

**REQUISITI MINIMI PER L'EROGAZIONE DI SOLUZIONI SOFTWARE A FAVORE
DELL'ISTITUTO ONCOLOGICO VENETO IRCCS**

Di seguito vengono elencati i requisiti di conformità richiesti ad ogni progetto applicativo per poter essere qualificato come installabile on-premise presso le strutture datacenter dell'Istituto Oncologico Veneto IRCCS o su ambiente cloud qualificato:

- a. Ogni soluzione applicativa proposta che preveda accesso da parte del personale dell'Istituto tramite client HTML deve poter essere fruibile dall'utente finale esclusivamente da browser standard, senza la necessità di installare software aggiuntivo sulle postazioni client.
- b. La fruizione della soluzione applicativa 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 piattaforma applicativa qualificabile deve essere complessivamente strutturata come soluzione multilivello con l'implementazione di una separazione logica e funzionale dei seguenti elementi:
 - i. Front-end di accesso;
 - ii. Back-end applicativo;
 - iii. Back-end di integrazione (se previsto dal progetto complessivo);
 - iv. Dati strutturati (database relazionali);
 - v. 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'Istituto.
- 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:
 - i. supportare obbligatoriamente connettività radio a 5Ghz e (a titolo preferenziale) a 6Ghz;
 - ii. supportare tutti i canali disponibili sulle frequenze 5Ghz (U-NII-1, U-NII-2A, U-NII-2B, U-NII-2C, U-NII-3);
 - iii. supportare canali con ampiezza a 40Mhz;
 - iv. supportare l'utilizzo di canali DFS;
 - v. 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 applicativa non può richiedere livelli di priorità o accesso esclusivo a specifiche risorse.

UOC SISTEMI INFORMATIVI

- h. In conformità alle normative relative al mantenimento di un adeguato livello di aggiornamento delle piattaforme IT, l'Istituto 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 applicativa proposta deve essere compatibile con le politiche descritte.
- i. L'Istituto limita in modo vincolante le piattaforme computazionali messe a disposizione dalla propria infrastruttura. Sono pertanto disponibili esclusivamente sistemi basati su:
- Microsoft Windows;
 - Red Hat Enterprise Linux;
 - Altre versioni Linux (free) possono essere utilizzate in ambienti di test o riproduzione solo previa autorizzazione dell'Istituto

Tali sistemi operativi vanno intesi come disponibili nella più aggiornata Major Release disponibile al momento della proposizione della soluzione applicativa.

- j. L'Istituto, nell'ambito dei servizi di data management mette a disposizione esclusivamente le seguenti soluzioni PAAS:
- MariaDB 10 o 11
 - PostgreSQL 14 o 15
 - MongoDB 5 o 6
 - ElasticSearch 8
 - MS SQL Server 2019 o superiore
 - NFS v3 e v4
 - SMB v3

Non sono considerati accettabili vincoli relativi a soluzioni di data management che differiscono da quelli elencati, a meno che non siano fornite assieme alla soluzione anche le licenze della soluzione di data management da utilizzare

- 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:
- 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)
 - Utenza applicativa (abilitato all'esecuzione dei servizi applicativi ma senza alcun privilegio amministrativo o abilitazione ai servizi di accesso da remoto)
 - Utenza amministrativa (riservata esclusivamente ad attività infrastrutturali e senza alcuna abilitazione ai servizi di accesso da remoto)

L'Istituto 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 applicativa 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:

UOC SISTEMI INFORMATIVI

- i. COLLAUDO: ambito di verifica delle funzionalità applicative e della stabilità del livello di deploy, operante su dati non reali
- ii. 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
- iii. 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 HTTPS. Sono pertanto esclusi modelli di integrazione basati su file-sharing, DB-link, multiDB access, FTP, etc.
- n. Viene imposto, come requisito vincolante, l'utilizzo della crittografia TLS 1.2 o superiore per qualsiasi comunicazione da e per la piattaforma applicativa e in particolare:
 - i. Integrazioni applicative di qualsiasi tipo
 - ii. Comunicazioni Front-end Back-end
 - iii. Erogazione applicative verso l'utenza
 - iv. Accesso a servizi esterni

Inoltre si richiede che l'applicazione sia configurabile per utilizzare socket TCP/UDP di tipo standard senza nessuna necessità di apertura di porte specifiche di comunicazione. È consentito l'utilizzo di trasmissione dati non cifrata esclusivamente nel caso di dati non sensibili.

- o. Al fine di ottimizzare i workflow gestionali dell'infrastruttura, l'Istituto 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, alla continuità di mantenimento del progetto:
 - i. Wildfly
 - ii. Tomcat
 - iii. Apache/PHP
 - iv. Liferay
 - v. IIS/ASP
 - vi. Mirthconnect
 - vii. Dotnet Framework
 - viii. Mule
 - ix. OpenJDK

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

- p. Altri framework applicativi sono valutabili solo se aderenti ai seguenti requisiti di base:
 - i. Disponibilità come progetto open-source (no technology lock-in);
 - ii. Soluzione multiplatforma (Windows, Linux, etc.);
 - iii. Compatibilità a deploy di tipo ibrido (on-premise & cloud);

UOC SISTEMI INFORMATIVI

- iv. LTS (progetto adeguatamente mantenuto nel tempo e costantemente aggiornato).
- q. L'Istituto 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'Istituto adotta rigide politiche di application content analysis. Il progetto applicativo deve pertanto dettagliare in modo adeguato la tipologia di protocollo applicativo utilizzato per ogni singola tipologia di transazione applicativa. 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'Istituto 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 applicativa 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):
- i. SCORE da 10.0 a 7.0, fix implementato entro 48 ore dalla segnalazione
 - ii. SCORE da 6.9 a 4.0, fix implementato entro 7 giorni solari dalla segnalazione
 - iii. SCORE inferiore a 4.0, fix implementato entro 30 giorni solari dalla segnalazione.
- u. Con riferimento alle eventuali componenti client, si richiede il rispetto dei seguenti requisiti:
- i. Necessità di eseguire l'applicazione come utente standard (non amministratore)
 - ii. Utilizzo di sistemi operativi e componenti software aggiornati all'ultima versione ed esenti da vulnerabilità
 - iii. Nessuna necessità di chiavi hardware per il funzionamento dell'applicazione
 - iv. Nessuna necessità di esclusione da parte dell'antivirus aziendale
 - v. Cifratura di eventuali dati personali/sensibili memorizzati localmente

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



Regione del Veneto
Istituto Oncologico Veneto
Istituto di Ricovero e Cura a Carattere Scientifico



REGIONE DEL VENETO

UOC SISTEMI INFORMATIVI

soluzione OTP basata su google authenticator), r) e s). 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.