ALLEGATO A: SPECIFICHE ICT

1. SPECIFICHE TECNICHE DI SICUREZZA INFORMATICA 2
   1.1 Scopo dell'Allegato 2
   1.2 Caratteristiche generali dei sistemi/software 2
   1.3 Configurazioni specifiche dei sistemi/software 3
   1.4 Caratteristiche degli account amministrativi 4
2. SPECIFICHE GENERALI DI IMPLEMENTAZIONE NEL CONTESTO AZIENDALE 5
3. SCENARIO DI INTEGRAZIONE CON L'INFRASTRUTTURA AZIENDALE 6
   3.1 Data Center 6
   3.2 Sistema di Autenticazione 6
   3.3 Gestione dei profili 7
   3.4 Application Server 7
   3.5 Database Server 8
   3.6 Postazioni di Lavoro 8
   3.7 Sistema di Backup, Disaster recovery e Business Continuity 9
4. AMBIENTE DI TEST 9

1. SPECIFICHE TECNICHE DI SICUREZZA INFORMATICA

1.1 Scopo dell'Allegato

L'Azienda Ospedaliero- Universitaria S. Orsola-Malpighi di Bologna (d'ora in poi AOUBO per brevità) pone particolare attenzione agli aspetti della sicurezza informatica, che ritiene debba essere considerata come un fattore intrinseco dell'architettura dei sistemi oggetto della presente fornitura e delle caratteristiche tecniche degli elementi che li compongono, al fine di garantire la disponibilità, l'integrità e la riservatezza dei dati e delle informazioni proprie di un sistema informativo in un ambito complesso come quello ospedaliero.

Strategica in questo senso è la sicurezza applicativa, per la quale si chiede col presente allegato di considerarla come facente parte di un processo orientato ad adottare contromisure di sicurezza a diversi livelli (fisico, logico, organizzativo), all'interno di un contesto così critico come quello ospedaliero-sanitario in cui i sistemi applicativi operano e sono utilizzati.

L'aggiudicatario dovrà perciò garantire che l'architettura e gli elementi costituenti il sistema siano progettati, implementati e manutenuti nel tempo in modo da **minimizzare quanto più possibile il rischio informatico residuo**, per difendere ogni componente del sistema da possibili minacce accidentali o intenzionali, e comunque in osservanza alle normative e best practices citate nei successivi paragrafi del presente documento.

In generale, tutti gli elementi forniti 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 ad un anno dal collaudo definitivo dei sistemi.

1.2 Caratteristiche generali dei sistemi/software

In generale, tutti i sistemi/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);
- dotati di **impostazioni internazionali** di Microsoft Windows IT standard (se presente), 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 practices 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 ad un anno dal collaudo definitivo dei sistemi;
- pensati, progettati e realizzati nel **rispetto del quadro legislativo vigente**, 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, 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.

1.3 Configurazioni specifiche dei sistemi/software

Per quanto concerne le modalità di configurazione degli applicativi, sia per la parte server e sia per la parte client, esse dovranno tener conto che:

- per la parte **server**, le configurazioni dovranno essere ricomprese nel database dell'applicativo oppure nelle chiavi di registro del sistema, 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 file e cartelle di installazione dell'applicativo (a cui quindi avranno accesso solo gli utenti con ruolo Amministratore) oppure nel registro di sistema (ove presente) nella sottochiave appositamente creata in fase di installazione, ed in ogni caso informazioni critiche in termini di sicurezza e funzionalità dovranno essere cifrate (a titolo di esempio e non esaustivo: le stringhe di connessione ai database, le credenziali necessarie per instaurare eventuali altre connessioni client/server, ecc.);
- quelle **personali** degli **applicativi client,** ovvero riferite alle personalizzazioni dei singoli account, dovranno risiedere nel profilo dell'account a cui si riferiscono (ove presente).

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 forniti:

- non devono prevedere nessun utente impersonale né per gli operatori né di servizio a meno di casi concordarti con l'AOUBO
- devono consentire azioni di software inventory: con ciò si intende che tutti i file eseguibili devono contenere all'interno il certificato che ne garantisce l'autenticità, oltre ai metadati (di minima: *vendor* e *application name*) che ne consentano facilmente l'identificazione;
- devono poter essere distribuiti in "package" fruibili dai sistemi di distribuzione aziendali;
- devono utilizzare solo sistemi di comunicazione sicuri (crittografati, ad esempio utilizzare il protocollo HTTPS per il collegamento vero l'Application Server o verso web services o siti esterni);
- 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 Ospedaliera o dalle aziende ad esse deputate;

L'ottemperanza a tutti questi requisiti deve essere perseguita in stretta collaborazione con il servizio ICT.

L'aggiudicatario sarà nominato "Responsabile del trattamento dei dati personali" ai sensi dell'art. 4, par. 1, n. 8 GDPR (Regolamento UE 2016/679). Questi verrà in tal senso nominato dal titolare del trattamento dei dati personali AOUBO e dovrà inviare, nel rispetto delle procedure dell'azienda, 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 solo a livello

nominale, secondo le proprie procedure ed in ogni caso con i privilegi minimi necessari e sufficienti allo svolgimento delle mansioni di competenza.

1.4 Caratteristiche degli account amministrativi

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:

- dovranno sempre avere il minimo livello di privilegi di accesso sufficiente però per svolgere i compiti per i quali è stato creato;
- 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'AOUBO, 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;
- dovranno, nel caso di account amministrativi non locali che consentano l'accesso interattivo a macchine/sistemi/applicativi collegati alla LAN aziendale, essere sempre personali;
- 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, 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 e che consentano di effettuare operazioni non autorizzate al di fuori dell'ambito definito;

In ogni caso l'accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo con account nominativi in possesso di opportuni permessi autorizzativi.

L'ottemperanza a tutti questi requisiti deve essere perseguita in stretta collaborazione con il servizio ICT.

2. SPECIFICHE GENERALI DI IMPLEMENTAZIONE NEL CONTESTO AZIENDALE

Il sistema/software offerto dalla Ditta assegnataria dovrà essere implementato all'interno del contesto infrastrutturale IT della struttura ospedaliera nel rispetto delle "best practices", delle norme tecniche e della legislazione vigente, in particolar modo in materia di sicurezza e privacy, dei regolamenti e in coerenza con le politiche di sicurezza e di privacy adottate dall'AOUBO nello specifico contesto di installazione.

Tutti i sistemi/applicativi forniti dovranno permettere ad AOUBO di rispondere, per lo specifico dei sistemi offerti, a tutte le prescrizioni del complesso quadro normativo vigente, in primis:

- al Regolamento Europeo sulla Protezione dei Dati 2016/679 (GDPR) e D.Lgs. 101/2018 e seguenti (https://www.eugdpr.org/) e al D. Lgs. 196/2003, cosiddetto Codice Privacy;
- alla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni";

Inoltre l'aggiudicatario dovrà collaborare attivamente, per gli aspetti attinenti all'oggetto della fornitura e di competenza, alla produzione di documentazione che l'AOUBO è chiamata a redigere in ottemperanza ai due punti precedenti, e in generale al quadro normativo di riferimento nel contesto della PA e sanitario. A titolo di esempio, l'aggiudicatario dovrà collaborare fattivamente nel processo di monitoraggio del proprio sistema/software e susseguente comunicazione in caso di violazione dei dati (DATA BREACH) per il seguito di competenza del titolare e del DPO.

Per i Medical Device, qualora i sistemi forniti necessitino di un collegamento alla rete aziendale, come previsto dalla norma IEC 80001-1, prima dell'installazione dell'intero sistema e successivo collaudo, il fornitore si impegna a sottoscrivere un accordo di responsabilità (responsibility agreement). Tale documento farà esplicito riferimento alle condizioni di installazione, integrazione nel contesto aziendale, e di manutenzione del sistema nel tempo. Il responsibility agreement, redatto dall'aggiudicatario e revisionato/validato da AOUBO, conterrà espliciti riferimenti alla "marcatura CE" (secondo la 93/42/CE e s.m.i., in particolare la 47/2007/CEE) dei sistemi offerti ed al fatto che i requisiti essenziali di sicurezza non verranno inficiati nella particolare installazione aziendale e nel tempo, così come intesa sopra.

Qualora i sistemi forniti non s'intendano collegati in alcuna maniera alla rete dati, essi devono comunque rispondere ai requisiti dettati dalla normativa citata.

Nel caso in cui la fornitura riguardi un Medical Device, L'AOUBO potrà richiedere all'aggiudicatario di compilare specifica modulistica e sottoscrivere il modulo di Manufacturer Disclosure Statement for Medical Device Security (MDS2), in maniera da permettere la valutazione di tutti gli aspetti critici e non della messa in uso dei sistemi offerti, anche secondo EC/TR 80001-2-2. In caso, sarà onere del fornitore ottenere la versione più recente dal sito NEMA.

In generale l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e del trattamento dei dati affidato nell'ambito di quanto richiesto dalla presente procedura d'acquisto, in particolare in merito all'integrità, disponibilità e riservatezza dei dati e dei sistemi.

3. SCENARIO DI INTEGRAZIONE CON L'INFRASTRUTTURA AZIENDALE

La proposta tecnica del fornitore dovrà descrivere l'architettura e le relative funzionalità dell'impianto in rapporto alla dislocazione logistica e ai requisiti di connettività.

3.1 Data Center

In linea con quanto previsto dall'AgID in termini di centralizzazione e razionalizzazione dei servizi, il sistema/software offerto dovrà essere implementato presso il Data Center di Lepida S.p.A presente a Ravenna e fruibile da qualunque postazione client AOUBO, fatto salvo che non vi siano vincoli tecnologici che ne giustifichino l'implementazione in loco, come ad esempio la necessità di un collegamento diretto di un dispositivo medicale col server/PC fornito dalla ditta assegnataria.

In linea generale, l'AOUBO mette a disposizione senza oneri aggiuntivi per l'aggiudicatario:

- le infrastrutture server e storage presenti nel Data Center di Lepida a Ravenna, per ospitare il sistema offerto secondo l'architettura proposta. L'offerta tecnica del fornitore dovrà perciò indicare il dimensionamento complessivo delle macchine (CPU, RAM, disco) e il dimensionamento dello storage per soddisfare le esigenze del sistema progettato;
- la connettività tra il Data Center di Lepida e le sedi delle aziende interessate dal presente capitolato, che è garantita attraverso la rete regionale Lepida mediante un collegamento ridondato in fibra ottica con banda a 1 Gbps;
- licenze del RDBMS Oracle ultima versione disponibile, su piattaforma Exadata
- Infrastruttura WMware 6.x

Si precisa che tutte le ulteriori 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'architettura 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 delle aziende, sulla base di opportuna documentazione ricevuta dal fornitore del sistema.

Per le attività di manutenzione e assistenza da remoto la modalità consentita per l'accesso ai server e ai dispositivi in rete è l'utilizzo del sistema OpenVPN aziendale: per ogni tecnico della ditta verranno generate appositi certificati e credenziali personali.

3.2 Sistema di Autenticazione

Il sistema/software offerto dovrà integrarsi con i meccanismi di autenticazione dell'AOUBO, con l'obiettivo di utilizzare le credenziali di autenticazione già assegnate agli operatori nelle aziende, in quanto esse forniscono alcune importanti garanzie di rispetto della normativa privacy (es. tipologia password, cambio password, disattivazione alla chiusura del rapporto di lavoro) e facilitano l'accesso degli utenti agli applicativi cui sono autorizzati.

L’autenticazione degli utenti all’interno dei SW integrati nel contesto aziendale viene gestista utilizzando differenti modalità e protocolli, in particolare:

- In ambiente clinico-sanitario: si richiede l’integrazione con il sistema aziendale openLdap utilizzato per l’accesso alle procedure sanitarie. Le utenze in uso hanno una naming standard del tipo “SOnnnnn” o “SPnnnnn”.
- In ambiente web based: Per le procedure in ambiente web, è stato implementato il Single Sign On mediante il prodotto open source Shibboleth, integrato all’openLdap aziendale.
- In ambiente client-server: Per le procedure non web è necessario che l'autenticazione venga gestita collegandosi direttamente via l'LDAP. In questo ambito, nel caso in cui fosse necessario richiamare un’altra procedura integrata, il passaggio delle credenziali utente deve avvenire in modalità sicura e mediante passaggio di token secondo specifiche da concordare tra le ditte e validate dai sistemisti AOUBO.

Non è possibile effettuare l’autenticazione degli utenti mediante logon Windows.

3.3 Gestione dei profili

La gestione dei profili di abilitazione degli utenti deve essere realizzata all’interno del sistema/software offerto. Inoltre, dovrà essere garantita, anche in fasi successive rispetto all’avvio del contratto, l’integrazione con i sistemi aziendali di gestione delle abilitazioni tramite web service su protocollo SOAP o API REST su HTTPS.

Le offerte dovranno esplicitare in maniera chiara le modalità di integrazione con i sistemi di autenticazione AOUBO e in ogni caso la ditta aggiudicataria deve rendersi da subito disponibile a definire la configurazione ottimale con i tecnici del servizio ICT.

3.4 Application Server

Per quanto riguarda la componente server degli applicativi, rientra nelle competenze dei tecnici dell’AOUBO:

- l’installazione e la configurazione del sistema operativo secondo le richieste del fornitore, rispettando i requisiti di sicurezza aziendali (ad esempio relativi all’antivirus, all’inserimento nel dominio aziendale e/o integrazione Ldap, la registrazione centralizzata dei log di accesso, l’implementazione del monitoraggio, 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;
- il supporto alla configurazione e al setup dei servizi di autenticazione e di bilanciamento.

Rimane invece di competenza dei tecnici del fornitore tutto quanto non compreso nel precedente elenco, tra cui:

- l’installazione, configurazione e messa in produzione degli application server;
- fornire assistenza e manutenzione secondo le modalità concordate e 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);

Si precisa inoltre che l'applicativo deve essere presentato ai client attraverso un unico punto di accesso: unico URL web su porta standard https, nascondendo quindi le eventuali complessità o molteplicità dei server e servizi presentati dietro al bilanciatore/reverse proxy.

L'applicativo deve evitare che venga persa la sessione dei client collegati ad un particolare application server qualora tale server dovesse presentare dei problemi o essere soggetto a manutenzione: si chiedono quindi dei meccanismi per disaccoppiare il client dal singolo application server, quali transazioni stateless o sessione condivisa tra gli application server.

3.5 Database Server

È competenza dei sistemisti dell'AOUBO:

- la fornitura dell'ambiente data base secondo le specifiche di configurazione che devono essere fornite dalla Ditta assegnataria, rispettando i requisiti di sicurezza (ad esempio relativi alla registrazione centralizzata dei log di accesso, l'implementazione del monitoraggio, etc;)
- l'assegnazione di credenziali amministrative nominative ai tecnici del fornitore incaricati delle operazioni di installazione/aggiornamento dei vari software;
- gli interventi di manutenzione ed aggiornamento della piattaforma di virtualizzazione VMware, sistema Exadata Oracle e istanza MS SQL Server;
- le attività di backup secondo quanto riportato al paragarafo Sistema di Backup, Disaster recovery e Business Continuity

È competenza dei tecnici del fornitore tutto quanto non compreso nel precedente elenco tra cui:

- l'installazione, configurazione e messa in produzione del DB
- la risoluzione di qualsiasi problematica relativa al contenuto e al funzionamento del DB (ad esempio i lock, i rallentamenti e i malfunzionamenti bloccanti di servizi o di componenti del sistema, le scheduled procedure, le tablespace, le integrazioni con altre procedure, etc)

3.6 Postazioni di Lavoro

La postazione di lavoro aziendale (PdL) ha una configurazione standard ed è installata da immagine. Di seguito le carattristiche salienti:

- sistema operativo Windows 7 Professional 64bit o Windows 10 Pro 64 bit, CPU i3-i5, RAM 4 GB, HDD 500GB SATA o SSD 250GB;
- i PC sono normalmente parte di un dominio Active Directory; gli utenti che vi accedono sono nello stesso dominio o in un dominio universitario in trust;
- gli utenti non hanno diritti amministrativi o di power user sui PC in uso;
- gli applicativi normalmente installati sulle PDL sono: LibreOffice v. 5 o superiore, Antivirus Kaspersky, Adobe Acrobat Reader, Endpoint Security (con funzioni di antivirus, antispyware, webcontrol, mail control, firewall, application control), UltraVNC, 7Zip, Java versione 1.6 o superiore, browser Firefox/IE 11. MSOffice è installato esclusivamente in postazioni dedicate ad attività specifiche;

Sui PC nel dominio vengono distribuite e installate mensilmente le patch critiche e di sicurezza.

La manutenzione remota delle postazioni viene effettuata mediante sistema centralizzato Guacamole integrato con UltraVNC.

Il parco delle PdL 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 nazionali o regionali;

Il parco stampanti è costituito prevalentemente da stampanti laser e sono acquistate tramite le convenzioni delle sopracitate centrali di acquisto.

3.7 Sistema di Backup, Disaster recovery e Business Continuity

La Ditta aggiudicataria deve prevedere per il proprio sistema/software soluzioni tecnico-organizzative a diversi livelli funzionali al suo ripristino secondo tempi e modalità coerenti con il livello di criticità dello stesso.

Il fornitore deve rendersi disponibile a collaborare con l'Azienda committente alla redazione e validazione delle policy di back up, di continuità di servizio e dei flussi di assistenza riferiti ai sistemi/software oggetto di appalto, fornendo tutti i riferimenti e le informazioni necessarie, nonché alla definizione delle procedure e modalità alternative di lavoro in caso di fault del sistema o di una sua componente.

4. AMBIENTE DI TEST

Per tutte le Ditte fornitrici di sistemi e applicativi è fatto esplicito ed assoluto divieto di trasferire nella propria o proprie sedi dati personali o copie di essi in qualunque formato.

Per questo l'AOUBO consapevole delle necessità da parte dei diversi fornitori di poter eseguire test in loco dei propri prodotti, si rende disponibile a fornire un ambiente di test opportunamente dimensionato al fine di consentire alla Ditta assegnataria di eseguire i test di pre-produzione del proprio sistema/software relativi a nuove release, verifiche di funzionamento post-modifiche o variazioni delle configurazioni, applicazioni di patch/fix applicative o dei Sistemi Operativi.

Per questo il fornitore dovrà prodursi per mantenere allineate quanto più possibile le configurazioni e le condizioni dell'ambiente di test rispetto quello di produzione.

La ditta assegnataria dovrà inoltre prevedere una o più sessioni di formazione per l'utilizzo del sistema/software commisurato alla complessità dello stesso.