Allegato
SPECIFICHE ICT

Versione 1, 20241028

Sommario

Allegati:
Checklist Validazione software per Studi Clinici

Information & Communication Technology (ICT)
Direttore Ing. Luca Capitani
Via Massarenti, 9 - 40138 Bologna
T. +39.051.214.3292/3917 - F. +39.051.636.3299
segreteria.ict@aosp.bo.it

Azienda Ospedaliero - Universitaria di Bologna (IRCCS)
Via Albertoni, 15 - 40138 Bologna
T. +39.051.214.1111 - F. +39.051.636.1202
Cod. Fisc. 92038610371 - P. Iva 02553300373

1 Scopo dell'Allegato

Il presente documento descrive i requisiti dei nuovi sistemi hardware e software oggetto di fornitura, nonché le modalità di integrazione nel Sistema Informativo dell'IRCCS Policlinico di Sant'Orsola di Bologna (d'ora in poi **IRCCS** per brevità).

I requisiti descritti di seguito sono da considerarsi come vincolanti, e anche se l'offerta formale o la documentazione relativa al sistema non dovessero dichiarare esplicitamente la rispondenza a tali requisiti, si assume l'accettazione implicita degli stessi. Qualsiasi offerta o documentazione che presenti elementi di incoerenza rispetto a requisiti indicati sarà da ritenersi nulla, in toto o nella parte che presenti gli elementi di incoerenza.

Il presente documento non tratta eventuali vincoli derivanti dalla classificazione del sistema software come Dispositivo Medico (Rif. disciplina relativa vigente). Tali vincoli sono oggetto di verifica da parte del Servizio Ingegneria Clinica (**IC**), indipendente dal livello di integrazione del software all'interno del Sistema Informativo aziendale.

Il presente documento non tratta eventuali vincoli derivanti dalla trasmissione dati verso l'esterno dell'azienda (es. soluzioni "cloud"). Questo ambito, essendo la normativa specifica ancora in evoluzione, deve essere trattato in modo specifico col Servizio ICT dell'IRCCS (**ICT d'ora in poi**) attraverso valutazioni della soluzione proposta; tali valutazioni verteranno ad esempio su requisiti di sicurezza derivanti dalla normativa privacy vigente, crittografia dei dati, segregazione tra tenant, definizione delle responsabilità in carico all'organizzazione e al cloud provider.

Nel presente documento sono trattati i seguenti requisiti, con le relative sigle:

- Requisiti di Cybersicurezza (identificati con sigla **RC**)
- Requisiti Minimi di sicurezza informatica per il sistema e principi generali (identificati con sigla **RM**)
- Requisiti Sistemistici, di rete e generali per l'implementazione nel contesto aziendale (identificati con sigla **RS**)
- Requisiti di Integrazione coi principali componenti del Sistema Informativo aziendale (identificati con sigla **RI**)
- Requisiti Aggiuntivi (identificati con sigla **RA**)
- Specifiche per l'ambito degli studi clinici
- Verifiche e controlli

2 Clausola contrattuale concernente i cyber-rischi (RC)

Qualora il sistema oggetto di acquisizione venga considerato, dal Servizio ICT, con un alto potenziale di rischio cyber ai sensi della Direttiva (UE) 2022/2555 – NIS 2 (recepita in Italia con D.Lgs. 138/2024) devono essere obbligatoriamente accettate le seguenti clausole:

- **RC1:** il fornitore si impegna, ai fini dell'esecuzione del contratto e durante l'esecuzione dello stesso, a proteggere nel proprio ambito di responsabilità i sistemi informatici e di telecomunicazione (in particolare i sistemi infrastrutturali, le reti, i dispositivi e le applicazioni, come pure i dati[1] e le informazioni[2]) – di seguito denominati «sistemi» – contro eventuali attacchi, adottando misure economicamente ragionevoli e possibili dal punto di vista tecnico e organizzativo secondo lo stato attuale della tecnica;
- **RC2:** ai fini della corretta esecuzione del contratto il fornitore si impegna in particolare a proteggere, i dati e le informazioni messi a sua disposizione o a disposizione di terzi incaricati[3] (ad es. subappaltatori e fornitori) oppure prodotti da essa o da terzi incaricati. Questo vale in particolare se si tratta di dati rilevanti per la sicurezza o di dati personali. In tale contesto, occorre osservare i requisiti e le prescrizioni del Codice in materia di protezione dei dati personali (artt. 167, 167bis, 167ter).
- **RC3:** il fornitore si impegna a comunicare all'IRCCS e/o al servizio designato nel contratto qualsiasi evento che potrebbe pregiudicare l'osservanza dei propri obblighi, subito dopo il verificarsi dell'evento o dopo averne preso atto. Comunica in particolare i tentativi di attacco o gli attacchi riusciti come pure altre compromissioni tecniche sospettate o avvenute di sistemi, dati e/o informazioni, nonché gli eventuali danni arrecati. Informa altresì sulle misure previste oppure adottate per rimediare a tali danni. Per evitare danni o ulteriori attacchi, accorda all'IRCCS o a terzi da esso incaricati il pieno accesso ad analisi, rapporti d'indagine e altre constatazioni (documenti, dati, dati d'accesso, oggetti ecc.) che consentono di analizzare l'evento. Il fornitore si accerta che le attività predefinite con l'IRCCS siano registrate (logging) e valutate, al fine di individuare ed evitare gli attacchi. Le falle di sicurezza scoperte devono essere chiuse al più presto;

[1] Ad esempio i dati personali relativi a collaboratori, indirizzi email, codici di accesso ecc.
[2] Ad esempio la descrizione di processi, fasi lavorative, piani, regole di accesso, infrastrutture ecc.
[3] Sono considerate tutte le parti della catena di fornitura e di produzione, compresi i titolari di diritti e i fabbricanti

- **RC4:** l'IRCCS (o un terzo da esso incaricato) può, se necessario e al massimo due volte all'anno, eseguire audit presso il fornitore. Gli audit sono preceduti da un preavviso di 7 giorni lavorativi. Ciascuna parte si assume i propri costi dell'audit. Tuttavia, se nell'ambito dell'audit si dovessero constatare lacune gravi ai sensi della presente disposizione, il fornitore si assumerebbe anche i costi per colmare tali lacune e quelli sostenuti dall'Azienda a seguito dell'audit. Il fornitore è tenuto a colmare le lacune entro 15 giorni dalla comunicazione e a notificare all'IRCCS l'avvenuta esecuzione dei relativi lavori.

In caso di violazione sostanziale della presente clausola o di mancata collaborazione nei casi sopracitati, l'IRCCS si riserva il diritto di non acquisire altre prestazioni e di porre fine al rapporto contrattuale.

3 Requisiti Minimi di sicurezza informatica (RM)

L'IRCCS 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 all'adozione di 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.

3.1 Principi generali per i sistemi e per i software

In generale, tutti i sistemi e i software forniti dovranno essere:

- **coerenti** con la necessità di implementare applicazioni, servizi e procedure secondo l'approccio "**privacy by design e privacy by default"** per ogni percorso di trattamento. Tutti i sistemi devono essere costruiti per proteggere i dati trattati e farlo come impostazione predefinita. L'aggiudicatario è tenuto a fornire documentazione delle misure implementate anche allo scopo di permettere le necessarie valutazioni al Titolare;
- **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** e delle direttive di settore, 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;
- integrati con altri sistemi e/o software tramite tecnologie avanzate, sicure e performanti rispetto ai volumi di dati scambiati, evitando quelle obsolete.

3.2 Requisiti Minimi di sicurezza informatica

Di seguito sono descritti i requisiti minimi di sicurezza che ciascun sistema software deve soddisfare per la sua adozione presso l'IRCCS. I requisiti descritti costituiscono vincoli indotti dalla attuale normativa sul Trattamento Dati Particolari (Rif. disciplina Privacy vigente).

- **RM1:** il fornitore deve fornire autocertificazione di conformità al Regolamento Europeo per la Protezione dei Dati Personali (GDPR; Regolamento UE 2016/679), alla Legge 196/2003 e s.m.i. e alla normativa italiana di recepimento della Direttiva NIS 2 (Network and Information Security Directive 2) dell'UE (nota anche come "Direttiva 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione"), D.Lgs. 138/2024 e relativi decreti attuativi.
  Qualora il sistema offerto non fosse conforme ad uno o più dei requisiti descritti, è necessario che sia esplicitato in forma scritta, specificando il motivo della non-conformità (es. sistema classificato come DM di produzione estera, non immediatamente adeguabile alla normativa vigente in Italia). Le non conformità sono oggetto di verifica in fase di collaudo, e deroga qualora la motivazione fosse ritenuta accettabile.
- **RM2:** 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.

3.2.1 Confidenzialità del dato

- **RM3:** il sistema deve prevedere autenticazione tramite username e password personali (o altra metodologia più forte in relazione alla classificazione fatta dal Codice Amministrazione Digitale (CAD));
- **RM4:** il sistema di autenticazione deve prevedere integrazione con i server di autenticazione aziendale (tramite protocollo LDAPS o integrazione col sistema SSO aziendale basato su SAML2, in specifico Shibboleth IDP) così come descritto nel paragrafo "Sistema di gestione di Identità e Accessi (IAM)".
  In alternativa, il sistema deve prevedere la scadenza periodica della password, con periodicità in linea con la disciplina Privacy vigente, così come la complessità e la gestione del ciclo di vita (attivazione e disattivazione) degli account utente. Non è possibile effettuare l'autenticazione degli utenti mediante logon Windows. L'offerta dovrà esplicitare in maniera chiara le modalità di integrazione con i sistemi di autenticazione IRCCS e in ogni caso la ditta aggiudicataria deve rendersi da subito disponibile a definire la configurazione ottimale con i tecnici ICT;
- **RM5:** il sistema deve prevedere la profilazione degli utenti abilitati al sistema, consentendo agli utenti classificati come "amministratori di sistema" di limitare le possibilità di accesso degli utenti a singole sezioni/funzionalità del sistema stesso secondo il criterio di assegnazione dei privilegi minimi necessari e sufficienti allo svolgimento delle mansioni di competenza. La gestione dei profili di abilitazione degli utenti deve essere realizzata all'interno del sistema e/o del software offerto. Inoltre, dovrà essere garantita l'integrazione con il sistema aziendale di gestione delle abilitazioni, così come descritto nel paragrafo "Sistema di gestione di Identità e Accessi (IAM)";
- **RM6:** il ruolo di "amministratori di sistema" deve essere assegnabile anche a utenti IRCCS (non vincolato ai soli utenti di supporto fornitore);
- **RM7:** il sistema e/o il software deve utilizzare solo sistemi di comunicazione sicuri (crittografati, ad esempio utilizzare il protocollo HTTPS per il collegamento verso l'Application Server o verso web services o siti esterni);
- **RM8:** il sistema deve prevedere tecnologie di protezione delle banche dati di dati personali e sensibili;
- **RM9:** il sistema deve prevedere la tracciabilità di tutti gli accessi al sistema, indicando in particolare il contesto a cui si è fatto accesso (es. riferimento al paziente i cui dati sono stati oggetto di consultazione/modifica, identificazione del dato consultato/modificato);
- **RM10:** deve essere effettuata la cancellazione profonda dei dati dai supporti fisici prima del loro riutilizzo;
- **RM11:** deve essere effettuata la cancellazione profonda dei dati dai supporti fisici o la distruzione dei supporti stessi prima del loro smaltimento.

3.2.2 Integrità del dato

- **RM12:** il sistema deve prevedere l'archiviazione dei dati esclusivamente su server (nessun dato deve essere archiviato sui client e/o sulle workstation);
- **RM13: p**er 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;

- **RM14:** il sistema e/o il software deve prevedere un sistema di backup dei dati (o eventualmente appoggiarsi su sistemi di backup aziendali, si veda in seguito);
- **RM15:** il fornitore deve prevedere, come parte integrante della fornitura, servizi di Test di Restore da backup, con cadenza minima annuale;
- **RM16:** il sistema e/o il software deve prevedere un sistema antivirus, con relativi processi e policy di aggiornamento automatico delle firme (o appoggiarsi sui sistemi antivirus aziendali, si veda di seguito);
- **RM17:** il sistema e/o il software deve prevedere aggiornamenti in modalità automatica, o eventualmente gestiti manualmente dal fornitore (in quest'ultimo caso devono essere compresi in fornitura i servizi) dei principali componenti di sistema operativo e di firmware ai più recenti aggiornamenti di sicurezza (es. patch di sistema operativo).

3.2.3 Continuità e disponibilità del dato

La Ditta aggiudicataria deve prevedere per il proprio sistema e/o software soluzioni tecnico-organizzative, a diversi livelli, funzionali al suo ripristino secondo tempi e modalità coerenti con il livello di criticità dello stesso.
L'offerta tecnica dovrà descrivere:

- **RM18:** descrizione del piano di backup indicando relativa periodicità, stima dell'occupazione disco iniziale e incremento annuale, test di ripristino;
- **RM19:** proposta architetturale del piano di Disaster Recovery, se previsto, con stima dei parametri caratteristici (RTO, RPO ecc.) coerenti con il Service Level Agreeement richiesto;
- **RM20:** proposta architetturale del piano di Business Continuity, se previsto, al fine di garantire la continuità di servizio del sistema e/o del software.

In base alla soluzione proposta, il Servizio ICT valuterà la messa a disposizione dell'infrastruttura di backup aziendale ad integrazione dei sistemi forniti. In alternativa sarà onere dell'aggiudicatario fornire l'infrastruttura necessaria a supportare il piano di backup e di continuità di servizio.

- **RM21:** il fornitore deve rendersi disponibile a collaborare con l'Azienda committente alla redazione e validazione dei flussi di assistenza riferiti ai sistemi e/o ai 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 Requisiti Sistemistici, di rete e generali (RS)

Di seguito sono descritti:

- I requisiti generali di implementazione del sistema e/o del software nel contesto aziendale;
- la configurazione della rete dati, della infrastruttura server e dei client/workstations;
- i requisiti di integrazione sistemistici e di rete.

Il fornitore dovrà riportare nell'apposita sezione dell'offerta tecnica di descrizione del sistema informativo offerto la rispondenza ai requisiti descritti, motivando eventuali non-conformità. Sempre in tale sezione dell'offerta tecnica sarà necessario descrivere l'architettura e le funzionalità dell'impianto in rapporto alla dislocazione logistica e alle esigenze

di connettività del sistema, allo scopo di valutare l'impatto sulla infrastruttura aziendale e predisporre in seguito gli adeguamenti e il supporto necessari.
Il coordinamento delle attività di integrazione col Sistema Informativo aziendale sarà svolto congiuntamente dal Servizio Gestore del contratto (es. Ingegneria Clinica, Progettazione Sviluppo ed Investimenti, Gestione Servizi & Operation, Analitycs and operations research) e ICT.

4.1 Requisiti generali di implementazione nel contesto aziendale

Il sistema e/o il software offerto 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'IRCCS nello specifico contesto di installazione.

- **RS1:** tutti i sistemi e/o gli applicativi forniti dovranno permettere ad IRCCS 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 dare piena disponibilità a produrre il dettaglio del servizio offerto per consentire alle singole Aziende di rispondere a quanto indicato nella Direttiva "NIS" 2016/1148.
- **RS2:** l'aggiudicatario dovrà collaborare attivamente per gli aspetti attinenti all'oggetto della fornitura e di competenza, alla produzione di documentazione che l'IRCCS è chiamata a redigere in ottemperanza ai 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 e/o software e susseguente comunicazione in caso di violazione dei dati (DATA BREACH) per il seguito di competenza del titolare e del DPO;
- **RS3:** per quanto attiene 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). Il documento fornito dovrà contenere almeno le informazioni richieste nel report 07 della PA11.
  Il responsibility agreement, redatto dall'aggiudicatario e revisionato/validato da IRCCS, conterrà espliciti riferimenti alla "marcatura CE" (secondo il regolamento europeo 745 del 2017) 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;
- **RS4:** nel caso in cui la fornitura riguardi un Medical Device, l'IRCCS 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;
- **RS5:** 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. L'aggiudicatario sarà nominato "Responsabile del trattamento dei dati personali" ai sensi dell'art. 4, par. 1, n. 8 GDPR (Regolamento UE 2016/679).

4.2 Descrizione della infrastruttura aziendale

4.2.1 Infrastruttura Server

Il parco server aziendale per gli applicativi software è organizzato su DataCenter presso il campus ospedaliero del Policlinico di Sant'Orsola e presso le strutture Regionali gestite dalla società In-house Lepida, dislocate sul territorio regionale.
Come da direttive nazionali, il punto centrale dell'attuale infrastruttura server dell'IRCCS è da identificarsi presso i DataCenter Regionali a gestione Lepida, situati a Ferrara, Ravenna e Parma. Il DataCenter locale presso le strutture aziendali è da considerarsi come esclusivo mantenimento di sistemi cached su applicazioni critiche sanitarie già definite.

I servizi su server fisici sono stati quasi tutti dismessi, a favore di server virtuali su una infrastruttura VMware versione 6.7 (in previsione migrazione a versione 7).
Presso i Datacenter Lepida, è presente un sistema principale virtuale multinodo VMware versione 6.7. La sede Lepida di Ravenna è il sito ove principalmente risiedono tutti i server in produzione. Per i sistemi individuati come critici, esiste una replica sincrona nel sito di Ferrara e/o asincrona a fini di DR delle macchine sul sito secondario di Parma.
I sistemi server aziendali sono installati in ambiente linux OracleLinux, Debian e Ubuntu, oltre che su piattaforma Microsoft costituita da macchine con S.O. MS Windows 2016, MS Windows 2019 e MS Windows 2022.
I database degli applicativi aziendali sono principalmente Oracle Enterprise 19 e MS SQL 2019 o successivi.
La ridondanza dei sistemi è realizzata con configurazioni HA dei sistemi virtuali (funzionalità di VMware) unita al bilanciamento applicativo con sistemi appositi previsti dai fornitori applicativi. È in corso di implementazione l'infrastruttura di business continuity tra i siti di Ravenna e Ferrara mediante funzionalità HA di VMware.
Questa infrastruttura è collegata alla rete LAN dell'IRCCS tramite doppio collegamento ridondato su rete Lepida e consegnato su percorsi distinti e ridondati nella sede del campus S.Orsola. La banda nominale di ciascun collegamento è di 10G (Lepida non garantisce alcuna banda minima) con una latenza di 4-5 ms.
Il traffico di rete con i client è regolato da appositi firewall per ogni DataCenter gestiti internamente da ICT, che autorizza e verifica il traffico da e verso le reti DataCenter regionali in cui sono collocati i server applicativi.

4.2.2 Client

Di seguito si riportano le caratteristiche principali:

- sistema operativo Windows 10 Pro 64 bit o Windows11 Pro 64bit, CPU i3-i5, RAM 4/8 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, Office 365 (diversi piani di licensing), Antivirus Bitdefender (con funzioni di antivirus, antispyware, webcontrol, mail control, firewall, application control), Adobe Acrobat Reader, UltraVNC, 7Zip, Java versione 1.6 o superiore, browser predefinito aziendale EDGE (Firefox e Chrome solo se motivati) aggiornati periodicamente alle ultime versioni. 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 acquistate tramite le convenzioni delle centrali di acquisto nazionali o regionali.
La messa in rete dei dispositivi è consentita solamente previa accettazione e mantenimento dei requisiti minimi di sicurezza necessari.

4.2.3 Infrastruttura di rete

Di seguito si riporta una descrizione delle principali caratteristiche dell'infrastruttura di rete.
La rete informatica dell'IRCCS è costituita da una rete capillare di distribuzione sia di tipo wired che di tipo wireless, caratterizzata da 2 centri stella di campus.
L'infrastruttura si sviluppa all'interno di un unico campus, connesso da un'unica lan, suddivisa in "aree"; un'area può corrispondere a un grosso padiglione o a un aggregato di alcuni padiglioni vicini più piccoli. L'architettura di rete è di tipo L3: ciascuna area ha una sua VLAN per i client, più altre VLAN per usi specifici (server decentrati, wifi, etc.); ogni VLAN è separata dalle altre e comprende sottoreti con indirizzi di classe B o C e default gateway distinti. Complessivamente sono presenti circa 23 aree e oltre 150 VLAN.
Gli apparati di rete sono in tecnologia di connessione switched-ethernet.
Tutte le dorsali di rete dai centri stella agli armadi principali di area sono realizzate con collegamenti in fibra ottica ridondati a 1Gbps o 10Gbps; la distribuzione dall'armadio principale ai secondari di area è su collegamenti in fibra ottica ridondati a 1Gbps; l'utenza è servita da cavi a coppie UTP di cat.6 o cat.5e, secondo lo standard TIA/EIA 568 collegati a switch con porte 10-100-1000.
La copertura wireless, realizzata secondo lo standard IEEE 802.11a/b/g/n/ac, è stata implementata sull'intero campus, compresi i reparti sanitari. L'infrastruttura è di tipo centralizzato e governata da Wireless Control System (WLC) ridondato. L'autenticazione di rete è basata su tecnologia WPA2 e la crittografia dati è la AES, con certificato aziendale autofirmato lato server.

L'unico protocollo di rete ammesso è IP unicast.
Le connessioni web verso Internet avvengono tramite proxy server aziendali, che gestiscono tutte le richieste di accesso a Internet con autenticazione NTLM.
Sistemi di firewall ridondati gestiscono i collegamenti dei client sia verso i server aziendali che verso le altre reti.
Per le caratteristiche intrinseche delle tecnologie wireless, l'unica infrastruttura wi-fi ammessa è quella centralizzata sopra descritta, ciò per garantire l'assenza di interferenze.
Sistemi di firewall ridondati gestiscono i collegamenti verso i server aziendali e verso i collegamenti periferici (Internet, Lepida, rete interaziendale, MAN AUSLBO, etc.).
Le connessioni verso l'esterno/Internet vengono limitate con opportune regole di filtri e verificate da sistemi antivirus/antimalware.

4.2.4 Sistema di gestione di Identità e Accessi (IAM)

I sistemi applicativi presenti nell'IRCCS si integrano con i meccanismi di autenticazione dell'IRCCS, con l'obiettivo di utilizzare le credenziali di autenticazione già assegnate agli operatori nell'azienda, 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 software integrati nel contesto aziendale viene gestita 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 IDP basato su protocollo SAML2 (nello specifico con il prodotto open source Shibboleth IDP), integrato all'OpenLDAP aziendale.
- in ambiente client-server: per le procedure non web è necessario che l'autenticazione venga gestita collegandosi direttamente con protocollo LDAPS. 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 IRCCS.

La gestione dei profili di abilitazione degli utenti è realizzata all'interno dei singoli sistemi applicativi. Questi ultimi sono integrati con il sistema aziendale di gestione delle abilitazioni (IAM), tipicamente mediante web service basato su stile architetturale API REST su HTTPS.

4.3 Requisiti di integrazione server, client e rete

Gli scenari di integrazione server, client e rete proposti per lo specifico sistema informativo devono essere esplicitati nell'apposita sezione dell'offerta tecnica di Descrizione del sistema informativo offerto, tenendo conto dei requisiti indicati nel presente Allegato.

4.3.1 Server

4.3.1.1 Hardware e licenze

- **RS6:** in linea con quanto previsto dall'AgID in termini di centralizzazione e razionalizzazione dei servizi, il sistema/software offerto dovrà essere implementato presso uno o più DataCenter di Lepida S.c.p.A (**Lepida**) di afferenza aziendale e fruibile da qualunque postazione client IRCCS, 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 tal caso le specifiche infrastrutturali e di rete devono essere esplicitate nell'offerta e saranno valutati assieme a ICT preliminarmente all'istallazione. Gli eventuali oneri impiantistici/infrastrutturali per garantire il servizio saranno a carico del fornitore (collegamenti elettrici o prese aggiuntivi, UPS, armadi rack, ecc.). La gestione e manutenzione HW di tali sistemi dovrà essere compresa nel servizio offerto per tutta la durata del contratto;
- **RS7:** in linea generale, laddove l'istallazione avvenisse su datacenter regionale, l'IRCCS mette a disposizione senza oneri aggiuntivi per l'aggiudicatario:
  - le infrastrutture server e storage presenti nel DataCenter di Lepida, 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 DataCenter 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 10 Gbps;
- licenze del RDBMS Oracle ultima versione disponibile;
- Infrastruttura VMware 6.x o 7.x;

- **RS8: s**i 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 terminal server, RDBMS SQL server, add-on, etc).

4.3.1.2 Aggiornamenti

- **RS9:** tutta l'infrastruttura software deve basarsi sulle ultime versioni disponibili e supportate dei prodotti (sistemi operativi, framework, etc). L'aggiornamento deve avvenire 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;
- **RS10:** su tutti i software offerti dovranno essere installate e manutenute le eventuali patch entro due mesi dalla data di rilascio da parte del produttore;
- **RS11:** 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.

4.3.1.3 Attività sistemistiche sugli Application Server

Per quanto riguarda gli Application Server (AS) ospitati in ambiente di virtualizzazione dell'IRCCS, rientrano nelle competenze dei tecnici dell'IRCCS i seguenti aspetti:

- 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 (LDAP, Shibboleth).

- **RS12:** 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 e di eventuali bilanciatori;
  - 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 Apache Tomcat, produzione eccessivi di log, etc);

- **RS13:** nel caso di applicazione con logica web-based, si precisa 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. Inoltre, 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.

4.3.1.4 Attività sistemistiche sui Database Server

Rientrano nelle competenze dei servizi sistemistici dell'IRCCS le seguenti attività:

- 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;
- le attività di backup secondo quanto riportato al paragrafo Backup Dati.

➢ **RS14:** rientrano nelle competenze dei tecnici del fornitore tutte le attività non comprese nel precedente elenco tra le quali cui:

  - l’installazione, configurazione, messa in produzione e manutenzione 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).

4.3.1.5 Ambiente di Test

➢ **RS15:** 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’IRCCS, 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.

➢ **RS16**: il fornitore dovrà prodursi per mantenere allineate quanto più possibile le configurazioni e le condizioni dell’ambiente di test rispetto quello di produzione;

➢ **RS17**: gli ambienti di sviluppo e test devono essere separati dall'ambiente di produzione. È da implementare la segregazione tra le reti che ospitano i server di produzione e quelle che ospitano i server di sviluppo o test.

4.3.1.6 Assistenza remota

➢ **RS18**: 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 credenziali personali con doppio fattore di autenticazione. Per l’accesso degli amministratori ai sistemi ospitati presso i datacenter regionali è previsto l’utilizzo del sistema PAM aziendale.

4.3.1.7 Antivirus

Per ogni server incluso in fornitura deve essere compreso un sistema di gestione antivirus. Tale antivirus può essere oggetto della fornitura, o essere mutuato dalla infrastruttura aziendale.
Qualora compreso nella fornitura:

➢ **RS19**: il sistema antivirus deve prevedere aggiornamento automatico delle firme/configurazioni;

➢ **RS20**: il sistema antivirus deve prevedere console di verifica dello stato di aggiornamento e dello stato di tutte le macchine poste sotto copertura.

Il sistema antivirus (in fornitura o aziendale) potrà essere configurato secondo le modalità ritenute più consone alla funzione di ciascun server.

4.3.1.8 Firewall

Il traffico di rete è regolato da appositi firewall, per ogni DataCenter, gestiti da ICT. Nel caso in cui il sistema offerto debba fornire servizi in internet, in aggiunta ai firewall di datacenter si tenga presente che:

➢ **RS21**: sui server esposti in internet, il fornitore deve attivare il firewall locale, configurato con regole quanto più restrittive possibile e concordate con ICT.

4.3.1.9 Backup Dati

Il sistema deve prevedere un sistema di backup dei dati (requisito già incluso tra quelli minimi di sicurezza). Tale sistema di backup dati può essere autonomo, o appoggiarsi sui sistemi di backup aziendale.

➢ **RS22**: qualora applicabile, il sistema informatico offerto si può appoggiare sul backup aziendale tramite:

- Utilizzo delle funzionalità per il backup degli ambienti virtuali e dei database disponibili nel sistema centralizzato di backup in gestione ICT;
- Trasferimento periodico dei files dati verso spazi condivisi di rete soggetti a backup aziendale.

- **RS23**: se ci si avvale di sistema di backup autonomo da quello aziendale, il sistema deve prevedere strumenti di reportistica/monitoraggio sulla corretta esecuzione del backup.

4.3.2 Client

4.3.2.1 Client in Fornitura

Il sistema può prevedere la fornitura autonoma di dispositivi client.
In questo caso sono previsti i seguenti requisiti:

- **RS24**: il client deve prevedere la connessione (join) verso il Dominio aziendale di competenza (gestito tramite controllers Microsoft Active Directory). Qualora non fosse possibile la connessione verso il Dominio è necessario documentarne il motivo nell'apposita sezione dell'offerta tecnica di descrizione del sistema informativo offerto.

4.3.2.2 Appoggio su Client Aziendali

Nel caso in cui il sistema dovesse essere istallato o utilizzato su postazioni di lavoro in gestione dell'IRCCS:

- **RS25**: deve essere fornita periodicamente o su richiesta di ICT la matrice di compatibilità software e hardware;
- **RS26**: a seguito di aggiornamento dell'immagine delle postazioni di lavoro, su richiesta di ICT il fornitore deve testare il corretto funzionamento del proprio sistema entro 1 settimana;
- **RS27**: deve essere concordata con ICT la modalità di aggiornamento dell'applicativo, tenendo conto anche della presenza del software antivirus con funzionalità application control.

4.3.2.3 Backup Funzionale

- **RS28**: per ogni client/workstation che svolga ruolo critico per la continuità funzionale del sistema, e che preveda l'archiviazione locale di dati di configurazione necessari al suo funzionamento deve essere previsto un sistema di backup di tali dati, autonomo o appoggiato sui sistemi di backup aziendali (in questo caso tramite copia dei files di interesse in apposito spazio oggetto di backup aziendale).

4.3.2.4 AntiVirus

Per ogni client previsto in fornitura deve essere compreso un sistema di gestione antivirus. Tale antivirus può essere oggetto della fornitura, o essere mutuato dalla infrastruttura aziendale.
Qualora compreso nella fornitura:

- **RS29**: per tutti i dispositivi client (in fornitura o aziendali), il sistema antivirus deve prevedere aggiornamento automatico delle firme/configurazioni (tramite linea dati in fornitura o passaggio attraverso rete aziendale);
- **RS30**: il sistema antivirus deve prevedere console di verifica dello stato di aggiornamento.

Il sistema antivirus (in fornitura o aziendale) potrà essere configurato secondo le modalità ritenute più consone alla funzione di ciascun client/workstation.

4.3.2.5 Aggiornamenti

- **RS31**: il software di base dei client (in fornitura o aziendali) deve essere regolarmente aggiornato relativamente alle patch ed agli aspetti (upgrade) di sicurezza.

4.3.2.6 Firewall

- **RS32**: il client (in fornitura o aziendali) devono essere dotati di sistema firewall e IPS personale.

4.3.2.7 Software autorizzati

Per tutti i dispositivi client (in fornitura o aziendali):

- **RS33**: deve essere gestito l'elenco di software autorizzati e relative versioni necessarie. Non deve peraltro essere consentita l'installazione di software non compreso nell'elenco;
- **RS34**: devono essere eseguite regolari scansioni al fine di rilevare la presenza di software non autorizzato.

4.3.3 Rete

Si ritengono impliciti (ma oggetto di verifica) i requisiti di compatibilità elettrica e di rete con le reti di alimentazione e dati presenti nell'IRCSS.
Nel caso in cui fossero implementate soluzioni dedicate di rete cablata o wireless:

- **RS35**: la realizzazione degli impianti, completamente a carico del fornitore, deve essere condotta nel rispetto delle indicazioni fornite dai servizi tecnici aziendali. Eventuali collegamenti di tali reti dedicate con il Sistema Informativo aziendale devono essere realizzati condividendo le modalità e gli aspetti di sicurezza con il Servizio ICT nell'ambito dell'accordo di responsabilità;
- **RS36**: eventuali sistemi che necessitino di diverse comunicazioni wireless devono utilizzare infrastrutture dedicate che garantiscano l'assenza di interferenze con le tecnologie wifi aziendali.

5 Requisiti di Integrazione coi principali componenti del Sistema Informativo aziendale (RI)

Le integrazioni tra il sistema software fornito e il Sistema Informativo Ospedaliero sono indicate nel capitolato tecnico o negli accordi con il Servizio ICT. Si riportano nel seguito alcuni requisiti di carattere generale che devono essere rispettati.

5.1 Integrazioni di base

Per documenti di specifiche relativi ai sistemi citati, rivolgersi al Servizio ICT.

- **RI1**: qualora il sistema informativo offerto gestisca dati nominali di assistiti/pazienti è necessario integrarlo con l'anagrafe provinciale e con la cartella clinica elettronica, principalmente per poter ricevere il piano di lavoro (lista appuntamenti);
- **RI2**: qualora il sistema informativo offerto preveda la generazione di dati sanitari (referti o altro), è necessario integrarlo con il repository aziendale (direttamente o tramite altro strato SW) per la pubblicazione elettronica dei dati. Inoltre, qualora la pubblicazione preveda un invio all'infrastruttura del Fascicolo Sanitario Elettronico, i documenti dovranno essere prodotti in conformità agli standard regionali e nazionali;
- **RI3**: qualora il sistema offerto preveda la firma digitale di documenti/referti è necessario integrarlo con gli ARSS (Aruba Remote Sign Server) aziendali Aruba;
- **RI4**: qualora il sistema offerto preveda la generazione/gestione di contenuti *imaging* è necessario integrarlo con il sistema PACS/VNA aziendale.

5.2 Integrazione con i Sistemi Informativi Amministrativi

Per documenti di specifiche relativi ai sistemi citati, rivolgersi a ICT.

- **RI5**: qualora il sistema informativo offerto preveda la configurazione di strutture/entità aziendali (ad es. codifiche di reparti/ambulatori) il fornitore si impegna a integrarsi con il code repository aziendale in modo da recepire automaticamente gli aggiornamenti;
- **RI6**: qualora il sistema informativo offerto preveda la rilevazione di prestazioni erogate oggetto di rendicontazione economica, è necessario integrarlo con il Repository Amministrativo (HUB);
- **RI7**: tutti i dati gestiti dal sistema devono essere messi a disposizioni dell'IRCCS anche con accesso diretto alle tabelle. Dovrà essere fornita adeguata documentazione e formazione per l'accesso ai dati.

Le specifiche di dettaglio delle integrazioni, se non già disponibili nella documentazione di gara, saranno fornite all'aggiudicatario in fase di progettazione preliminare.
Le suddette integrazioni, di cui ai precedenti paragrafi 5.1 e 5.2 o le ulteriori non precedentemente menzionate ma richieste per lo specifico progetto, si intendono realizzate tramite interfacce e protocolli sicuri e standard secondo le linee guida e best practice più moderne (generalmente vengono adottati i protocolli FHIR o HL7 su canale HTTPS, web-services). Non sono accettate interfacce con tecnologie obsolete (ad es. file di scambio, tabelle, DBlink) o su canale non sicuro se non previa autorizzate del servizio ICT.

6 Requisiti Aggiuntivi (RA)

6.1.1.1 Fine contratto

- **RA1**: se non diversamente specificato in altre sezioni del capitolato/contratto, alla cessazione del contratto i dati gestiti dal sistema dovranno essere resi disponibili all'IRCCS, in formato da condividere col Servizio Gestore del contratto, che ne permetta la portabilità su altri sistemi. Al termine del contratto dovranno essere disattivati tutti gli account in uso al fornitore ed interrotti eventuali flussi dati da/verso i sistemi del fornitore. Il fornitore, inoltre, dovrà prontamente eliminare eventuali dati di titolarità IRCCS precedentemente nelle sue disponibilità in virtù del contratto stesso.

6.1.1.2 Incidenti di sicurezza

- **RA2**: l'IRCCS effettua regolarmente, anche avvalendosi di soggetti terzi incaricati, attività di vulnerability assessment e penetration test al fine di verificare la sicurezza dei propri sistemi; il fornitore si impegna ad effettuare un'analisi congiunta degli esiti entro 2 settimane dalla scansione e a pianificare le eventuali attività per la messa in sicurezza dei sistemi di propria competenza (2 settimane per update o vulnerabilità molto gravi, 6 mesi per upgrade o vulnerabilità basse/medie);
- **RA3**: è responsabilità del fornitore la definizione di procedure e strumenti per la gestione degli incidenti di sicurezza, che prevedano la definizione dei ruoli del proprio personale e comprendano necessariamente la comunicazione entro 24 ore ai referenti IRCCS, in particolare Servizio Gestore e ICT, del tipo di incidente e dei tempi e modi di risposta, ripristino e verifica finale.

6.1.1.3 Formazione

- **RA4**: il personale del fornitore coinvolto nella gestione delle attività previste dal contratto, in particolare quello con ruolo amministrativo, deve ricevere una formazione a cadenza periodica specifica in materia di cybersecurity (es. amministrazione sicura dei sistemi). Devono essere interessati in tal senso anche i dirigenti e i vertici aziendali (es. gestione dei rischi di cybersecurity, importanza di sensibilizzare tutto il personale);
- **RA5**: il personale del fornitore addetto allo sviluppo del software fornito deve ricevere una formazione a cadenza periodica specifica in materia di cybersecurity (es. scrittura di codice sicuro, OWASP Top 10).

6.1.1.4

6.1.1.5 Ciclo di vita del sistema/software e change management

Il fornitore deve implementare, relativamente al sistema offerto, un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle), avente almeno le seguenti caratteristiche:

- **RA6**: sono definite politiche e/o procedure per la gestione sicura del ciclo di vita dei sistemi e delle applicazioni sviluppate (standard di progettazione, pratiche di codifica, rilevazione e correzione delle vulnerabilità in base al rischio, test di accettazione);
- **RA7**: sono definiti modelli di hardening standard per la configurazione dei componenti infrastrutturali (es. server, database, server web, container, componenti PaaS e SaaS) delle applicazioni;
- **RA8**: sono applicati principi di progettazione sicura nelle architetture delle applicazioni (es. concetto di privilegio minimo, validazione di ogni input e operazione dell'utente, controllo degli errori, riduzione al minimo della superficie di attacco dell'infrastruttura dell'applicazione);
- **RA9**: sono definiti i requisiti di sicurezza;
- **RA10**: è verificata l'implementazione dei requisiti di sicurezza per i nuovi sistemi e applicazioni prima della messa in produzione;
- **RA11**: negli ambienti di test vengono utilizzati solo dati fittizi o pseudonimizzati;
- **RA12**: viene utilizzato un sistema per la conservazione e il versioning del codice sorgente in grado di garantirne l'integrità e la protezione da accessi non autorizzati;
- **RA13**: nelle applicazioni è utilizzato esclusivamente software di terze parti (es. framework, librerie) aggiornato e affidabile, di cui viene mantenuto un inventario;
- **RA14**: nelle applicazioni vengono utilizzati moduli o servizi pronti all'uso per i componenti di sicurezza, tra cui gestione delle identità, crittografia e logging;
- **RA15**: viene effettuata la modellazione delle minacce e dei punti deboli dell'applicazione, dell'architettura e dell'infrastruttura, al fine di identificare e risolvere i difetti di progettazione prima della codifica;
- **RA16**: sono utilizzati strumenti di analisi statica e dinamica del codice durante lo sviluppo software;
- **RA17**: sono effettuati penetration test sulle applicazioni, possibilmente in modalità autenticata, prima del rilascio in produzione;
- **RA18**: viene eseguita l'analisi della causa principale sulle vulnerabilità rilevate, al fine di consentire al personale addetto allo sviluppo di andare oltre la correzione dei singoli problemi quando si presentano.

Inoltre, il fornitore deve redigere la procedura di gestione del *change management* che deve essere condivisa con il servizio gestore competente per il sistema. Tale procedura dovrà almeno prevedere le seguenti caratteristiche:

- **RA19**: sono definite politiche e/o procedure per la gestione dei cambiamenti alle configurazioni degli asset, compresi i casi di emergenza;
- **RA20**: le proposte di cambiamento alle configurazioni sono analizzate per verificare gli impatti sulla sicurezza e classificate sulla base del rischio;
- **RA21**: i cambiamenti alle configurazioni sono pianificati e approvati prima di essere messi in produzione;
- **RA22**: viene utilizzato un sistema di gestione centralizzato delle configurazioni;
- **RA23**: i cambiamenti alle configurazioni eseguiti vengono registrati;
- **RA24**: i cambiamenti alle configurazioni sono verificati dopo essere stati messi in produzione;
- **RA25**: viene utilizzato un sistema di controllo delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.

7 Studi clinici

Nel caso il sistema software, nel corso dell'appalto, venga utilizzato anche per la raccolta dati per sperimentazioni cliniche il fornitore dovrà compilare le parti di sua competenza dell'apposita checklist e fornire la documentazione richiesta per la validazione del software secondo le linee guida EMA/GCP.

Il fornitore si deve rendere inoltre disponibile a garantire la catena di tracciabilità delle sperimentazioni gestendo la codifica aziendale degli studi clinici da associare ai pazienti arruolati nello studio stesso e garantire un accesso adeguatamente profilato a tali pazienti ai data manager e study coordinator aziendali nonché alle figure dei monitor, in base alle indicazioni fornite dal Servizio ICT.

8 Verifiche e controlli

Nell'ambito nel proprio ruolo di Titolare dei dati trattati e dei processi aziendali di gestione del rischio inerenti alla catena di approvvigionamento cyber, l'IRCSS effettua attività di controllo della fornitura mediante audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali.

In particolare, i fornitori sono monitorati, a campione o periodicamente, per verificare il rispetto dei requisiti contrattuali di cybersecurity (es. tramite questionari, audit di seconda parte, verifica delle certificazioni possedute). L'IRCCS potrà inoltre utilizzare strumenti automatizzati (es. cyber threat intelligence) per monitorare e valutare il livello di rischio cyber dei propri fornitori in relazione ai componenti e servizi forniti.

L'IRCCS inoltre terrà monitorate periodicamente le attività del personale del fornitore impegnato nell'erogazione del servizio per individuare eventuali variazioni nella conduzione delle stesse e rilevare di conseguenza potenziali eventi di sicurezza.