'infrastruttura fornita per l'erogazione del servizio, intesa come insieme di componenti di calcolo, di storage e di complemento, devono essere adatte ad essere ospitate nel datacenter di Insiel S.p.A, inhouse regionale del FVG, situato a Trieste.

Quest'ultima erogherà pertanto il servizio di housing o co-location presso i propri locali.

Insiel offre la disponibilità di armadi rack da 19" già attrezzati, certificati secondo lo standard UL 60950-1, di dimensione 600mm di larghezza, 1200mm di profondità e 42U di altezza, in grado di sostenere un peso massimo di almeno 1300 kg in condizioni di carico static, e la possibilità di una doppia linea di alimentazione, oltre doppio canale di connettività.

Le sale sono dotate di sistema di rilevazione e soppressione fumi, con parco bombole dedicato e relativa serranda per il lavaggio della sala. In tutte le sale è presente un controllo accessi a doppio fattore di autenticazione e telecamere per il controllo perimetrale.

Viene inoltre garantito l'accesso h24x365gg, tramite la guardiania presente per accedere all'edificio, e alla control room per accedere al data center

L'obiettivo di disponibilità del servizio di co-location/housing, inteso come disponibilità di alimentazione e condizionamento, è del 99,99% misurata su base annuale.

Di conseguenza, si richiede la messa a disposizione di tutte le componenti di infrastruttura

necessari all'erogazione del servizio, con caratteristiche adeguate a fruire del servizio di housing/co-location sopra descritto. In particolare, gli eventuali server dovranno essere del tipo da installazione da rack standard 19'' con una occupazione massima di 2 rack unit (a meno di documentata necessita) e dotati di doppio modulo di alimentazione integrato oltre e di doppio modulo di connettività (es scheda di rete).

Considerata la criticità del servizio, l'infrastruttura messa a disposizione, e i servizi con essa erogati, dovranno raggiungere un RTO (Return Time Objective) minore di **un'ora** e un RPO (Recovery Point Objective) minore di **due ore.**

Modalità di autenticazione degli applicativi.

Coerentemente con l'esercizio del ruolo di Responsabile del Trattamento, assunto dall'aggiudicatario, quest'ultimo deve farsi carico di eseguire l'autenticazione agli applicativi mediante la piattaforma Regionale di Interoperabilità, che offre servizi di autenticazione SAML o OpenID/connect federando gli Identity Provider delle Aziende Sanitarie.

Utilizzando tale meccanismo di autenticazione federata, gli operatori potranno usare il servizio con le credenziali di dominio, ad esempio con cui accedono ai PC aziendali.

Qualora ciò non fosse possibile, l'aggiudicatario ha **12 MESI** di tempo per sviluppare e mettere in produzione adeguati strumenti, pena una riduzione del canone di servizio fatturato dell'1% fino alla messa in produzione della funzionalità. Nel periodo di assenza della funzionalità le procedure per la corretta erogazione di credenziali rimangono a carico dell'aggiudicatario.

Inoltre, l'aggiudicatario deve prevedere e implementare una soluzione di autenticazione in fall back, nell'ambito delle proprie funzionalità di business continuity, nel caso l'autenticazione federata non funzioni. A titolo di esempio, l'aggiudicatario può implementare una soluzione per avvalersi della propria autenticazione locale, sulla base di una procedura le cui informazioni per procedere e il riconoscimento dell'operatore possono essere erogate dal proprio servizio di assistenza H24.

Segmentazione della rete dei client

I sistemi oggetto del servizio dovranno essere integrati ed interfacciati con l'infrastruttura informatica di rete e sistemistica dell'Azienda, 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 dell'Azienda seguendo lo scenario descritto nel seguito.

In particolare, gli host oggetto di fornitura saranno integrati nella sola infrastruttura di rete dell'Azienda e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico verrà effettuata assegnando agli host stessi una specifica classe di indirizzi IP statici (se il numero di host complessivi afferenti alla rete assegnata è minore di 50) o dinamici (se il numero di host complessivi afferenti alla rete assegnata è maggiore di 50) coerente con il piano di indirizzamenti aziendale e verranno inseriti in una VLAN dedicata, assegnata dall'Azienda, dalla quale

potranno effettuare solo l'eventuale traffico necessario per svolgere le funzioni richieste in capitolato e l'eventuale traffico relativo all'assistenza remota da parte del fornitore. La segregazione del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali (ISFW – Internal Segregation Firewall), stilate per rete IP e per porta, o per protocollo o altro filtro intelligente, sulla base delle sole effettive necessità di traffico per svolgere le funzioni richieste in capitolato. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall aziendali (ISFW – Internal Segregation Firewall), per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia, in particolare la rete IP/VLAN assegnata non avrà in alcun caso visibilità di rete sulle ret IP/VLAN dei PC in dominio aziendale o altra rete comprendente host non in gestione. L'azienda si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.

È attivo sulla LAN un sistema di autenticazione degli host di rete. Tutti gli host forniti e collegati alla LAN dell'Azienda dovranno essere tali da consentire l'autenticazione di rete tramite MAC address (cosiddetta MAC authentication). A titolo di esempio non esaustivo, l'autenticazione avviene solo a seguito di traffico effettuato a partire dall'host che dovrà essere in tal senso caratterizzato/configurato. Nel merito, in particolare, l'autenticazione tramite MAC address viene scatenata – come previsto dal protocollo – a partire dall'host che si connette in rete, pertanto gli host forniti dovranno effettuare traffico ad ogni connessione fisica alla rete e presentare allo switch di accesso della LAN il loro MAC address; tale condizione verrà verificata in fase di collaudo e se l'autenticazione non andrà a buon fine il collaudo avrà esito negativo e l'host dovrà essere sostituito, a carico del fornitore, con uno adeguato. Non saranno considerati accettabili workaround per scatenare il processo di autenticazione tramite MAC address, come ad esempio l'abilitazione del protocollo DHCP sugli host forniti. Il protocollo DHCP verrà attivato a discrezione dell'Azienda solo nel caso in cui essa stessa abbia effettiva necessità di assegnare dinamicamente gli indirizzi (per esempio per lo spostamento dei dispositivi tra le sedi aziendali).

I collegamenti cablati dovranno essere realizzati con un adeguato grado di resistenza meccanica, nel caso per esempio dei dispositivi palmari o mobile, dovrà essere fornita una docking station e non saranno consentiti adattatori stand-alone di alcun tipo (ad esempio adattatori USB-RJ45). I dispositivi di tipo palmare e mobile dovranno essere specificatamente previsti dal fabbricante per uso in ambienti sanitari e locali ad uso medico (secondo la CEI 64-8/7), se del caso, ovvero rispondenti ai seguenti requisiti: rispondenza alle norme IEC 60601-1, grado di protezione IP pari almeno ad IP54; certificazione per resistenza alle cadute da 1 metro di altezza (per esempio secondo MIL-STD-810F/G); involucro/custodia certificato sanificabile, privo di spigoli (seamless) e realizzato in materiale antibatterico/antimicrobico soprattutto in relazione a MRSA. Le attività svolte dagli operatori dell'Azienda su tali dispositivi dovranno essere garantite dal fornitore con la migliore operatività in termini di facilità d'uso ed efficacia, in particolare per i dispositivi mobile i servizi dovranno essere resi disponibili dal fornitore per mezzo di specifiche applicazioni (non sarà consentito l'uso di applicazioni web su dispositivi mobile) e tali applicazioni dovranno essere pensate anche per l'uso off-line, data la necessità di avere connettività esclusivamente cablata di cui sopra.

Assistenza remota e telemonitoraggio

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dagli

amministratori di sistema formalmente nominati dall'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali, su cui la modalità Split Tunnel è per policy sempre disattivata. L'accesso verrà consentito solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario – compilando il modulo standard aziendale – ed inviata da casella PEC all'indirizzo PEC Aziendale, con allegati i documenti di identità e CF in corso di validità dei soggetti da abilitare. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali con bassi privilegi (livello user), ed in alcun caso saranno consentite 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 scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi da parte dell'Azienda. Il servizio di connessione remota VPN non verrà prestato all'aggiudicatario con livelli di servizio garantiti; perciò, il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio VPN in altro modo (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio VPN.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo da internet degli host oggetto di assistenza, nel presente scenario, lo strumento messo a disposizione da dalle Aziende è il firewall di navigazione gestito dalla società in house della Regione Autonoma Friuli Venezia Giulia denominata Insiel SpA: gli host forniti potranno raggiungere solo un numero limitato di destinazioni internet, su specifiche porte; in ogni caso il traffico consentito sarà quello minimo necessario per il funzionamento dei sistemi e non sarà consentita la navigazione internet nonché l'esfiltrazione di dati tramite questo canale. Verranno perciò effettuate specifiche abilitazioni basate su IP sorgente, IP destinazione e porta solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario – compilando il modulo standard Aziendale – ed inviata da casella PEC alla casella PEC aziendale. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'Azienda per la definizione delle suddette abilitazioni. Nel presente scenario, la risoluzione dei nomi sarà basata esclusivamente su uno specifico servizio DNS (Domain Name Service) dedicato a tutti i dispositivi segregati/isolati presenti sulla rete aziendale, compresi quelli oggetto del servizio. In ogni caso nessuna connessione configurata sul sistema oggetto del servizio dovrà utilizzare l'indirizzo IP. Tutte le connessioni tra il sistema e gli altri host/applicativi dovranno supportare il DHCP ed utilizzare, dunque, i nomi Full Qualified Domain Name (FQDN). Ad esempio, la configurazione applicativa dei nodi DICOM non deve essere legata all'indirizzo IP fisico dei nodi.

Analogamente al servizio VPN di cui sopra, anche il servizio di connettività in uscita tramite firewall di navigazione Insiel non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio in altro modo (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio.

Prescrizioni in merito alla fornitura di postazioni di lavoro e server

Si specifica infine che sono da intendersi oggetto del servizio 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 del servizio.

Nel caso in cui le applicazioni fornite dall'aggiudicatario fossero rispondenti alle specifiche del paradigma SaaS e del SSO così come descritte all'inizio del presente documento, l'aggiudicatario stesso potrà proporre in offerta tecnica di utilizzare le applicazioni offerte sui PC client aziendali standard (postazioni di lavoro aziendali). In tal caso non sarà necessaria la fornitura dei PC client dedicati da parte dell'aggiudicatario. l'Azienda, tuttavia, si riserva di verificare gli estremi ed i dettagli tecnici della proposta e si riserva di rifiutarla a suo insindacabile giudizio. In tal caso l'aggiudicatario dovrà comunque fornire tutti i PC client necessari.

Interoperabilità con gli applicativi del sistema informativo sanitario regionale

L'integrazione con il sistema Trasfusionale Emonet/Emolife avverrà attraverso una "piattaforma di integrazione" gestita dal fornitore GPI in collaborazione con la società in house della Regione Autonoma Friuli Venezia Giulia denominata Insiel.

È possibile prevedere scenari di integrazione sia tra Emonet/Emolife ed un unico middleware collettore di più sistemi (strumentazione di Immunoematologia, Virologia e Biologia Molecolare), sia verso singoli sistemi (bilance e scompositori, Emocromo POCT, frigoemoteche intelligenti, strumenti aferesi terapeutica, strumenti per assemblaggi automatici ecc.)

L'integrazione dovrà essere puramente applicativa e garantire lo scambio bidirezionale dei dati, inoltre dovrà essere flessibile nel supportare il flusso di lavoro ed eventuali variazioni dello stesso nel tempo. L'integrazione con la piattaforma fornita sarà realizzata necessariamente secondo standard HL7, mentre nel caso di integrazione con singola strumentazione sarà possibile usare anche altri protocolli di comunicazione (evitando in assoluto lo scambio file).

In fase di offerta andranno indicate tutte le integrazioni che si ritiene di dover realizzare verso Emonet/Emolife e per ciascuna di esse andrà indicato se tali integrazioni sono già state realizzate e sono in uso presso altre strutture sanitarie.

Ogni componente hardware, compresi eventuali elementi considerati accessori (a solo titolo di esempio non esaustivo cavi, convertitori interfaccia) e ogni eventuale sviluppo del software oggetto di fornitura, necessari all'integrazione con il sistema Emonet/Emolife, sono a totale carico del fornitore.

In fase di avvio del sistema, Insiel SpA, per quanto di sua competenza, metterà a disposizione tutte le informazioni tecniche necessarie per le integrazioni richieste.

Per l'intero periodo temporale della fornitura, per tutte le integrazioni dovrà essere garantita la manutenzione per l'intera durata dell'appalto, sia in termini di manutenzione correttiva sia in termini di manutenzione evolutiva, al fine di salvaguardare la possibilità da parte dell'Azienda di mantenere l'aderenza agli standard nel tempo.

In generale tutti i sistemi forniti dovranno consentire la disponibilità di dati aperti e le relative interfacce di accesso secondo le linee guida di interoperabilità AgID.

Specifiche tecniche di sicurezza informatica

Di seguito vengono definite le specifiche che i sistemi oggetto del servizio dovranno rispettare, sia nel caso di non collegamento in rete, sia nello scenario descritto nel presente documento, 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 del presente servizio 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") e comunque in osservanza delle normative e best practice già citate dal primo paragrafo del presente documento e sempre in coerenza con il paradigma "Zero Trust".

Pertanto, l'Aggiudicatario è responsabile per danni o violazioni dei dati dovuti a condizioni di vulnerabilità del software stesso e si impegna a correggere prontamente qualsiasi vulnerabilità software che gli venisse segnalata o di cui venisse a conoscenza considerando tale evento alla pari di un guasto bloccante e pertanto con gli stessi SLA previsti nel contratto.

Verranno eseguite periodicamente dall'Azienda o da personale a tal scopo incaricato procedure di
Vulnerability Assessment e Penetration Test e l'aggiudicatario si impegna pertanto a risolvere criticità o vulnerabilità che dovessero in tal modo emergere. Analogamente l'aggiudicatario si impegna a collaborare con il SOC (Security Operation Center) aziendale per il miglioramento continuo dei sistemi oggetto del servizio.

Inoltre, i sistemi oggetto del servizio dovranno rispettare le seguenti prescrizioni.
In generale, tutti gli elementi 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 per tutta la durata contrattuale.

In generale, tutti i software oggetto del servizio dovranno essere:

- coerenti con la necessità di richiedere applicazioni, servizi e procedure privacy by design e privacy by default per ogni percorso di trattamento. Tutti i sistemi devono essere costruiti per proteggere i dati trattati e farlo come impostazione predefinita. L'aggiudicatario è tenuto a fornire documentazione delle misure implementate anche allo scopo di permettere le necessarie valutazioni al Titolare;
- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
- dotati di impostazioni internazionali di Microsoft Windows (se presente) IT standard, comprese le tastiere, allo scopo di non incorrere in nessun caso in errori nelle date, nei dati numerici e nei dati personali locali;
- 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 per tutta la durata contrattuale;
- 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'Azienda, 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 oggetto del servizio che verranno installati su dispositivi collegati alla LAN e inseriti nei domini Aziendali, 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 nella cartelle %HOMEDRIVE%\ProgramData, 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, a titolo esemplificativo e non esaustivo, si ricorda che, anche nel perimetro delle prescrizioni previste dalla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", i sistemi oggetto del servizio:
- non devono prevedere nessun account locale;
- non devono prevedere nessun account impersonale per gli operatori e account di servizio solo se del tipo gMSA, group Managed Service Account;
- devono consentire azioni di software inventory;
- devono poter essere distribuiti in "package" fruibili dai sistemi di distribuzione aziendali;
- se installati con account amministrativi, non devono richiedere la connessione ad internet contemporanea all'installazione;
- devono utilizzare solo sistemi di comunicazione sicuri (crittati);
- devono rispettare le tecnologie di protezione delle banche dati di dati personali e sensibili;
- devono consentire le valutazioni di vulnerabilità e il fornitore deve adoperarsi per la risoluzione in tempi certi ed accettabili delle anomalie rilevate dall'Azienda o dalle aziende ad esse deputate.

In ogni caso i software oggetto del servizio non dovranno fare uso di Applet Java e ActiveX.

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 gMSA autorizzati, sulla base di opportuni permessi settati in modo che il livello dei privilegi di accesso sia il più basso possibile e 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'Azienda, salvo esplicita autorizzazione da parte dell'Azienda.

Non sarà in alcun caso consentita la fornitura ed installazione di apparati attivi di rete standard (switch, router, firewall, access point Wi-Fi, VPN concentrator, Mi-Fi etc.) a meno di eccezioni concordate con l'Azienda, che in ogni caso si riserva di accettarle a suo insindacabile giudizio, a seguito di presentazione di adeguata documentazione tecnica che ne giustifichi la necessità. In particolare: nel caso di apparati di sicurezza, l'aggiudicatario si impegna, come precedentemente riportato, a considerare il trasferimento delle logiche di sicurezza sui firewall aziendali (ISFW – Internal Segregation Firewall) aziendali nel caso di apparati per la connettività remota, l'aggiudicatario si impegna a far uso degli strumenti aziendali messi a disposizione dall'Azienda, come precedentemente riportato.

I firewall aziendali, utilizzati come ISFW a protezione di ciascuno dei contesti di rete descritti nel presente documento (reti e VLAN), sono tecnologicamente dei NGFW (Next Generation Firewall) dotati di funzionalità di stateful inspection e con application control attivo, conseguentemente tutti i sistemi e le applicazioni oggetto del servizio, nonché i servizi di assistenza remota e manutenzione, anche erogati tramite VPN, dovranno essere compatibili con tali tecnologie. A titolo di esempio non esaustivo, sistemi e applicazioni dovranno effettuare una gestione attiva del ciclo di vita delle sessioni ed in alcun caso per evitare malfunzionamenti o blocchi delle stesse dovrà essere necessario modificare sui firewall aziendali i relativi parametri TTL (Time-To-Live). L'azienda si riserva di bloccare qualunque tipologia di traffico ritenuto malevolo, in particolare a fronte di specifiche vulnerabilità che dovessero emergere nel corso della durata contrattuale.

Prescrizioni sulla posa in opera del cablaggio

Non sarà in generale consentita la fornitura di sistemi di cablaggio dati dedicati, a meno di casi particolari tecnicamente motivati, che dovranno essere esplicitati in offerta tecnica, motivati dettagliatamente ed approvati in ultima istanza dall'Azienda. Riguardo al cablaggio strutturato, dovranno essere utilizzati sempre e comunque i sistemi aziendali e gli eventuali ampliamenti necessari saranno eseguiti dall'Azienda. Dovranno essere indicati in offerta tecnica il numero e la dislocazione spaziale dei punti rete necessari al funzionamento dei sistemi oggetto del servizio, indicando per ciascun punto l'eventuale necessità di installazione di dispositivi di separazione (Separation Device) conformi alle norme IEC 60601-1, la cui installazione sarà a carico dell'Azienda.

Nel caso in cui l'aggiudicatario volesse comunque offrire servizi di posa in opera di cablaggio strutturato, dovrà sottostare a tutte le policy aziendali, oltre alle norme tecniche di riferimento, e l'Azienda si riserva di indicare ogni singolo dettaglio realizzativo (compresi marca e modello, classe CPR, categoria, ecc. dei materiali da utilizzare) che costituiranno vincolo contrattuale inderogabile.