

ALLEGATO E – SPECIFICHE PER L’INTEGRAZIONE CON I SISTEMI INFORMATIVI AZIENDALI

Sommario

Sistemi e Architettura Informatica previste in Fornitura	2
1 Sistema Informativo a supporto del Core-Lab.....	2
1.1 Perimetro di gestione	2
1.2 Requisiti Funzionali di Massima	2
1.3 Infrastruttura Client.....	3
1.4 Infrastruttura di Rete.....	3
1.5 Infrastruttura Server.....	3
1.6 Architettura Sistemistica	4
1.6.1 Sicurezza	4
1.6.2 Gestione Utenti	5
1.7 Integrazioni.....	5
1.7.1 Integrazione con Infrastruttura Aziendale	5
1.7.2 Integrazione con il LIS.....	5
1.8 Servizi di Assistenza	6
2 Sistemi Accessori	6
2.1 Infrastruttura	6
2.1.1 Infrastruttura Server.....	6
2.1.2 Infrastruttura Client.....	7
2.2 Sistema di preparazione automatica delle provette	7
2.2.1 Requisiti Funzionali.....	7
2.2.2 Integrazioni con LDAP.....	8
2.2.3 Integrazioni con Sistemi Informativi AUSLRE	8
2.3 Sistema di Monitoraggio dei costi delle prestazioni.....	8
2.3.1 Requisiti Funzionali.....	8
2.3.2 Integrazioni con LDAP.....	8
2.3.3 Integrazione con il repository della produzione sanitaria (HUB)	8
2.3.4 Integrazione con la componente di gestione del magazzino	9

Sistemi e Architettura Informatica previste in Fornitura

Oggetto del presente documento è la descrizione delle caratteristiche richieste dal sistema informatico a supporto della nuova strumentazione centralizzata del Laboratorio Analisi (di seguito Core-Lab) in acquisizione da parte dell'Azienda USL di Reggio Emilia (di seguito AUSLRE), per le sedi di Reggio Emilia, Guastalla e Castelnuovo Monti. Per sistema informatico si considerano tutte le componenti hardware e software necessarie per la gestione della strumentazione e per l'integrazione con il Sistema Informativo Ospedaliero, nello specifico con il LIS.

Le strutture di AUSLRE deputate al governo della infrastruttura ICT sono il Servizio Tecnologie Informatiche e Telematiche (STIT) e il Servizio di Ingegneria Clinica (SIC) aziendali.

La ditta offerente (di seguito Offerente) dovrà fare riferimento per approfondimenti alla documentazione prodotta dai due servizi sopra elencati, o tramite richiesta tramite i canali previsti dalle procedure di gara.

La fornitura prevede:

- Sistema Informativo a supporto del Core-Lab: sistemi informativi, hardware, servizi di installazione, servizi di gestione e servizi di assistenza e manutenzione relativi ad ogni componente hw e sw necessaria per il funzionamento del Core-Lab;
- Sistemi Accessori: sistemi richiesti in fornitura non legati direttamente alla architettura Core-Lab ma necessari ad un efficientamento dell'operatività complessiva dei laboratori.

1 Sistema Informativo a supporto del Core-Lab

1.1 Perimetro di gestione

Tutti i dispositivi di ambito ICT (PC, server, ecc...) a supporto dell'attività dei laboratori dovranno essere interamente forniti e gestiti dall'Offerente e saranno posti in tre sotto-reti dedicate ed isolate presso le sedi previste di Reggio Emilia, Guastalla e Castelnuovo Monti. Le tre sotto-reti isolate potranno comunicare solo attraverso una infrastruttura server condivisa.

La fornitura deve anche comprendere la posa delle componenti di cablaggio rete dati, degli apparati di rete e ogni altro dispositivo a supporto della stessa.

Il collegamento del Core-Lab con l'esistente infrastruttura middleware-LIS dovrà essere realizzato a livello di apparati di rete e interposto vi sarà un firewall gestito da AUSLRE. Tale collegamento è l'unico previsto e autorizzato.

Il progetto complessivo della infrastruttura ICT a supporto del Core-Lab dovrà essere oggetto di Progettazione Esecutiva dopo avvenuta aggiudicazione, e dovrà essere espressamente autorizzata da parte di STIT e SIC.

1.2 Requisiti Funzionali di Massima

Il sistema software dovrà gestire tutte le strumentazioni secondo i protocolli più evoluti, al fine di ottenere il riconoscimento positivo univoco di ogni campione e azzerare il rischio di passaggio di dati non congrui.

Alcune delle funzioni che il sistema dovrà garantire sono:

- Gestione delle attività pre-analitiche;
- Gestione delle non conformità e degli allarmi strumentali;
- Controllo di processo attraverso la tracciabilità del campione e degli eventi che lo accompagnano (ad esempio, data ora del check-in, data ora del passaggio da ogni strumentazione, ecc...);
- Gestione dei carichi di lavoro;
- Gestione del controllo di qualità;

- Funzioni di assistenza alla validazione tecnica, con la possibilità di implementare regole definibili dall'utente;
- Tracciabilità completa in tempo reale dei campioni, dei Controlli di Qualità, delle calibrazioni e delle attività di manutenzione;
- Controllo in tempo reale tramite allarmi della funzionalità dell'intero sistema;
- Interfacciabilità con i software gestionali intermedi per emocromo ed esame urina completo;
- Archivio storico per pazienti e controlli.

1.3 Infrastruttura Client

La fornitura e futura gestione per la durata contrattuale (ivi comprese sostituzioni in caso di guasto o per obsolescenza) dei client (PC o qualsiasi altro dispositivo necessario per la fruizione della componente software del sistema) necessari per la gestione del Core-Lab e dei sistemi accessori è in carico all'Offerente.

Su tali client:

- non è ammesso l'uso per archiviazione dati (che deve essere interamente gestita su infrastruttura server, vedi di seguito);
- non sono ammessi client con sistemi operativi obsoleti e non più gestiti (esempio: Win7);
- a tutela della complessiva sicurezza aziendale, i client non devono consentire l'accesso tramite dispositivi di archiviazione di massa esterni (es. chiavette USB).

1.4 Infrastruttura di Rete

La fornitura deve comprendere tutto quanto necessario per la realizzazione ex-novo dell'infrastruttura di rete del nuovo sistema Core-Lab.

Si specifica che, anche nella fase transitoria, qualora si preveda la necessità di collegare in rete le apparecchiature (strumenti e pre-analitica), dovrà essere predisposta una rete temporanea avente le medesime caratteristiche.

Caratteristiche della infrastruttura di rete:

- l'ubicazione degli apparati di rete dovrà essere valutata dall'Offerente, ma non potrà essere all'interno del cavedio di rete aziendale;
- gli apparati di rete dovranno essere previsti in raddoppio in modo da garantire adeguato backup funzionale in caso di guasto del singolo dispositivo;
- i cablaggi dati dovranno essere previsti in raddoppio, quindi doppie prese di rete attestata su apparati di rete distinti. La parte wired dovrà essere realizzata con cavi a coppie UTP di cat.6, secondo lo standard TIA/EIA 568. Eventuali collegamenti in fibra potranno essere realizzati in fibra ottica monomodale 9-125. Se prevista una connettività wireless, la ditta offerente dovrà fornire le antenne e predisporre i relativi cablaggi. Inoltre dovrà predisporre analisi e progettazione onde evitare interferenze con la copertura wireless ad uso sanitario già presente all'interno del Campus ospedaliero S. Maria Nuova e nelle sedi provinciali. Nello specifico, l'infrastruttura wireless di AUSL RE è di tipo centralizzato e costituita da Wireless Control System (WLC) e antenne di marca Cisco, sul presidio ospedaliero S. Maria, e di tipo distribuito con antenne Extreme Networks e controller centrale sulle altre sedi. È realizzata secondo lo standard IEEE 802.11a/b/g/n/ac ed in particolare, sulle frequenze a 2.4Ghz sono utilizzati i canali 1,6,11.

1.5 Infrastruttura Server

Come da direttive nazionali e regionali, il punto centrale dell'attuale infrastruttura server di AUSLRE è collocato presso DataCenter di Lepida Scpa, nei DataCenter primario a Ferrara e come sito di Disaster

Recovery su Parma. I DataCenter locali presso le strutture aziendali sono da considerarsi come deputati esclusivamente al mantenimento dei sistemi cached (sistemi di archiviazione temporanea a garanzia della continuità operativa in caso di indisponibilità dei DataCenter primario e secondario).

L'infrastruttura server è collegata alla rete LAN di AUSLRE tramite doppio collegamento ridondato su rete Lepida e consegnato su percorsi distinti e ridondati nella sede del campus S. Lazzaro e nell'Ospedale S. Maria Nuova.

Il traffico di rete con i client è regolato da appositi firewall per ogni DataCenter gestiti internamente da STIT, che autorizza e verifica il traffico da e verso le reti DataCenter regionali.

La fornitura dell'Offerente deve prevedere tutta l'infrastruttura server a supporto del Core-Lab. Tale infrastruttura potrà essere composta da server virtuali e fisici, ospitati internamente presso i DataCenter Lepida. La negoziazione delle modalità e condizioni economiche per tale servizio è in capo totalmente all'Offerente.

Eventuali server fisici, da intendersi per la sola continuità operativa (vedi sopra), dovranno essere collocati presso i DataCenter locali, ospitati presso l'Ospedale S. Maria Nuova in modalità rack.

E' oggetto di fornitura ogni dispositivo necessario all'operatività server (es. armadi, supporti, dispositivi di continuità, ecc.).

La gestione del parco server sarà in totale carico dell'Offerente. Sono in particolare comprese le attività inerenti il mantenimento della sicurezza, quindi gli aggiornamenti del S.O, patching, fixing, antivirus.

Deve essere oggetto di fornitura anche la progettazione e la predisposizione di tutte le misure, organizzative e tecniche atte a garantire continuità operativa in caso di indisponibilità dei DataCenter primari o di DataCenter primari e secondari (es. avvalendosi di infrastruttura cache presso DataCenter locali).

1.6 Architettura Sistemistica

1.6.1 Sicurezza

Per garantire la sicurezza dell'intero sistema sono obbligatori i seguenti requisiti, applicabili ai client e server oggetto della fornitura:

- **Antivirus**

Per ogni server e client incluso in fornitura deve essere compreso un sistema di gestione antivirus/antimalware. Nello specifico il sistema antivirus deve prevedere aggiornamento automatico delle firme / configurazioni (tramite linea dati in fornitura o passaggio attraverso il SIO) e deve, ove possibile, essere attivata la protezione real-time dello stesso. Inoltre il sistema antivirus deve prevedere console di verifica dello stato di aggiornamento e dello stato di tutte le macchine poste sotto copertura, oltre all'invio di dati periodici di allarme e/o rilevazione virus.

Il sistema antivirus potrà essere configurato secondo le modalità ritenute più consone alla funzione di ciascun server e client, nel rispetto delle misure minime di sicurezza vigenti.

- **Patching**

Per ogni server e client compreso in fornitura il fornitore deve prevedere aggiornamenti automatici relativi alla sicurezza dei principali componenti di sistema operativo e di firmware ai più recenti aggiornamenti di sicurezza (es. patch di sistema operativo).

Il fornitore deve prevedere che a seguito di segnalazione di vulnerabilità emerse dalle scansioni o da annunci ufficiali, sia possibile risolverle sia per mezzo di patch specifiche, o implementando opportune contromisure oppure documentando e dichiarando il livello di rischio da assumere, come da misure minime di sicurezza vigenti.

- **Backup**

Per ogni server incluso nella fornitura deve essere previsto un sistema di backup dei dati, che si potrebbe anche appoggiare a sistemi di backup aziendale.

Nel caso in cui sia previsto un sistema di backup autonomo, devono essere forniti anche strumenti di monitoraggio sulla sua corretta esecuzione.

Per i client inclusi nella fornitura, deve essere previsto un sistema di backup funzionale che permetta l'archiviazione dei dati di configurazione necessari al suo funzionamento, autonomo o in appoggio su sistemi aziendali.

1.6.2 Gestione Utenti

- **Gestione centralizzata degli utenti**

Deve essere prevista una gestione centralizzata degli utenti di accesso a tutti i dispositivi previsti in fornitura. La definizione delle modalità è oggetto di progettazione da parte dell'Offerente. La gestione delle utenze deve rispettare le normative e linee guida vigenti (es. per quanto attiene scadenza e complessità delle password). La gestione delle utenze deve essere allineata con l'identità aziendale, resa disponibile da sistema Omnibus (SINFO srl); tale allineo deve prevedere la disabilitazione automatica delle utenze a fronte di terminazione della posizione aziendale ufficiale. E' disponibile, per l'implementazione di cui sopra, l'infrastruttura Active Directory aziendale (raggiungibile anche tramite protocollo LDAP).

- **Profilazione utenti**

Il sistema deve prevedere la profilazione degli utenti, con attribuzione di diritti diversi a seconda dei ruoli.

Per questo è necessario l'individuazione di uno o più utenti come "amministratori di sistema" che avrà il compito di profilare e autorizzare a specifiche funzioni gli altri utenti del sistema (l'amministratore di sistema sarà oggetto di nomina formale da parte dell'azienda e da parte dell'Offerente). Gli amministratori saranno individuati tra il personale di AUSLRE e non esclusivamente tra quello dell'Offerente.

- **Tracciabilità degli accessi**

Il sistema deve poter avere una tracciabilità completa degli accessi ai dispositivi oggetto di fornitura.

1.7 Integrazioni

1.7.1 Integrazione con Infrastruttura Aziendale

Come da precedente sezione relativa alla gestione utenti, deve essere prevista integrazione verso i sistemi di gestione della identità aziendali, in alternativa:

- Active Directory (via protocollo LDAP);
- Sistema Omnibus (per recupero e gestione avanza delle identità degli utenti aziendali).

1.7.2 Integrazione con il LIS

Presso l'Azienda è attualmente installato la Suite Concerto, fornita dalla ditta Dedalus S.p.A.; tale sistema prevede un unico LIS a servizi sia dei laboratori analisi ubicati nella sede di Reggio Emilia che dei laboratori provinciali. L'interfaccia tra il LIS e la strumentazione avviene unicamente tramite il middleware PentaWeb, già presente nella Suite sopra citata.

Le integrazioni tra il sistema Core-Lab ed il LIS dovranno avvenire tramite tale middleware PentaWeb, di cui l'Offerente si impegna ad installare e gestire istanza dedicata all'interfacciamento con il Core-Lab (o sotto-istanza/partizionamento della istanza attuale).

Le licenze necessarie, la progettazione, l'implementazione e l'assistenza sul canale di collegamento tra il sistema Core-Lab e il middleware PentaWeb sono a totale carico dell'Offerente.

1.8 Servizi di Assistenza

Dovranno essere previsti sistemi e relativi servizi per:

- assistenza remota (diagnostica ed eventuale risoluzione di malfunzionamenti HW e SW);
- monitoraggio remoto (verifiche di routine allo scopo di prevenire, per quanto possibile, malfunzionamenti hardware e software).

I sistemi di assistenza e monitoraggio remoti non potranno appoggiarsi esclusivamente alla connessione Internet dell'ASMN, ma utilizzeranno una linea dati dedicata (xDSL) che l'Offerente dovrà includere nella fornitura e sarà totalmente a suo carico in termini di installazione e gestione. Deve essere prevista una linea dati dedicata per ciascuno dei laboratori coinvolti nella fornitura.

I servizi di monitoraggio dovranno fornire report periodici sul funzionamento del sistema, disponibili sia all'Offerente per gestione operativa che ad AUSLRE per verifica e ispezione.

Per garantire l'assistenza (H24 365gg/anno), l'Offerente deve prevedere un numero dedicato unico (al più distinto su due numeri tra orario lavorativo e orario di reperibilità) per quanto riguarda tutto l'ambito informatico (hardware, software, rete).

La chiamata dell'utente al servizio di assistenza dell'Offerente può prevedere una escalation sui servizi di assistenza e reperibilità aziendali (gestiti dallo STIT): tale ingaggio deve essere fatto direttamente dall'assistenza dell'Offerente (a cui saranno forniti opportuni contatti) e non demandato dall'utente iniziale.

E' oggetto di fornitura la progettazione dei servizi di assistenza, manutenzione e reperibilità.

2 Sistemi Accessori

A corredo dei sistemi informativi previsti per il Sistema Core-Lab, si richiede anche la fornitura di due sistemi accessori a supporto dell'attività complessiva dei laboratori analisi.

I sistemi accessori richiesti sono:

- sistema di preparazione automatica delle provette/contenitori per i Centri Prelievo principali dell'AUSL, compresi tutti i consumabili/etichette e interfacciamento;
- sistema per il monitoraggio e analisi dei costi di tutta l'attività laboratoristica.

2.1 Infrastruttura

2.1.1 Infrastruttura Server

Come da direttive nazionali e regionali, il DataCenter principale di AUSLRE è collocato presso Lepida Scpa, con sito primario a Ferrara e sito di Disaster Recovery su Parma. I DataCenter locali presso le strutture aziendali sono da considerarsi come deputati esclusivamente al mantenimento dei sistemi cached (sistemi di archiviazione temporanea a garanzia della continuità operativa in caso di indisponibilità dei DataCenter primario e secondario).

Nel caso in cui sia quindi prevista una infrastruttura server, sarà necessario appoggiarsi su tale infrastruttura e la negoziazione delle modalità e condizioni economiche per tale servizio è in capo totalmente all'Offerente.

Sui server devono inoltre essere previsti:

- la gestione, a carico dell'Offerente, degli aggiornamenti del S.O., patching, fixing ecc.;

- il sistema di backup dati; tale sistema può essere autonomo, o appoggiarsi sui sistemi di backup aziendale di AUSLRE. Se ci si avvale di sistema di backup autonomo da quello aziendale, il sistema deve prevedere strumenti di reportistica/monitoraggio sulla corretta esecuzione del backup;
- Il sistema di gestione antivirus: tale antivirus può essere oggetto della fornitura oppure può essere mutuato dalla infrastruttura aziendale ASMN.

2.1.2 Infrastruttura Client

Il sistema può prevedere la fornitura autonoma di client oppure l'appoggio su quelli aziendali. Di seguito sono riportati i requisiti minimi richiesti:

- **Client in fornitura**
In caso di fornitura autonoma da parte dell'Offerente, il client deve prevedere la connessione (join) verso il Dominio aziendale di competenza (gestito tramite controllers Microsoft Active Directory). Non sono ammessi client con sistemi operativi obsoleti e non più gestiti (esempio: Win7).
- **Appoggio su Client aziendali**
 - Eseguibili: eventuali applicativi da installare o eseguire su client aziendali devono essere files eseguibili a 32 bit.
 - Setup: il setup della installazione dell'applicativo deve essere in tecnologia Windows Installer.
 - Collocazione applicativi su file system client aziendali: I componenti (eseguibili, DLL o altro) delle applicazioni devono essere installati in %ProgramFiles%\<nome azienda>\<nome applicazione> se non sono condivisi. Se devono essere condivisi da altri applicativi in: directory file comuni\<nome società> o %ProgramFiles%\<nome fornitore>\File condivisi.
 - Versione e Release: per ogni applicativo software offerto deve essere chiaramente indicato il numero di versione e release.

Per entrambe le soluzioni deve essere comunque garantito:

- **Backup Funzionale**
Per ogni client/workstation che svolga ruolo critico per la continuità funzionale del sistema, e che preveda l'archiviazione locale di dati di configurazione necessari al suo funzionamento deve essere previsto un sistema di backup di tali dati, autonomo o appoggiato sui sistemi di backup aziendali (in questo caso tramite copia dei files di interesse in apposito spazio oggetto di backup aziendale).
- **AntiVirus**
Per ogni client previsto in fornitura deve essere compreso un sistema di gestione antivirus. Tale antivirus può essere oggetto della fornitura, o essere mutuato dalla infrastruttura aziendale ASMN. Qualora compreso nella fornitura:
 - il sistema antivirus deve prevedere aggiornamento automatico delle firme / configurazioni (tramite linea dati in fornitura o passaggio attraverso il SIO);
 - il sistema antivirus deve prevedere console di verifica dello stato di aggiornamento;
 - il sistema antivirus (in fornitura o aziendale) potrà essere configurato secondo le modalità ritenute più consone alla funzione di ciascun client/workstation.

2.2 Sistema di preparazione automatica delle provette

2.2.1 Requisiti Funzionali

Il Sistema richiesto, composto da hardware e software, deve consentire una gestione al punto prelievo delle seguenti funzionalità:

- identificazione dell'operatore al punto prelievo;
- identificazione del paziente/prelievo attraverso la lettura del barcode;
- conferma della tipologia di provetta/contenitore corrispondente al paziente/prelievo;
- stampa ed etichettatura univoca del campione (con numero identificativo generato da LIS).

2.2.2 Integrazioni con LDAP

Il sistema si deve appoggiare, per l'identificazione dell'utente e la relativa autorizzazione sul sistema, di gestione credenziali aziendali (Active Directory), preferibilmente tramite integrazione applicativa LDAP.

2.2.3 Integrazioni con Sistemi Informativi AUSLRE

Il sistema software dovrà integrarsi con il modulo di Order Entry (OE) di HConnect (fornitore 4WardPro S.p.a. - Argelato (BO)).

L'integrazione prevede la trasmissione in modalità push da parte di OE verso il sistema software delle seguenti informazioni, per ogni richiesta/ordine destinato ai punti prelievo gestiti tramite il sistema oggetto di fornitura:

- la testata anagrafica strutturata del paziente;
- la testata ordine, comprendente il codice di prenotazione (oggetto di lettura con barcode);
- l'elenco delle prestazioni (analisi) previste nell'ordine, con relativi dati accessori;
- l'insieme delle etichette (intese come sequenza di PDF), associate all'ordine, con relativo codice di corrispondenza con il tipo provetta, o codice identificativo della destinazione dell'etichetta stessa (quando non destinate alla stampa su provetta).

Il sistema software dovrà garantire la stampa delle etichette mantenendo inalterato contenuto e grafica trasmesso come PDF. Non deve essere prevista alcuna configurazione sul sistema software dei contenuti o del formato grafico della etichetta stessa, che deve essere conforme a quanto trasmesso dal sistema OE.

Ogni attività di configurazione/adequamento sui sistemi di integrazione di OE necessaria al collegamento verso il sistema software oggetto di fornitura sarà a carico dell'Offerente.

2.3 Sistema di Monitoraggio dei costi delle prestazioni

Il sistema di monitoraggio dei costi dovrà ricevere i dati necessari dal Sistema informativo aziendale per il monitoraggio ed analisi dei costi dei laboratori dell'AUSL RE.

2.3.1 Requisiti Funzionali

Il Sistema richiesto, composto da hardware e software, deve prevedere:

- l'effettuazione di statistiche di produzione per diverse variabili di analisi (per esempio: sede, esame, richiedente, ecc....);
- l'effettuazione di statistiche di monitoraggio della spesa in relazione agli esami refertati per diverse variabili di analisi (per esempio: sede, esame, richiedente, ecc....).

2.3.2 Integrazioni con LDAP

Il sistema si deve appoggiare, per l'identificazione dell'utente e la relativa autorizzazione sul sistema, di gestione credenziali aziendali (Active Directory), preferibilmente tramite integrazione applicativa LDAP.

2.3.3 Integrazione con il repository della produzione sanitaria (HUB)

Il sistema deve prevedere l'integrazione con HUB, il Repository della Produzione Sanitaria dell'AUSLRE (fornitore Maps Group S.p. A., Parma).

HUB svolge ruolo di concentratore di tutte le prestazioni erogate nell'azienda sanitaria, ivi comprese tutte le analisi (e relativi esiti) generati dai laboratori analisi. I dati contenuti sono relativi al solo refertato, ed è quanto di interesse per l'ambito specifico del sistema accessorio in oggetto.

I dati presenti su HUB consentono una stratificazione del dato per esame (analisi ed esito, come da codifiche di laboratorio), sede, richiedente e generiche caratterizzazioni amministrative di richiesta e paziente.

2.3.4 Integrazione con la componente di gestione del magazzino

Il sistema deve prevedere l'integrazione con la componente di gestione del magazzino reagenti prevista per il Core-Lab per i dati relativi ai costi e consumi.