**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 medicale 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 2013 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. E' comunque onere del fornitore verificare la versione più recente del modulo dal sito NEMA e compilare e fornire tale versione.

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.

In coerenza con quanto stabilito dal Piano Triennale AGID che suggerisce un approccio "cloud first", i servizi 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 erogati in modalità SaaS dovranno essere pubblicati sul Cloud Marketplace di AgID, la piattaforma che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018. 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 supportati dai tre principali vendor mondiali 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, per esempio tramite opportuna implementazione del protocollo HTTPS (TLS 1.1 o 2.0), 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, il SSO così come di seguito descritto: ASUGI è dotata di un sistema IdP, 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, 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 nello Scenario 1.

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 vincolate 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.

**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 per ASUGI da Insiel SpA. E' 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.

**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 uno dei due scenari, mutuamente esclusivi, descritti nel seguito.

**Scenario 1: sistemi isolati**

Nel primo scenario, 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. 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, 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 dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUGI, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'ASUGI. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali, 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 potrà avvenire 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 e della loro configurazione da parte dell'ASUGI.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, nel presente scenario, lo strumento messo a disposizione dall'ASUGI è il proxy di navigazione autenticata, gestito da Insiel e basato su tecnologia Blue Coat: gli host forniti dovranno essere tali da consentire la configurazione del proxy internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici. Verranno effettuate specifiche eccezioni all'autenticazione basate su IP sorgente che consentiranno il traffico solo sulle porte necessarie e solo verso gli IP necessari. L'aggiudicatario dovrà fornire la massima collaborazione in tal senso all'ASUGI per la definizione delle suddette eccezioni.

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 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, 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.

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.

**Scenario 2: sistemi integrati**

Nel secondo scenario, in alternativa, l'aggiudicatario dovrà integrare i sistemi oggetto di fornitura anche con l'infrastruttura sistemistica dell'ASUGI. Di seguito vengono riportate, in prima istanza, alcune caratteristiche peculiari dell'infrastruttura informatica dell'ASUGI; successivamente vengono definite le specifiche di interfacciamento all'infrastruttura ASUGI che i sistemi oggetto di fornitura dovranno avere 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.

ASUGI comprende più di 40 sedi e in tali sedi le logiche di integrazione sono le medesime e di seguito descritte. In funzione della complessità del sito, non sono implementati localmente tutti i servizi d'infrastruttura, ma sono resi disponibili tramite la connettività WAN nel sito dell'Ospedale di Cattinara, che ospita il locale tecnico principale

per i servizi accessori per le applicazioni, oppure presso il sito di continuità di servizio dell'Ospedale Maggiore.

L'ASUGI è dotata di un dominio Active Directory (AD) 2016 (denominato "aouts.it"), che nel prossimo futuro verrà migrato alla versione 2012 R2. Nel sito AD principale (Ospedale di Cattinara) e nel sito di continuità (Ospedale Maggiore) 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 ASUGI di appartenenza.

La default domain policy impone l'utilizzo di password complesse di almeno 12 caratteri, con password history a 24 e cambio password obbligatorio ogni 90 giorni. Gli aggiornamenti di sistema per i client e per i server vengono distribuiti tramite il servizio Microsoft WSUS, su base mensile e appena rilasciati da Microsoft.

Le postazioni di lavoro ASUGI (PC) sono inserite nel dominio aouts.it. 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 7 Professional Italiano
- browser Microsoft Internet Explorer 8 (nel seguito anche IE8) e Google Chrome di ultima versione
- CPU Intel Core Due Duo 2,93 GHz o equivalente
- memoria RAM DDR2 2 GB
- HDD da 250 GB

a

- sistema operativo Microsoft Windows 10 Professional Italiano, ultima Build disponibile e non end of service
- browser Microsoft Internet Explorer 11 (nel seguito anche IE11; non configurabile in modalità compatibilità con versioni precedenti) e Google Chrome di ultima versione
- CPU core i7-6700
- 8 GB RAM
- SSD da 256 GB

Tutte le postazioni di lavoro ASUGI sono dotate di connettività di rete Gigabit Ethernet (secondo quanto definito dagli standard IEEE 802.3). Tutti gli operatori aziendali accedono, nell'operatività quotidiana, alle postazioni di lavoro (PC) tramite account e relative credenziali personali con bassi privilegi; 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 (Domain Name Service), integrato in AD, che accetta solo registrazioni sicure. I server Microsoft aziendali appartengono a due subnet IP dedicate – una per ciascun sito AD – e sono virtualizzati tramite due sistemi VMware vSphere v6.x, uno installato presso l'Ospedale di Cattinara ed uno presso l'Ospedale Maggiore; tutte le macchine ivi ospitate sono dotate di sistema operativo Microsoft Windows Server in supporto. L'architettura di rete ASUGI è realizzata in modo che tutti i servizi sono raggruppati nel locale tecnico principale ASUGI del sito di pertinenza; in particolare i server virtualizzati appartengono ad una rete IP/VLAN dedicata.

In generale la LAN ASUGI 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, 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 d'infrastruttura e applicativi) alla periferia (client/host) e viceversa.

È attivo sulla LAN ASUGI un servizio DHCP (Dynamic Host Configuration Protocol) che in generale rilascia gli indirizzi IP a tutti gli host in rete, ad esclusione dei server (per i quali sono previste specifiche configurazioni) e degli host con IP statico.

Come precedentemente riportato, è attivo sulla LAN ASUGI un sistema di autenticazione degli host di rete basato su protocollo IEEE 802.1x e su tecnologia Microsoft NPS. L'autenticazione è basata, a seconda delle caratteristiche dell'host, su uno dei seguenti criteri (ordinati per livello di sicurezza e quindi per preferenza di implementazione):

- certificato o account macchina Microsoft Active Directory, se l'host è dotato di client AD;
- nome utente e password, se l'host non è dotato di client AD ma è dotato di client IEEE 802.1x;
- MAC address, solo se l'host non è dotato di client IEEE 802.1x.

La struttura di backup ASUGI è basata su due tape library: una Sun Storage Tek SL500 e una Sun Storage Tek SL48. Tramite il software Symantec Backup Exec 10d, le tape library effettuano – con periodicità variabile a seconda dei casi – le copie di sicurezza: dei sistemi operativi di tutti i server ASUGI, della configurazione dei DB ASUGI, dei dati (presenti sui NAS e sui file server), delle macchine virtuali, dei registri di log dei sistemi.

ASUGI dispone di istanze Microsoft SQL Server 2019 Enterprise 64 bit che nel prossimo futuro verrà migrato alla versione 2019 Standard; tutti i database delle applicazioni aziendali basati su tale tecnologia vengono ivi istanziati. Tali istanze supportano solo l'autenticazione nativa (Native Mode o Windows Integrated) e l'istanza di default non viene utilizzata.

L'applicativo antivirus (AV) aziendale è l'ESET Endpoint Protection Advanced (Security) distribuito su tutti i server (nella versione ESET File Security) e su tutti i client e aggiornato automaticamente ogni tre ore.

Su tutti i client aziendali è presente l'agente CA IT Client Manager v14.x, che consente l'accesso interattivo alle sessioni utente per fini di assistenza tecnica.

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) e comunque non 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 ASUGI 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 ASUGI.

Nel caso in cui i sistemi forniti utilizzino Java, a qualunque titolo, si intendono incluse nella presente fornitura le licenze necessarie, secondo quanto stabilito dalle licencing policy di Oracle, senza oneri aggiuntivi per ASUGI. In alternativa potranno essere utilizzate le distribuzioni che utilizzano licencing open source o similari (a titolo di esempio non esaustivo openJDK, basato su licenza GPL), fermo 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 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, gli eventuali server forniti dovranno essere virtualizzati nel sistema ASUGI VMware vSphere v6.x e seguirne le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, di backup e di disaster recovery. 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 almeno con il sistema operativo Windows Server 2016 Standard Edition ENG e inserite nel dominio aouts.it e conseguentemente nel sistema WSUS ASUGI.

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.

Tutte le licenze Windows Server necessarie al funzionamento del sistema non sono da intendersi a carico del fornitore e non saranno in alcun caso di tipo OEM, bensì licenze Retail intestate all'ASUGI e comunque in ogni caso compatibili con l'ambiente di virtualizzazione dell'ASUGI descritto precedentemente.

Allo scopo di uniformare i sistemi forniti agli standard ASUGI, compresi quelli di sicurezza e autorizzazione (authorization), tali macchine server verranno dotate di sistema operativo Microsoft Windows Server 2016 e inserite in una Organizational Unit (OU) generica dedicata ai server ASUGI oppure in una OU dedicata al fine di definire ed applicare su di esse specifiche Group Policy concordate con l'ASUGI; la default domain policy verrà applicata in ogni caso su tutte le OU. Ai server verrà in ogni caso assegnata una opportuna classe di indirizzi IP fissi.

Nel presente scenario potranno essere installate negli ESX ASUGI specifiche schede GPU (Graphics Processing Unit) tipo PCI express full size, che dovranno essere oggetto di fornitura e in numero pari a tre (una per ciascun ESX). In tal caso l'aggiudicatario dovrà dettagliarne le caratteristiche tecniche, marca e modello, nonché le funzioni applicative per cui sono necessarie.

Nel presente scenario, i dati acquisiti e generati dal sistema e/o i loro riferimenti, nonché tutti quelli direttamente o indirettamente necessari al funzionamento degli applicativi forniti, dovranno essere organizzati in uno o più RDBMS, che potranno essere istanziati sui server Microsoft SQL ASUGI; in tal caso dovranno seguirne le politiche di gestione, comprese quelle di backup e disaster recovery. In particolare verranno dedicati ai sistemi forniti uno o più database, in accordo con l'ASUGI, i cui nomi dovranno essere parametrizzabili e modificabili sulla base delle necessità tecniche di ASUGI. In ogni caso non verrà variata la configurazione di default del motore di database del server Microsoft SQL ASUGI in essere al momento dell'installazione, eventuali adeguamenti del sistema oggetto di fornitura al fine di renderlo compatibile con quanto sopra sono da intendersi

inclusi nella presente fornitura; potrà a discrezione di ASUGI essere concesso un periodo di adeguamento pari a massimo tre mesi dall'aggiudicazione.

L'aggiudicatario dovrà comunicare le richieste ad ASUGI in materia di politiche di maintenance dei database, oltre ad una descrizione delle attività delle applicazioni sui database stessi e sulla dinamica dei dati ospitati. Il piano definitivo dovrà essere proposto dall'aggiudicatario e redatto con le finalità di una gestione efficiente ed efficace dei database e sarà poi validato ed eseguito da ASUGI.

Sarà esclusivo onere dell'aggiudicatario, nel caso intenda utilizzare diversi motori di database, comunicare le necessarie politiche di manutenzione e controllo, anche a livello sistemistico, allo scopo di garantire i necessari standard di performance e sicurezza.

In base alle specifiche scelte, progettuali e di infrastruttura, l'aggiudicatario dovrà usufruire della struttura di backup ASUGI per i sistemi operativi di tutti i server e per la configurazione dei database. Dovrà essere fornito all'ASUGI supporto per il loro inserimento nel sistema di backup dell'ASUGI, nonché per la redazione delle procedure di backup e disaster recovery.

Qualora il motore di database scelto sia diverso da SQL Server, le politiche di backup e disaster recovery saranno concordate con l'aggiudicatario che dovrà comunque comunicarne i requisiti ritenuti opportuni all'Azienda.

Ogni attività di tipo change lato server, inteso come intervento o aggiornamento sui sistemi oggetto di fornitura, non dovrà in ogni caso causare disservizio maggiore di 10 minuti ovvero di 3 ore quando sono previste soluzioni di businness continuity ritenute accettabili da ASUGI, 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 ASUGI, 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. Sono da ritenersi a carico di ASUGI solo ed esclusivamente gli oneri e le licenze esplicitate nel presente documento: le licenze VMware di base, le licenze di Microsoft Windows Server e SQL Server legate all'infrastruttura centralizzata di ASUGI. Sono quindi a carico dell'aggiudicatario 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 ASUGI nelle attività di costante aggiornamento dei sistemi, in rispondenza al quadro normativo e legislativo in essere.

Relativamente agli archivi correnti di dati e documenti, ASUGI 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 ASUGI, ovvero ogni attività necessaria per ottenere archivi correnti con dati e documenti di età inferiore all'orizzonte temporale definito da ASUGI.

Nel presente scenario, lato utente, ovvero lato postazione ASUGI (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.

Gli eventuali applicativi client forniti, necessari all'espletamento di una o più funzionalità richieste, verranno installati sulle postazioni ASUGI – senza limitazioni in termini di numero di postazioni – e dovranno essere adeguati alle caratteristiche software e hardware delle postazioni stesse, in particolare alle policy del dominio aouts.it e conseguentemente a quelle del sistema WSUS ASUGI. La distribuzione sulle postazioni di lavoro ASUGI di tali applicativi, nonché degli aggiornamenti, verrà eseguita esclusivamente a seguito della fornitura ad ASUGI, da parte dell'aggiudicatario, dei pacchetti di aggiornamento con tecnologia MSI o Installshield. Tali pacchetti saranno poi distribuiti ed eseguiti dalle Aziende attraverso il sistema di gestione CA IT Client Manager.

Gli eventuali applicativi web, forniti nell'ambito della presente fornitura, dovranno essere compatibili con almeno uno dei browser attualmente installati su ciascuna delle postazioni ASUGI. 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 1.1 o 2.0).

Nel presente scenario non saranno considerati accettabili eventuali PC forniti, se non identici ad uno dei modelli standard già in produzione presso ASUGI che in tal caso potranno essere inseriti nel dominio aouts.it a seguito di clonazione e hardening standard ASUGI e a condizione di seguire le policy e caratteristiche dei PC ASUGI, così come descritte nel presente documento.

Nel presente scenario, tutte le funzionalità dei sistemi forniti dovranno essere garantite con il sistema di indirizzamento IP dinamico (DHCP) attivo sulle postazioni ASUGI e non verranno in alcun caso create sul servizio DHCP configurazioni di tipo reservation e exclusion.

Nel presente scenario, tutte le funzionalità dei sistemi forniti dovranno essere garantite con il client antivirus aziendale l'ESET Endpoint Protection Advanced (Security) di cui ogni postazione ASUGI è dotata, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'ASUGI, a meno di eccezioni concordate con l'ASUGI che in ogni caso si riserva di accettare. Inoltre, saranno 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 con l'agente CA IT Client Manager v14.x di cui ogni postazione ASUGI è dotata.

Nel presente scenario, eventuali host (di tipologia non server) oggetto di fornitura che non siano dotati di client AD e che necessitano di connettività con la rete dati ASUGI, verranno connessi alla stessa 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 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 ASUGI. 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 le stesse prescrizioni riportate nello Scenario 1 del presente documento.

ASUGI si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.

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

Nel presente scenario, tutti i dispositivi forniti collegati alla LAN ASUGI dovranno autenticarsi in rete secondo il protocollo 802.1x, con uno dei tre criteri sopra esposti. In particolare:

- tutti i client tramite certificato o account macchina;
- tutti gli host non dotati di client AD, dovranno autenticarsi per mezzo di nome utente e password o di MAC address.

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali ASUGI, a cui sarà dato accesso solo a seguito di domanda scritta rivolta all'ASUGI. La connessione VPN dovrà essere di tipo client-to-site ed effettuata per mezzo di credenziali personali, 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 aziendali ASUGI CA IT Client Manager v14.x e Microsoft Windows RDP, nel caso di host dotati di client AD; potrà avvenire 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 e della loro configurazione da parte dell'ASUGI, nel caso di host non dotati di client AD.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, nel presente scenario, lo strumento messo a disposizione dall'ASUGI è il proxy di navigazione autenticata, gestito da Insiel e basato su tecnologia Blue Coat: gli host forniti dovranno essere tali da consentire la configurazione del proxy internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici.

È in uso presso l'ASUGI 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 ASUGI e successivamente

vengono definite le specifiche dei sistemi da fornire in tal senso, nell'ambito del presente scenario.

Il SSO ASUGI permette al singolo account di autenticarsi una sola volta e di essere successivamente autenticato automaticamente – ovvero in maniera trasparente e senza dover reinserire le proprie credenziali – ogni volta che tenta di accedere ad una risorsa di rete di rete a cui è abilitato. Gli account possono essere associati sia a credenziali personali (ad uso esclusivo di una persona fisica, ovvero di un operatore) che impersonali (ad uso non esclusivo di una sola persona fisica, ovvero di un operatore), nonché account digitali (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 ASUGI 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 2008 R2 (aouts.it) e non accetta bind anonimi né senza cifratura (ovvero senza LDAP over SSL/TLS). Per quanto riguarda l'autenticazione degli account, questa si basa sul protocollo kerberos versione 5 (in seguito anche v.5) e viene effettuata dal dominio aouts.it. Il SSO ASUGI ricalca quanto trova nome in letteratura 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.

I sistemi forniti dovranno essere coerenti ed integrati con la soluzione di SSO ASUGI, in alternativa all'autenticazione integrata Windows il fornitore potrà implementare, in accordo con ASUGI, 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 suddetto, l'unico repository di account ASUGI (personali e impersonali) è il directory service Active Directory e a ciascun account di dominio sono associate le rispettive credenziali informatiche. In tal senso tutte le credenziali personali, previste negli applicativi e nei sistemi forniti, dovranno essere quelle del dominio aouts.it; gli account associati a credenziali personali si autenticheranno 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, dovranno essere opportunamente create e configurate nel dominio aouts.it senza funzione di logon interattivo; gli account AD associati a credenziali impersonali si autenticheranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi in base al proprio livello di autorizzazione minimo necessario e a seguito di auto log-on (in ogni caso senza l'immissione delle credenziali impersonali da parte degli operatori).

In ogni caso l'autenticazione degli account personali e impersonali - che devono essere sempre singolarmente autenticati ad ogni accesso - dovrà avvenire tramite protocollo kerberos v.5. Ciò significa in particolare che, nell'architettura kerberos, i domain controller del dominio aouts.it 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 ASUGI (dominio aouts.it), 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 consolle amministrativa su un client ASUGI afferente alla SC Informatica e Telecomunicazioni e dovrà formare una risorsa ASUGI alla profilatura degli account nei sistemi forniti, in modo da rendere l’ASUGI autonoma nelle procedure di abilitazione e successiva reinstallazione della consolle 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’ASUGI. La profilatura e l’attribuzione dei ruoli degli applicativi/servizi forniti dovrà essere tale da garantire il massimo livello di dettaglio di configurazione, ed in ogni caso 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) 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 manutenuti 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”.

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;
- manutenuti 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 cartelle %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 utente locale;
- non devono prevedere nessun utente impersonale per gli operatori e di servizio solo secondo le regole sopra descritte;
- 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.

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, 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;
- 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;
- potranno, nel caso di account digitali amministrativi, essere configurati dall'aggiudicatario solo in accordo con l'ASUGI e dovranno essere personali. Essi dovranno essere tutti comunicati all'ASUGI, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza;

- non dovranno, nel caso di account digitali amministrativi impersonali, essere in alcun caso presenti;
- 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, 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;
  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 digitali 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, sono tecnologicamente dei NGFW (Next Generation Firewall) dotati di funzionalità di statefull inspection, conseguentemente tutti i sistemi e le applicazioni oggetto di fornitura 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).

Non sarà in generale consentita la fornitura di sistemi di cablaggio dedicati, a meno di casi particolari tecnicamente motivati, che dovranno essere esplicitati in offerta tecnica e motivati dettagliatamente. Nella fattispecie del cablaggio strutturato, dovranno essere utilizzati sempre e comunque i sistemi aziendali e gli eventuali ampliamenti necessari saranno eseguiti da ASUGI; nel caso in cui l'aggiudicatario volesse offrire tale tipologia di servizi 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 dei materiali da utilizzare) che costituiranno vincolo contrattuale inderogabile.