ALLEGATO AI CAPITOLATI PER LA GESTIONE DELLE COMPONENTI INFORMATICHE HW E SW DI FORNITURE DI APPARECCHIATURE MEDICALI E/O DI LABORATORIO

Da inserire nel capitolato, per gare riguardanti apparecchiature elettromedicali, di laboratorio o di altro ambito che includono dotazioni informatiche, quali PC o componenti software.

CARATTERISTICHE MINIME DEI PC

Le caratteristiche minime dei PC richieste sono le seguenti:

- PROCESSORE: Processore Intel® Core™ i5 di decima generazione
- SISTEMA OPERATIVO: Windows 10 Pro 64 bit versione 22H2 o successive
- MEMORIA: 8 GB
- UNITÀ DISCO FISSO: SSD 256 GB o superiori
- GARANZIA: 1 anno servizio On-site
- SCHEDA GRAFICA: risoluzione minima 1366 x 768 pixel
- SCHEDA DI RETE: 100/1000

SERVER (da verificare per singola gara con ICT)

Al fine di garantire lo stesso livello di servizio e continuità operativa già in essere per la maggior parte delle applicazioni aziendali, l'architettura software necessaria al corretto funzionamento del sistema fornito dovrà essere installata sull'infrastruttura tecnologica dell'ASST PGXXIII che consta di un ambiente di server virtuali e di un sistema di gestione dei dati pienamente ridondato in ogni sua componente e distribuito su due Data Center distinti, sincronizzati in tempo reale. A tal fine viene richiesto all'aggiudicatario di fornire un server fisico Dell corredati da licenza software di virtualizzazione (VmWare) e licenza per backup, ripristino e gestione dati (Veeam). Qual ora sia necessario utilizzare un sistema di database (es. oracle o microsoft sql) sarà cura dell'aggiudicatario fornire le idonee licenze dei prodotti che verranno introdotti nelle infrastrutture del Papa Giovanni XXIII. Le caratteristiche tecniche dei server e delle licenze verranno definiti a seguito dell'aggiudicazione della procedura di gara in modo da garantirne la conformità con gli standard aziendali vigenti al momento. La predisposizione degli ambienti software di base è interamente a carico dell'ASST mentre i servizi di installazione dei software applicativi necessari per lo svolgimento dei servizi previsti è interamente a carico dell'affidatario.

LE POLICY DI SICUREZZA

Per quanto riguarda le disposizioni di sicurezza informatica_se la fornitura prevede componenti software installati su computer o su calcolatori integrati nelle apparecchiature, si richiede che la configurazione, a carico del fornitore, di queste macchine sia eseguita in ottemperanza con le regole di sicurezza definite dalla SC Sistemi Informativi - ICT.

Inoltre, dovranno essere rispettate le seguenti informazioni generali:

- La configurazione di rete (TCP/IP) dovrà essere coerente e integrata con la rete informatica dell'Azienda Ospedaliera. Analogamente le impostazioni di sicurezza dovranno essere integrate nell'architettura di dominio Windows dell'Azienda Ospedaliera;
- Il sistema operativo, Windows 10 Professional a 64 bit, dovrà essere configurato in modo da permettere l'installazione di patch di sicurezza e critiche anche attraverso il sistema di distribuzione centralizzato dell'Azienda Ospedaliera, secondo le politiche e i tempi di aggiornamento definite da ASST-PG23;
- Su ciascun computer e su ciascuna apparecchiatura fornita, in particolare se presente sistema operativo Microsoft Windows, dovrà essere attivo e idoneo il software antivirus del medesimo produttore di quello utilizzato in ASST-PG23, costantemente aggiornato secondo gli obblighi legislativi e le politiche di sicurezza dell'Azienda Ospedaliera.

La ASST-PG23 considera la sicurezza dei sistemi (HW e SW) condizione irrinunciabile per erogare servizi ICT affidabili e di qualità elevata, come peraltro previsto da normative e direttive di riferimento.

Al fornitore del singolo sistema è richiesto di mantenere aggiornati, senza oneri aggiuntivi a carico di ASST-PG23, tutti i sistemi SW che concorrono al funzionamento della soluzione offerta – in sede contrattuale – nell'ambito del sistema informativo aziendale, anche quando l'ICT dovrà aggiornare i sistemi di base causa la fine del supporto sui prodotti.

Con 'sistemi di base' si intende ogni software residente sui PC e su server che ospitano la fornitura: in particolare il sistema operativo, lo 'application server', il 'web server', il 'database server', eventuali middleware e/o altre componenti necessarie al corretto funzionamento delle applicazioni fornite.

I sistemi SW di base potranno essere aggiornati, secondo il seguente criterio:

- Ad intervalli regolari ed in generale ad ogni segnalazione di criticità da parte degli Enti esterni preposti:
  - Comunque, separati da non più di tre mesi per la componente server;
  - Mensilmente per la componente PC installata dal fornitore con la soluzione SW.
- Con applicazione di tutti gli aggiornamenti disponibili relativi all'incremento della sicurezza del sistema o al bug fixing, con applicazioni delle patch di sicurezza e critiche quando disponibili;
- Non oltre la "fine del supporto" di prodotto da parte del produttore.

Quando si rende necessaria la migrazione ad un sistema SW di base più recente l'attività, sempre senza oneri aggiuntivi a carico dell'Ente, viene definita in tempi e modalità (test e collaudo della soluzione sw del fornitore) con la SC Sistemi informativi - ICT.

Relativamente all'aggiornamento e sicurezza delle postazioni di lavoro:

- L'attività di installazione delle 'patch' sarà effettuata autonomamente da ASST-PG23, tramite apposito sistema di distribuzione ed applicazione degli aggiornamenti;
- Su ogni postazione PC inserita nella rete aziendale, necessaria all'erogazione del servizio, la ASST-PG23 procederà con l'installazione del software di 'end-point security' (con piene funzionalità operative): su queste postazioni è necessario vengano comunicate le eccezioni per le esclusioni da configurare.

Eventuali deroghe dalle prescrizioni qui sopra indicate andranno richieste alla SC Sistemi informativi - ICT.

NB L'aggiudicatario dovrà concordare con la SC Sistemi informativi – ICT tutte le attività di consegna, allestimento e installazione delle componenti informatiche HW e SW, comunicando all'indirizzo ict.segreteria@asst-pg23.it l'oggetto della fornitura.

POLICY PER LA GESTIONE DELLE UTENZE APPLICATIVE PRESSO L'ASST PAPA GIOVANNI XXIII

L'ASST Papa Giovanni XXIII è dotata di un sistema di IAM (Identity and Access Management) per la gestione delle utenze applicative (applicazioni e servizi).

Per quanto riguarda la componente di Identity Management (gestione centralizzata ed automatizzata del provisioning delle utenze applicative - ossia il ciclo di vita: creazione, modifica, dismissione -) si procede ad integrare* la nuova applicazione solo se il numero di utenze applicative è significativamente elevato (SW in uso in tutto o in gran parte dell'ospedale). Diversamente, se non in presenza di specifiche esigenze di gestione, non si procede all'integrazione, e questo implica che le utenze applicative dovranno essere gestite a mano dal fornitore.

Di seguito le indicazioni da rispettare per quanto riguarda la gestione manuale delle applicazioni:

1. ogni operatore dovrà usare la propria utenza applicativa (non sono consentite utenze generiche);
2. l'integrazione LDAP con il dominio Windows di ASST Papa Giovanni XXIII non è possibile in quanto gli operatori utilizzano una smart card con certificato crittografico RSA per l'accesso sui PC, e quindi non conoscono la propria password. Se si riesce ad ottenere l'integrazione LDAP leggendo il certificato della smart card inserita nel lettore (e di conseguenza non dovendo prevedere l'inserimento della password da parte dell'operatore) allora si può percorrere questa strada, diversamente le utenze vanno create a mano una ad una sul server dell'applicazione, o qualora l'applicazione non preveda un server centralizzato su ogni singolo PC sul quale l'applicazione è installata. Devono essere definite credenziali personali per ciascun operatore;
3. lo USERID per ogni singolo operatore deve corrispondere alla matricola aziendale (codice numerico presente sul badge personale di ogni operatore, comprensivo di eventuali zeri iniziali);
4. le utenze applicative vanno gestite nel tempo (provisioning), ovvero saranno create le utenze nuove, modificate al bisogno le utenze esistenti e rimosse quelle non più necessarie;
5. deve essere garantito il principio del minimo privilegio: ogni utenza applicativa deve possedere il minor numero di privilegi tali da permettere all'operatore di effettuare solo le attività a lui/lei necessarie. Eventuali privilegi aggiunti e non necessari dovranno essere rimossi (modifica utenza applicativa).

La componente di 'Access Management' (Single Sign On tramite smart card) può essere gestita con o senza la parte di 'Identity'; se si utilizza quest'ultima funzionalità la gestione delle utenze sarà completamente automatizzata - compreso la creazione e la futura gestione delle credenziali di accesso -, diversamente le utenze dovranno essere gestite a mano, da parte degli uffici preposti o da un amministratore locale dell'applicazione che effettuerà la definizione delle credenziali, ed eventuali disallineamenti dovranno essere gestiti manualmente.

Anche in quest'ultimo caso si procede ad integrare** la nuova applicazione solo se il numero di utenze è significativamente elevato, ovvero se vi sono richieste specifiche in tal senso (es. per avere un maggior controllo degli accessi). Diversamente l'accesso all'applicazione avverrà digitando manualmente USERID e password (quest'ultima non può essere uguale a quella dell'utente di dominio Windows, come spiegato precedentemente).

* l'integrazione prevede tipicamente lo sviluppo di interfacce REST API tra l'applicazione e il sistema di Identity Management per la gestione dei casi d'uso (creazione nuova utenza applicativa, modifica utenza applicativa, dismissione logica utenza applicativa, gestione password).
Il costo dell'integrazione è a carico del fornitore dell'applicazione.

** l'integrazione prevede lo sviluppo di uno 'script' specifico per l'applicazione in modo che il client SSO installato su tutti i PC aziendali possa intercettare l'interfaccia applicativa di login ove inserire le credenziali utente e, laddove previsto, gestire il cambio password.
Il costo dell'integrazione è a carico del fornitore dell'applicazione.