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 wiredsia 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) per l'infrastruttura rete dati/fonia e per quella dei server.
La copertura wireless è realizzata secondo lo standard IEEE 802.1a/b/g/n ed è distribuita su tutti i reparti sanitari, nei laboratori di Ricerca e nelle Direzioni. L'infrastruttura wifi è di tipo centralizzato, governata da due wireless lan controller (WLC) in HA e access point di tipo PoE. 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.
La parte wired a servizio della periferia utente è realizzata con cavi a coppie UTP di cat.6, 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 Aruba. L'unico protocollo di rete ammesso è il TCP/IP. L'architettura di rete è di tipo L3, 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.
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 le postazioni di lavoro è a 100 Mpbs o 1 Gbps in rame, mentre è a 1 Gbps o 10 Gbps in rame o in fibra verso i server e storage dei soli servizi infrastrutturali, ospitati nelle server farm locali dell'Istituto.
I server dell'Istituto sono tutti ospitati nei data centerregionali gestiti dalla società in house Lepida SpcA, ubicati a Ravenna, Ferrara e Parma; la connettività geografica verso i data center è ridondata, in fibra ottica single mode a 2Gpbs, con una latenza mediainferiorea 5 ms.
La connettività geograficadell'Istituto versoInternet avviene per mezzo delle reti e dei sistemi del Cesia-Università di Bologna/GARR; nei data center la connettività internet è fornita direttamente da Lepida.
L'Istituto ha una sede geografica, il Dipartimento Rizzoli Sicilia (DRS), ubicata presso la struttura di Villa Santa Teresa a Bagheria (PA). 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 di Villa Santa Teresa.
Sulla rete informatica sono installatialtri 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 specificato nel "Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli".

DATACENTER E INFRASTRUTTURA HARDWARE DEI SISTEMI

I sistemi dell'Ente sono ospitati in hosting nel data center regionale gestito da Lepida SpcA a Ravenna, in housing e hosting nel data center regionale gestito da Lepida ScpA a Parma, mentre le due server farm locali dell'Istituto ospitano i soli servizi infrastrutturali (dns interno e pubblico, dhcp, radius, ldap, active directory), il sistema PACS della Radiologia e l'IP PBX.
I sistemi presenti a Ravenna e a Parma sono virtualizzati su infrastruttura VMware 6.7 in HA, i server hanno in maggioranza sistema operativo Linux/Oracle linux, ma sono presenti server con sistema operativo Windows Server, disponibili aggiornati alle ultime release di sistema.
Il sistema dell'Istitutoinstallato in housing a Parmaè basato su storage a due nodi in HA gestito attraverso il software DatacoreSansymphony: su tale infrastruttura risiedono macchine di test, di preproduzione e di disaster recovery.
Il sistema di backup dell'Istituto è installato su hardware server e storage in hosting nel data center regionale gestito da Lepida ScpA a Ravenna ed è basato sul software Simpana di Commvault; un secondo sistema Simpana per la copia secondaria del backup è installato nella server farm locale dell'Istituto a Bologna. Il progetto di revisione del backup nell'ottica dell'implementazione del disaster recovery prevede una copia secondaria del backup nella sede data center di Parma.
In generale nei data center regionali gestiti da Lepida ScpA a Ravenna, Ferrara e a Parma sono disponibili soluzioni hardware per sistemi server e storage ad alto grado di performance e di affidabilità.

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. Microsoft Office 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.
Le PDL dell'Istituto navigano tramite proxy server e firewall perimetrali di tipo UTM: gli utenti aziendali si autenticano per la navigazione ad LDAP aziendale.

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 al sistema oggetto di fornitura si richiede l'integrazione con l'IdP aziendale basato sul software open source Shibboleth, integrato con LDAP aziendale. Per le procedure non in ambiente web è richiesta invece 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.

Gli applicativi in ambito aziendale richiedono spesso 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.

Le integrazioni tra procedure che prevedono flussi di dati tra sistemi dipartimentali verticali aziendali o sovraziendali sono da realizzare attraverso servizi di web service, in accordo con l'Istituto.

REQUISITI DELL'INFRASTRUTTURA

Il sistema oggetto di fornitura dovrà essere installato presso uno dei data center regionali gestiti da Lepida ScpA, presumibilmente a Ravenna o a Ferrara.

L'Istituto 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 in una logica multi istanza
- La connettività tra il data center di Lepida e le sedi dell'Ente come sopra descritto.
- Licenza del RDBMS Oracle
- Infrastruttura di VM in ambiente WMware 6.7.

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 patchentro due mesi dalla data di rilascio da parte del produttore.

Il fornitore del sistema 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'Istituto, in caso di aggiornamento della release di Oracle da parte dell'Istituto, 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:

- L'installazione e la configurazione del sistema operativo, rispettando i requisiti di sicurezza aziendali (ad esempio relativi all'antivirus, all'inserimento nel dominio aziendale, registrazione centralizzata dei log di accesso, implementazione del monitoraggio dell'hostattraverso 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, incluse eventuali componenti aggiuntive ad hoc del 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:

- L’installazione e la configurazione del sistema operativo rispettando i requisiti di sicurezza aziendali (ad esempio relativi all’antivirus, all’inserimento nel dominio aziendale, registrazione centralizzata dei log di accesso, implementazione del monitoraggio dell’host e del dbattraverso 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.
- 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).