Azienda Sanitaria Universitaria Integrata di Udine

Allegato tecnico per capitolati d'appalto riguardanti forniture e servizi concernenti l'infrastruttura informatica aziendale.

Versione: 1.0

Del: 10 ottobre 2016

Sommario

1. Definizioni

Utenza amministrativa: è un *account* con associato un ruolo di tipo amministratore o, in generale, dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore a livello qualunque livello (dispositivi, sistemi operativi, applicativi, ecc.).

Utenza di servizio: è un *account* con associato un ruolo che può anche essere dotato di privilegi amministrativi utilizzato per l'autenticazione tra sistemi informatici (es. *web service*, LDAP, *database*, ecc.).

RPO: *Recovery Point Objective*, indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto;

LAN: *Local Area Network*

LDAP: *Lightweight Directory Access Protocol*

NET-VO: LAN dell'Azienda Sanitaria Universitaria Integrata di Udine – P.O. *S. Maria della Misericordia* distribuita nei padiglioni del "vecchio ospedale";

NET-NO: LAN dell'Azienda Sanitaria Universitaria Integrata di Udine – P.O. *S. Maria della Misericordia* distribuita nei padiglioni del "nuovo ospedale"

P.O.: Presidio Ospedaliero

2. Premessa

L'*Azienda Sanitaria Universitaria Integrata di Udine* (ASUI_UD) mette a disposizione la **sua infrastruttura informatica** al fine di ospitare le componenti *hardware* e *software* di sistemi informatici necessari per l'erogazione di servizi da parte dei fornitori, con il vincolo di non diminuire o compromettere l'integrità, la sicurezza e le *performances* dei componenti costituenti il più generale Sistema Informativo Aziendale.

Il presente documento descrive sommariamente l'ecosistema ICT aziendale ed i requisiti, per l'integrazione al suo interno, di sistemi informatici contrattualmente acquisiti da terzi parti.

3. Descrizione infrastruttura aziendale

3.1. Networking

Il **protocollo di rete** utilizzato è IPv4. La **risoluzione dei nomi** è basata esclusivamente sul servizio DNS *(Domain Name Service*), integrato in *Active Directory Microsoft*, che accetta solo registrazioni sicure.

La LAN aziendale ASUI_UD è una rete che ha una configurazione specifica suddivisa in:

- NET-VO: distribuita nei padiglioni del "vecchio ospedale" del P.O. *S. Maria della Misericordia*;
- NET‑NO: distribuita nei padiglioni del nuovo ospedale del P.O. *S. Maria della Misericordia* e del "*Centro Servizi Laboratori*" (CSL)

La NET-VO è una rete *layer* 2/3 ISO/OSI a due livelli: *core* e *access*, dove per ciascun armadio dati gli apparati di periferia sono collegati agli apparati di core in *layer* 2. La rete *NET-NO* è layer 2/3 a tre livelli: *core*, *distribution* e *access*. I *Data Center* sono collegati agli apparati di *core*.

La LAN aziendale ASUI_UD è suddivisa in VLAN definite in base alla tipologia delle utenze ed ubicazione fisica (coordinate padiglione + piano).

Tutti i *server* inseriti nella rete sono configurati con IP statico. Nella NET-VO l'indirizzamento IP dei *client* è di tipo statico, mentre nella NET-NO l'indirizzamento IP dei *client* è di tipo dinamico gestito da una coppia di *server DHCP* in *failover*. All'occorrenza, per preservare l'indirizzamento di alcune postazioni, vengono adottate opportune configurazioni di *reservation* o *fixed address*.

Il Presidio Ospedaliero di Cividale è collegato in *WAN* alla rete aziendale attraverso un collegamento *xDSL*, acquisto nell'ambito del Sistema Pubblico di Connettività (SPC), con 8 Mbit/s di banda massima e 4 Mbit/s di banda garantita, con livello di servizio L5.

Rete geografica (WAN) sedi produttive Laboratorio Unico Integrato di Udine

Le sedi produttive del Laboratorio Unico Integrato di Udine fanno riferimento a diverse aziende sanitarie del Sistema Sanitario Regionale e sono collegate telematicamente attraverso una WAN *(Wide Area Network*).

Ciascuna sede è collegata, in maniera ridondata, alla propria rete aziendale e le diverse reti aziendali sono interconnesse tramite apparati di instradamento centralizzati gestiti da Insiel S.p.A., società *in house* della Regione *Friuli Venezia Giulia*.

Nella tabella seguente sono indicate le sedi con le velocità massime delle dorsali geografiche per ciascuna sede:

Sede operativa Laboratorio Unico Integrato di Udine	Azienda sanitaria	Velocità (Mbit/s)
Centro Servizi e Laboratori (ospedale Udine)	Azienda Sanitaria Universitaria Integrata di Udine	120

Sede operativa Laboratorio Unico Integrato di Udine	Azienda sanitaria	Velocità (Mbit/s)
ospedale Gemona	Azienda per l'Assistenza Sanitaria n. 3 "Alto Friuli-Collinare-Medio Friuli"	200
ospedale Tolmezzo	Azienda per l'Assistenza Sanitaria n. 3 "Alto Friuli-Collinare-Medio Friuli"	200
ospedale San Daniele	Azienda per l'Assistenza Sanitaria n. 3 "Alto Friuli-Collinare-Medio Friuli"	100
ospedale Latisana	Azienda per l'Assistenza Sanitaria n.2 "Bassa Friulana-Isontina"	60
ospedale Palmanova	Azienda per l'Assistenza Sanitaria n.2 "Bassa Friulana-Isontina"	60

3.2. Active Directory Microsoft

Il sistema è caratterizzato da un **dominio** *Active Directory Microsoft 2008 R2* denominato "*aoud.sanita.fvg.it*" che è inserito nella "foresta regionale" del Sistema Informativo Socio Sanitario del Friuli Venezia Giulia. Per l'aggiornamento dei *server* è utilizzato il servizio *WSUS - Windows Server Update Service* - cui è applicata una politica di scarico quotidiano delle *patch* rilasciate da *Microsoft*.

3.3. Infrastruttura di virtualizzazione

L'**infrastruttura di virtualizzazione** è costituita da un *cluster VmWare vSphere v5.x* formato da due nodi collocati in due distinti *Data Center* insediati all'interno del *campus* del Presidio Ospedaliero di Udine. In funzione dei servizi erogati i *server* virtualizzati possono appartenere a VLAN dedicate.

L'infrastruttura di virtualizzazione è dotata di un sistema di ***backup*** dedicato, effettuato secondo regole e politiche, personalizzabili per le singole macchine virtuali, in funzione delle peculiarità del servizio.

3.4. Postazioni di lavoro

Le **postazioni di lavoro aziendali** (*personal computer*) sono inserite nel dominio "aoud.sanita.fvg.it" e sono dotate di S.O. *Microsoft Windows XP Professional Italiano SP3* o *Microsoft Windows 7 Professional Italiano*, di browser *Microsoft Internet Explorer 8* (default *browser*) e *Google Chrome* versione *Portable*. L'*hardware* dei *client* è eterogeneo e varia, nelle prestazioni e caratteristiche di base,

da	CPU Intel Pentium 4 2,4 GHz o equivalente	a	CPU Dual Core Intel I3 3,6 GHz o equivalente
	memoria DDR-SDRAM 512 MB		memoria DDR3 4 GB (dual channel)
	hard disk da 40 GB		hard disk 500 GB

Tutte le postazioni di lavoro aziendali sono dotate di **connettività di rete** (IEEE 802.3) *Fast Ethernet* o superiore.

Per consentire la connessione utente ai fini dell'**assistenza tecnica**, su tutti i *client* aziendali è installato l'agente *CA Unicenter Remote Control v11.x*. Gli utenti aziendali accedono alle postazioni di lavoro utilizzando credenziali personali con privilegi di utente *standard*.

3.5. Antivirus

Su tutte le postazioni *client* ed i *server* aziendali è distribuito ed installato l'agente **antivirus** *Trend Micro OfficeScan 12.x*, che consente l'aggiornamento del sistema di protezione informatica con frequenza almeno quotidiana.

4. Inserimento sistemi della Ditta Aggiudicataria

Le **licenze** necessarie al funzionamento del sistema fornito, riguardanti qualunque componente (*S.O.*, *DBMS*, *Application Server*, ecc.), sono da intendersi a carico della Ditta Aggiudicataria. Le licenze *software* dovranno essere fornite in numero adeguato per consentire la piena funzionalità e utilizzabilità dei sistemi, anche in uso concorrente, da parte degli utenti.

È onere esclusivo della Ditta Aggiudicataria mantenere costantemente e tempestivamente aggiornati i sistemi, in termini di *patching* e di sicurezza. La Ditta Aggiudicataria è comunque obbligata ad installare l'**antivirus** aziendale che deve essere costantemente aggiornato secondo le politiche aziendali definite.

4.1. Server fisici (*housing*)

I ***server*** o le ***appliance* fisiche** devono essere ospitati all'interno dei *Data Center* presenti nel *campus* del Presidio Ospedaliero di Udine.

Le schede di rete devono essere *Gigabit Ethernet TX* con connessione RJ45. A ciascun dispositivo sono riservati 2 indirizzi IP, utilizzati per:

- il collegamento alla rete aziendale
- la *console di management* (tipo ILO).

La console ***di management*** deve obbligatoriamente comunicare, utilizzando il protocollo SMTP, tutta l'allarmistica riguardante l'*hardware* del sistema (*power failure, fan failure, disk failure, RAID failure,* ecc.).

I dispositivi forniti devono avere caratteristiche fisiche atte all'installazione degli stessi in armadi *rack* da 19" con profondità di 1000 mm; il numero di unità richieste deve essere minimizzato. Tutti i dispositivi forniti devono essere *rack* nativi 19" muniti di apposite slitte per l'installazione; non possono essere utilizzati *server tower* nativi trasformabili/trasformati a *rack*.

In base alla specifiche scelte progettuali e di infrastruttura, il fornitore deve dotarsi di un idoneo sistema di *backup* nativo "a *rack*", distinto dai *server* che svolgono i servizi applicativi - *Application Sever* - DBMS - *DB Server* -. Preventivamente al collaudo la Ditta Aggiudicataria deve fornire un documento in cui sono illustrate le procedure di *backup* e *disaster recovery* (laddove previsto).

L'**installazione dei dispositivi** all'interno degli armadi *rack* è di competenza della Ditta Aggiudicataria e deve avvenire con la supervisione dei tecnici dell'AOU_UD. I dispositivi devono essere forniti già preparati a livello *hardware* e *software*, pronti per l'installazione nei *rack*.

4.2. Client

Gli **applicativi *client*** oggetto di fornitura sono installate preferibilmente sulle postazioni di lavoro aziendali, seguendo le indicazioni fornite dal personale tecnico di ASUI_UD. Gli applicativi devono essere compatibili con le caratteristiche *software* e *hardware* delle postazioni stesse, e rispondere alle *policy* del dominio AD *aoud.sanita.fvg.it*. La distribuzione degli applicativi sulle postazioni di lavoro aziendali, ed i conseguenti necessari aggiornamenti, devono essere eseguiti dalla Ditta Aggiudicataria per un numero illimitato di volte, anche in caso di sostituzione delle postazioni aziendali.

Gli **applicativi *web*** forniti devono essere compatibili con il *browser IE8* e/o *Google Chrome Portable*.

Tutte le funzionalità del sistema fornito devono essere *compliance* con il client *antivirus* aziendale di cui ogni postazione aziendale è dotata, a meno di eccezioni preventivamente concordate ed autorizzate dai tecnici dell'AOU_UD. Le funzionalità del sistema fornito devono essere compatibili con l'agente *CA Unicenter Remote Control v11.x* installato su ogni postazione aziendale.

Sulle postazioni di lavoro aziendali sono periodicamente installate tutte le *patch* rilasciate da *Microsoft* ritenute necessarie per garantire la sicurezza informatica aziendale.

Sugli eventuali *client* forniti dalla Ditta Aggiudicataria non possono essere installati applicativi aziendali, fatta esclusione per l'*antivirus*.

4.3. Strumentazione

La strumentazione fornita deve essere collegata alla LAN ASUI_UD e inserite in una specifica VLAN/sottorete.

5. Caratteristiche del software

In generale, tutti i **software** forniti dovranno essere:

- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori a prescindere dal ruolo;
- localizzati in italiano e dovranno utilizzare le impostazioni internazionali di *Microsoft Windows IT standard* (non sarà consentita alcuna modifica alle impostazioni di default IT sulle postazioni), compresa la tastiera;
- 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 dei "modelli di qualità del software", secondo le norme tecniche, le linee guida e le *best practice* internazionali (es. ISO/IEC 12207, 25010, …). In ogni caso non dovranno utilizzare librerie deprecate e/o obsolete, né dovranno essere scritti e sviluppati con versioni del linguaggio di programmazione non più coperti dal supporto tecnico del fabbricante o a fine ciclo di vita (*end of life*), e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo definitivo del sistema;
- progettati e realizzati nel rispetto delle norme vigenti, nonché in modo da non mettere in alcun caso gli operatori in condizione di violare la legge durante il normale utilizzo del sistema;
- installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità, nello specifico contesto aziendaleASUI_UD, 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 gli applicativi forniti che saranno installati o eseguiti su dispositivi collegati alla LAN, dovranno essere eseguiti sempre:

- in un contesto di spazio utente del sistema operativo nel caso di client;
- come servizio nel caso di server,
- come servizio nel caso di client se non è richiesta interazione con l'operatore.

In ogni caso non dovranno essere modificati in alcun modo i permessi di default del *file system* e del registro di sistema Microsoft.

Gli applicativi forniti che saranno installati e/o eseguiti sulle postazioni di lavoroASUI_UD, non dovranno essere protetti da copia o distribuzione per mezzo di sistemi che utilizzino dispositivi *hardware* (ad esempio chiavi *USB*). Gli applicativi forniti saranno installati su sistema operativo *Microsoft Windows Server 2008* o *Microsoft Windows 7* (e seguenti) e dovranno essere compatibili con il sistema UAC (*User Access Control*).

Per quanto concerne le configurazioni:

- degli applicativi server dovranno essere memorizzate in database;
- globali degli applicativi client (ovvero non riferite alle personalizzazioni dei singoli account) dovranno risiedere in uno spazio del disco a cui possono aver accesso solo gli utenti con ruolo Amministratore oppure nel registro di sistema nella sottochiave appositamente creata in fase di installazione in *HKEY_LOCAL_MACHINE\SOFTWARE*. In ogni caso tutti i dati critici 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 con algoritmi di caratteristiche e robustezza analoghe o superiori ad *AES256*;
- personali degli applicativi client dovranno risiedere nel profilo dell'account a cui si riferiscono.

I software forniti dovranno essere dotati di:

- un sistema di autenticazione informatica degli operatori per mezzo di account e relative credenziali personali;
- un sistema di autorizzazione degli *account* personali.

6. Credenziali e trattamento dati

La Ditta Aggiudicataria dovrà individuare all'interno della sua organizzazione un ***Responsabile privacy*** che sarà nominato ***Responsabile esterno del trattamento dati*** da parte del *Titolare del trattamento dei dati personali* di ASUI_UD. Il ***Responsabile esterno del trattamento dati*** dovrà inoltrare all'Ufficio Password di ASUI_UD, secondo le procedure previste dall'Ente, le necessarie richieste di credenziali individuali per tutto il personale della ditta aggiudicataria che opererà, anche per le attività di assistenza svolte da remoto, sia in qualità di incaricato che di amministratore di sistema. A ciascun utente sarà assegnato un *account* con credenziali personali ed associato un profilo autorizzativo con abilitazioni sufficienti per lo svolgimento delle funzioni di competenza. Gli *account* e le credenziali di accesso saranno sempre individuali, ad esclusione di quelle relative all'accesso *VPN Cisco* che avranno valenza aziendale.

Il ***Responsabile esterno del trattamento*** dovrà dichiarare di aver formato gli incaricati al trattamento dei dati personali e sensibili, così come richiesto dalla normativa vigente.

La Ditta Aggiudicataria dovrà ottemperare agli obblighi derivanti dalla normativa in merito alla protezione dei dati personali, in tutti gli ambiti dove ciò sia richiesto. In particolare, deve essere garantito il rispetto delle misure di sicurezza idonee, a partire da quelle minime ai sensi dell'Allegato B al D.Lgs 196/2003 e ss.mm.ii..

7. Autenticazione e autorizzazione

Gli applicativi *software* del sistema fornito dovranno essere dotati di:

- una **componente di autenticazione informatica** degli operatori per mezzo di account e credenziali personali, che ottemperino i requisiti della normativa vigente;
- una **componente di autorizzazione** degli account personali.

Quale elemento vincolante al collaudo del sistema fornito, la Ditta Aggiudicataria dovrà:

- rendere indipendente l'AOU_UD nella gestione delle credenziali di accesso al sistema e di profilatura degli *account*;
- ovvero, svolgere in proprio l'attività di gestione delle credenziali di accesso al sistema e di profilatura degli *account*, concordando un protocollo di comunicazione per una sicura trasmissione della richiesta e fornitura delle credenziali per gli utenti.

La soluzione software fornita dovrà:

- preferenzialmente integrarsi mediante protocollo LDAP con l'*Active Directory* (AD) *Microsoft* aziendale se il numero di utenti aziendali è inferiore a 10 unità;
- obbligatoriamente integrarsi mediante protocollo LDAP con l'*Active Directory* (AD) *Microsoft* aziendale se il numero di utenti aziendali è superiore o uguale a 10 unità.

Per l'autenticazione mediante LDAP il sistema presenterà una finestra di login in cui l'utente dovrà inserire le credenziali personali assegnate (username/password). Il sistema verificherà l'esistenza dell'utente delegando all'AD la verifica di consistenza delle credenziali senza eseguire alcun tipo di *caching* della *password* digitata. Eseguita l'autenticazione, il sistema potrà acquisire dall'AD gli attributi che eventualmente caratterizzano l'utente (es. "*First Name*", "*Last Name*", "*Email Address*"). L'utente sarà assegnato ad un gruppo di default associato all'applicazione.

L'accesso all'LDAP sarà fatto esclusivamente mediante connessione sicura LDAP over TLS/SSL (LDAPS su porta 636).

Il sistema deve tracciare tutte le attività svolte dagli utenti sui dati, anche in sola visualizzazione.

8. Utenze amministrative

Le **utenze amministrative** dovranno avere le seguenti caratteristiche:

Tipologia di utenza	**Personali/impersonali**	**Modalità d'utilizzo**
utenze amministrative locali di default	anche impersonali (a titolo di esempio non esaustivo: "*admin*", "*administrator*", "*root*", ecc.);	comunicate all'AOU_UD, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza
utenze amministrative locali non di default	anche impersonali	comunicate all'AOU_UD, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza (non dovranno essere configurati account amministrativi in numero maggiore dello stretto necessario)
utenze amministrative non locali che consentano l'accesso interattivo a dispositivi/sistemi/applicativi collegati alla LAN aziendale	obbligo esclusivamente personali, devono rispettare quanto riportato nel presente documento relativamente alle modalità di autenticazione degli operatori per mezzo di account e relative credenziali personali	create e gestite da ASUI_UD
utenze di servizio	obbligo esclusivamente impersonali	comunicate all'AOU_UD, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza

Per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel presente documento, questi non dovranno in alcun caso permettere:

- di modificare le configurazioni, impostazioni e settaggi di macchine/sistemi/applicativi;
- di visualizzare, modificare o cancellare dati personali diversi da quelli eventualmente trattati contestualmente all'uso dell'account stesso.

Eventuali dati personali salvati in ulteriori archivi, diversi da quelli descritti nel presente documento, saranno ammessi solo con funzioni di "archivi provvisori", ovvero di passaggio intermedio dei dati prima dell'invio agli archivi definitivi. I dati personali devono permanere negli archivi provvisori il minor tempo possibile, ovvero per un tempo massimo che sia configurabile e che in ogni caso non superi le 24 ore naturali, con l'implementazione di opportune procedure di cancellazione automatica che non consentano il recupero locale dei dati.

In ogni caso l'accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo da parte degli account personali e degli account digitali autorizzati, sulla base di opportuni permessi settati in modo che il livello dei privilegi di accesso sia il più basso possibile e preferibilmente che l'accesso ai dati avvenga sempre per tramite dell'applicativo e non direttamente da parte dell'account.

A meno di accordi specifici concordati fra le parti, non è consentita l'archiviazione, anche temporanea ed anche in forma anonima, dei dati su macchine situate esternamente alla rete aziendale dell'AOU_UD.

La Ditta Aggiudicataria dovrà ottemperare agli adempimenti previsti dal *Provvedimento 27 novembre 2008 del Garante della Privacy* riguardante gli amministratori di sistema.

9. Assistenza

Tutti gli elementi forniti dovranno essere coperti dal supporto tecnico del fabbricante. Nessuno degli elementi forniti dovrà essere a fine ciclo di vita (end of life) e comunque non dovrà essere in tale stato ad un anno dal collaudo definitivo del sistema.

Per tutte le macchine appartenenti al dominio *aoud.sanita.fvg.it*, *CA Unicenter Remote Control v11.x* ed il programma *Microsoft Remote Desktop Client* (RDP) integrato nei sistemi operativi *Microsoft Windows* saranno gli unici strumenti consentiti per le attività di assistenza remota effettuate dal personale tecnico della Ditta Aggiudicataria e da quelli dell'AOU_UD. Per le macchine non appartenenti al dominio *aoud.sanita.fvg.it*, potranno essere utilizzati per le attività di assistenza remota effettuate dal personale tecnico della Ditta Aggiudicataria altri strumenti purché segnalati puntualmente all'AOU_UD e dalla stessa autorizzati.

Tali attività potranno essere svolte per mezzo dei sistemi VPN Cisco aziendali e con credenziali personali di dominio rilasciate *ad hoc*, a seguito di presentazione di opportuna richiesta rivolta all'AOU_UD.

10. Manutenzione

Sono oggetto di fornitura i servizi di manutenzione ordinaria preventiva e correttiva su tutte le forniture di ambito IT, che prevedono:

- esecuzione, con cadenza almeno semestrale, di tutte le operazioni necessarie a prevenire eventuali anomalie sull'hardware e sul software (comprese tutte le cosiddette "*minor release*", che devono in ogni caso essere installate subito dopo il loro rilascio); in occasione di tali attività, la Ditta Aggiudicataria dovrà eseguire un *backup* delle macchine oggetto di intervento, in modo da garantirne il ripristino in caso di problemi al riavvio;
- numero illimitato di interventi di manutenzione ordinaria correttiva su tutto quanto oggetto di fornitura (hardware e software). La riparazione delle componenti hardware guaste dovrà essere effettuata con parti originali, intendendo per originali parti garantite come nuove e almeno dello stesso livello di revisione della parte da sostituire.

11. Collaudo

Il collaudo dell'intero sistema sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un *responsability agreement*. Tale documento farà esplicito riferimento all'installazione ASUI_UD, nei modi e nei termini definiti dal presente capitolato e che verranno a presentarsi all'atto pratico dell'installazione e della manutenzione del sistema nel tempo. Il *responsability agreement* conterrà espliciti riferimenti al fatto che i requisiti funzionali e prestazionali non verranno inficiati nella particolare installazione AOU_UD, così come sopra descritta.

12. Documentazione

La Ditta Aggiudicataria dovrà presentare con i tempi indicati la seguente documentazione:

- Entro 30 giorni dall'aggiudicazione:
  - DOC-PROG ossia progetto tecnico di dettaglio contenente almeno le seguenti sezioni:
    - scheda tecnica dei server (caratteristiche hardware e software)
    - scheda tecnica delle eventuali stazioni di lavoro client
    - descrizione della continuità operativa (*backup* e *disaster recovery*)
    - schema grafico con indicati collegamenti di rete (IP e numero di presa di rete associato) di tutte le componenti del sistema informatico (server, analizzatori, client, ecc.)
    - schema architetturale della soluzione da realizzare (application server, DBMS, ecc.)
- al momento del collaudo:
  - DOC-COLL, ossia lo stato dell'arte al momento del collaudo contenente almeno le sezioni indicate per il DOC-PROG;
- post collaudo, prima di ogni intervento sul sistema per aggiornamento e/o estensione che ne modifichi, anche in parte, la configurazione così come indicata nel DOC-COLL:
  - DOC-PROG_CH, ossia il progetto tecnico di dettaglio contenente almeno le sezioni del documento
- post collaudo, dopo ogni intervento sul sistema per aggiornamento e/o estensione che produca un documento DOC-PROG_CH:
  - DOC-PROG_CH_SA: stato dell'arte al momento del collaudo post modifica.

13. Cessazione del contratto

Gli eventuali **dati archiviati presso la Ditta Aggiudicataria** dovranno essere restituiti o distrutti definitivamente alla scadenza del contratto in essere secondo quanto previsto dalle peculiarità del contratto di servizio sottoscritto.

La Ditta Aggiudicataria al momento della scadenza del contratto è obbligata a fornire un'esportazione in un formato aperto e documentato di tutti i dati presenti nel sistema.