

Specifiche tecniche IT Azienda Sanitaria Universitaria “Friuli Centrale”

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare relativamente ad aspetti della sfera dell'IT (Information Technology). Qualunque elemento riportato in offerta tecnica dai partecipanti in contrasto o non in coerenza con i principi ed i contenuti di seguito riportati non avrà alcun valore contrattuale.

Il sistema nel suo complesso dovrà essere coerente con le politiche di sicurezza e di privacy dell'Azienda Sanitaria Universitaria “Friuli Centrale” (ASUFC) e più in generale dovrà funzionare 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.

I sistemi forniti dovranno permettere ad ASUFC di rispondere, per lo specifico dei sistemi offerti, a tutte le prescrizioni del complesso quadro normativo vigente.

Dal punto di vista della sicurezza, in primis dovrà rispondere a quanto richiesto:

- dal Regolamento Europeo sulla Protezione dei Dati – GDPR del 14.04.2016 (<https://eur-lex.europa.eu/>) e al D. Lgs. 196/2003 s.m.i., cosiddetto Codice Privacy, così come novellato dal D.Lgs. 101/2018; l'aggiudicatario verrà designato responsabile ex art.28 del GDPR e dovrà produrre ed attuare tutto quanto richiesto, per quanto pertinente prima del collaudo e per tutta la durata del contratto;
- dalla Circolare dell'“Agenzia per l'Italia Digitale” (AgID) 18 aprile 2017, n. 2/2017, recante “Misure minime di sicurezza ICT per le pubbliche amministrazioni”, con livello ALTO; inoltre l'aggiudicatario dovrà collaborare attivamente per quanto oggetto di fornitura alla produzione di documentazione che l'ASUFC è chiamata a redigere in ottemperanza alla suddetta circolare AgID;
- dalla Determinazione AgID n. 220/2020 del 17/05/2020 “Adozione delle Linee Guida - La sicurezza nel procurement ICT” e dalle Linee Guida allegate.

Dovranno, inoltre, rispettare le indicazioni AgID inerenti lo sviluppo e l'acquisizione di software e, in particolare:

- il rispetto di quanto prescritto nelle “linee guida di sicurezza nello sviluppo delle applicazioni” AgID, anche dette “linee guida AgID per lo sviluppo sicuro del software”;
- la conformità alle regole sull'interoperabilità prescritte dalle linee guida emanate in attuazione dell'articolo 73 del CAD;
- la possibilità di esportare l'intera base di dati (inclusi di ogni tipo di indice o metadato utilizzato per implementare le funzionalità del software stesso) in formato standard e aperto, per scongiurare la possibilità di lock-in, come meglio specificato nelle linee guida n.8 di ANAC.

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. Pertanto, anche nei casi in cui la sicurezza dei dati gestiti dai sistemi oggetto di fornitura possa essere legata agli effetti di altro hardware e software in gestione da parte di altro soggetto, l'aggiudicatario rimane responsabile di monitorare tali elementi e segnalare in via formale qualora dovesse riscontrare aspetti di inadeguatezza. In tale responsabilità ricade anche l'onere di richiedere gli strumenti per fare gli audit ed il monitoraggio, per eseguire le ricerche di anomalie, oltre alla comunicazione formale delle proposte percorribili per raggiungere gli obiettivi.

Il quadro normativo nazionale attuale prevede la dismissione dei datacenter presenti all'interno delle sedi di ASUFC entro il 30 giugno 2026. In coerenza con quanto stabilito dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri nella “Strategia Cloud Italia” relativa all'adozione di soluzioni cloud nel mondo pubblico e alla progressiva razionalizzazione dei data center delle PA italiane, dal Piano Triennale AgID che suggerisce un approccio “cloud first” e dai provvedimenti dell'“Agenzia per la Cybersicurezza Nazionale” (ACN), i servizi oggetto di fornitura dovranno essere erogati preferibilmente in

modalità SaaS, ferme restando tutte le prescrizioni riportate nel presente documento, in particolare quelle relative al single sign-on. I servizi erogati in modalità SaaS dovranno soddisfare le caratteristiche definite dalle norme nazionali, in particolare quelle emanate dall'ACN. I servizi SaaS forniti dovranno avere caratteristiche tecniche compatibili con tale modalità di erogazione in maniera nativa, ovvero dovranno essere SaaS by design. In tal senso, tra gli altri aspetti caratteristici del paradigma SaaS by design, i sistemi offerti dovranno essere progettati secondo l'architettura 3-Tier, ovvero con una separazione tra il livello di presentazione ed il livello applicativo, in modo che gli utenti finali non abbiano in alcun modo accesso diretto alle risorse al livello dati (a titolo di esempio non esaustivo, non dovrà essere necessario realizzare trust di dominio tra il dominio degli utilizzatori e il dominio del server, ovvero non dovrà essere necessaria alcuna interazione sistemistica finalizzata all'accesso diretto dell'utente finale ad eventuali risorse locali del server, che dovrà essere gestita in sicurezza tramite meccanismi strettamente applicativi, fermo restando le prescrizioni relative al Single Sign On così come di seguito descritte). I servizi SaaS offerti dovranno essere fruibili attraverso un collegamento internet e tramite i web browser in uso presso ASUFC e senza alcun componente aggiuntivo sul browser stesso o sul client in generale; la sicurezza delle connessioni tra browser e servizi SaaS remoti dovrà essere adeguata alla tipologia di dati scambiati, in ogni caso dovrà essere adottato il protocollo HTTPS (TLS 1.2 o superiore – in ogni caso non deprecato – con certificato pubblico in gestione e a carico dell'aggiudicatario; tale certificato dovrà essere riconosciuto come valido dai browser di cui sopra, senza specifiche configurazioni, ovvero non dovranno essere usati certificati di tipo self-signed) e non verranno mai realizzate connessioni VPN o di altro tipo ad hoc, (es. sistemi di virtualizzazione applicativa o del desktop) per sopperire ad eventuali carenze architetturali in termini di sicurezza o funzionalità, ovvero i servizi dovranno sempre essere fruibili in maniera efficace e sicura tramite internet. I server che contengono i dati trattati di titolarità ASUFC dovranno risiedere all'interno della UE e per nessuna ragione dovranno essere effettuate copie di tali dati al di fuori del perimetro della UE, neppure per motivi di continuità di servizio e disaster recovery.

Relativamente al Single Sign On (SSO), dovrà essere possibile attivare nel corso di tutta la durata contrattuale, a discrezione di ASUFC e senza oneri aggiuntivi per ASUFC stessa, il SSO così come di seguito descritto: ASUFC è dotata di un sistema IdP basato su tecnologia Microsoft ADFS v3.0, accessibile sia dalla rete privata regionale RUPAR che da internet, ed i sistemi oggetto di fornitura dovranno interfacciarsi con tale IdP (Identity Provider) tramite il protocollo SAML (Security Assertion Markup Language) v2.0. In tal senso dovrà essere possibile l'autenticazione ai sistemi forniti tramite le credenziali di dominio Microsoft Active Directory di ASUFC, se i servizi sono fruiti all'interno delle reti private RUPAR, e – in maniera configurabile – tramite le credenziali di dominio Microsoft Active Directory di ASUFC e/o tramite l'infrastruttura di autenticazione nazionale SPID/CIE, se i servizi sono fruiti da internet.

Nello scenario SaaS potranno essere forniti, se indispensabili per gli scopi della presente fornitura, anche specifici dispositivi connessi anch'essi con i servizi SaaS. Tale connettività verrà garantita unicamente per mezzo di connessione cablata alla rete LAN dell'ASUFC e secondo le modalità descritte di seguito nello Scenario 1. Se la fornitura prevede l'utilizzo di dispositivi mobili (tablet, palmari,...) essi dovranno essere in grado di utilizzare connettività e infrastruttura autonoma (es. SIM dati, piano di connettività mobile) totalmente a carico e sotto la responsabilità del fornitore, che pertanto deve prescindere da risorse e infrastruttura dell'ASUFC.

Inoltre, sempre in coerenza con quanto stabilito da AgID, i sistemi forniti dovranno essere progettati, realizzati e installati in modo da minimizzare fenomeni di lock-in e in ogni caso, durante gli ultimi due trimestri di durata del contratto ed eventualmente per i tre mesi successivi, e comunque fino al raggiungimento dell'obiettivo, l'aggiudicatario dovrà favorire in ogni modo il travaso e la fruizione dei dati verso sistemi di terze parti, attraverso l'utilizzo di formati di dato aperti e documentati, il che sarà vincolante al pagamento dei corrispettivi. Tali attività ed i servizi professionali e tecnici associati sono perciò da intendersi oggetto di fornitura del presente contratto.

Dovrà essere indicato chiaramente in offerta tecnica in quale scenario tecnologico (SaaS, Scenario 1 o Scenario 2, così come descritti nel presente documento) ricade l'offerta presentata e dovrà essere dettagliato come - tecnicamente e organizzativamente - l'aggiudicatario intende rispondere alle prescrizioni del presente documento.

In caso di adesione allo Scenario 2 dovranno inoltre essere indicati in offerta tecnica il numero di risorse computazionali richieste (almeno: numero di macchine virtuali, tipo e versione di sistema operativo, funzione, quantità di RAM, numero di core, spazio disco, necessità e procedure documentate in termini di backup e

disaster recovery). Se tali richieste dovessero risultare non congrue rispetto alle finalità del contratto o non sostenibili per la stazione appaltante ad insindacabile giudizio di ASUFC, la medesima ASUFC si riserva di richiedere il passaggio allo Scenario 1 o al SaaS senza oneri aggiuntivi. Allo stesso modo, nel caso in cui i sistemi offerti nello Scenario 2 non dovessero risultare rispondenti alle specifiche IT o troppo onerosi da gestire per ASUFC, anche nel corso della durata contrattuale, ASUFC si riserva di convertire l'installazione nello Scenario 1 o SaaS e gli oneri derivanti saranno tutti a carico dell'aggiudicatario.

In generale, l'aggiudicatario per l'analisi preliminare e l'avviamento all'uso dei sistemi oggetto di fornitura ASUFC metterà a disposizione 5 giornate uomo di tecnico sistemista senior e 5 giornate uomo di project manager. La mancanza di autonomia operativa da parte dell'aggiudicatario o particolari necessità di assistenza svolta da personale ASUFC, che vadano oltre i limiti sopra riportati, verranno computati da ASUFC che si riserva la facoltà di quantificare le relative spese in base alle tariffe riferite per analoga figura professionale riguardante la Convenzione Consip "Servizi di System Management" in vigore e di dedurle dal piano di fatturazione previsto. Con la partecipazione alla gara si intende accettato tale meccanismo compensativo.

Specifiche di integrazione con l'infrastruttura IT

I sistemi oggetto di fornitura dovranno essere integrati ed interfacciati con l'infrastruttura informatica di rete e sistemistica dell'ASUFC, secondo quanto riportato nel seguito.

Non sono ammesse soluzioni che prevedano l'utilizzo di una DMZ (Demilitarized Zone) dell'ASUFC.

I dispositivi dotati di connettività di rete (host) che necessitano di collegamento alla rete dati per svolgere le funzioni richieste, potranno essere inseriti nella LAN dell'ASUFC seguendo uno dei due scenari, mutuamente esclusivi, descritti nel seguito.

Scenario 1: sistemi isolati

Gli host oggetto di fornitura saranno integrati, nel caso di sistemi fisici, nella sola infrastruttura di rete dell'ASUFC e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico verrà effettuata assegnando agli host medesimi una specifica classe di indirizzi IP coerente con il piano di indirizzamento dell'ASUFC e verranno inseriti in una VLAN dedicata, assegnata dall'ASUFC, dalla quale potranno effettuare solo l'eventuale traffico necessario per svolgere le funzioni richieste in capitolato, secondo il principio di minimizzazione, e l'eventuale traffico relativo all'assistenza remota da parte del fornitore. La segregazione del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali (ISFW – Internal Segregation Firewall), stilate per rete IP e per porta, sulla base delle sole effettive necessità di traffico per svolgere le funzioni richieste in capitolato. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall aziendali ISFW (Internal Segregation Firewall), quantificate in almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia, in particolare la rete IP/VLAN assegnata non avrà in alcun caso visibilità verso le reti IP/VLAN degli altri dispositivi client ASUFC. ASUFC si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.

Considerato che sulla base delle norme vigenti gli attuali datacenter di ASUFC dovranno essere dismessi entro e non oltre il 30 giugno 2026, gli host che svolgono funzioni di server potranno essere temporaneamente ospitati all'interno dei locali tecnici di ASUFC. Il fornitore dovrà già prevedere, progettare e pianificare le attività e quantificare gli oneri per la migrazione in cloud delle soluzioni ospitate presso i datacenter di ASUFC, con il seguente ordine di preferenza:

1. migrazione dei servizi svolti dagli host server fisici in un'infrastruttura del fornitore da erogare in modalità SaaS secondo la normativa vigente;
2. virtualizzazione degli host server fisici nello IaaS messo a disposizione da ASUFC. Il fornitore mette a disposizione di ASUFC una virtual appliance compatibile con l'infrastruttura IaaS, la cui configurazione e gestione sarà a totale carico e sotto la piena responsabilità del fornitore, analogamente a quanto già descritto per i dispositivi fisici, come se i sistemi oggetto di fornitura fossero ospitati all'interno dei locali tecnici di ASUFC;
3. spostamento dei server host fisici in modalità housing presso infrastrutture messe a disposizione da ASUFC in datacenter idonei dal punto di vista della normativa. La riconfigurazione e gestione dei

sistemi sarà a totale carico e sotto la piena responsabilità del fornitore, analogamente a quanto già descritto per i dispositivi fisici.

Il fornitore deve assicurare un piano di migrazione coerente con le tempistiche dettate dalle normative vigenti e garantire la capacità di svolgere l'attività entro le scadenze definite dalle norme medesime, ponendo in essere uno degli scenari sopra descritti.

Nei casi 2 e 3 sopra descritti saranno assegnati al fornitore accessi attraverso i sistemi VPN aziendali dell'ASUFC, inoltre tutte le attività che riguardano i sistemi oggetto di fornitura e i servizi (installazione, configurazione, attivazione, gestione, aggiornamento, manutenzione, ecc.) sono a carico e sotto la totale responsabilità del fornitore, inclusi la tempestiva applicazione di patch software, anche dei sistemi operativi, e la responsabilità della sicurezza informatica.

È attivo sulla LAN ASUFC un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x e realizzato per mezzo di tecnologia Microsoft NPS. Tutti gli host forniti e collegati alla LAN ASUFC dovranno essere tali da consentire l'autenticazione di rete tramite MAC address (cosiddetta MAC authentication). A titolo di esempio non esaustivo, l'autenticazione avviene solo a seguito di traffico effettuato a partire dall'host che dovrà essere in tal senso caratterizzato/configurato.

Nel caso in cui gli host forniti siano di tipo trasportabile, palmari o mobile (tablet, smartphone, ecc) la connettività verrà garantita alternativamente:

1. per mezzo di connessione cablata alla rete LAN ASUFC, secondo quanto riportato precedentemente. Non sarà consentito in alcun caso il collegamento di tali dispositivi tramite le postazioni di lavoro ASUFC (PC) – per esempio con collegamenti USB;
2. tramite rete Wi-Fi solo con dispositivi compatibili con Wi-Fi Protected Access WPA2/WPA3-Enterprise via Extensible Authentication Protocol - Transport Layer Security (EAP-TLS), su cui saranno installati certificati a chiave pubblica x.509 privati erogati da ASUFC.

I collegamenti cablati dovranno essere realizzati con un adeguato grado di resistenza meccanica, nel caso per esempio dei dispositivi palmari o mobile, dovrà essere fornita una docking station e non saranno consentiti adattatori stand-alone di alcun tipo (ad esempio adattatori USB-RJ45). I dispositivi di tipo palmare e mobile dovranno essere specificatamente previsti dal fabbricante per uso in ambienti sanitari e locali ad uso medico.

Il fornitore dovrà garantire agli utenti dell'ASUFC la migliore operatività in termini di facilità d'uso ed efficacia, in particolare per i dispositivi mobile i servizi dovranno essere resi disponibili dal fornitore per mezzo di specifiche applicazioni (non sarà consentito l'uso di applicazioni web su dispositivi mobile) e tali applicazioni dovranno essere pensate anche per l'uso off-line, in quanto non è garantita la copertura Wi-Fi di tutti i locali delle sedi dell'ASUFC.

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dagli amministratori di sistema formalmente nominati dall'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUFC, basati su tecnologia Cisco AnyConnect e su cui la modalità Split Tunnel è per policy sempre disattivata. L'accesso sarà consentito solo al termine del compimento di un iter autorizzativo aziendale con modulistica dedicata. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali con bassi privilegi (livello user). Nel presente scenario, a valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza dovrà avvenire esclusivamente con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi da parte dell'ASUFC. Il servizio di connessione remota VPN dell'ASUFC verrà assegnato all'aggiudicatario con livelli di servizio "best effort", ossia non garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire con modalità alternativa all'indisponibilità della VPN (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta gli specifici livelli di servizio in caso di indisponibilità del servizio VPN.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo da internet degli host oggetto di assistenza, nel presente scenario, lo strumento messo a disposizione da ASUFC è il firewall di navigazione gestito da Insiel SpA: gli host forniti potranno raggiungere solo un numero limitato di destinazioni internet (fino al numero massimo di 10), su specifiche direttrici identificate da indirizzi IP e porte, in quanto non saranno ammessi nomi DNS (Domain Name Service); in ogni caso il traffico consentito sarà quello minimo necessario per il funzionamento dei sistemi e non sarà consentita la navigazione internet nonché l'esfiltrazione di dati

tramite questo canale. Verranno perciò effettuate specifiche abilitazioni basate su IP sorgente, IP destinazione e porta/e TCP/UDP solo al termine del compimento di un iter autorizzativo aziendale con modulistica dedicata. L'aggiudicatario dovrà fornire la massima collaborazione all'ASUFC per la definizione delle suddette abilitazioni. Nel presente scenario, la risoluzione dei nomi host sarà basata esclusivamente su uno specifico servizio DNS dedicato a tutti i dispositivi segregati/isolati presenti sulla rete ASUFC, compresi quelli oggetto di fornitura. Analogamente al servizio VPN ASUFC di cui sopra, anche il servizio di connettività in uscita tramite firewall di navigazione Insiel SpA non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dall'aggiudicatario dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio in altro modo (per esempio con intervento sul posto o utilizzando altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta i livelli di servizio in caso di indisponibilità del servizio.

Nel presente scenario, l'aggiudicatario sarà responsabile in toto delle prescrizioni di ambito 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 continuità operativa, di backup e disaster recovery, gli aggiornamenti di sicurezza di tutti i software installati sugli host oggetto di assistenza, la protezione antivirus e da altre tipologie di cyber attacco, ad eccezione della disponibilità di energia elettrica e di connettività della rete dati aziendale.

Per il servizio erogato l'aggiudicatario sarà responsabile della continuità operativa dei sistemi e dovrà garantire il rispetto dei parametri di RTO e RPO specificati nel capitolato.

Per il servizio erogato il fornitore dovrà garantire la continuità operativa e in caso di disaster recovery il rispetto dei seguenti parametri:

- RTO: 24 ore lavorative
- RPO: 0 minuti

Gli oneri di licenza e di qualunque altro tipo, diretti e indiretti, finalizzati al corretto e sicuro funzionamento del sistema oggetto di fornitura saranno completamente a carico dell'aggiudicatario, come pure l'onere della continua verifica nei dizionari di vulnerabilità internazionali (al minimo dovrà essere monitorato CVE - Common Vulnerabilities and Exposures) dei sistemi operativi in uso e di qualunque altra componente software fornita od installata dall'aggiudicatario, nonché la sostituzione immediata ed incondizionata dei sistemi operativi stessi in caso di criticità contrassegnate con livello maggiore o uguale al range "6-7".

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

Nel caso in cui le applicazioni fornite dall'aggiudicatario fossero rispondenti alle specifiche del paradigma SaaS e del SSO basato su protocollo SAML, così come descritte all'inizio del presente documento, l'aggiudicatario stesso potrà proporre in offerta tecnica di utilizzare le applicazioni offerte sui PC client aziendali standard (postazioni di lavoro ASUFC). In tal caso non sarà necessaria la fornitura dei PC client dedicati da parte dell'aggiudicatario. ASUFC tuttavia si riserva di verificare gli estremi ed i dettagli tecnici della proposta e si riserva di rifiutarla a suo insindacabile giudizio. In tal caso l'aggiudicatario dovrà comunque fornire tutti i PC client necessari.

Gli eventuali server forniti dovranno, inoltre, essere del tipo per l'installazione da rack standard 19" con una occupazione massima di 2 rack unit (a meno di documentata necessità), dotati di doppio modulo di alimentazione integrato, di doppia scheda di rete e scheda di management.

Inoltre, tali server non dovranno/potranno per alcun motivo essere utilizzati dagli operatori come stazioni di lavoro.

Scenario 2: sistemi integrati

Nel secondo scenario, alternativo al precedente, l'aggiudicatario dovrà integrare i sistemi oggetto di fornitura con l'infrastruttura sistemistica dell'ASUFC. Di seguito vengono riportate, in prima istanza, alcune caratteristiche peculiari dell'infrastruttura informatica dell'ASUFC; successivamente vengono definite le specifiche di interfacciamento all'infrastruttura ASUFC che i sistemi oggetto di fornitura dovranno garantire, in caso di adesione al presente scenario. L'architettura generale e le caratteristiche dei singoli elementi dei sistemi forniti dovranno in ogni caso essere pienamente coerenti e allineati con le logiche di seguito descritte.

L'articolazione territoriale di ASUFC si sviluppa su più di 100 sedi e in tali sedi le logiche di integrazione sono le medesime e sono di seguito descritte. In funzione della complessità del sito, non sono implementati localmente tutti i servizi di infrastruttura, ma sono resi disponibili tramite la connettività WAN nel sito dell'Ospedale di Udine e presso l'infrastruttura IaaS in cloud che ASUFC mette a disposizione dei propri fornitori.

L'infrastruttura IaaS sopra menzionata ha caratteristiche analoghe all'infrastruttura CSP AgID, con uptime garantito del 99,9%, e si basa sul sistema di virtualizzazione VMware.

L'ASUFC è dotata di più domini Active Directory (AD) con livelli funzionali di dominio/foresta diversi. Nel sito AD principale è presente almeno un domain controller global catalog ed un file server. Ogni account del directory service aziendale è associato ad almeno un gruppo di dominio (gruppi locali al dominio, domain local) corrispondente alla struttura amministrativa ASUFC di appartenenza. La default domain policy impone l'utilizzo di password complesse, con password history e cambio password obbligatorio con frequenza predefinita. Gli aggiornamenti di sistema per i client e per i server vengono distribuiti tramite il servizio Microsoft WSUS e gestiti, con periodicità mensile, da Insiel SpA.

Le postazioni di lavoro ASUFC (PC) sono inserite in uno dei domini aziendali. Il software di base e l'hardware di tali postazioni è eterogeneo e varia, nelle prestazioni e caratteristiche di base, da:

- sistema operativo Microsoft Windows 10 Professional Italiano, versione di Build più vetusta ancora in supporto;
- browser Microsoft Edge (non configurabile in modalità compatibilità con versioni IE precedenti) ultima versione e Google Chrome ultima versione;
- CPU Intel Core Duo o equivalente;
- RAM 4 GB;
- HDD da 256 GB;

a:

- sistema operativo Microsoft Windows 10 Professional Italiano, ultima Build rilasciata;
- browser Microsoft Edge ultima versione (non configurabile in modalità compatibilità con versioni IE precedenti) e Google Chrome ultima versione;
- CPU Intel Core i7 o equivalente;
- RAM 16 GB;
- SSD da 256 GB.

Le postazioni di lavoro ASUFC sono tipicamente dotate di connettività di rete Gigabit Ethernet/100Mbps. Tutti gli operatori aziendali accedono alle postazioni di lavoro (PC) tramite account AD e relative credenziali personali con bassi privilegi (user); su tutte le postazioni è attivo il servizio Microsoft DEP (Data Execution Prevention).

Il protocollo di rete utilizzato è IPv4. La risoluzione dei nomi è basata esclusivamente sul servizio DNS integrato in AD. L'architettura di rete ASUFC è realizzata in modo che tutti i servizi siano raggruppati in parte nei locali tecnici principali ASUFC ed in parte nell'infrastruttura IaaS in cloud.

In generale la LAN ASUFC è una rete layer 2-3 (pila ISO/OSI) a due livelli (core e periferia): per ciascun presidio, gli apparati di periferia sono collegati in layer 2 agli apparati di core; il data center è collegato direttamente agli apparati di core in layer 3. Al fine della segmentazione del traffico, la rete è suddivisa in VLAN separate, sia a livello server che di periferia, a cui corrispondono specifiche sottoreti IP, sulla base della tipologia di host e del traffico dati che effettuano, ovvero nell'intento di isolare il traffico dati stesso sulla base dei servizi e dei domini di competenza degli amministratori degli host. La segregazione del traffico viene effettuata tra le reti IP/VLAN e con le logiche di cui sopra tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali (ISFW – Internal Segregation Firewall), stilate almeno per rete IP e per porta TCP/UDP, sulla base delle sole effettive necessità di traffico, che in ogni caso non è consentito tra apparati di periferia appartenenti a differenti reti IP/VLAN, in quanto i flussi funzionali sono sempre dal centro (servizi di infrastruttura e applicativi) alla periferia (client/host) e viceversa.

Tutte le licenze dei sistemi operativi Microsoft Windows Server necessarie al funzionamento del sistema verranno messe a disposizione da ASUFC, saranno di tipo Retail (non OEM) e comunque in ogni caso compatibili con l'ambiente di virtualizzazione dell'ASUFC.

Le fasce orarie nelle quali il personale IT dell'ASUFC sarà in grado di supportare il fornitore per le attività tecnico-sistemistiche sono le seguenti:

- nei giorni feriali:
 - o dalle 9:00 alle 15:00 in regime ordinario;
 - o dalle 19:00 alle 7:00 in regime di reperibilità;
- dalle 19:00 di venerdì alle 7:00 di lunedì (festivi compresi) in regime di reperibilità.

In base alle specifiche scelte, progettuali e di infrastruttura, l'aggiudicatario dovrà usufruire dell'infrastruttura di backup ASUFC per i sistemi operativi di tutti i server e per la configurazione dei database. L'aggiudicatario dovrà fornire all'ASUFC il supporto per definire e configurare l'attivazione del backup, nonché per la redazione delle relative procedure di backup e disaster recovery. Per i database, le politiche di backup e disaster recovery saranno concordate con l'aggiudicatario che dovrà comunque comunicarne i requisiti ritenuti opportuni all'Azienda, insieme alle procedure dettagliate per eseguire le attività di export e dump. Il fornitore prima dell'avvio dei sistemi in produzione dovrà, in collaborazione con l'ASUFC:

- definire formalmente, documentare e collaudare le procedure di backup e disaster recovery, inclusi i tempi di ripristino (RTO e RPO);
- implementare i processi di backup e disaster recovery delle macchine virtuali;
- implementare i processi di backup e disaster recovery di eventuali database, dati e configurazioni di sistema.

ASUFC si riserva di valutare la congruità delle richieste in termini di backup e disaster recovery, contestando richieste non ritenute congrue o tecnicamente sostenibili; in tal caso l'aggiudicatario sarà tenuto ad adeguarsi di conseguenza.

L'antivirus aziendale è Trendmicro Officescan, distribuito su tutti i server e su tutti i client MS Windows e aggiornato automaticamente secondo una periodicità stabilita sulla base di criteri di sicurezza stabiliti dal fornitore del servizio.

Su tutti i client aziendali sono installati agent di monitoraggio, assistenza remota e sicurezza.

La navigazione internet dai client aziendali viene effettuata per mezzo di proxy server gestito e vincolato da un fornitore esterno.

Per l'intera durata contrattuale il fornitore dovrà gestire il ciclo di vita dei sistemi forniti in modo che siano sempre compatibili con le versioni più aggiornate dei sistemi operativi (sia build client che server) che non dovranno in alcun caso trovarsi nello stato di "fuori supporto standard", nonché con i web browser, i database e altri software con cui l'applicativo fornito dovesse avere delle dipendenze e/o interagire (es. librerie Java, Adobe Reader, Microsoft Office, ecc.) ed utilizzare costantemente tutti e soli protocolli non deprecati. Entro il semestre precedente dell'end of support (non esteso) dei sistemi operativi, dei web browser, dei database e di altri software o protocolli con cui l'applicativo fornito dovesse avere delle dipendenze e/o interagire, il fornitore dovrà quindi rendere disponibile la release, aggiornata e compatibile, dei software forniti che non dovranno in alcun caso costituire un vincolo per ASUFC in relazione all'aggiornamento tecnologico obbligatorio dei sistemi, comprensivo della disinstallazione dei componenti obsoleti e deprecati. Tali release sono da intendersi sia di tipo minor che di tipo major e senza oneri aggiuntivi per ASUFC.

Nel caso in cui i sistemi forniti utilizzino l'ambiente Java, a qualunque titolo, si intendono incluse nella presente fornitura le licenze necessarie, secondo quanto stabilito dalle licensing policy di Oracle, senza oneri aggiuntivi per ASUFC. In alternativa potranno essere utilizzate le distribuzioni che utilizzano licensing open source o similari (a titolo di esempio non esaustivo OpenJDK, basato su licenza GPL), fermi restando i vincoli di cui al paragrafo precedente, ovvero l'obbligo per l'aggiudicatario di aggiornare tali componenti con continuità e conseguentemente i sistemi forniti (a titolo di esempio non esaustivo l'unica versione in supporto di Oracle OpenJDK è sempre e solo l'ultima versione disponibile). Le considerazioni del presente paragrafo si applicano anche ad ambienti analoghi a Java.

Nel presente scenario, i server oggetto di fornitura verranno installati nel sistema di virtualizzazione VMware dell'infrastruttura IaaS e dovranno seguire le politiche di gestione, comprese quelle di indirizzamento

IP, di aggiornamento, di backup e di disaster recovery di ASUFC. Potranno essere create una o più macchine virtuali a seconda delle necessità e dell'architettura proposte dall'aggiudicatario, ma in ogni caso tali macchine dovranno essere compatibili con il sistema operativo Windows Server 2019 Standard Edition ENG o superiore, e inserite nel dominio Active Directory delle risorse dedicato e nel sistema WSUS aziendale. Non sarà consentito l'utilizzo di tecnologie basate su container virtuali (a titolo di esempio Docker o simili). ASUFC si riserva di valutare la congruità delle richieste in termini di numero e funzione delle macchine virtuali, contestando richieste non ritenute congrue o tecnicamente sostenibili; in tal caso l'aggiudicatario sarà tenuto ad adeguarsi di conseguenza. Il fornitore dovrà garantire piena collaborazione nella redazione delle ACL e/o regole sui firewall aziendali (ISFW – Internal Segregation Firewall), al fine di attuare le politiche di segregazione di cui sopra, sia a livello server che di periferia, per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso.

Allo scopo di uniformare i sistemi forniti agli standard ASUFC, compresi quelli di sicurezza e autorizzazione (authorization), tali macchine server verranno dotate di sistema operativo Microsoft Windows Server 2019 o superiore e inserite in una Organizational Unit (OU) generica dedicata ai server ASUFC oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l'ASUFC; la default domain policy verrà applicata in ogni caso su tutte le OU.

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 a carico del fornitore; in tal caso dovranno seguirne le politiche di gestione, comprese quelle di backup e disaster recovery.

Ogni attività di tipo change lato server, inteso come intervento o aggiornamento sui sistemi oggetto di fornitura, non dovrà in alcun caso causare disservizio maggiore di 10 minuti ovvero di 3 ore quando sono previste soluzioni di business continuity ritenute accettabili dall'ASUFC, salvo differenti accordi da definirsi anticipatamente con gli utenti finali interessati. In ogni caso le attività di change dovranno essere anticipatamente comunicate e concordate con l'ASUFC, nonché documentate e deve essere previsto un sistema di rollback con le medesime caratteristiche di disservizio.

In generale gli oneri di licenza e di qualunque altro tipo, diretti e indiretti, finalizzati al corretto e sicuro funzionamento del sistema oggetto di fornitura saranno completamente a carico dell'aggiudicatario, inclusi tutti gli oneri e le licenze dipendenti dalle scelte tecnologiche dell'aggiudicatario stesso, a titolo di esempio le eventuali licenze di Microsoft Terminal Services (sia server che CAL).

Sono inoltre a carico dell'aggiudicatario tutte le attività di gestione e manutenzione sistemistica, per l'intera durata contrattuale, intesa come componente di interazione tra i sistemi forniti (di cui solo il fornitore ha competenze specifiche) ed i software di base, sistemi operativi in primis. In tale voce sono da intendersi perciò incluse tutte le attività preventive e correttive, nonché il coordinamento ed il supporto ai tecnici ASUFC nelle attività di costante aggiornamento dei sistemi, in rispondenza al quadro normativo e legislativo in essere.

Relativamente agli archivi correnti di dati e documenti, l'ASUFC si riserva di modificare le proprie policy di retention, attualmente tarate su un orizzonte temporale di cinque anni. Pertanto si intende inclusa, nel servizio oggetto della presente fornitura e per tutta la durata contrattuale, ogni attività finalizzata all'applicazione di delete policy di dati strutturati e documenti gestiti nell'ambito dei sistemi forniti che superino i periodi di retention definiti da ASUFC, ovvero ogni attività necessaria per ottenere archivi correnti con dati e documenti di età inferiore all'orizzonte temporale definito da ASUFC.

Nel presente scenario, lato utente, ovvero lato postazione ASUFC (PC client), gli applicativi eventualmente forniti potranno essere basati su tecnologia client/server o web. Non saranno considerati compatibili con l'infrastruttura IT sistemi basati sul paradigma client/database. In ogni caso non sarà consentita la fornitura di postazioni client e le applicazioni eventualmente fornite dovranno essere utilizzate dalle postazioni ASUFC standard, così come descritte nel presente documento.

Gli eventuali applicativi client forniti, necessari all'espletamento di una o più funzionalità richieste, verranno installati sulle postazioni – senza limitazioni in termini di numero di postazioni – e dovranno essere adeguati alle caratteristiche software e hardware delle postazioni stesse, in particolare alle policy dei domini ASUFC e conseguentemente a quelle del sistema WSUS ASUFC. La distribuzione sulle postazioni di lavoro ASUFC di tali applicativi, nonché degli aggiornamenti, verrà eseguita esclusivamente a seguito della fornitura

ad ASUFC, da parte dell'aggiudicatario, dei pacchetti di aggiornamento con tecnologia MSI o Installshield. Tali pacchetti saranno poi distribuiti ed eseguiti dall'ASUFC attraverso il sistema di gestione Microsoft SCCM.

Gli eventuali applicativi web, forniti nell'ambito della presente fornitura, dovranno essere compatibili con almeno uno dei browser attualmente installati su ciascuna delle postazioni ASUFC. Non saranno considerati accettabili applicativi web compatibili con altri browser diversi da quelli riportati nel presente documento. Tali applicativi web dovranno adottare una opportuna implementazione del protocollo HTTPS (TLS 1.2 o superiore – in ogni caso non deprecato). I certificati utilizzati a tal scopo saranno erogati dalla CA (certification authority) privata ASUFC basata su tecnologia Microsoft: nel caso di utilizzo di web server basati su tecnologia Microsoft IIS (Internet Information Services), i certificati verranno aggiornati con i meccanismi di auto-enrollment nativi Microsoft; nel caso invece di utilizzo di altre tecnologie di web server, il rinnovo dei certificati sarà a carico dell'aggiudicatario, senza oneri aggiuntivi per ASUFC. Nel secondo caso, eventuali disservizi dovuti al mancato rinnovo dei certificati, per tempo, da parte dell'aggiudicatario saranno imputati all'aggiudicatario stesso.

Non saranno accettati eventuali PC forniti, se non identici ad uno dei modelli standard già in produzione presso ASUFC che in tal caso potranno essere inseriti nei domini di ASUFC a seguito di clonazione da golden image ASUFC e hardening standard ASUFC e a condizione di seguire le policy aziendali e caratteristiche dei PC client dell'ASUFC così come indicate nel presente documento.

Tutte le funzionalità dei sistemi forniti dovranno essere garantite con il client antivirus aziendale Trend Micro Officescan di cui ogni postazione ASUFC è dotata, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'ASUFC, a meno di eccezioni concordate con l'ASUFC che in ogni caso si riserva di accettare. Inoltre, potranno essere attivati sui client anche dei servizi di host intrusion prevention system e di local firewall. In tal senso l'aggiudicatario dovrà garantire piena collaborazione nella redazione di tali eccezioni sul client, per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso.

Tutte le funzionalità dei sistemi forniti dovranno essere garantite e compatibili con:

- con l'agente Microsoft SCCM di cui ogni postazione ASUFC è dotata;
- con il proxy server basato su tecnologia ForcePoint gestito da Insiel SpA e con le relative policy di sicurezza, in particolare nel caso di eventuali sistemi SaaS oggetto di fornitura;
- con la funzionalità di cambio rapido utente di Windows.

Nel presente scenario, eventuali host (di tipologia non server) oggetto di fornitura non dotati di client AD e che necessitano di connettività con la rete dati ASUFC, verranno connessi alla stessa e saranno oggetto di policy di segmentazione e segregazione del traffico. La segregazione del traffico verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali (ISFW – Internal Segregation Firewall), stilate almeno per rete IP e per porta, sulla base delle sole effettive necessità di traffico per svolgere le funzioni richieste in capitolato. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia. In ogni caso, gli host non dotati di client AD non avranno visibilità di rete sugli applicativi client/web installati sulle postazioni ASUFC. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sui firewall aziendali (ISFW – Internal Segregation Firewall), per una durata complessiva di almeno un giorno lavorativo uomo e comunque fino al raggiungimento del risultato atteso. Più in generale, si applicano a tali host segregati/isolati le stesse prescrizioni riportate nello Scenario 1 del presente documento, incluse le policy di autenticazione di rete: dovranno perciò autenticarsi in rete ASUFC secondo il protocollo 802.1x per mezzo di nome utente e password o di MAC address a discrezione di ASUFC.

ASUFC si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta, sia lato server che lato client, che host segregati/isolati.

Nel presente scenario, in generale, sia lato server che lato client, verranno installate tutte le patch rilasciate da Microsoft. Potranno essere segnalate all'ASUFC patch contrassegnate come "non applicabili", solo se di natura non critica; per tali patch "non applicabili" verranno generate dall'ASUFC delle eccezioni in WSUS, che avranno una durata limitata di 6 mesi entro cui l'aggiudicatario dovrà provvedere alla risoluzione del problema di compatibilità.

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dagli amministratori di sistema formalmente nominati dall'aggiudicatario, la connettività ai sistemi oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali dell'ASUFC, basati su tecnologia Cisco AnyConnect e su cui la modalità Split Tunnel è per policy sempre disattivata. L'accesso sarà consentito

solo al termine del compimento di un iter autorizzativo aziendale con modulistica dedicata. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali con bassi privilegi (livello user). Nel presente scenario, a valle dell'instaurazione della connessione VPN, il collegamento ai singoli sistemi oggetto di assistenza dovrà avvenire esclusivamente secondo le seguenti modalità: per i sistemi server, tramite Microsoft Windows RDP, una volta avuto accesso al server le operazioni di amministratore avverranno con l'elevazione dei privilegi per mezzo di apposite credenziali personali di livello administrator che verranno fornite ove richieste. Il servizio di connessione remota VPN dell'ASUFC verrà assegnato all'aggiudicatario con livelli di servizio "best effort", ossia non garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire con modalità alternativa all'indisponibilità della VPN (per esempio con intervento sul posto o altri sistemi di allarme e sicurezza), senza inficiare i livelli di servizio offerti né la sicurezza degli stessi, o evidenziando in offerta gli specifici livelli di servizio in caso di indisponibilità del servizio VPN.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo da internet dei server e degli host segregati/isolati oggetto di assistenza, nel presente scenario, lo strumento messo a disposizione da ASUFC è il firewall di navigazione gestito da Insiel SpA: i server e gli host potranno raggiungere solo un numero limitato di destinazioni internet (fino al numero massimo di 10), su specifiche direttrici identificate da indirizzi IP e porte, in ogni caso il traffico consentito sarà quello minimo necessario per il funzionamento dei sistemi e non sarà consentita la navigazione internet nonché l'esfiltrazione di dati tramite questo canale. Verranno perciò effettuate specifiche abilitazioni basate su IP sorgente, IP destinazione e porte TCP/UDP solo al termine del compimento di un iter autorizzativo aziendale con modulistica dedicata. L'aggiudicatario dovrà fornire la massima collaborazione all'ASUFC per la definizione delle suddette abilitazioni. Sui client ASUFC non sono previste attività di telemonitoraggio da internet delle applicazioni. Nel presente scenario, la risoluzione dei nomi avverrà: da parte dei server, tramite il servizio DNS integrato in AD di cui sopra, che accetta solo registrazioni sicure; da parte degli eventuali host isolati forniti dall'aggiudicatario sarà basata esclusivamente su uno specifico servizio DNS dedicato a tutti i dispositivi segregati/isolati presenti sulla rete ASUFC, compresi quelli oggetto di fornitura.

È in uso presso l'ASUFC una soluzione di single sign-on (SSO) per l'autenticazione (authentication) ed il conseguente accesso alle risorse informatiche. Di seguito vengono riportate, in prima istanza, le caratteristiche peculiari del SSO ASUFC e successivamente vengono definite le specifiche dei sistemi da fornire in tal senso, nell'ambito del presente scenario.

Il SSO ASUFC permette al singolo account di autenticarsi una sola volta e di essere successivamente riconosciuto ogni volta che accede ad una risorsa di rete a cui è abilitato. Gli account possono essere associati unicamente a credenziali personali (ad uso esclusivo di una persona fisica, ovvero di un operatore); tutti gli altri casi sono gestiti esclusivamente per mezzo dei gMSA (group Managed Service Account) Microsoft (a titolo di esempio non esaustivo, un'applicazione che deve autenticarsi verso un'altra applicazione, un servizio, ecc.). Per risorsa di rete si intende un qualsiasi servizio erogato su qualsiasi sistema operativo (a titolo di esempio non esaustivo, l'accesso ad un applicativo web o client/server, interattivo ssh, a file, a stampanti, ecc.).

La soluzione SSO ASUFC prevede un repository centrale realizzato attraverso il protocollo Lightweight Directory Access Protocol (LDAP), che contiene gli account e la configurazione delle macchine e dei servizi correlati; tale repository è il directory service aziendale Microsoft AD e non accetta bind anonimi né senza cifratura (ovvero senza LDAP over SSL/ TLS - LDAPS). L'autenticazione degli account si basa sul protocollo kerberos versione 5 (in seguito anche v.5) e viene effettuata dai domini di ASUFC. Il SSO ASUFC ricalca ciò che in letteratura viene identificato come "Windows Integrated Single Sign-On" o "Windows Integrated Authentication". Le credenziali utilizzate sono ad oggi "nome utente" e "password", e seguono le politiche descritte precedentemente; in futuro verranno adottati sistemi basati su certificati digitali e/o Multi-Factor Authentication (MFA).

I sistemi forniti dovranno essere coerenti ed integrati con la soluzione di SSO ASUFC. In alternativa all'autenticazione integrata Windows il fornitore potrà implementare, in accordo con ASUFC, soluzioni di SSO basate su protocollo SAML, secondo le specifiche riportate all'inizio del presente documento. Le modalità operative di accesso agli applicativi ed ai sistemi forniti da parte degli operatori dovranno essere personali, avverranno cioè per mezzo di credenziali informatiche personali; a queste potranno inoltre essere associati uno o più ruoli.

Come descritto in precedenza, l'unico repository di account ASUFC (personali e gMSA) è il directory service Active Directory in cui a ciascun account di dominio sono associate le rispettive credenziali informatiche. Per

questo motivo tutte le credenziali personali, previste negli applicativi e nei sistemi forniti dall'aggiudicatario, dovranno corrispondere a quelle dei domini ASUFC: gli account associati a credenziali personali si autenticeranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi, in base al proprio livello di autorizzazione (definito in base al ruolo) e a seguito dell'accesso alla sessione di lavoro. Tutte le credenziali impersonali, eventualmente presenti negli applicativi e nei sistemi forniti dall'aggiudicatario, dovranno essere opportunamente create e configurate nei domini ASUFC e saranno del tipo gMSA, si autenticeranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi in base al proprio livello di autorizzazione, che dovrà sempre essere il minimo necessario (e mai tramite l'immissione di credenziali impersonali da parte degli operatori).

L'autenticazione degli account - che devono essere sempre singolarmente autenticati ad ogni accesso - dovrà sempre avvenire tramite protocollo kerberos v.5. Ciò significa in particolare che, nell'architettura kerberos, i domain controller dei domini ASUFC svolgeranno il ruolo di KDC (Key Distribution Center), mentre gli applicativi/sistemi forniti assolveranno i ruoli di Client e SS (Service Server); a titolo di esempio non esaustivo, i Service Server forniti dovranno essere in grado di interpretare e validare correttamente i Service Ticket inviati dai Client, nonché instaurare successivamente le Client/Server Session (sia in caso di architetture fornite tipo client/server che web).

L'autorizzazione (authorization) è intesa in questo contesto come profilatura dell'account e gestione dei ruoli e delle abilitazioni ad esso associati. In particolare gli applicativi/servizi forniti dovranno importare gli account da abilitare dal repository LDAP ASUFC (domini ASUFC), sulla base di un Gruppo AD specifico che verrà realizzato ad hoc, e circoscrivere la profilatura e l'attribuzione dei ruoli all'interno degli applicativi/servizi stessi solo per gli account appartenenti a quello specifico gruppo. In via propedeutica al collaudo dei sistemi forniti, l'aggiudicatario dovrà installare la console amministrativa su un client ASUFC afferente alla SOC Tecnologie Informatiche e Agenda Digitale e dovrà formare una risorsa ASUFC alla profilatura degli account nei sistemi forniti, in modo da rendere l'ASUFC autonoma nelle procedure di abilitazione e successiva reinstallazione della console amministrativa.

Non dovrà essere possibile creare, configurare e profilare altri account non appartenenti ad AD, ad eccezione di specifiche situazioni opportunamente motivate ed in ogni caso concordate con l'ASUFC. La profilatura e l'attribuzione dei ruoli degli applicativi/servizi forniti dovrà essere tale da garantire il massimo livello di dettaglio di configurazione, e dovrà garantire tutto quanto descritto nel presente documento.

Altre soluzioni di SSO, autenticazione e account/identity management diverse da SAML e "Windows Integrated Authentication" non saranno consentite, a titolo di esempio non esaustivo: il cosiddetto "secondary logon" (ovvero uno scenario nel quale l'utente debba reinserire le credenziali di dominio), sistemi basati sul protocollo LDAP/LDAPS e l'autenticazione con protocollo NTLMv2.

Specifiche tecniche di sicurezza informatica

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare, sia nel caso di non collegamento in rete, sia nello Scenario 1 che nello Scenario 2, relativamente ad aspetti generali della sfera dell'IT (Information Technology) con particolare riferimento alla sicurezza informatica (security).

Vale in ogni caso il principio generale per cui la sicurezza informatica è un fattore intrinseco dell'architettura dei sistemi oggetto della presente fornitura e delle caratteristiche tecniche degli elementi che li compongono; perciò l'aggiudicatario dovrà garantire che, sia l'architettura che gli elementi, siano progettati, implementati e mantenuti nel tempo in modo da minimizzare il rischio informatico residuo (sia di "attacchi ai sistemi" che di "attacchi dai sistemi") e comunque in osservanza delle normative e best practice già citate nel primo paragrafo del presente documento e sempre in coerenza con il paradigma "Zero Trust".

Verranno eseguite periodicamente da ASUFC, o da personale a tal scopo incaricato, procedure di Vulnerability Assessment e Penetration Test e l'aggiudicatario si impegna pertanto a risolvere criticità o vulnerabilità che dovessero emergere a seguito di tale attività. Analogamente l'aggiudicatario si impegna a collaborare con il SOC (Security Operation Center) aziendale ASUFC per il miglioramento continuo dei sistemi forniti.

Inoltre i sistemi forniti dovranno rispettare le seguenti prescrizioni.

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 per tutta la durata contrattuale.

In generale, tutti i software forniti dovranno essere:

- coerenti con la necessità di richiedere applicazioni, servizi e procedure 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 (se presente) IT standard, comprese le tastiere, allo scopo di non incorrere mai 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 practice internazionali; non dovranno mai 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 per tutta la durata contrattuale;
- pensati, 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'ASUFC, così come descritto nel presente documento;
- mantenuti e gestiti in modo da conservare e mantenere stabili nel tempo tutte le caratteristiche possedute al momento del collaudo definitivo.

In particolare, tutti i software forniti che verranno installati su dispositivi collegati alla LAN ASUFC e inseriti nei domini ASUFC, dovranno essere eseguiti sempre:

- in un contesto user space per i client,
- come servizio per tutti i server,
- come servizio per i client se non è richiesta interazione con l'operatore.

Non dovranno mai essere modificati in alcun modo i permessi di default del file system e del registro di sistema Microsoft (ove presente).

In particolare, per quanto concerne le configurazioni:

- quelle degli applicativi server dovranno risiedere in database e mai sui 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 nella cartella %HOMEDRIVE%\ProgramData, oppure nel registro di sistema (ove presente) nella sottochiave appositamente creata in fase di installazione in HKEY_LOCAL_MACHINE\SOFTWARE, ed in ogni caso 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 AES256;
- quelle personali degli applicativi client (ovvero riferite alle personalizzazioni dei singoli account) dovranno risiedere nel profilo dell'account a cui si riferiscono (ove presente).

Ovvero, non dovranno mai risiedere configurazioni globali degli applicativi client nei profili degli account, né altresì configurazioni personali degli applicativi client fuori dai profili degli account.

In particolare, a titolo esemplificativo e non esaustivo, si ricorda che, anche nel perimetro delle prescrizioni previste dalla Circolare AgID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni", i sistemi forniti:

- non devono prevedere alcun account locale;

- non devono prevedere alcun account impersonale per gli operatori e possono utilizzare account di servizio solo se del tipo gMSA, group Managed Service Account;
- devono consentire azioni di software inventory;
- devono poter essere distribuiti in “package” fruibili dai sistemi di distribuzione ASUFC;
- devono utilizzare solo sistemi di comunicazione sicuri (con protocolli basati su crittografia allo stato dell’arte);
- devono rispettare le tecnologie di protezione delle banche dati di dati personali e sensibili;
- devono consentire azioni di audit (es. vulnerability assessment) e il fornitore deve adoperarsi per la risoluzione in tempi certi ed accettabili delle anomalie rilevate dall’ASUFC o da ditte da quest’ultima incaricate.

In ogni caso i software oggetto di fornitura non dovranno fare uso di Applet Java e ActiveX.

Come indicato in premessa, l’aggiudicatario verrà designato responsabile ex art.28 del GDPR, ed in quest’ambito dovrà, tra l’altro, inviare, nel rispetto delle procedure ASUFC, 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’ASUFC e a livello personale, secondo le proprie procedure ed in ogni caso con i privilegi necessari e sufficienti allo svolgimento delle mansioni di competenza.

Per quanto concerne gli “account amministrativi” (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), questi:

- potranno, nel caso di account amministrativi locali di default (a titolo di esempio non esaustivo: “admin”, “administrator”, “root”, ecc.), essere impersonali e dovranno, ove richiesti, essere tutti comunicati all’ASUFC, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi locali ulteriori rispetto a quelli di default; ove non richiesti da ASUFC la gestione e responsabilità si intende a carico dell’aggiudicatario;
- dovranno, nel caso di account amministrativi non locali che consentano l’accesso interattivo a macchine/sistemi/applicativi collegati alla LAN ASUFC, essere sempre personali e rispettare quanto riportato nel presente documento relativamente alle modalità di autenticazione (authentication) degli operatori per mezzo di account – e relative credenziali – personali;
- non dovranno, nel caso di account amministrativi impersonali, essere in alcun caso presenti, se non del tipo gMSA;
- dovranno, nel caso di tutti gli account di sistemi non in LAN, essere gestiti a cura e responsabilità dell’aggiudicatario;
- potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN ASUFC, essere impersonali, ove richiesti, e dovranno essere tutti comunicati all’ASUFC, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza; in ogni caso non dovranno essere configurati account amministrativi in numero maggiore dello stretto necessario; ove non richiesti da ASUFC la gestione e responsabilità si intende a carico dell’aggiudicatario;

in tal caso, ovvero per quanto concerne gli account impersonali, consentiti solo secondo quanto riportato nel punto precedente, questi non dovranno in alcun caso permettere:

- di modificare le configurazioni, impostazioni e settaggi di macchine / sistemi / applicativi;
- di visualizzare, modificare o cancellare dati personali diversi da quelli eventualmente trattati contestualmente all’uso dell’account stesso.

Eventuali dati personali salvati in ulteriori archivi, diversi da quelli descritti nel presente documento, saranno ammessi solo con funzioni di “archivi provvisori”, ovvero di passaggio intermedio dei dati prima dell’invio agli archivi definitivi. I dati personali devono permanere negli archivi provvisori il minor tempo possibile, ovvero per un tempo massimo che sia configurabile e che non superi mai le 24 ore naturali, con l’implementazione di opportune procedure di cancellazione automatica che non consentano il recupero locale dei dati.

In ogni caso l’accesso agli archivi di dati personali (anche provvisori) dovrà avvenire solo da parte degli account personali e degli account gMSA autorizzati, sulla base di opportuni permessi settati in modo che il

livello dei privilegi di accesso sia il più basso possibile e che l'accesso ai dati avvenga sempre per tramite dell'applicativo e non direttamente da parte dell'account.

Non è consentita l'archiviazione, anche temporanea ed anche in forma anonima, dei dati su macchine situate esternamente rispetto alla rete dati dell'ASUFC, salvo esplicita autorizzazione da parte dell'ASUFC.

L'Aggiudicatario dovrà individuare, all'interno della sua organizzazione, una figura di "Responsabile per la sicurezza informatica delle forniture" da indicare prima dell'avvio dell'esecuzione contrattuale, nonché disporre di una struttura/funzione aziendale per la prevenzione e gestione degli incidenti informatici con il compito di interfacciarsi con l'IT di ASUFC, attraverso la figura sopra citata, per la gestione di eventuali incidenti informatici, oltre che adoperarsi per la segnalazione tempestiva nel caso di riscontro di eventuali incidenti informatici.

Qualora i sistemi dell'Aggiudicatario siano oggetto di attacco, in conseguenza del quale vengano compromessi sistemi da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di piena operatività garantendo di aver rimosso ogni possibile minaccia, adoperandosi con massima tempestività e prestando la massima disponibilità all'ASUFC.

L'Aggiudicatario deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati. Le utenze applicative dovranno essere nominali e le credenziali erogate dal medesimo Aggiudicatario secondo un percorso definito e sicuro che tenga separate username e password, in modo che sia possibile:

- definire la complessità della password secondo le migliori pratiche (lunghezza, maiuscole/minuscole e caratteri speciali);
- la gestione di più profili utente con privilegi di autorizzazione diversi; sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni, in modo che l'utente abbia accesso alle sole risorse relative all'attività che deve svolgere, secondo il principio di minimizzazione;
- la funzionalità di "richiesta creazione o cambio della password al primo accesso";
- il blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso;
- registrare gli accessi degli utenti in un archivio (log) non cancellabile;
- gestire i log di sistema (accessi, allarmi, ecc.).

Gli "account amministrativi" (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito), dovranno essere gestiti a cura e responsabilità dell'Aggiudicatario, seguendo le norme e le migliori pratiche in materia.

Su richiesta dell'ASUFC, l'Aggiudicatario dovrà fornire le credenziali di accesso degli apparati firewall eventualmente utilizzati in sola consultazione, inoltre dovrà configurare tali apparati affinché inviino in tempo reale i log degli eventi di sicurezza verso la piattaforma Security Information and Event Management (SIEM) aziendale.

Non sarà in alcun caso consentita la fornitura ed installazione di apparati attivi di rete (switch, router, firewall, access point Wi-Fi, VPN concentrator, Mi-Fi etc.) a meno di eccezioni concordate con l'ASUFC che in ogni caso si riserva di accettarle a suo insindacabile giudizio, a seguito di presentazione di adeguata documentazione tecnica che ne giustifichi la necessità. In particolare: nel caso di apparati di sicurezza, l'aggiudicatario si impegna, come precedentemente riportato, a documentare e mettere a disposizione ad ASUFC le regole di sicurezza sui firewall aziendali (ISFW – Internal Segregation Firewall) ASUFC; nel caso di apparati per la connettività remota, l'aggiudicatario si impegna a far uso degli strumenti aziendali messi a disposizione da ASUFC, come precedentemente riportato.

I firewall aziendali ASUFC, utilizzati come ISFW a protezione di ciascuno dei contesti di rete descritti nel presente documento (reti e VLAN), sono tecnologicamente dei NGFW (Next Generation Firewall) dotati di funzionalità di stateful inspection e con application control attivo, conseguentemente tutti i sistemi e le applicazioni oggetto di fornitura, nonché i servizi di assistenza remota e manutenzione, anche erogati tramite VPN, dovranno essere compatibili con tali tecnologie. A titolo di esempio non esaustivo, sistemi e applicazioni dovranno effettuare una gestione attiva del ciclo di vita delle sessioni e, per evitare malfunzionamenti o blocchi delle stesse non dovrà mai essere necessario modificare i relativi parametri di timeout (Session-TTL) sui firewall

aziendali. ASUFC si riserva di bloccare qualunque tipologia di traffico ritenuto malevolo, in particolare a fronte di specifiche vulnerabilità che dovessero emergere nel corso della durata contrattuale.

Documentazione

L'Aggiudicatario prima dell'avvio della fornitura/servizio dovrà predisporre un documento tecnico sintetico, ma esaustivo, che illustra la progettualità relativamente alle componenti IT, che tenga conto delle eventuali relazioni con altri sistemi collegati. Nel documento dovranno essere esplicitati i seguenti aspetti:

- descrizione delle finalità della soluzione, i reparti e il personale coinvolti
- rappresentazione grafica architettuale dell'infrastruttura hardware e software del sistema qualora ne sia prevista l'installazione, anche solo di parte, presso l'ASUFC
- illustrazione grafica del flusso dati della soluzione
- aspetti di sicurezza della soluzione anche tenendo in conto dei livelli di servizio e della tipologia di dati trattati: continuità del servizio, gestione incidenti e disaster recovery; manutenzione del sistema, aggiornamento sistema operativo e applicativi
- la modalità erogazione delle credenziali agli utenti
- censimento degli eventuali applicativi che saranno installati sulle postazioni di lavoro aziendali dell'ASUFC, al fine di essere inseriti nella white list del software.

Il documento dovrà essere completato integrato con le analoghe informazioni relative ad altri eventuali forniture/servizi dell'Aggiudicatario in ambito IT presenti nell'ASUFC, in modo che sia chiaramente descritto l'installato complessivo del fornitore in ASUFC. Nell'allegato denominato "Kit redazione documentale" sono riportate le linee guida per la redazione della documentazione a cui il fornitore dovrà attenersi. Solo se la documentazione che descrive la progettualità dell'intervento sarà completa, chiara e sintetica, si procederà con la fase realizzativa. Al termine della fase realizzativa, il fornitore dovrà integrare la documentazione con tutte le informazioni reperite durante l'implementazione della soluzione (ad esempio gli indirizzi IP assegnati agli apparati) e contenere le eventuali varianti intervenute con l'autorizzazione dell'ASUFC.

Definizioni

RPO: Recovery Point Objective, indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto; si misura in minuti oppure ore.

RTO: Recovery Time Objective, massimo tempo di indisponibilità del servizio, cioè tempo entro il quale il servizio deve essere ripristinato; si misura in minuti oppure ore.

Lock-in: situazioni in cui le decisioni di acquisto in un certo momento vincolano le decisioni future.

IaaS: Infrastructure as a Service (IaaS), è un modello di servizio cloud, per cui viene lasciata facoltà all'utente di acquisire elaborazione, memoria, rete e altre risorse fondamentali di calcolo, inclusi sistemi operativi e applicazioni. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante, ma controlla sistemi operativi, memoria, applicazioni ed eventualmente, in modo limitato, alcuni componenti di rete.

SaaS: Software as a Service (SaaS), identifica la classe di servizi fully-managed in cui il gestore del servizio si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura cloud propria o di terzi), lasciando al fruitore del servizio il solo ruolo di utilizzatore delle funzionalità offerte.

Insiel SpA: società in house della Regione Autonoma Friuli Venezia Giulia che eroga servizi alle Aziende Sanitarie della regione medesima, secondo quanto previsto dalla Legge regionale 14 luglio 2011, n. 9 "Disciplina del sistema informativo integrato regionale del Friuli Venezia Giulia".

Allegati

- "Kit redazione documentale"

