Allegato C
Aspetti Infrastrutturali rete di telecomunicazioni e sistemi

CONTESTO TECNOLOGICO E SITUAZIONE ATTUALE

RETE DI TELECOMUNICAZIONE

La rete informatica dell'Istituto Ortopedico Rizzoli è costituita da una rete capillare di distribuzione sia di tipo wired che di tipo wireless, caratterizzata da un centro stella di piano a servizio del blocco operatorio al primo piano, 2 centri stella di campus ed un nodo di disaster recovery (nodo DR) sia per la parte rete dati e fonia che per la parte server infrastrutturali. La parte wired a servizio della periferia utente è realizzata con cavi a coppie UTP di cat.6 o cat.5e, secondo lo standard TIA/EIA 568 mentre i collegamenti di dorsale periferica, dei centri stella ed il collegamento tra ciascuna sala del blocco operatorio ed il relativo centro di piano sono realizzati in fibra ottica, sia di tipo multi che single mode. La rete è realizzata completamente in tecnologia switched ethernet, servita anche da dispositivi PoE+ e gli apparati sono del produttore HP. La connettività di dorsale dai rack periferici verso i due centri stella e il DR è ridondata in fibra ottica single mode a 1Gbps; la connettività tra ciascuna delle dieci sale operatorie del blocco operatorio e il relativo centro di piano è ridondata in fibra ottica multi mode a 1Gbps; la connettività di dorsale di campus tra i due centri stella e il nodo DR è ridondata in fibra ottica single mode a 10 Gbps; la connettività verso i client è a 100 Mpbs o 1 Gbps in rame, a 1 Gbps o 10 Gbps in rame o in fibra verso i server e storage nelle server farm locali; la connettività geografica verso il data center di Lepida SpA a Ravenna è ridondata in fibra ottica single mode a 1 Gpbs con latenza media pari a 5 ms.

L'unico protocollo di rete ammesso è il TCP/IP. L'architettura di rete è di tipo L3 e ogni rack periferico prevede una sottorete (subnet) separata e distinta dalle altre con indirizzi di classe A o di classe B definiti nella RFC 1918 e default gateway distinti. Gli indirizzi IP sono assegnati dinamicamente tramite il servizio DHCP alle postazioni di lavoro fisse e mobili e gli host sulla rete sono tutti registrati nel dns interno aziendale. Le connessioni verso l'esterno/Internet sono su rete geografica di Lepida attraverso il Cesia/Garr e avvengono tramite proxy server e firewall perimetrali con autenticazione mediante il server LDAP aziendale; viene inoltre gestito il dns esterno per i domini registrati in ior.it

La copertura wireless è realizzata secondo lo standard IEEE 802.1a/b/g/n ed è distribuita su tutti i reparti sanitari e alcune zone dei laboratori di Ricerca e dell'area Generale e Amministrativa. L'infrastruttura wifi è di tipo centralizzato, governata da due wireless lan controller (WLC) in HA e access point di tipo PoE del produttore HP. I protocolli di sicurezza e l'autenticazione della rete wireless sono basati su WPA2, PEAP, EAP/TLS e la crittografia dati AES, con certificato SSL self signed di IOR. L'Ente intende rinnovare l'infrastruttura di rete wireless nel corso del 2018-2019 con ampliamento della copertura.

Sulla rete informatica sono installati anche altri impianti tecnici quali: IP PBX, telefoni SIP, impianto cercapersone, telecamere, totem per le prenotazioni, riscuotitrici, sonde e allarmi.

Non è consentito, se non su esplicita autorizzazione del servizio ICT interno, l'inserimento di alcun dispositivo di rete estraneo alla infrastruttura di rete aziendale, come dal Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli.

L'Istituto ha una sede geografica, il Dipartimento Rizzoli Sicilia (DRS), ubicata presso la struttura di Villa Santa Teresa a Bagheria. La sede DRS è collegata con una linea dati MPLS tipo Intranet di Telecom a 10 Mbps, attestata a Bologna sul punto di accesso alla rete Lepida dell'Istituto. La connettività della sede DRS con il data center di Lepida a

Ravenna è assicurata attraverso la linea dati MPLS di Telecom e attraverso la rete geografica di Lepida utilizzata dall'Istituto. La rete LAN wired e wireless del DRS, messa a disposizione dell'Istituto, è di proprietà ed in gestione della struttura di Villa Santa Teresa.

DATACENTER E INFRASTRUTTURA HARDWARE DEI SISTEMI

I sistemi dell'Ente sono ospitati in due server farm aziendali locali e in housing nel data center di Lepida SpA a Ravenna. Le due server farm locali sono poste rispettivamente nella palazzina ICT e nel nodo DR e ospitano alcuni server critici ridondati in HA, come ad esempio: l'IP PBX, il PACS, i server infrastrutturali della rete (dhcp, dns, ldap, radius, firewall etc). I server sono ospitati su due nodi VMware 5.5 in HA e sue due nodi Proxmox VE in HA.
Tutti gli altri sistemi e in particolare quelli di area sanitaria, come ad esempio i server dei DB Oracle e SQL, gli application server, il mail server e altri server per l'esecuzione di applicativi e sistemi dell'area della ricerca ed amministrativa, sono ospitati in housing nel data center di Lepida a Ravenna, su di una infrastruttura a due nodi VMware 6.0 in HA.
I server hanno in maggioranza sistema operativo Linux/Oracle linux, sono presenti VM con sistema operativo Windows Server.
Presso il data center di Lepida sono disponibili soluzioni in hosting ad alta affidabilità su macchine virtuali VMware 6.x, su host fisici e su piattaforma exadata per Oracle.
Il sistema di storage a due nodi in HA è basato sul software datacore SANsymphony. Il sistema di backup principale è installato su hardware (server e storage) in hosting nel data center di Lepida ed è basato sul software Simpana di Commvault; un secondo sistema Simpana per la copia secondaria del backup è nella server farm locale nella palazzina ICT, in una sede diversa rispetto al data center Lepida.

POSTAZIONI DI LAVORO

La postazione di lavoro aziendale standard (PDL) viene installata da immagine con sistema operativo Windows 7 o Windows 10. Gli applicativi normalmente installati sulle PDL sono: Libre Office v. 5 o superiore, Antivirus Kaspersky, Adobe Acrobat Reader, WinZip/7Zip, Java versione 1.6 o superiore, browser Firefox/Chrome/IE 11. Sono ancora presenti alcune postazioni con sistema Windows XP, in via di sostituzione. MSOffice è installato esclusivamente in postazioni dedicate ad attività specifiche. Si precisa che il parco delle postazioni di lavoro fisse e mobili è soggetto a continue evoluzioni e la scelta delle tipologie e dei modelli è vincolata di prassi alle convenzioni delle centrali di acquisto.

REQUISITI PER LA GESTIONE DELL'AUTENTICAZIONE E DELL'ABILITAZIONE DEGLI UTENTI ALLE PROCEDURE APPLICATIVE

Tutte le procedure informatiche aziendali devono utilizzare credenziali di autenticazione già in essere presso l'Istituto Ortopedico Rizzoli, in quanto esse forniscono alcune importanti garanzie di rispetto della normativa privacy (ad es. tipologia password, cambio password, disattivazione alla chiusura del rapporto di lavoro) e facilitano l'accesso degli utenti agli applicativi cui sono autorizzati.

Per l'autenticazione degli utenti aziendali a SIO IOR si richiede l'integrazione con il sistema LDAP aziendale basato sul software open source Openldap; le utenze in uso hanno una naming standard del tipo nome.cognome.
Qualora ritenuto utile e supportato dalla ditta offerente, per le procedure in ambiente web è stato implementato il Single Sign On (SSO) mediante il software open source Shibboleth, integrato con LDAP aziendale.
Gli applicativi sanitari richiedono integrazioni con altre procedure; a tal fine è necessario realizzare le integrazioni effettuando in modo sicuro il passaggio dei dati relativi all'utente collegato, che deve avvenire su canale cifrato e non essere replicabile.

- Se le procedure si integrano con il SSO Shibboleth, tali caratteristiche di sicurezza sono nativamente garantite
- Se le procedure utilizzano l'autenticazione LDAP il passaggio dell'utente deve avvenire in modalità sicura e mediante passaggio di token secondo specifiche da concordare tra i fornitori delle varie procedure da validare da parte dei tecnici ICT di IOR.

La gestione dei profili di abilitazione degli utenti deve essere realizzata all'interno delle singole procedure poiché il sistema LDAP aziendale non può essere utilizzato ai fini della profilazione e delle abilitazioni/autorizzazioni; LDAP gestisce i gruppi di utenti.

REQUISITI DELL'INFRASTRUTTURA

SIO IOR dovrà essere installato presso uno dei data center di Lepida SpA, società *in house* della Regione Emilia Romagna.

L'Ente metterà a disposizione senza oneri aggiuntivi per l'aggiudicatario:

- Le infrastrutture presenti nel data center di Lepida a Ravenna, per ospitare il sistema offerto secondo l'architettura proposta. L'offerta tecnica del fornitore dovrà indicare il dimensionamento complessivo delle macchine (CPU, RAM, disco) per soddisfare le esigenze del sistema progettato.
- La connettività tra il data center di Lepida e le sedi dell'Ente come sopra descritto.
- Licenza del RDBMS Oracle.
- Infrastruttura WMware 6.x.

Si precisa che tutte le ulteriori ed eventuali licenze necessarie per il corretto funzionamento del sistema offerto, sia lato server sia lato client, sono a carico del fornitore (ad esempio: sistemi operativi, CAL, add-on, etc). Inoltre tutta l'infrastruttura software deve basarsi sulle ultime versioni disponibili e supportate dei prodotti (sistemi operativi, framework, etc). Su tutti i software offerti dovranno essere installate e manutenute le eventuali patch entro due mesi dalla data di rilascio da parte del produttore. Il fornitore si impegna inoltre ad aggiornare tutta l'infrastruttura software all'ultima versione disponibile nel più breve tempo possibile e comunque non oltre sei mesi dal rilascio dell'aggiornamento o della nuova release da parte del produttore, anche mediante programmi di software assurance a carico dell'offerente, a meno di deroghe per iscritto da parte dell'Ente, sulla base di opportuna documentazione ricevuta dal fornitore del sistema.

Qualora l'aggiudicatario utilizzi l'ambiente Oracle messo a disposizione dall'Ente, in caso di aggiornamento della release di Oracle da parte dell'Ente, l'aggiudicatario della presente

fornitura dovrà garantire la migrazione del sistema alla nuova versione in un tempo massimo di nove mesi.

Al fine di una corretta interpretazione dei confini delle competenze tra l'Ente e l'aggiudicatario della fornitura, si precisano di seguito le modalità degli interventi sulle componenti del sistema:

Application Server

È competenza dell'Ente:

- La configurazione del sistema operativo, rispettando i requisiti di sicurezza aziendali (ad esempio relativi all'antivirus, all'inserimento nel dominio aziendale e/o integrazione ad ldap, registrazione centralizzata dei log di accesso, implementazione del monitoraggio attraverso la piattaforma Sanet3 via snmp, etc.
- L'assegnazione di credenziali amministrative personali ai tecnici del fornitore incaricati delle operazioni di installazione/aggiornamento dei vari software.
- L'intervento sul contenitore VMware (ad esempio relativamente al ridimensionamento dei parametri quali RAM, CPU, disco; la manutenzione su VMware).
- La gestione dei backup dei sistemi e dei dati secondo le politiche aziendali.

È competenza del fornitore aggiudicatario:

- L'installazione, configurazione e messa in produzione degli application server incluso il sistema operativo.
- La risoluzione di qualsiasi problematica relativa al contenuto della VM (ad esempio rallentamenti e/o malfunzionamenti bloccanti di servizi o di componenti quali il tomcat, produzione eccessivi di log, etc).

Database Server

È competenza dell'Ente:

- La configurazione del sistema operativo rispettando i requisiti di sicurezza aziendali (ad esempio relativi all'antivirus, all'inserimento nel dominio aziendale e/o integrazione ad ldap, registrazione centralizzata dei log di accesso, implementazione del monitoraggio attraverso snmp, etc.
- L'assegnazione di credenziali amministrative personali ai tecnici del fornitore incaricati delle operazioni di installazione/aggiornamento dei vari software.
- La gestione dei backup dei sistemi e dei dati secondo le politiche aziendali.

È competenza del fornitore aggiudicatario:

- L'installazione e la configurazione dell'ambiente del motore DB, la creazione e messa in produzione del DB.
- L'implementazione delle procedure di backup del DB (ad esempio export, redo log, etc).
- La risoluzione di qualsiasi problematica relativa al contenuto e al funzionamento del DB (ad esempio lock, rallentamenti e/o malfunzionamenti bloccanti di servizi o di componenti del sistema, scheduled procedure, tablespace, integrazioni con altre procedure, etc).

Sistema di Backup, Disaster recovery e Business Continuity

L'aggiudicatario dovrà fornire il piano di backup del sistema offerto che dovrà consentire, per ogni funzionalità fornita, il ripristino delle informazioni fino all'ultimo "commit" eseguito. L'implementazione del piano di backup sarà concordato con l'Ente e realizzato congiuntamente. Il piano dovrà essere dettagliato e documentato in ogni sua parte, includendo anche il ripristino del sistema in produzione.

L'aggiudicatario dovrà proporre una soluzione per la gestione del Disaster Recovery (di seguito DR) il cui dimensionamento e architettura dovranno garantire il regolare funzionamento dell'Ente per le sue attività istituzionali, specificando anche le modalità di ripristino e le tempistiche.
La soluzione proposta sarà oggetto di valutazione tecnica. La proposta tecnica del fornitore dovrà quindi riportare l'architettura del sistema DR e le caratteristiche delle componenti.

L'Ente mette a disposizione senza oneri aggiuntivi per l'aggiudicatario:

- Le infrastrutture presenti in un data center di Lepida diverso dal sito primario, per ospitare l'infrastruttura del sistema DR secondo l'architettura proposta. L'offerta tecnica del fornitore dovrà indicare il dimensionamento complessivo delle macchine (CPU, RAM, disco) per soddisfare le esigenze del sistema DR progettato.
- La connettività tra il data center di Lepida primario e quello di DR mediante un collegamento diretto ridondato in fibra ottica con banda 10 Gbps; la connettività delle sedi dell'Ente verso il DR, che è garantita attraverso la rete regionale Lepida mediante un collegamento ridondato in fibra ottica con banda a 1 Gbps.
- Licenza del RDBMS Oracle.
- L'infrastruttura WMware 6.x.

La soluzione proposta dovrà essere caratterizzata da un'architettura che garantisca la continuità operativa (business continuity) in caso di rallentamento e/o malfunzionamento bloccante con interruzione del funzionamento di una parte qualsiasi del sistema.

Nell'ambito delle misure di continuità operativa è necessario che SIO IOR preveda specifiche procedure atte a garantire la sicurezza del paziente in caso di indisponibilità del sistema informativo per qualsivoglia fattore, anche esterno a SIO IOR (ad esempio rallentamenti e/o malfunzionamenti bloccanti legati alla connettività LAN e/o WAN, a integrazioni con altri sistemi, a servizi e/o componenti specifiche, etc). Tali procedure devono prevedere modalità e strumenti per l'accesso in lettura alle informazioni critiche per le attività in corso da parte degli operatori sanitari e amministrativi abilitati. Al fine di facilitarne la fruibilità, tutte le informazioni dovranno essere aggregate per paziente, per ambito (ad es. reparto) o secondo criteri mirati all'esigenza specifica.

La soluzione proposta sarà oggetto di valutazione tecnica.

Ambiente di test/corsi

È richiesta la creazione e la gestione di un ambiente di test per le verifiche di preproduzione a seguito di rilasci di nuove versioni, modifiche o variazioni di configurazioni e per corsi di formazione al personale.

I dati di tale ambiente dovranno essere anonimizzati rendendo impossibile risalire ai dati anagrafici reali a cui i dati clinici si riferiscono. Dovranno essere illustrate le modalità di anonimizzazione dei dati.