



Regione del Veneto

AZIENDA OSPEDALE–UNIVERSITÀ PADOVA

Via Giustiniani, 1 – 35128 PADOVA – Tel. + 39 049 821111

Cod.Fisc./P.IVA 00349040287 – www.aopd.veneto.it– P.E.C.: protocollo.aopd@pecveneto.it

REQUISITI INFRASTRUTTURALI MINIMI PER L'EROGAZIONE DI SERVIZI A FAVORE DELL'AZIENDA OSPEDALE UNIVERSITÀ PADOVA

Di seguito vengono elencati i requisiti di conformità richiesti ad ogni progetto per poter essere qualificato come installabile on-premise presso le strutture datacenter dell'Azienda Ospedale Università di Padova o su ambiente cloud qualificato, o più in generale per acquisizioni di soluzioni che devono essere integrate nella rete informatica dell'AOUP :

- a. Ogni soluzione proposta deve poter essere fruibile dall'utenza finale esclusivamente da browser di tipo standard, senza la necessità di installare software aggiuntivo sulle postazioni client.
- b. La fruizione della soluzione non deve imporre vincoli relativamente alla tipologia di postazione client di accesso. In particolare, non sono considerate accettabili restrizioni a specifiche versioni di sistema operativo o a livelli massimi di patching.
- c. la soluzione qualificabile deve essere complessivamente strutturata come multilivello con l'implementazione di una separazione logica e funzionale dei seguenti elementi:
 - c.1.Front-end di accesso
 - c.2.Back-end applicativo
 - c.3.Back-end di integrazione (se previsto dal progetto complessivo)
 - c.4.Dati strutturati (database relazionali)
 - c.5.Dati non strutturati (file system o database non relazionali)
- d. La soluzione proposta non deve porre vincoli di nessun genere relativamente alla distribuzione topologica degli elementi costitutivi sopra elencati la quale potrà essere ingegnerizzata secondo le specifiche esigenze infrastrutturali dell'Azienda.
- e. Nel caso in cui la soluzione proposta includa la fornitura di dispositivi client portatili che utilizzano connettività WIFI, tali client dovranno soddisfare almeno i seguenti requisiti:
 - e.1.supportare obbligatoriamente connettività radio a 5Ghz e (a titolo preferenziale) a 6Ghz;

- e.2.supportare tutti i canali disponibili sulle frequenze 5Ghz (U-NII-1, U-NII-2A, U-NII-2B, U-NII-2C, U-NII-3);
 - e.3.supportare canali con ampiezza a 40Mhz;
 - e.4.supportare l'utilizzo di canali DFS;
 - e.5.supportare diverse modalità di autenticazione quali WPA2, WPA3 e WPA2-Enterprise con autenticazione 802.1X.
- f. Le piattaforme computazionali messe a disposizione delle infrastrutture aziendali sono esclusivamente di tipo virtuale in un ambiente a risorse condivise senza possibilità di allocazioni statiche o riservate/prioritarie. Gli elementi consistenti relativi alla componente computazionale (c.1, c.2, c.3) devono essere completamente compatibili con tale modalità di deployment, escludendo pertanto qualsiasi qualificazione specifica relativa a particolari componenti hardware o vincoli relativi a requisiti di priorità o esclusività nell'accesso alle risorse computazionali.
- g. Gli elementi infrastrutturali relativi alle componenti di data management (c.4, c.5) si basano su sistemi centralizzati a risorse condivise non riservabili. La soluzione non può richiedere livelli di priorità o accesso esclusivo a specifiche risorse.
- h. In conformità alle normative relative al mantenimento di un adeguato livello di sicurezza delle piattaforme IT, l'Azienda implementa esclusivamente le versioni di sistemi operativi sotto pieno supporto da parte dei vendor relativi e ad un livello di aggiornamento prossimo allo stato dell'arte (ultimo patch level stabile disponibile). Le piattaforme vengono periodicamente e costantemente aggiornate senza previa notifica. Qualsiasi soluzione proposta deve essere compatibile con le politiche descritte.
- i. L'Azienda limita in modo vincolante le piattaforme computazionali messe a disposizione dalla propria infrastruttura. Sono pertanto disponibili esclusivamente sistemi basati su:
- i.1.Microsoft Windows
 - i.2.Red Hat Enterprise Linux
 - i.3.CentOS (limitatamente ad ambienti di test o deployment di tipo IAAS)
- Tali sistemi operativi vanno intesi come disponibili nella più aggiornata Major Release disponibile al momento della proposizione della soluzione.
- j. L'Azienda, nell'ambito dei servizi di data management mette a disposizione esclusivamente le seguenti soluzioni PAAS:
- j.1.Oracle 19
 - j.2.MariaDB 10 o 11
 - j.3.PostgreSQL 14 o 15
 - j.4.MongoDB 5 o 6
 - j.5.ElasticSearch 8
 - j.6.MS SQL Server 2019 o superiore

j.7.NFS v3 e v4

j.8.SMB v3

Non sono considerati accettabili vincoli relativi a soluzioni di data management che differiscono da quelli elencati

k. Limitatamente agli elementi computazionali (c.1, c.2, c.3) viene richiesto il rigido rispetto delle raccomandazioni relative ai requisiti minimi di sicurezza relativamente alla separazione funzionale degli utenti. In particolare, la soluzione applicativa deve essere compatibile con la seguente classificazione degli utenti di sistema operativo:

k.1.Utenza di accesso per gestione/manutenzione (abilitato ai servizi di accesso remoto quali SSH e RDP ma senza alcun privilegio di amministrazione o esecuzione di servizi applicativi)

k.2.Utenza applicativa (abilitato all'esecuzione dei servizi applicativi ma senza alcun privilegio amministrativo o abilitazione ai servizi di accesso da remoto)

k.3.Utenza amministrativa (riservata esclusivamente ad attività infrastrutturali e senza alcuna abilitazione ai servizi di accesso da remoto)

L'Azienda prevede la possibilità di escalation interattiva (bottom-up) tra utenza di livello differente mediante una rigida profilazione dettata da specifiche esigenze gestionali. Escalation motivate da esigenze applicative sono tassativamente escluse.

l. Il progetto complessivo della soluzione deve prevedere la gestione di diversi ambienti di erogazione specifici per far fronte alla gestione del life-cycle applicativi. Tali ambiti sono limitati, per esigenze infrastrutturali a:

l.1.COLLAUDO: ambito di verifica delle funzionalità applicative e della stabilità del livello di deploy, operante su dati non reali

l.2.PRE-PRODUZIONE: ambito di test di un deploy già collaudato utilizzabile per formazione o simulazione di carico, operante su sub cloni di dati reali o dati reali in sola lettura

l.3.PRODUZIONE: ambito di erogazione applicativa full scale su dati reali

In conformità alla normativa vigente, gli ambiti descritti non comunicano tra di loro. Per ragioni di limitazione infrastrutturale, l'ambito di sviluppo on-premise non è disponibile e non può essere imposto come requisito di progetto.

m. Sono considerate come accettabili esclusivamente le soluzioni applicative che prevedono workflow di integrazione (inter-soluzione o intra-soluzione) basati su modelli di tipo SOA e in particolare su un'implementazione di tipo ESB (Enterprise Service Bus) tramite protocollo di trasporto HTTP. Sono pertanto esclusi modelli di integrazione basati su file-sharing, DB-link, multiDB access, etc.

n. Viene imposto, come requisito vincolante, l'utilizzo della crittografia TLS 1.2 o superiore per qualsiasi comunicazione da e per la piattaforma e in particolare:

- n.1.Integrazioni applicative di qualsiasi tipo
- n.2.Comunicazioni Front-end Back-end
- n.3.Erogazione applicative verso l'utenza
- n.4.Accesso a servizi esterni

Inoltre si richiede che la soluzione sia configurabile per utilizzare socket TCP/UDP di tipo standard senza nessuna necessità di apertura di porte specifiche di comunicazione.

- o. Al fine di ottimizzare i workflow gestionali dell'infrastruttura, l'Azienda ha individuato una serie di framework applicativi standard a cui vincolare il deploy delle soluzioni applicative proposte. Tali framework sono stati individuati in base alla disponibilità in ambito open-source o alla continuità di mantenimento del progetto:

- o.1.Wildfly
- o.2.Tomcat
- o.3.Apache/PHP
- o.4.Liferay
- o.5.IIS/ASP
- o.6.Mirthconnect
- o.7.Dotnet Framework
- o.8.Mule
- o.9.OpenJDK
- o.10.OpenShift

Tutti i framework qualificati sono da considerarsi disponibili all'ultima Major Release disponibile al momento della proposizione della soluzione e vengono costantemente aggiornati secondo le necessità infrastrutturali.

- p. Altri framework applicativi sono valutabili solo se aderenti ai seguenti requisiti di base:

- p.1.Disponibilità come progetto open-source (no technology lock-in)
- p.2.Soluzione multiplatforma (Windows, Linux, etc.)
- p.3.Compatibilità a deploy di tipo ibrido (on-premise & cloud)
- p.4.LTS (progetto adeguatamente mantenuto nel tempo e costantemente aggiornato)

- q. L'Azienda richiede che la gestione delle funzionalità di autenticazione delle componenti applicative sia di tipo centralizzato e basata sulla piattaforma aziendale di gestione degli account. Tale piattaforma mette a disposizione i protocolli standard LDAPS e CAS per l'interfacciamento delle soluzioni applicative. Viene inoltre richiesta la conformità della piattaforma applicativa proposta alle soluzioni OTP basate su RSA SecureID e Google Authenticator già attive nell'infrastruttura aziendale. Si richiede infine la possibilità di attivare workflow MFA, basate sulle piattaforme di autenticazione aziendali sopracitate, per garantire la conformità dell'autenticazione dell'utenza all'accesso applicativo alle normative vigenti.

- r. Al fine di garantire un adeguato livello di sicurezza infrastrutturale, l'Azienda rigide politiche di application content analysis. Il progetto deve pertanto dettagliare in modo adeguato la tipologia di protocollo applicativo utilizzato per ogni singola tipologia di transazione. Sebbene non esplicitamente proibiti, è fortemente sconsigliato l'utilizzo di data pattern di tipo proprietario. Viene inoltre richiesta una piena compatibilità della piattaforma applicativa a soluzioni di Application delivery basate sull'utilizzo di Reverse Proxy, SSL Off loader, workload balancer con logiche sia statiche che dinamiche, etc.
- s. La soluzione applicativa proposta deve essere sviluppata tenendo conto dei principali principi di sicurezza, solidità e stabilità applicativa. In tale senso vanno tenute in considerazione linee guida quali "OWASP Top 10 2021", "NIST SP 800-53".
- t. L'Azienda esegue controlli periodici sull'intera infrastruttura al fine di rilevare possibili vulnerabilità di sicurezza. Tali controlli sono basati sia su routine di monitoraggio automatiche sia su costante confronto tra i database relativi alle vulnerabilità note e la base software installata nell'infrastruttura aziendale. Nel caso di rilevamento di una specifica vulnerabilità relativa alla piattaforma proposta, anche in fase di esercizio, il fornitore è tenuto a provvedere alla mitigazione e successiva eliminazione della stessa entro una tempistica proporzionale alla gravità della vulnerabilità stessa (RIF, classificazione CVSS v3):
 - t.1.SCORE da 10.0 a 7.0, fix implementato entro 48 ore dalla segnalazione
 - t.2.SCORE da 6.9 a 4.0, fix implementato entro 7 giorni solari dalla segnalazione
 - t.3.SCORE inferiore a 4.0, fix implementato entro 30 giorni solari dalla segnalazione
- u. Le politiche adottate in merito alla sicurezza informatica impongono che ogni sistema collegato all'infrastruttura aziendale disponga di una sicurezza intrinseca di base; questo al fine di limitare ai minimi termini la possibilità che l'endpoint stesso possa divenire un vettore d'attacco per il resto dell'infrastruttura. Per tale ragione è richiesto che qualsiasi endpoint sia conforme ai seguenti requisiti:
 - u.1.Sistema operativo di base in corso di supporto da parte del vendor e costantemente aggiornato all'ultima versione disponibile
 - u.2.Software applicativi, eventualmente installati, senza vulnerabilità note
 - u.3.Software EDR in corso di supporto da parte del vendor, costantemente aggiornato all'ultima versione disponibile e opportunamente configurato e gestito
 - u.4.Corretta gestione del ciclo di vita delle credenziali di accesso al sistema (se non derogata a un sistema centralizzato)
- v. Con riferimento alle eventuali componenti client, si richiede il rispetto dei seguenti requisiti:
 - v.1.Necessità di eseguire l'applicazione come utente standard (non amministratore)
 - v.2.Utilizzo di sistemi operativi e componenti software aggiornati all'ultima versione ed esenti da vulnerabilità

- v.3.Nessuna necessità di chiavi hardware per il funzionamento dell'applicazione
- v.4.Nessuna necessità di esclusione da parte dell'antivirus
- v.5.Cifratura di eventuali dati personali/sensibili memorizzati localmente

Tali requisiti sono da considerarsi vincolanti anche per proposizioni che contemplino il deploy su ambiente cloud qualificato in gestione dell'Azienda (soluzioni IAAS e PAAS). In caso di proposizione di una soluzione SAAS vanno considerati vincolanti esclusivamente i punti relativi all'architettura, e in particolare i punti a), b), m), p) (limitato al protocollo CAS e alla soluzione OTP basata su google authenticator), r) e s).

In merito all'integrazione delle soluzioni proposte all'interno della rete informatica AOUP viene applicata la seguente suddivisione:

Soluzione Air-Gapped:

- **Isolamento totale:** Non è connessa alla rete aziendale.
- **Requisiti:** Nessun requisito specifico per la messa in rete, in quanto completamente isolata.

Soluzione Local Access:

- **Connessione limitata:** Connessa a un segmento di rete locale specifico.
- **Requisiti:** la soluzione dovrà rispettare quanto indicato ai punti "a", "b", "h", "n" (limitatamente al punto n.3), "r", "t".

Soluzione Restricted Access:

- **Connettività estesa:** Oltre alla connessione locale, include connessioni specifiche ai sistemi centrali.
- **Requisiti:** la soluzione, oltre a tutti i requisiti della "Soluzione Local Access", dovrà rispettare anche quanto indicato ai punti "c", "e", "k", "m", "q", "u", "v".

Soluzione Standard Access:

- **Accesso completo:** Accesso completo ai servizi aziendali
- **Requisiti:** la soluzione deve rispettare tutti i requisiti delle soluzioni precedenti, inclusi quelli specificati nelle politiche di sicurezza aziendali.

Eventuali non conformità ai requisiti precedentemente dettagliati potranno essere oggetto di valutazione specifica nel caso di dispositivi o software dedicati alle attività di diagnosi e cura; al fine di consentire tale valutazione sarà necessario comunque dettagliare i requisiti infrastrutturali secondo lo schema del presente documento evidenziando gli eventuali scostamenti e le relative motivazioni. Resta sottointeso che l'eventuale accettazione delle non conformità è sottoposta all'insindacabile giudizio di AOUP.

Per quanto non espressamente richiamato nel presente documento, si rimanda alle normative attualmente vigenti in tema di protezione dei dati personali, sicurezza informatica e infrastrutture qualificate per l'erogazione di servizi a favore della PA.