

SPECIFICHE IT ASUGI

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'ASUGI 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 ASUGI 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. Il modulo fac simile di designazione è riportato in allegato ed è parte integrante della documentazione di gara.
- dalla Circolare 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'ASUGI 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.

Qualora i sistemi forniti intendano essere collegati nella rete aziendale, essendo quest'ultima intrinsecamente una rete IT medica secondo la norma IEC 80001-1, s'intende che 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 stessa norma. Tale documento farà esplicito

riferimento all'installazione ASUGI, 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, redatto dall'aggiudicatario e revisionato/validato da ASUGI, conterrà espliciti riferimenti alla "marcatura CE" dei sistemi offerti ed al fatto che i requisiti essenziali di sicurezza non verranno inficiati nella particolare installazione ASUGI e nel tempo, così come intesa sopra.

Qualora i sistemi forniti non s'intendano collegati in alcuna maniera alla rete dati, essi devono comunque rispondere ai requisiti dettati dalla normativa citata.

Se l'oggetto di fornitura include dispositivi medici, il fornitore dovrà compilare, sottoscrivere e allegare all'offerta tecnica il modulo Manufacturer Disclosure Statement for Medical Device Security (MDS2) versione 2019 per ciascuno di essi, in maniera da permettere all'Azienda una più agevole valutazione delle eventuali criticità della messa in uso dei sistemi offerti anche secondo EC/TR 80001-2-2. È comunque onere del fornitore verificare la versione più recente del modulo dal sito NEMA e compilare e fornire tale versione.

In caso di fornitura di dispositivi medici, inoltre, l'aggiudicatario con la partecipazione alla presente procedura di gara dichiara che le caratteristiche tecniche dell'infrastruttura IT descritte in capitolato e nel presente documento, sono adeguate ai dispositivi medici oggetto di fornitura, nei termini previsti dal Regolamento Europeo 2017/745 con particolare riferimento all'Allegato I – par. 17.4 (*"I fabbricanti indicano i requisiti minimi in materia di hardware, caratteristiche delle reti informatiche e misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato, necessari per far funzionare il software come previsto"*).

Inoltre, sempre nel caso in cui l'oggetto di fornitura include dispositivi medici, il sistema fornito dovrà rispondere a quanto richiesto:

- dal IHE Patient Care Device (PCD) White Paper, "Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide";
- dalla linea guida "MDCG 2019-16 Guidance on Cybersecurity for medical devices".

In generale l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e nel 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 di altro soggetto, l'aggiudicatario rimane responsabile di monitorare tali elementi e segnalare in via formale qualora ritenga vi siano 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. Analogamente l'aggiudicatario accetta e collabora pienamente a qualsiasi attività di assessment e audit che ASUGI o società da essa incaricate dovessero condurre sui sistemi oggetto di fornitura.

In coerenza con quanto stabilito dal "Piano triennale per l'informatica nella Pubblica Amministrazione" di AGID e della "Strategia Cloud Italia" del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, tutti i "servizi digitali" forniti nell'ambito della presente procedura ad ASUGI dovranno rispondere al "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica

amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione” (cosiddetto “Regolamento Cloud e Infrastrutture”, adottato da AGID con Determinazione 628/2021) e pertanto tali servizi digitali dovranno essere qualificati come SaaS sul Marketplace ACN con livello coerente necessario con la classificazione dei dati oggetto di trattamento (“ordinari”, “critici” o “strategici”) nell’ambito della presente fornitura.

Pertanto, in linea con il principio “cloud first”, i servizi digitali oggetto di fornitura potranno essere erogati in modalità SaaS, fermo restando tutte le prescrizioni riportate nel presente documento, in particolare quelle relative al single sign-on.

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 tramite collegamento internet e tramite i web browser in uso presso ASUGI 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 in alcun caso verranno 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 ASUGI 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 ASUGI e senza oneri aggiuntivi per ASUGI stessa, il SSO così come di seguito descritto: ASUGI 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 tramite il protocollo SAML v2.0. In tal senso dovrà essere possibile l’autenticazione ai sistemi forniti tramite le credenziali di dominio Microsoft Active Directory di ASUGI, se i servizi sono fruiti dall’interno delle reti private RUPAR, e – in maniera configurabile – tramite le credenziali di dominio Microsoft Active Directory di ASUGI 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 ASUGI e secondo le modalità descritte di seguito.

Inoltre, sempre in coerenza con quanto stabilito da AGID, i sistemi forniti dovranno essere progettati, realizzati ed 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, il che sarà vincolato al pagamento delle ultime due fatture. 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 o "Integrazione con l'infrastruttura IT", 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 generale per l'analisi preliminare e l'avviamento all'uso dei sistemi oggetto di fornitura ASUGI 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 ASUGI, che vadano oltre i limiti sopra riportati, verranno computati da ASUGI che si riserva la facoltà di quantificare le relative spese in base al listino allegato alla Convenzione Consip "Servizi di System Management" e di dedurle dal piano di fatturazione previsto. Con la partecipazione alla gara si intende accettato tale meccanismo compensativo.

Specifiche di integrazione con il sistema informativo ospedaliero

L'integrazione con il LIS avverrà attraverso la soluzione di middleware strumentale HALIA, fornita ad ASUGI e gestita dalla società in house della Regione Autonoma Friuli Venezia Giulia denominata Insiel SpA. È possibile prevedere scenari di integrazione sia tra HALIA ed un unico middleware collettore per tutti i sistemi, sia verso singoli sistemi.

L'integrazione dovrà garantire lo scambio bidirezionale dei dati ed essere flessibile nel supportare il flusso di lavoro ed eventuali variazioni dello stesso nel tempo. L'integrazione con il middleware fornito sarà realizzata necessariamente secondo standard HL7, mentre nel caso di integrazione con singoli analizzatori sarà possibile usare anche altri protocolli di comunicazione.

L'integrazione dovrà garantire anche la comunicazione di immagini e grafici, laddove presenti, al fine di poter generare referti completi di ogni informazione.

In fase di offerta andranno indicate tutte le integrazioni che si ritiene di dover realizzare verso HALIA e per ciascuna di esse andrà indicato se tali integrazioni sono già state realizzate e sono in uso presso altre strutture sanitarie.

Se alcune delle integrazioni tra strumenti ed HALIA non fossero ancora state realizzate, sarà a carico del fornitore ogni attività legata alla procedura di marcatura CE dei moduli software utilizzati allo scopo.

Ogni componente hardware e software, compresi eventuali elementi considerati accessori (a solo titolo di esempio non esaustivo cavi, convertitori interfaccia), necessari all'integrazione con il LIS sono a totale carico del fornitore, fatta eccezione per il costo delle attività di integrazione di competenza di Insiel SpA.

Il software acquisito dovrà prevedere inoltre la possibilità di integrazione con il sistema di gestione della logistica fornito ad ASUGI da Insiel SpA, per garantire la comunicazione con i magazzini in uso presso il laboratorio al fine di condividere scorte e movimenti di materiali con gli stessi. In particolare si richiede che il sistema sia in grado di effettuare il controllo centralizzato dei materiali impiegati e quindi il riordino automatico quando sotto

scorta, garantendo un cruscotto di monitoraggio dei movimenti di magazzino in base alle informazioni ricavate dalle integrazioni.

Il sistema dovrà prevedere dunque la possibilità di scambio di informazioni attraverso l'invocazione di web-services o attraverso la possibilità di ricevere ed inviare messaggi in formato HL7.

In fase di avvio del sistema, Insiel SpA, per quanto di sua competenza, metterà a disposizione tutte le informazioni tecniche necessarie per le integrazioni richieste.

Visto l'importante periodo temporale della fornitura, per tutte le integrazioni dovrà essere garantita la manutenzione per l'intera durata dell'appalto, sia in termini di manutenzione correttiva sia in termini di manutenzione evolutiva, al fine di salvaguardare la possibilità da parte di ASUGI di mantenere l'aderenza agli standard nel tempo.

In generale tutti i sistemi forniti, in qualunque scenario tecnologico (SaaS o "Integrazione con l'infrastruttura IT", così come descritti nel presente documento) dovranno consentire la disponibilità di dati aperti e le relative interfacce di accesso secondo le linee guida di interoperabilità AgID.

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'ASUGI, secondo quanto riportato nel seguito.

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 ASUGI seguendo lo scenario descritto nel seguito.

In particolare, gli host oggetto di fornitura saranno integrati nella sola infrastruttura di rete ASUGI e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico verrà effettuata assegnando agli host stessi una specifica classe di indirizzi IP statici (se il numero di host complessivi afferenti alla rete assegnata è minore di 50) o dinamici (se il numero di host complessivi afferenti alla rete assegnata è maggiore di 50) coerente con il piano di indirizzamenti ASUGI e verranno inseriti in una VLAN dedicata, assegnata dall'ASUGI, dalla quale potranno effettuare solo l'eventuale traffico necessario per svolgere le funzioni richieste in capitolato 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), per una durata complessiva di 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 di rete sulle reti IP/VLAN dei PC in dominio ASUGI. ASUGI si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.

È attivo sulla LAN ASUGI 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 ASUGI 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 unicamente per mezzo di connessione cablata alla rete LAN ASUGI, secondo quanto riportato precedentemente. Non sarà consentito in alcun caso il collegamento di tali dispositivi tramite le postazioni di lavoro ASUGI (PC) – per esempio con collegamenti USB – o tramite rete Wi-Fi, in quanto ASUGI non è dotata di tale tipo di infrastruttura a servizio di tali casi d'uso. 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 (secondo la CEI 64-8/7), se del caso, ovvero rispondenti ai seguenti requisiti: rispondenza alle norme IEC 60601-1, grado di protezione IP pari almeno ad IP54; certificazione per resistenza alle cadute da 1 metro di altezza (per esempio secondo MIL-STD-810F/G); involucro/custodia certificato sanificabile, privo di spigoli (seamless) e realizzato in materiale antibatterico/antimicrobico soprattutto in relazione a MRSA. Le attività svolte dagli operatori ASUGI su tali dispositivi dovranno essere garantite dal fornitore con 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, data la necessità di avere connettività esclusivamente cablata di cui sopra.

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 ASUGI, basati su tecnologia Cisco AnyConnect e su cui la modalità Split Tunnel è per policy sempre disattivata. L'accesso verrà consentito solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario – compilando il modulo standard ASUGI – ed inviata da casella PEC ad asugi@certsanita.fvg.it, con allegati i documenti di identità e CF in corso di validità dei soggetti da abilitare. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali con bassi privilegi (livello user), ed in alcun caso saranno consentite connessioni di tipo site-to-site. 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'ASUGI. Il servizio di connessione remota VPN ASUGI non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio VPN in altro modo (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 i 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 ASUGI è il firewall di navigazione gestito dalla società in house della Regione Autonoma Friuli Venezia Giulia denominata Insiel SpA: gli host forniti potranno raggiungere solo un numero limitato di destinazioni internet, su specifiche 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'essfiltrazione di dati tramite questo canale. Verranno perciò effettuate specifiche abilitazioni basate su IP sorgente, IP destinazione e porta solo a seguito di domanda sottoscritta digitalmente dal legale rappresentante o procuratore protempore dell'aggiudicatario – compilando il modulo standard ASUGI – ed inviata da casella PEC ad asugi@certsanita.fvg.it. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'ASUGI per la definizione delle suddette abilitazioni. Nel presente scenario, la risoluzione dei nomi sarà basata esclusivamente su uno specifico servizio DNS (Domain Name Service) dedicato a tutti i dispositivi segregati/isolati presenti sulla rete ASUGI, compresi quelli oggetto di fornitura. Analogamente al servizio VPN ASUGI di cui sopra, anche il servizio di connettività in uscita tramite firewall di navigazione Insiel non verrà prestato all'aggiudicatario con livelli di servizio garantiti, perciò il servizio offerto dovrà essere organizzato in modo da sopperire all'indisponibilità del servizio in altro modo (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 i livelli di servizio in caso di indisponibilità del servizio.

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 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.

In caso di sistemi operativi server di tipo non Windows, 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 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 ASUGI). In tal caso non sarà necessaria la fornitura dei PC client dedicati da parte dell'aggiudicatario. ASUGI tutta via 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 da installazione da rack standard 19" con una occupazione massima di 2 rack unit (a meno di documentata necessità) e dotati di doppio modulo di alimentazione integrato.

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

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 descritto nel presente documento, 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 dal primo paragrafo del presente documento e sempre in coerenza con il paradigma "Zero Trust".

Verranno eseguite periodicamente da ASUGI 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 in tal modo emergere. Analogamente l'aggiudicatario si impegna a collaborare con il SOC (Security Operation Center) aziendale ASUGI 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 in nessun caso in errori nelle date, nei dati numerici e nei dati personali locali;
- stabili, in particolare che siano in grado di gestire le eccezioni;
- sicuri, sia dal punto di vista della sicurezza informatica che della qualità delle funzioni svolte;
- ottimizzati, in termini di rapporto tra uso delle risorse e prestazioni;
- sviluppati tenendo conto dei principi del "ciclo di vita del software" e dell'"analisi del rischio", secondo le norme tecniche (o principi e metodologie almeno equivalenti) e le best 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 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'ASUGI, 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 ASUGI e inseriti nel dominio aouts.it, 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,

ed in ogni caso non dovranno 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 comunque 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, in ogni caso non dovranno risiedere configurazioni globali degli applicativi client nei profili degli account, né altresì configurazioni personali degli applicativi client fuori dai profili degli account.

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 nessun account locale;
- non devono prevedere nessun account impersonale per gli operatori e 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 ASUGI;

- devono utilizzare solo sistemi di comunicazione sicuri (crittati);
- devono rispettare le tecnologie di protezione delle banche dati di dati personali e sensibili;
- devono consentire le valutazioni di vulnerabilità e il fornitore deve adoperarsi per la risoluzione in tempi certi ed accettabili delle anomalie rilevate dall'Azienda o dalle aziende ad esse deputate.

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 ASUGI, 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'ASUGI 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 essere tutti comunicati all'ASUGI ove richiesti, 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 ASUGI 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 ASUGI, 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 ASUGI, essere impersonali e dovranno essere tutti comunicati all'ASUGI ove richiesti, 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 ASUGI 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 in ogni caso non superi 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'ASUGI, salvo esplicita autorizzazione da parte dell'ASUGI.

Non sarà in alcun caso consentita la fornitura ed installazione di apparati attivi di rete standard (switch, router, firewall, access point Wi-Fi, VPN concentrator, Mi-Fi etc.) a meno di eccezioni concordate con l'ASUGI 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 trasferire le logiche di sicurezza sui firewall aziendali (ISFW – Internal Segregation Firewall) ASUGI; nel caso di apparati per la connettività remota, l'aggiudicatario si impegna a far uso degli strumenti aziendali messi a disposizione da ASUGI, come precedentemente riportato.

I firewall aziendali ASUGI, 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 statefull inspection e con application controll 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 ed in alcun caso per evitare malfunzionamenti o blocchi delle stesse dovrà essere necessario modificare sui firewall aziendali i relativi parametri TTL (Time-To-Live). ASUGI 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.

Non sarà in generale consentita la fornitura di sistemi di cablaggio dati dedicati, a meno di casi particolari tecnicamente motivati, che dovranno essere esplicitati in offerta tecnica, motivati dettagliatamente ed approvati in ultima istanza da ASUGI. Riguardo al cablaggio strutturato, dovranno essere utilizzati sempre e comunque i sistemi aziendali e gli eventuali ampliamenti necessari saranno eseguiti da ASUGI. Dovranno essere indicati in offerta tecnica il numero e la dislocazione spaziale dei punti rete necessari al funzionamento dei sistemi oggetto di fornitura, indicando per ciascun punto l'eventuale necessità di installazione di dispositivi di separazione (Separation Device) conformi alle norme IEC 60601-1, la cui installazione sarà a carico di ASUGI. Nel caso in cui l'aggiudicatario volesse comunque offrire servizi di posa in opera di cablaggio strutturato,

dovrà sottostare a tutte le policy ASUGI, oltre alle norme tecniche di riferimento, e ASUGI si riserva di indicare ogni singolo dettaglio realizzativo (compresi marca e modello, classe CPR, categoria, ecc. dei materiali da utilizzare) che costituiranno vincolo contrattuale inderogabile.

Non saranno in alcun caso fornite da ASUGI SIM voce o dati per garantire la connettività dei dispositivi oggetto di fornitura. Le SIM eventualmente necessarie per garantire ai dispositivi forniti le funzionalità richieste nella documentazione di gara sono pertanto da intendersi incluse nella presente fornitura e funzionanti per tutta la durata contrattuale.