AZIENDA SANITARIA LOCALE ROMA 1

DISCIPLINARE TECNICO

per l'integrazione di sistemi con l'infrastruttura IT

Versione: 2.0

Data: **Giugno 2025**

Documento conforme a GDPR 90/2024, ISO/IEC 27001:2022 e Direttiva NIS2

UOC Sistemi e Tecnologie Informatiche – ASL Roma 1

Tabella delle Revisioni

Versione	Data	Descrizione Modifica	Redatto da
2.0	08/2025	Riformulazione conforme a NIS2, ISO/IEC 27001:2022 e GDPR 90/2024	CISO ASL Roma1 Stefano Scaramuzzino

Nome e Cognome	Ruolo	Firma / Data
Presentato da: Stefano Scaramuzzino	CISO/NIS2 – ASL Roma 1	Firmato digitalmente da: STEFANO SCARAMUZZINO Organizzazione: ASL ROMA 1/13664791004 Data: 20/08/2025 12:57:16
Approvato da: Giuseppe Guarnieri	Direttore UOC STI – ASL Roma 1	Firmato digitalmente da: GIUSEPPE GUARNIERI Organizzazione: ASL ROMA 1/13664791004 Data: 20/08/2025 14:50:36

TABELLA TERMINI E ABBREVIAZIONI

Termine / Abbreviazione	Descrizione
Account	Funzionalità e contenuti assegnati a un utente in un contesto operativo.
Active Directory (AD)	Servizi Microsoft per la gestione centralizzata di utenti, computer, e risorse.
AGID	Agenzia per l'Italia Digitale – emana linee guida per la digitalizzazione della PA.
Backup	Copia di sicurezza di dati per prevenire perdita permanente.
Client	Componente che richiede servizi da un server.
DHCP	Protocollo che assegna dinamicamente la configurazione IP ai dispositivi.
DNS	Sistema che risolve i nomi in indirizzi IP.
Indirizzo IP	Codice numerico che identifica univocamente un dispositivo in rete.
IAM	Identity Access Management – sistema per gestione centralizzata degli accessi.
LAN	Rete locale che collega computer e dispositivi in un'area ristretta.
RDBMS	Sistema di gestione per database relazionali.
Server	Sistema che fornisce servizi a client in una rete.
Single Sign-On (SSO)	Accesso unico per autenticarsi a più sistemi o applicazioni.
VLAN	Rete logica isolata all'interno di una rete fisica condivisa.
VPN	Rete privata virtuale per connessioni sicure su rete pubblica.
WSUS	Sistema Microsoft per la gestione centralizzata degli aggiornamenti.
PAM	Privileged Access Management – controllo degli accessi con privilegi elevati.
SIEM	Security Information and Event Management – sistema per log management e analisi sicurezza.
DPIA	Data Protection Impact Assessment – valutazione impatto sulla protezione dei dati.
ISO/IEC 27001	Norma internazionale per la gestione della sicurezza delle informazioni.
NIS2	Direttiva UE 2022/2555 sulla sicurezza delle reti e dei sistemi informativi.
GDPR 90/2024	Normativa italiana di adeguamento al Regolamento UE 2016/679.

Scopo

La presente procedura disciplina gli obblighi, le misure tecniche e organizzative e le modalità di integrazione di sistemi informatici e dispositivi, forniti da ditte terze, con l'infrastruttura IT di ASL Roma 1, al fine di garantire:

- Che il sistema nel suo complesso sia coerente con le politiche di sicurezza e di privacy dell'Azienda Asl Roma 1 e più in generale funzioni nel rispetto delle norme di buona tecnica, delle "best practice", dei regolamenti, delle norme tecniche e della legislazione vigente, in particolar modo in materia di sicurezza e privacy
- Coerenza con le politiche di sicurezza, privacy e business continuity dell'Azienda;
- Conformità al Regolamento UE 2016/679, al D.Lgs. 90/2024 (attuativo italiano del GDPR), alla Direttiva (UE) 2022/2555 (NIS2) e alla norma ISO/IEC 27001:2022;
- L'adozione delle Misure Minime di Sicurezza ICT (Circolare AGID 2/2017);
- Garantire collaborazione attiva da parte dei fornitori nella documentazione, nell'analisi dei rischi e nella gestione della sicurezza.

Campo di applicazione

Il presente disciplinare si applica a tutti i sistemi, dispositivi hardware/software, apparecchiature IT, elettromedicali, soluzioni SaaS/PaaS/IaaS, che necessitino di connessione, scambio dati o gestione integrata con l'infrastruttura IT dell'Azienda ASL Roma 1.

Definizioni e riferimenti normativi

Principali riferimenti normativi:

- Regolamento (UE) 2016/679 (GDPR)
- D.Lgs. 90/2024 – Adeguamento italiano al GDPR
- Direttiva (UE) 2022/2555 (NIS2)
- ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni (ISMS)
- ISO/IEC 27002:2022 – Controlli di sicurezza
- ISO/IEC 80001 – Gestione del rischio IT in ambito sanitario
- D.Lgs. 82/2005 (CAD) e D.Lgs. 217/2017
- Circolare AGID 2/2017 – Misure minime di sicurezza ICT per la PA

Adempimenti dell'aggiudicatario

L'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'Azienda Asl Roma 1 è chiamata a redigere in ottemperanza alla circolare AGID 18 Aprile 2017, n. 2/2017

Il collaudo dell'intero sistema sarà condizionato alla redazione e sottoscrizione da parte del fornitore di un accordo di responsabilità (responsibility agreement) redatto secondo i dettami della norma IEC 80001. Tale documento farà esplicito riferimento all'installazione presso l'Azienda Asl Roma 1, nei modi e nei termini definiti dal presente documento e che verranno a presentarsi all'atto pratico dell'installazione e della manutenzione del sistema nel tempo.

Il responsibility agreement dovrà riportare espliciti riferimenti alla "marcatura CE" degli eventuali dispositivi offerti ed al fatto che i requisiti essenziali di sicurezza non vengano inficiati nella specifica installazione presso l'Azienda Asl Roma 1, così come intesa sopra.

Il responsibility agreement verrà redatto in relazione al contratto stipulato con il fornitore facendo riferimento allo scenario individuato e alle specifiche assunzioni di responsabilità.

Sommario

Requisiti Generali

Tutti i sistemi forniti devono:

- Essere **marcati CE** e conformi alle normative sanitarie e tecniche applicabili;
- Non risultare End-of-Life o End-of-Support;
- Garantire la **separazione dei dati** personali/sanitari/logistici e una gestione conforme ai principi di **privacy by design** e **by default** (art. 25 GDPR);
- Essere dotati di **meccanismi di autenticazione robusta** (MFA, SSO con AD, integrazione con IAM aziendale);
- Rispettare i requisiti di sicurezza minimi (AGID), ma anche quelli **avanzati** previsti dalla ISO/IEC 27001:2022;
- Avere configurazioni, patch e aggiornamenti **gestiti**, **tracciabili** e **verificabili**, in linea con le policy aziendali.

5. INTEGRAZIONE CON INFRASTRUTTURA IT

I sistemi Hardware e software in uso in Azienda sono indicati in tassonomie, come previsto dalla vigente normativa NIS, attraverso il sistema di asset (CMDB) SecurityView, disponibile al seguente indirizzo:

PORTALE CMDB SecurityView

Il quale viene tenuto aggiornato dalla UOC Sistemi e Tecnologie Informatiche.

I sistemi oggetto di fornitura dovranno essere interfacciati o integrati con l'infrastruttura IT dell'Azienda Asl Roma 1 rispettando le direttive riportate di seguito e basate sullo specifico scenario di utilizzo.

I dispositivi dotati di connettività di rete (host) e che necessitano di collegamento alla rete dati per svolgere le proprie funzioni, potranno essere collegati solo se riconducibili ad uno dei seguenti scenari, mutuamente esclusivi:

- **Scenario 1**: Sistemi e/o dispositivi da integrare con la rete LAN o con i sistemi già presenti nell'Azienda Asl Roma 1 (es: integrazione con Active Directory o con altri software/sistemi già attivi) utilizzando in alcuni casi anche le risorse hardware preesistenti (es: hypervisor, infrastrutture cluster, ecc…).
- **Scenario 2**: Sistemi e/o dispositivi forniti dall'assegnatario che possono essere confinati ad una rete VLAN dedicata (isolamento totale dai sistemi dell'Azienda Asl Roma 1) e che prevedono l'utilizzo di hardware dedicato e non condiviso con quello preesistente.

SCENARIO 1 – Integrazione completa

In questo scenario l'aggiudicatario avrà la possibilità di integrare più strettamente i sistemi oggetto della fornitura con l'infrastruttura IT dell'Azienda Asl Roma 1, sia dal punto di vista della rete che dei server, facendo affidamento in generale sulle infrastrutture di virtualizzazione e cloud ,e sui servizi di rete preesistenti. Tale scenario è applicabile per esempio nel caso dell'implementazione di sistemi la cui fornitura non preveda l'installazione di hardware dedicato e può usufruire di sistemi di autenticazione basati su Active Directory.

le caratteristiche peculiari dell'infrastruttura informatica dell'Azienda Asl Roma1 sono determinate nel capitolo "Infrastruttura esistente" in questo documento, definendo inoltre le specifiche di interfacciamento all'infrastruttura esistente alle quali i sistemi oggetto di fornitura dovranno adeguarsi.

L'architettura generale e le caratteristiche dei singoli elementi dei sistemi forniti dovranno in ogni caso essere coerenti con le direttive indicate nel presente documento e andranno preventivamente valutate e concordate con il servizio informatico dell'Azienda.

SCENARIO 2 - Rete isolata o VLAN dedicata

Lo scenario 2 comprende a sua volta due tipologie di seguito esposte:

SCENARIO 2A

In questo scenario, i sistemi che sono oggetto della fornitura e che non necessitano di connettività di rete (es: air gapped) dovranno essere conformi alle misure minime e alle normative privacy vigenti.

Inoltre la gestione del patching e della manutenzione di tali sistemi andrà esclusivamente gestita in locale, escludendo qualsivoglia sistema di gestione remota. Sarà pertanto onere del fornitore provvedere all'aggiornamento periodico dei sistemi non connessi alla rete in conformità alle misure minime indicate nell'Allegato n.2 – "Requisiti di conformità in ambito security".

SCENARIO 2B

Ai sistemi che non devono interfacciarsi con la rete di Asl Roma 1 ma che necessitano di connettività di rete per svolgere le loro funzioni, verrà assegnata una specifica classe di indirizzi IP (statici o dinamici) coerente con il

piano di indirizzamenti dell'Azienda Asl Roma 1 e tali dispositivi verranno inseriti in una VLAN dedicata dalla quale potranno effettuare solo il traffico necessario per svolgere le funzioni richieste e il traffico relativo all'assistenza remota da parte del fornitore. La disciplina del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali, stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico**. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall**.

Gli host forniti saranno soggetti a filtraggio della navigazione Internet. Potranno essere implementate specifiche eccezioni all'autenticazione basate su IP sorgente che consentiranno il traffico esclusivamente verso IP e porte specifiche. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'Azienda Asl Roma 1 per la definizione delle suddette eccezioni.

Nel presente scenario l'aggiudicatario sarà responsabile in toto delle prescrizioni in ambito di sicurezza informatica e privacy, secondo quanto previsto dal quadro legislativo e normativo vigente, nonché dal presente documento; in particolare per quanto riguarda le politiche di: autenticazione, autorizzazione e accounting (AAA), di backup e disaster recovery, sugli aggiornamenti di sicurezza di tutti i software installati sugli host oggetto di assistenza, di protezione antivirus e da altre tipologie di cyber attacco.

Si specifica infine che, qualora l'aggiudicatario aderisca al presente scenario, sono da intendersi oggetto di fornitura anche eventuali PC client ed eventuali server fisici che si rendessero necessari, nonché qualsivoglia dispositivo necessario al corretto e sicuro funzionamento dei sistemi oggetto di fornitura.

Gli eventuali server o dispositivi di storage forniti dovranno essere conformi con gli standard per l'installazione a rack 19"; dovranno inoltre essere dotati di requisiti di ridondanza sufficienti a garantirne almeno la continuità operativa (es: doppio alimentatore, doppio storage controller, gruppo di continuità, etc) e laddove possibile anche l'alta affidabilità (HA). Non dovranno infine essere utilizzati per alcun motivo come postazioni di lavoro da parte degli operatori.

Per quanto concerne l'accesso remoto tramite VPN ai dispositivi oggetto della fornitura, a fronte della connessione VPN effettuata tramite i sistemi messi a disposizione dall'Azienda Asl Roma 1, il collegamento ai singoli host oggetto di assistenza dovrà avvenire esclusivamente con gli strumenti istituzionalmente utilizzati da ASL Roma 1, nel rispetto delle modalità previste dal quadro legislativo e normativo vigente, previa validazione degli strumenti stessi e della loro specifica configurazione da parte del servizio informatico dell'Azienda Asl Roma 1.

Per rispondere ad eventuali esigenze di monitoraggio continuativo da remoto da parte del fornitore dello stato dei sistemi che sono oggetto della fornitura, lo strumento messo a disposizione dall'Azienda Asl ROMA 1, a fronte di specifica configurazione, consentirà al fornitore di tenere costantemente sotto controllo lo stato dei servizi e dei dispositivi oggetto della fornitura.

Infrastruttura esistente.

L'Azienda Asl Roma 1 dispone di un directory service aziendale basato su dominio Active Directory (AD). In ciascuno dei principali siti AD (Ospedale Santo Spirito, Ospedale San Filippo Neri) è presente almeno un domain controller global catalog.

Ogni account del directory service aziendale è associato ad almeno un gruppo di dominio (gruppi locali al dominio, local domain) corrispondente alla struttura amministrativa Azienda Asl Roma 1 di appartenenza.

Gli aggiornamenti di sistema per i client e per i server vengono distribuiti tramite il servizio Microsoft WSUS.

Il protocollo di rete in uso nelle reti LAN dell'Azienda Asl Roma 1 è IPv4. Presso le sedi è attivo un servizio DHCP bilanciato che rilascia indirizzi IP agli host in rete configurati con IP dinamico, ad esclusione dei server (per i quali sono previste specifiche configurazioni) e degli host con IP riservato (rilasciato solo in determinate situazioni di emergenza dove non è possibile effettuare una risoluzione DNS). La risoluzione dei nomi è basata esclusivamente sul servizio DNS, integrato in AD, che accetta solo registrazioni sicure.

Tutti i server aziendali appartengono a subnet IP dedicate per ciascun sito AD.

GLI OBBLIGHI QUINDI PER L'INSERIMENTO NEL PERIMETRO AZIENDALE SONO:

Scenario 2 – Integrazione completa

- Obbligo di adesione a dominio Active Directory aslroma1.it;
- Compatibilità con antivirus Sophos Central;
- Inserimento di agenti: SYSMON, QRADAR, WAZUH, RSYSLOG;
- Rispetto della matrice di compatibilità OS (Win 11 24H2+, Ubuntu LTS, Oracle Linux 8.x+, RHEL LTS, Windows Server 2022-2025);
- Utilizzo di ambienti virtualizzati (Nutanix, VMware);
- Backup su Veeam, NAS, tape library;
- Adeguamento alle policy di patching, aggiornamento, logging, autenticazione e hardening;
- Obbligo di accettare WSUS, PAM, VPN client-site autorizzate;
- Obbligo di redigere **Responsibility Agreement** secondo IEC 80001.

Scenario 2 – Rete isolata o VLAN dedicata

- Utilizzo di VLAN e ACL;
- Nessuna connessione diretta alla rete core aziendale;
- Fornitore responsabile dell'intero ciclo di gestione IT e sicurezza;
- Obbligo di garantire segregazione, autenticazione, backup, crittografia, tracciabilità;
- Patching locale, tracciatura accessi, VPN autorizzata previo validazione;
- Host soggetti a filtraggio e profilazione.

OBBLIGHI DEL FORNITORE (EXTENDED)

Oltre agli obblighi previsti dal disciplinare originario, si aggiungono:

- **Nomina di un Responsabile Privacy di progetto** (GDPR art. 28 e 29; ISO 27001:2022 – clausola A.6.1.1);
- Redazione del **Piano di Sicurezza Applicativa** in conformità alla ISO 27001:2022 (Allegato 3);
- Collaborazione alla **valutazione d'impatto (DPIA)** ove necessario (art. 35 GDPR);
- Obbligo di redigere un Inventario asset IT e di aggiornare la lista software autorizzato;
- Implementazione di standard di hardening e autenticazione forte;

- Gestione **account privilegiati** separati da quelli ordinari (con tracciabilità e scadenze password);
- Adozione di **crittografia AES-256** per dati sensibili;
- Obbligo di fornire report vulnerabilità e remediation tracking.

Backup

La struttura di backup dell'Azienda Asl Roma 1 è basata sulla presenza di due tape library (Nomentana e San Filippo Neri), 3 nas repository dislocati in ciascuna delle tre sedi principali, un repository immutabile per le vm e un servizio di backup in repository remoto per le vm più critiche.

Tramite il software per i backup (Veeam), con periodicità variabile a seconda dei casi – vengono effettuate le copie di sicurezza: dei sistemi operativi di tutti i server Azienda Asl Roma 1, della configurazione dei DB, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi.

In riferimento all' effettuazione del backup delle macchine virtuali Aslroma1 fornirà un template con compilazione a cura del fornitore delle vm.

Il template sarà così strutturato:

  - Nome VM : nome della macchina virtuale su cui eseguire il backup
  - Sistema Operativo: sistema operativo della vm
  - Fornire dati RPO/RTO desiderate
  - Schedulazione backup (orario partenza del job) se richiesto, altrimenti la schedulazione verrà configurata dai sistemisti di Aslroma1 in base ai carichi dei job
  - Tipologia di backup: viene utilizzata la configurazione determinata da Aslroma1
- NB: i Backup dei database sono a carico del fornitore, in base al sistema operativo su cui risiede il db si prevedono 2 opzioni:
- Ambiente Windows: Il backup del db deve essere effettuato dal fornitore in un disco separato ripsetto a dove risiede il db stesso; il disco viene messo a disposizione da Aslroma1 e sarà agganciato direttamente alla vm
- Ambiente Linux: Aslroma1 fornirà l' indirizzo di una share NFS su cui il fornitore dovrà effettuare il backup.La gestione del server NFS è in carico ad Aslroma1

Postazioni Client

Le postazioni di lavoro client prevedono una matrice di compatibilità di sicurezza di seguito presentata:

- Il sistema operativo dovrà essere Microsoft Windows dalla versione 11 24H2 (e comunque fuori OTS)
- La postazione Client dovrà obbligatoriamente essere inserita nel dominio aziendale aslroma1.it/aslroma1.local. (eventuali richieste in deroga per amministrazione locale dei sistemi dovrà essere comunque asseverata con utenza di dominio e relativo ribaltamento su local).
- L'applicativo antivirus (AV) aziendale è Sophos Central il quale è dotato di alcuni moduli aggiuntivi per la endpoint security XDR, EDR e (in servizio) MDR. Non è possibile derogare o installare altre sonde/antivirus, come non è consentito isolare eccezioni, il fornitore dunque dovrà dichiarare in sede di gara eventuali incompatibilità con questa postura.
- All'interno del client sono inoltre inseriti **SYSMON** e gli agenti:
  - **QRADAR**
  - **WAZUH**

In conclusione: eventuali PC o apparati oggetto di fornitura, qualora dispongano di sistema operativo Microsoft Windows, dovranno essere configurati come membri del dominio aslroma1.it in modo da essere conformi con le policy di dominio applicate ai computer dell'Azienda Asl Roma 1.

Non saranno accettati client lasciati in "workgroup" o con dominio diverso da aslroma1.it.

Serventi di sistema

Sono presenti in infrastruttura, sia elementi virtuali che fisici.

Gli elementi fisici dovranno seguire le stesse indicazioni delle configurazioni in virtuale.

Sono presenti due sistemi di virtualizzazione:

- **Nutanix 7.0**
- **VMWare 6.7**

Dispiegati presso la sede CED di San Filippo Neri (nutanix), e Santo Spirito (VMWare), dotati di ridondanza a livello di HA (High Availability).

Nel presente scenario, gli eventuali server virtuali oggetto della fornitura dovranno essere implementati utilizzando le seguenti versioni di sistema come da matrice di compatibilità presenti nel sistema dell'Azienda ASL Roma 1:

- Il sistema operativo dovrà essere:
    - **Os Linux UBUNTU (tutte le versioni che supportano versioni LTS - Long Term Support).**
    - **Os Linux Oracle dalla versione 8.x – 9.x (tutte le versioni che supportano versioni LTS - Long Term Support).**
    - **Os Linux RedHat (tutte le versioni che supportano versioni LTS - Long Term Support).**
    - **Os Microsoft Server da versione 2022 fino a 2025 (tranne quelle che andranno in EOS)**
- La postazione server dovrà obbligatoriamente essere inserita nel dominio aziendale **aslroma1.it** (eventuali richieste in deroga per amministrazione locale dei sistemi dovrà essere comunque asseverata con utenza di dominio e relativo ribaltamento su local).
- L'applicativo antivirus (AV) aziendale è **Sophos Central** il quale è dotato di alcuni moduli aggiuntivi per la endpoint security XDR, EDR e (in servizio) MDR. Non è possibile derogare o installare altre sonde/antivirus, come non è consentito isolare eccezioni, il fornitore dunque dovrà dichiarare in sede di gara eventuali incompatibilità con questa postura.
- All'interno del server dovranno essere inoltre inseriti gli agenti:
    - **QRADAR/SYSMON (per i sistemi Microsoft)**
    - **WAZUH**
    - **RSYSLOG (per i sistemi Linux)**

Di conseguenza tutte le configurazioni relative ai sistemi e ai software in esse presenti dovranno rispecchiarne le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, di backup e di disaster recovery.

Potranno essere messe a disposizione dell'aggiudicatario una o più VM (macchine virtuali) rispecchiando l'architettura proposta, assegnando sufficienti risorse hardware in base alle specifiche necessità.

Tali risorse devono essere definite in fase di contrattualizzazione e non potranno subire ulteriori escalation, non sono previsti contestualmente ambienti di Test e Collaudo, ma solo un'area di staging per il collaudo e la messa in produzione.

Sarà successivamente sarà cura del fornitore, introdurre sistemi in appoggio per eventuali staging di test, o specificatamente in sede di gara andranno determinate ed approvate risorse aggiuntive che devono trovare spazio nella disponibilità di virtualizzazione aziendale.

Dal punto di vista dei sistemi operativi, l'assegnatario proporrà al servizio informatico dell'Azienda Asl Roma 1 un ventaglio di possibili scelte (contenute all'interno del perimetro definito in narrativa) al fine di selezionare la più opportuna, sia per garantire la piena compatibilità con la piattaforma di virtualizzazione in uso, sia per omogeneità con i sistemi operativi già presenti nell'infrastruttura.

In linea generale laddove si debbano implementare VM con sistema operativo Windows Server, è obbligatorio legare tali VM al dominio aslroma.it e conseguentemente al sistema di aggiornamento WSUS dell'Azienda Asl Roma 1.

Le licenze dei sistemi operativi (es: Windows Server) necessarie al funzionamento del sistema sono da intendersi a carico del fornitore (ove non determinato in sede di gara) e non dovranno essere in alcun caso di tipo OEM, bensì licenze intestate all'Azienda Asl Roma 1 e comunque in ogni caso compatibili con l'ambiente di virtualizzazione dell'Azienda Asl Roma 1 descritto precedentemente.

Allo scopo di uniformare i sistemi forniti agli standard Aziendali di Asl Roma 1, compresi quelli di sicurezza e autorizzazione, nel contesto di Active Directory tali server verranno inserite in una Organizational Unit (OU) generica dedicata ai server Azienda Asl Roma 1 oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l'Azienda Asl Roma 1; la default domain policy verrà applicata in ogni caso su tutte le OU.

Per quanto concerne la connettività di rete, ai server verrà assegnato un range di indirizzi IP statici nella rete della LAN aziendale o, se lo si dovesse ritenere necessario, in una subnet di rete dedicata al servizio.

Dal punto di vista degli aggiornamenti dei sistemi operativi Microsoft Windows, è già presente un'infrastruttura server WSUS per l'aggiornamento centralizzato dei sistemi Windows alla quale andranno legati anche i server virtuali oggetto della fornitura.

DATABASE

Nel presente scenario, i dati acquisiti e generati dal sistema e/o i loro riferimenti, nonché tutti quelli direttamente o indirettamente necessari al funzionamento degli applicativi forniti, dovranno essere organizzati in uno o più RDBMS, che potranno essere istanziati su server Oracle di cui già dispone l'Azienda Asl Roma 1 o in nuovi RDBMS basati su altre piattaforme a discrezione dell'aggiudicatario, sempre previa valutazione con il servizio informatico al fine di stabilire l'eventuale conformità con le attuali politiche di sicurezza e compatibilità/sostenibilità con l'attuale sistema di backup e disaster recovery. In quest'ultimo caso l'aggiudicatario dovrà farsi carico di fornire le licenze d'uso per gli RDBMS forniti e della gestione delle politiche di backup se non integrabili con l'attuale sistema di backup e disaster recovery.

RDBMS Oracle in matrice di compatibilità: Oracle 19.x e superiori

Applicativi web-based

Nel presente scenario, gli applicativi destinati all'utilizzo da parte degli utenti dovranno essere basati su tecnologia web-based, sarà necessario analizzare e verificare la compatibilità di tali applicativi con i browser web e relativi plugin approvati dal servizio informatico per l'utilizzo dalle varie postazioni di lavoro dell'Azienda Asl Roma 1.

La matrice di compatibilità dei sistemi container browser sono:

- Microsoft Edge (non EOS)
- Google Chrome (non EOS)
- Safari versione (non EOS)

Applicativi Client/Server

Gli eventuali applicativi destinati all'installazione client server, lato client dovranno essere adeguati alle caratteristiche software e hardware delle postazioni di lavoro e dovranno garantire piena compatibilità con le policy del dominio Active Directory e con i software già installati nelle postazioni di lavoro.

La distribuzione di tali applicativi sulle postazioni di lavoro dell'Azienda Asl Roma 1, nonché degli aggiornamenti, verrà eseguita per mezzo del sistema di software distribution di Active Directory, ovvero tramite pacchetti MSI (Microsoft Installer). In alternativa, nel caso in cui non fosse possibile effettuare il deployment centralizzato di tali applicativi, l'installazione verrà effettuata – con analoghe caratteristiche qualitative e di risultato – a carico dell'aggiudicatario (ove non diversamente specificato in sede di gara).

Il fornitore deve fornire inoltre una matrice dei flussi specifici del traffico dati da consentire all'interno del perimetro infrastrutturale di ASL Roma 1.

Nel presente scenario, se non diversamente comunicato dall'aggiudicatario, i sistemi operativi Microsoft Windows verranno aggiornati tramite WSUS installando tutte le patch rilasciate da Microsoft che verranno approvate dagli amministratori. Le configurazioni di rete dei PC/apparati oggetto della fornitura dovranno garantite compatibilità con il sistema di indirizzamento IP dinamico (DHCP) attivo in generale sui client dell'Azienda Asl Roma 1.

Nel caso in cui l'architettura e le caratteristiche tecniche dei sistemi forniti impedissero tale configurazione, l'aggiudicatario sarà tenuto a redigere una relazione tecnica che giustifichi tale evenienza già in fase di gara (**non verranno ritenute idonee deroghe "dopo" l'assegnazione**) e sulla base della quale l'Azienda Asl Roma 1 si riserva di creare sul servizio DHCP opportune e specifiche configurazioni (reservation).

Nel presente scenario, le funzionalità dei PC/apparti forniti dovranno essere in grado di poter garantire piena compatibilità con l'antivirus presente nell'Azienda Asl Roma 1, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'Azienda Asl Roma 1, a meno di eccezioni concordate con il servizio informatico.

Eventuali PC/apparati non Windows già presenti nel perimetro, e che non sono rientrati nelle regole di questo disciplinare, che non siano compatibili con l'Active Directory e che necessitano di connettività con la rete dati Azienda Asl Roma 1, non potranno essere connessi alla stessa, ma segregati con specifici indirizzi IP statici di perimetro esclusivo riguardante l'operatività del sistema ed assegnati dal servizio informatico dell'Azienda Asl Roma 1.

La gestione del patching O.S. di tali sistemi è comunque obbligatoria ed è a carico dell'aggiudicatario .

Ovviamente questa eventualità è categoricamente esclusa per quanto riguarda le nuove acquisizioni, che sono regolamentate con i capoversi precedenti.

OBBLIGO DI SUPERAMENTO TEST DI VULNERABILITY ASSESSMENT E PENETRATION TEST

In ottemperanza ai seguenti riferimenti normativi:

- Regolamento UE 2016/679 e D.lgs. 90/2024 – artt. 5, 25, 32, 35 (principi di privacy by design, sicurezza dei trattamenti e valutazioni d'impatto);
- Direttiva (UE) 2022/2555 – NIS2, art. 21 (obbligo di test di sicurezza e gestione vulnerabilità per soggetti essenziali e importanti);
- ISO/IEC 27001:2022, controlli:
  - A.5.25 – *Response to Information Security Incidents*,
  - A.8.8 – *Management of Technical Vulnerabilities*,
  - A.5.26 – *Collection of Evidence*;

ASL Roma 1 rende obbligatoria l'esecuzione e il superamento di test di Vulnerability Assessment (VA) e Penetration Test (PT) su ogni sistema oggetto di fornitura prima della messa in esercizio (Go-Live).

Modalità operative

Il fornitore dovrà:

- Pianificare i test di VA/PT con il CISO di ASL Roma 1 entro le fasi conclusive del collaudo tecnico-funzionale.
- Utilizzare metodologie riconosciute (es. OWASP, NIST SP800-115, OSSTMM).
- Condividere con l'UOC Sistemi e Tecnologie Informatiche i seguenti deliverables:
  - Scope dell'infrastruttura coinvolta;
  - Finestra temporale prevista;
  - Lista delle vulnerabilità riscontrate (report ufficiale firmato);
  - Proposte di remediation.
  - Criteri di accettazione e blocco messa in produzione

La messa in produzione è vincolata al superamento dei test VA/PT.

- Se il CVSS (Common Vulnerability Scoring System) rilevato da VA/PT evidenzia:
  - **Vulnerabilità critiche** con score **≥ 9.0** → *messa in produzione bloccata fino a risoluzione completa*;
  - **Vulnerabilità gravi** (score **≥ 7.0**) → *obbligo di applicazione remediation entro 10 giorni lavorativi* e nuova validazione UOCSTI;
  - **Vulnerabilità medio-basse** (score < 7.0) → *remediation entro 30 giorni o mitigation accettata da UOCSTI con documentazione tecnica*.

Verifiche cicliche ASL Roma 1

ASL Roma 1 effettuerà mensilmente vulnerability scanning centralizzati su tutto il perimetro dei sistemi attivi. I fornitori sono tenuti a:

- Garantire la compatibilità dei propri sistemi con gli strumenti di scansione (es. Nessus, OpenVAS, Qualys, Wazuh, etc.);
- Rispondere alle richieste di remediation entro i tempi stabiliti dalla UOCSTI;
- Partecipare agli audit e controlli straordinari in caso di allerta nazionale (CERT/CSIRT, ACN).

Clausola risolutiva espressa

L'inosservanza dei criteri di accettazione sopra esposti, ovvero il mancato adeguamento alle remediation entro le scadenze previste, comporterà:

- La sospensione della fornitura fino a completa sanatoria;
- La risoluzione contrattuale nei casi di reiterata mancata conformità;
- La segnalazione all'ACN o Garante Privacy, ove previsto per violazione dei principi di sicurezza e continuità operativa.

Teleassistenza e Remotizzazione.

In caso di necessità di interventi in teleassistenza da remoto da parte del personale tecnico dell'aggiudicatario durante il periodo di validità del contratto, l'accesso agli host oggetto di assistenza **sarà garantita esclusivamente per mezzo di accesso tramite la piattaforma di Privileged Access Management (PAM)** dell'Azienda Asl Roma 1. Il personale tecnico potrà ottenere l'accesso alla piattaforma PAM solo a fronte della compilazione del modulo specifico che dovrà essere inviato per validazione al servizio informatico dell'Azienda Asl Roma 1.

La connessione sarà effettuata necessariamente utilizzando credenziali personali, utilizzando un doppio livello di autenticazione (pwd + OTP). Il secondo fattore di autenticazione sarà disponibile mediante invio codice tra- mite e-mail o tramite applicazione Google Authenticator. Non sono ammessi accessi utilizzando esclusivamente credenziali di tipo utenza/pwd.

La connessione al sistema avverrà tramite protocollo https.

Nel caso in cui l'aggiudicatario non fosse in condizione di poter garantire tale configurazione per valide ragioni tecniche, sarà tenuto a redigere una relazione che giustifichi tale evenienza sulla base della quale l'Azienda Asl Roma 1 si riserverà di attivare connessioni di tipo VPN client-to-site o site-to-site (es: tunnel IPSec).

L'aggiudicatario dovrà garantire la tracciatura interna degli accessi effettuati da parte degli operatori che svol- gono interventi in assistenza remota. L'Azienda Asl Roma 1 si riserva inoltre la facoltà di richiedere in qualsiasi momento il report di tali accessi.

Le sessioni aperte tramite il sistema PAM verso gli host oggetto di assistenza potranno essere video registrate per finalità di monitoring e controllo, in quanto avverranno tramite utenze con privilegi amministrativi.

Per rispondere ad eventuali esigenze di monitoraggio continuativo da remoto dello stato dei sistemi che sono oggetto della fornitura, lo strumento messo a disposizione dall'Azienda Asl Roma 1, a fronte di specifica confi- gurazione, consentirà all'aggiudicatario di tenere costantemente sotto controllo lo stato dei servizi e dei dispo- sitivi oggetto della fornitura.

Single Sign-On (SSO)

Tutti gli applicativi software forniti devono essere integrabili con l'LDAP messo a disposizione dal servizio Active Directory. Il collegamento dovrà passare tramite canale cifrato TLS/SSL debitamente autenticato tramite credenziali di sola lettura. L'integrazione del software oggetto della fornitura con il servizio LDAP di Active Directory andrà discussa di volta in volta con il servizio informatico al fine di fornire tutte le specifiche necessarie all'implementazione.

Identity, Access & Governance Management (IAG)

Tutti gli applicativi software forniti devono essere integrabili con la piattaforma di Identity & Access Management dell'Azienda Asl Roma 1 (provisioning utenze e sistema di autenticazione centralizzato tramite Multi Factor Authentication). L'integrazione del software oggetto della fornitura con la piattaforma IAM andrà discussa di volta in volta con il servizio informatico al fine di fornire tutte le specifiche necessarie all'implementazione.

Altre soluzioni di SSO, autenticazione e account/identity management non saranno consentite.

Gestione accessi e teleassistenza.

Tutti gli accessi remoti devono avvenire tramite PAM aziendale con MFA (OTP/Authenticator);

- Le sessioni possono essere videoregistrate;
- Ogni intervento richiede autorizzazione formale previa validazione modulo tecnico;
- I fornitori devono garantire il tracciamento interno degli accessi;
- Sono vietati accessi con account generici o condivisi.

ARCHITETTURA DI RIFERIMENTO

Contesto architetturale

La soluzione dovrà essere installata e gestita sul **Polo Strategico Nazionale (PSN)**, in un'architettura "cloud-ready" che consenta:

- **Connettività privata e sicura PSN–ASL Roma 1** (VPN site-to-site/IPsec o collegamenti privati equivalenti) con segregazione per ambienti **DEV/TEST/UAT/PROD** e separazione dei domini amministrativi.
- **Integrazione con i servizi aziendali esistenti** (Directory, IAM/SSO, PAM, SIEM, Data Lake, sistemi di backup) tramite canali cifrati, autenticazione forte e tracciatura centralizzata.
- **Allineamento alle policy aziendali** di patching, logging, hardening e monitoraggio già in uso in ASL Roma 1, come previsto dagli scenari di integrazione e dall'infrastruttura esistente.

Zone/landing e sicurezza perimetrale

- **VPC/VNET perimetrate** con subnet dedicate per livelli (presentation, API, data), **ACL** e regole sui firewall coerenti con il principio del **minimo privilegio**.
- **WAF e protezioni L7** davanti ai servizi web esposti; **reverse proxy/API Gateway** come unico punto d'accesso applicativo da rete esterna e da rete interna.
- **Gestione segreti/chiavi** tramite KMS del PSN o equivalenti, con rotazione periodica e accessi tracciati (principio Zero Trust).

Continuità operativa e DR

- **Alta disponibilità intra-PSN** (ridondanza componenti critici) e **piani RPO/RTO** allineati alle esigenze clinico–amministrative.
- **Backup immutabili e replica** verso repository conformi alla strategia aziendale (Veeam e repository dedicati), con test periodici di restore.

Architettura della soluzione

La soluzione deve adottare un'architettura **browser-based a microservizi**, containerizzata e orchestrata (es. Kubernetes o equivalente), che garantisca:

Accessibilità e fruizione

- **Accesso via browser** (Edge/Chrome/Firefox/Safari nelle versioni supportate), senza componenti client proprietarie non necessarie. Interfacce **responsive** per uso da desktop e mobilità (laptop/tablet).
- **Autenticazione centralizzata** con **SSO (LDAP/AD)** e **IAM aziendale** con **MFA**, nel rispetto del divieto di SSO/IdM alternativi a quelli aziendali. **PAM** per accessi privilegiati e teleassistenza.

Interoperabilità e API

- **API REST/JSON** (preferenziali) e supporto a **SOAP** ove necessario; code/eventi (es. publish/subscribe) per integrazioni asincrone.
- **Standard sanitari**: esposizione/consumo di HL7 v2/v3 e **FHIR R4** per anagrafica pazienti/episodi, **XDS.b** per repository/dossier documentale, **DICOM** ove pertinenti ai flussi di imaging.
- **Catalogo API** con specifiche (OpenAPI/Swagger), versioning e **circuit-breaker** a livello di API Gateway.

Sicurezza applicativa by design

- **Hardening** dei container/base-image, scansione delle immagini in CI/CD, **segregazione dei secret** e enforcement del **principio di minimo privilegio** tra microservizi.
- **Logging centralizzato** (app, sicurezza, accessi, configurazioni) con inoltro ai **SIEM aziendali (QRadar/Wazuh/RSYSLOG)** secondo formati concordati.
- **Crittografia** in transito (TLS ≥1.2) e a riposo (dataset sensibili), gestione chiavi tramite KMS.
- **Conformità VA/PT**: la pipeline di rilascio deve prevedere gate di sicurezza e il **superamento dei test VA/PT** prima del go-live, con blocco alla presenza di vulnerabilità **CVSS ≥ 9.0** e remediation tracciata per **CVSS ≥ 7.0**.

Dati e persistenza

- **RDBMS** in matrice di compatibilità aziendale (es. **Oracle 19.x+**) o DB proposti previo allineamento con backup/DR; in caso di RDBMS terzi non integrabili, **licenze e gestione backup** sono a carico del fornitore.
- **Data retention** e **classificazione** coerenti con policy aziendali e normativa; tracciatura completa degli accessi ai dati sanitari e di audit.

Requisiti di licenza e manutenzione

- **Licenza d'uso enterprise** dell'intero sistema (compresi eventuali componenti/terze parti: DB, middleware, ecc.) **illimitata nel tempo e nel numero di utenti**, senza costi aggiuntivi per moduli/funzionalità previste in offerta; inclusi **aggiornamenti (major e minor)**, **patch di sicurezza** e **nuove feature** rilasciate dal fornitore per tutta la durata contrattuale.
- Le licenze **OS/RDBMS** necessarie sono intestate ad **ASL Roma 1** e compatibili con gli ambienti di virtualizzazione adottati (Nutanix/VMware).

Integrazioni con i sistemi e le politiche esistenti

La soluzione, **senza oneri aggiuntivi** per ASL Roma 1, deve integrarsi in modo nativo con i seguenti sistemi/processi aziendali, rispettando gli scenari di integrazione già definiti nel disciplinare:

Sistemi di interoperabilità esistente

- Adozione degli **standard sanitari** indicati (HL7/FHIR, XDS.b, DICOM).
- API pubblicate nel catalogo aziendale e sottoposte a approvazione UOC STI (versioning, sicurezza, throughput).

Anagrafiche centralizzate (pazienti, operatori, tabelle di dominio)

- **Master-data** univoci con **fonte autorevole** aziendale; sincronizzazione tramite API/eventi; gestione conflitti/merge.

Sistemi di centralizzazione dati (Repository, Dossier)

- Deposito e indicizzazione documenti clinici verso repository aziendali/dossier, con metadati conformi e tracciabilità accessi.

Active Directory aziendale

- **Join logico** per SSO/ruoli; mappatura **RBAC/ABAC** con gruppi AD e profili IAM; **PAM** per amministrazione.

Sistema di autenticazione e profilazione unica centralizzata (IAM/SSO)

- Integrazione con **LDAP/AD** via TLS/SSL e **MFA**; non sono consentite piattaforme SSO alternative.

Piattaforme di Business Intelligence (presenti e future)

- Esposizione di **dataset sicuri** (view/API) con mascheramento/anonymizzazione ove richiesto; **cadenza di aggiornamento** definita; lineage e glossario dati.

Licenze software esistenti (es. Oracle)

- Riuso ove possibile; in alternativa, fornitura licenze a carico dell'aggiudicatario, con piena compatibilità a **backup/DR** aziendali.

Patching, antivirus e logging

WSUS per Windows; **Sophos Central** per endpoint/server; agenti **Sysmon/QRadar/Wazuh/RSYSLOG** per raccolta log e **SIEM**; rispetto delle policy di filtri/ACL e VLAN ove si adottasse lo **Scenario 2**.

Teleassistenza e accessi remoti

Accessi esclusivamente tramite **PAM aziendale** con MFA e **session recording**; divieto di account generici; VPN/IPsec se autorizzata e validata.

Collaudo sicurezza

Obbligo VA/PT pre-produzione, criteri di blocco e remediation come da disciplinare; scansioni **mensili** sul perimetro e **clausola risolutiva** in caso di mancata conformità.

Nota di coerenza (non duplicazioni)

Per evitare ridondanze, questo capitolo **rimanda** ai seguenti punti del Disciplinare già presenti:

- **Scenari di integrazione e infrastruttura esistente** (AD, WSUS, DHCP/DNS, VLAN/ACL, virtualizzazione Nutanix/VMware, backup Veeam): v. **"Infrastruttura esistente", "SCENARIO 1/2", "Backup"**.
- **Applicativi web-based, browser supportati**: v. **"Applicativi web-based"**.
- **SSO/IAM/PAM e teleassistenza**: v. **"Single Sign-On (SSO)", "Identity, Access & Governance Management (IAG)", "Gestione accessi e teleassistenza"**.
- **Database/RDBMS e licenze**: v. **"DATABASE"**.
- **VA/PT e criteri di accettazione**: v. **"OBBLIGO DI SUPERAMENTO TEST DI VA/PT"**.

SICUREZZA E PRIVACY – OBBLIGHI MINIMI (ESTESI)

Riferimento a **ISO/IEC 27001:2022 – Annex A**, in particolare:

Controllo	Obbligo del fornitore
A.5.1	Politica di sicurezza approvata e firmata
A.6.1.2	Ruoli e responsabilità definiti e documentati
A.8.1.1	Asset registrati, classificati e aggiornati
A.9.2.2	Gestione degli account privilegiati (principio di minimo privilegio)
A.12.6.1	Patching entro 90 giorni o immediato in caso di CVE critico
A.14.1.1	Requisiti di sicurezza per lo sviluppo software
A.17.1.3	Test di continuità operativa e restore

TRACCIATURA, AUDIT, VULNERABILITÀ

- Ogni sistema deve generare **log di sistema, sicurezza, accesso e configurazione** integrabili nei SIEM aziendali;
- Devono essere previsti **audit periodici** (interni/esterni) con report accessibili;
- L'aggiudicatario deve notificare in forma scritta ogni **incidente di sicurezza**, secondo tempistiche definite dal CSIRT aziendale;
- Obbligo di partecipazione a eventuali verifiche ISP, Garante o altre autorità preposte.

DIFFUSIONE E ARCHIVIAZIONE

La procedura è archiviata in formato elettronico e/o cartaceo in tutti gli uffici/strutture interessati all'utilizzo e/o alla revisione del documento quali fra l'altro la dalla Direzione sanitaria aziendale e pubblicata in Intranet nell'area assegnata (TABULARIUM/ONEDRIVE).

La **copia originale** della procedura viene archiviata presso l'Ufficio qualità aziendale. La procedura approvata è disponibile nella **intranet aziendale**.

Il presente disciplinare viene:

- Pubblicato in Intranet aziendale;
- Inviato via PEC ai Direttori/Responsabili delle strutture richiedenti;
- Archiviato digitalmente nel sistema Tabularium;
- Conservato in copia originale presso l'Ufficio Qualità.

VERSIONE E REVISIONE

Versione 2.0 – Approvata in data [da completare].

Revisione prevista: annuale o a seguito di aggiornamenti normativi.

MODULISTICA E ALLEGATI

Vengono allegati al presente disciplinare i seguenti **modelli**:

- **Allegato A** – Modulo Presentazione Soluzione Tecnica
- **Allegato B** – Modulo Richiesta Integrazione IT
- **Allegato C** – Dichiarazione Conformità GDPR/ISO27001/NIS2
- **Allegato D** – Accordo di Responsabilità Privacy (IEC 80001)

Vengono inoltre definiti i seguenti ulteriori allegati:

Allegato 1 (Requisiti generali di conformità del software):

Tutti i dispositivi o sistemi forniti, per almeno un anno dal collaudo definitivo dei sistemi, dovranno essere provvisti di contratto di manutenzione da parte del fabbricante e non dovranno risultare a fine ciclo di vita (end- of-life) o fuori dal periodo di supporto (end-of support). In generale, tutti i software forniti dovranno essere:

- conformi alle misure minime di sicurezza ("Misure minime AGID");
- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
- dotati di interfaccia utente grafica (GUI) in Italiano configurata in modo che le impostazioni internazionali del sistema operativo e della tastiera siano conformi alla mappatura IT standard;
- stabili dal punto di vista del funzionamento;
- in grado di gestire le eccezioni a runtime;
- 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 practice 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;

- rilasciati in versione definitiva e non in “alpha-release”, “beta-release” o “release candidate”;
- ideati, progettati e realizzati nel rispetto del quadro legislativo vigente, nonché 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 dell’Azienda Asl Roma 1, 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.

Collegamento alla rete

Relativamente ai software che andranno installati su dispositivi collegati alla LAN dell’Azienda Asl Roma 1 e inseriti nel dominio aslroma1.it, la condizione è che tali software vengano eseguiti:

- in un contesto “user space” nei client (PC),
- come servizio di sistema nei server,
- come servizio di sistema nei client nei quali non sia prevista interazione con l’operatore,ed in ogni caso non dovranno essere modificati in alcun modo i permessi di default delle cartelle di sistema file system e del registro di sistema Microsoft (ove presente).

Configurazioni e dati

Relativamente alle configurazioni e ai dati:

- quelle degli applicativi server dovranno risiedere in database e comunque non nei dischi locali dei PC client;
- quelle globali degli applicativi client (ovvero non riferite alle personalizzazioni dei singoli account) dovranno risiedere in un file nella cartella 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 in HKEY_LOCAL_MACHINE\SOFTWARE. In ogni caso le informazioni critiche in termini di sicurezza e funzionalità (a titolo di esempio non esaustivo: le stringhe di connessione ai database, le credenziali necessarie per instaurare eventuali altre connessioni client/server, ecc.) dovranno essere cifrate almeno con algoritmo AES-256;
- 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 sintesi, le configurazioni globali degli applicativi client non dovranno mai risiedere nei profili degli utenti, mentre le configurazioni personali degli applicativi client dovranno sempre e solo risiedere nei profili degli utenti.

Privacy e sicurezza

L’aggiudicatario dovrà individuare, all’interno della sua organizzazione, un “Responsabile per la privacy”. Questi verrà in tal senso nominato dal titolare del trattamento dei dati personali dell’Azienda Asl Roma 1 e dovrà inviare, nel rispetto delle procedure dell’Azienda, le richieste di abilitazione degli incaricati e degli amministratori afferenti all’aggiudicatario (anche quelle necessarie per lo svolgimento delle attività di assistenza remota). I relativi account e le relative autorizzazioni verranno sempre erogate dall’Azienda Asl

Roma 1 e a livello personale, secondo le proprie procedure ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

In tutti i software forniti che si configurano come "strumenti elettronici" che effettuano trattamento di dati personali, così come definito nel D.Lgs. 196/03 "Codice in materia di trattamento dei dati personali" e s.m.i., dovranno essere adottate:

- le "misure minime di sicurezza" previste dal suddetto codice e dal relativo disciplinare tecnico (Allegato B, D.Lgs. 196/03);
- le "idonee e preventive misure di sicurezza" previste dal medesimo codice all'art. 31 nell'ambito degli obblighi di sicurezza;
- le prescrizioni della Circolare AGID del 18 aprile 2017, n.2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" – vedi allegato n.2 Dovranno essere rispettati tali obblighi in particolare in termini di:
- ◦ adozione di un "sistema di autenticazione informatica", comunque nel rispetto di quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relativecredenziali – personali
- ◦ adozione di un "sistema di autorizzazione", comunque nel rispetto di quanto riportato nel presente documento relativamente alle modalità di autorizzazione (authorization) degli account personali;
- "protezione degli strumenti elettronici e dei dati", comunque nel rispetto di quanto riportato nel presente documento relativamente alla sicurezza informatica;
- "copie di sicurezza" e di "ripristino della disponibilità dei dati e dei sistemi", comunque nel rispetto di quanto riportato nel presente documento relativamente alle politiche di backup e di disaster recovery.

Ambienti di test

In caso di aggiornamenti di versione o patching dei software proprietari oggetto della fornitura, l'aggiudicatario dovrà predisporre, di comune accordo con il servizio informatico, una procedura di testing finalizzata alla verifica della funzionalità e della conformità alle misure minime AGID (allegato n.2) prima del rilascio in produzione degli stessi. L'ambiente di test rispecchierà quello di produzione, pertanto i dispositivi o i software necessari alla sua creazione saranno di volta in volta valutati in base allo scenario di riferimento.

Allegato 2 (Requisiti di conformità in ambito security):

In entrambi gli scenari appena descritti sarà compito dell'aggiudicatario adeguare le specifiche dei sistemi oggetto della fornitura (e le relative modalità di gestione da parte degli amministratori) ai principi generali di sicurezza delle infrastrutture IT, garantendo la piena conformità alle prescrizioni indicate in questo documento, con particolare riferimento a quelle relative all'ambito della IT Security.

L'aggiudicatario dovrà garantire che sia l'architettura che gli elementi forniti vengano progettati, implementati e manutenuti nel tempo in modo da risultare conformi alle misure minime di sicurezza, al fine di minimizzare il rischio informatico residuo sia di "attacchi ai sistemi" che di "attacchi dai sistemi".

Qui di seguito vengono esposte le indicazioni relative ai requisiti di conformità con le misure minime di sicurezza AGID applicabili al contesto delle forniture da parte di aziende esterne:

Inventario dei dispositivi:

Nel caso in cui i dispositivi oggetto della fornitura vadano connessi alla rete (Scenario 1 o 2B) i dispositivi oggetto della fornitura andranno inventariati e tali dati di inventario andranno mantenuti aggiornati seguendo un processo formale di approvazione. L'aggiudicatario dovrà compilare il modulo (esiste modulo?) fornendo tutte le informazioni tecniche necessarie all'implementazione della fornitura in oggetto ed inviarlo al servizio informatico per l'approvazione e la valutazione di eventuali "non conformità". Sarà compito dell'aggiudicatario provvedere a comunicare tempestivamente eventuali modifiche o sostituzioni seguendo di volta in volta lo stesso iter di approvazione.

Laddove i dispositivi siano raggiungibili via rete, l'assegnatario sarà inoltre tenuto a comunicare al servizio informatico le modalità di scansione remota delle informazioni inerenti l'hardware e il software installati nel dispositivo (es: SNMP, WMI) e relative credenziali.

Elenco software autorizzati:

il fornitore dovrà indicare preventivamente i sistemi operativi e i software che intenderà utilizzare nei propri dispositivi/sistemi sia come prima installazione che in caso di necessità di aggiornamenti a "major release" o in caso di sostituzione con altro software, seguendo anche in questo caso il processo formale di approvazione. I software non presenti nella lista di quelli autorizzati (fare lista se non esiste già) potranno essere installati solo a fronte di specifica richiesta e validazione da parte del servizio informatico.

Configurazioni sicure standard:

le configurazioni dei dispositivi e dei software devono rispettare le configurazioni sicure standard, implementate nei clients tramite immagini di installazione preconfigurate e/o mediante group policies, le quali vengono applicate ai sistemi operativi Microsoft Windows sia server che client. Nel caso di sistemi operativi non Microsoft o non agganciati al dominio, sarà cura del fornitore effettuare l'hardening ad-hoc dei propri sistemi tramite procedure che dovranno essere formalmente validate dal servizio informatico.

Connessioni protette per l'amministrazione remota:

l'aggiudicatario dovrà configurare opportunamente i dispositivi o i software oggetto della fornitura affinché le operazioni di amministrazione da remoto possano avvenire per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri), utilizzando protocolli cifrati (es: https/SSH/RDP) che dovranno essere formalmente validati dal servizio informatico.

Verifica vulnerabilità:

L'aggiudicatario deve verificare la presenza di eventuali vulnerabilità sia prima dell'installazione che dopo l'eventuale modifica/aggiornamento dei dispositivi e dei software oggetto della fornitura. I sistemi collegati alla rete dell'Azienda Asl Roma 1 sono sottoposti periodicamente a verifica di vulnerabilità tramite appositi strumenti pertanto l'Azienda Asl Roma 1 si riserva di verificare che le vulnerabilità emerse dalle scansioni vengano risolte per mezzo di patch, o implementando opportune contromisure.

Patching dei dispositivi e degli OS:

La politica di gestione degli aggiornamenti/patching dei dispositivi e dei sistemi operativi è naturalmente legata alla piattaforma in uso dallo specifico dispositivo fornito. In linea generale, nel caso in cui si tratti di sistemi basati su piattaforma Microsoft Windows sarà opportuno fare in modo che essi possano ricevere gli aggiornamenti dal server WSUS centralizzato già presente nell'Azienda Asl Roma 1, concordando con il

servizio informatico dell'Azienda Asl Roma 1 dei time-slot periodici per consentire l'applicazione degli aggiornamenti sui propri sistemi e verificarne l'esito. In tutti gli altri casi, ovvero per le applicazioni proprietarie, per i sistemi Windows non legati al dominio, per i sistemi operativi non Windows o per tutti gli altri dispositivi, l'aggiudicatario si dovrà far carico della verifica della disponibilità ed installazione

manuale delle patch, concordando con il servizio informatico dell'Azienda Asl Roma 1 dei time-slot periodici per consentirne l'esecuzione e la successiva verifica di funzionamento.

In linea generale le patch andranno installate entro 90gg dal rilascio, salvo la necessità di installarle con la massima urgenza nei casi in cui le patch vadano ad indirizzare e correggere bug o vulnerabilità ad alto livello di criticità.

Patching dei sistemi separati dalla rete (es: airgapped): In caso della fornitura di sistemi separati dalla rete, in particolare di quelli "airgapped", l'aggiudicatario dovrà farsi carico di assicurare l'aggiornamento tempestivo degli stessi. Anche in questo caso, in linea generale le patch andranno installate entro 90gg dal rilascio, salvo la necessità di installarle con la massima urgenza nei casi in cui le patch vadano ad indirizzare e correggere bug o vulnerabilità ad alto livello di criticità.

Gestione account privilegiati:

I privilegi amministrativi vengono concessi solo ad utenti dotati delle competenze necessarie e di un incarico/contratto relativo alla configurazione dei sistemi, solo per consentire lo svolgimento di attività che richiedano specifici livelli di privilegi.

Le utenze personali devono essere formalmente autorizzate seguendo una specifica procedura di validazione da parte del servizio informatico.

Gli accessi amministrativi vengono tracciati nei registri di auditing e conservati su piattaforma di Log Management, sia per quanto concerne i sistemi federati con Active Directory che per i sistemi standalone. Al fine di consentire la corretta acquisizione dei log dai sistemi/dispositivi oggetto della fornitura l'aggiudicatario sarà tenuto a fornire al servizio informatico le relative specifiche tecniche.

Gestione account locali: Prima di collegare alla rete un nuovo dispositivo o prima di mettere in produzione un software, l'aggiudicatario dovrà provvedere a sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso. L'Azienda Asl Roma 1 si riserva la facoltà di effettuare periodicamente delle verifiche a campione.

System hardening: Le password delle utenze amministrative devono rispondere a criteri di elevata robustezza: devono essere soggette a limiti minimi di lunghezza (es: 14 caratteri), rotazione (password history > 10) e durata (password aging <90gg). NB: tale prescrizione dovrà essere applicata a tutte le utenze con privilegi amministrativi, coinvolte nella fornitura, indipendentemente dal fatto che siano locali, legate all'Active Directory o definite in qualsiasi altra piattaforma software.

Gestione account privilegiati: L'aggiudicatario dovrà fare distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali distinte.

Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo

da assicurare l'imputabilità di chi ne fa uso. L'aggiudicatario dovrà inoltre conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.

Endpoint Protection: l'Azienda Asl Roma 1 provvederà ad installare l'antivirus centralizzato (Sophos Endpoint Security) in tutti i dispositivi oggetto della fornitura compatibili con esso, al fine di garantire adeguati livelli di protezione antivirus, firewall, IPS, controllo dei dispositivi USB, controllo web e controllo delle applicazioni. Le politiche di configurazione della suite antivirus sono gestite centralmente e ai requisiti delle misure minime AGID ai punti sopraindicati, pertanto eventuali eccezioni antivirus potranno essere create solo a fronte della verifica da parte del servizio informatico della conformità alle stesse. Non sarà inoltre possibile attivare l'utilizzo di servizi di posta elettronica esterni a quelli dell'Azienda Asl Roma 1.

Data Protection: In base allo scenario al quale potrà essere ricondotta la fornitura, dovrà essere garantita l'esecuzione di almeno un backup settimanale contenente le informazioni strettamente necessarie per il completo ripristino del sistema. Le modalità di esecuzione e la relativa pianificazione andranno concordate con il servizio informatico dell'Azienda Asl Roma 1 sulla base dello scenario applicabile. La riservatezza delle

informazioni contenute nelle copie di sicurezza dovrà essere assicurata mediante adeguata protezione fisica dei supporti. Sarà inoltre necessario assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

Crittografia dati rilevanti: L'aggiudicatario dovrà effettuare un'analisi dei dati manipolati dalla propria applicazione o dal sistema oggetto della fornitura al fine di individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e quelli ai quali va applicata la protezione crittografica, al fine di concordare con il servizio informatico di Asl Roma 1 le modalità più opportune per l'adempimento