

SPECIFICHE IT PER SERVIZI CLOUD A FAVORE DEGLI ENTI DEL SSR

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

Il sistema nel suo complesso dovrà essere coerente con le politiche di sicurezza e di privacy dell'Azienda Sanitaria (di seguito AS) 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 AS 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 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'AS 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.
- Dalle direttive UE NIS (Network and Information Security) e NIS2, nonché dai Decreti Legislativi di recepimento, come pure dalla Legge 90/2024.

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

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

In generale l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e 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 AS 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 AS 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 sul Marketplace ACN con livello coerente necessario con la classificazione dei dati oggetto di trattamento ("ordinari", "critici" o "strategici") nell'ambito della presente fornitura.

I dati per il servizio sono classificati CRITICI quindi la qualificazione sul Marketplace ACN deve essere di livello minimo QC2.

Pertanto, in linea con il principio "cloud first", i servizi digitali oggetto di fornitura dovranno essere erogati in modalità SaaS, fermo restando tutte le prescrizioni riportate nel presente documento.

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 (Chrome e Edge ultima versione) in uso presso AS 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 AS 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.

In merito ai sistemi di autenticazione e autorizzazione, questi dovranno essere adeguati al livello di classificazione del servizio SaaS ed alle indicazioni di ACN e AgID (es. SPID/CIE).

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 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 AS metterà a disposizione al più 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 AS, che vadano oltre i limiti sopra riportati, verranno computati da AS 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 tecniche di sicurezza informatica

Di seguito vengono definite le specifiche che i sistemi forniti dovranno rispettare 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 AS 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 AS 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'AS, 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 AS 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 AS;
- 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 AS, 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'AS 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’AS 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 ASUIGI 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 AS, 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 AS, essere impersonali e dovranno essere tutti comunicati all’AS 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 ASUIGI 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’AS, salvo esplicita autorizzazione da parte dell’AS.

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’AS 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) AS; nel caso di apparati per la connettività remota, l’aggiudicatario si impegna a far uso degli strumenti aziendali messi a disposizione da AS, come precedentemente riportato.

I firewall aziendali AS, 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). AS 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 saranno in alcun caso fornite da AS 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.