Südtiroler Informatik AG
Informatica Alto Adige SPA

CAPITOLATO TECNICO

RDA: 1002400301
Oggetto: Acquisto di un tool ITSM

1 Indice

2 Premessa

Il presente capitolato ha lo scopo di definire i servizi oggetto della fornitura, includendo l'acquisto di licenze perpetue di un tool ITSM avanzato, la manutenzione delle licenze, l'installazione e la preparazione dell'infrastruttura, l'analisi di business e funzionale, l'implementazione secondo il framework Scrum, il testing, il go live, il supporto post go live, la migrazione dei dati, l'integrazione con altri sistemi e la formazione del personale.

Glossario

Terminologia	**Descrizione**
Asset, Asset Management	Qualsiasi componente o risorsa tecnologica classificata con un numero di identificazione (numero asset) riportata in CMDB. A titolo esemplificativo ma non esaustivo, gli asset possono includere hardware (computer, monitor, stampanti, server, dispositivi mobili, dispositivi periferici ecc.); software (applicazioni, sistemi operativi, licenze ecc.), middleware, reti o altre componenti infrastrutturali IT.
CMDB	Configuration Management Database: database per l'archiviazione di informazioni sugli asset hardware, fonte del sistema di ticketing.
DEC (Direttore dell'Esecuzione del Contratto)	Figura che svolge il coordinamento, la direzione e il controllo tecnico contabile dell'esecuzione del contratto stipulato dalla stazione appaltante. Costituisce l'interfaccia nei confronti dell'Aggiudicatario; gestisce le comunicazioni e rappresenta il committente in tutti gli aspetti dei servizi erogati.
Fornitore, Appaltatore, Aggiudicatario, Prestatore di servizio, Operatore economico aggiudicatario	L'Impresa, il Consorzio di Imprese, il Raggruppamento Temporaneo di Imprese o il Contratto di Rete, aggiudicatario dell'appalto che si impegna ad eseguire, in favore della Amministrazione committente, le attività previste nel Capitolato Tecnico nonché in Offerta Tecnica.
Giorni	Giorni solari e consecutivi, salvo che non sia diversamente specificato.
IAA, Committente, Amministrazione committente	"Informatica Alto Adige S.p.A." (IAA) oppure "Südtiroler Informatik AG" (SIAG), titolare del Contratto.
ICT (Information and Communication Technologies)	Metodi e tecnologie utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni.
Incident	L'interruzione o la riduzione di qualità del servizio non programmati: può avere due livelli di gravità: "bloccante" e "non bloccante".
ITIL (Information Technology Infrastructure Library)	Linee guida (framework) per enti pubblici e privati dotati di infrastrutture informatiche, che hanno l'obiettivo di creare valore per i clienti finali sotto forma di servizi.
Knowledge Base	È inteso il deposito nella CMDB, di tutti i "Known Errors" e "How To's" noti e in costante crescita.
PAB (Provincia Autonoma di Bolzano)	La Provincia Autonoma di Bolzano (PAB) che usufruisce dei servizi oggetto del presente capitolato.
RUP (Responsabile Unico del Progetto)	Figura che garantisce il rispetto delle normative e delle procedure previste dal codice degli appalti pubblici, e

	assicurare la trasparenza, l'imparzialità e la regolarità del procedimento stesso.
SLA (Service Level Agreement)	Elementi che regolano i termini qualitativi e i livelli di servizio richiesti.

Tabella 1: Glossario capitolato

3 Contesto

3.1 Contesto Tecnologico Attuale

SIAG gestisce un'ampia gamma di servizi e infrastrutture IT, che spaziano dai data center e sistemi di database critici alle infrastrutture di rete e applicazioni per utenti finali.

SIAG offre una serie di servizi come SaaS (Software as a Service) per la gestione di processi interni dell'amministrazione, con oltre 300 applicazioni per più di 20 domini specifici per gli operatori della PA e servizi per i cittadini con oltre 100 servizi disponibili attraverso portali pubblici. WaaS (Workplace as a Service) include infrastrutture per dispositivi fissi e mobili per postazioni di lavoro, postazioni di lavoro virtuali, gestione delle stampanti, reti LAN e WAN per postazioni di lavoro, e infrastrutture per videoconferenze. Inoltre, fornisce software come sistemi operativi, software di produttività, software di sicurezza, strumenti di collaborazione e videoconferenza e strumenti per il lavoro remoto e VPN.

Nel contesto di PaaS (Platform as a Service), SIAG offre soluzioni come Cloud SAP, Cloud Microsoft, Cloud SIAG (DC-Südtirol) e DBaaS (Database as a Service). Per quanto riguarda IaaS (Infrastructure as a Service), i servizi includono Compute, Storage as a Service e Network as a Service. Infine, SIAG fornisce anche DCaaS (Data Center as a Service), offrendo servizi di Colocation.

3.2 Dimensionamento dei servizi erogati da SIAG

Al fine di consentire un corretto dimensionamento del carico del sistema, si riportano di seguito alcune utili informazioni che descrivono il contesto. Nei seguenti punti si riportano, a titolo esemplificativo e non esaustivo, alcuni dati di carattere generale:

Descrizione	**Dato**
Numero di ticket registrati nel 2022	96.548
Chiamate call center ricevute nel 2022	52.815
Applicazioni software pacchettizzate	620
Ticket elaborati dal gruppo Asset Management nel 2022	3.106
Gruppi di assegnazione support potenziali nel sistema di ticketing	774
Assets in gestione	41.000
Service areas	23
IT Service Groups	83
IT Services	360
Utenti soluzioni PA	8.000
Configuration Items nel CMDB	27.000

Tabella 2: Dati gestiti nel tool di ITSM

4 Oggetto del Capitolato

Il presente capitolato ha l'obiettivo di definire i requisiti per l'acquisto di:

- licenze d'uso perpetue di un tool ITSM installabile sulla private cloud di SIAG. Il tool deve soddisfare le esigenze di SIAG offrendo le macro-funzionalità delle seguenti 13 categorie:
  - Asset e Configuration Management
  - Change Management
  - Financial Management
  - Incident Management
  - Knowledge Management
  - Problem Management
  - Release Management
  - License Management
  - Service Portfolio / Service Catalog Management
  - Service Level Management
  - Contract Management
- manutenzione delle licenze per i primi due anni di esercizio.
- servizi professionali necessari per garantire una corretta implementazione del tool ITSM. Questi servizi, che saranno esplicitati nella parte seguente, includono:
  - Servizi di installazione e preparazione dell'infrastruttura
  - Analisi di business, disegno architetturale e analisi funzionale
  - Implementazione e testing
  - Go-live e supporto post-go-live
  - Migrazione dei dati e integrazione con altri sistemi
  - Formazione

Di seguito le informazioni di dettaglio relative ai punti precedentemente elencati.

4.1 Caratteristiche tool

Nei sottoparagrafi successivi vengono riportate le caratteristiche del tool (minime e ulteriori/premiali), sia a livello generale che specifico per ciascuna delle 13 macroaree funzionali che dovranno essere coperte dalle licenze d'uso acquistate.

In fase di gara sarà richiesto alle aziende di presentare le loro soluzioni nella sede di Informatica Alto Adige.

4.1.1 Caratteristiche Generali del Tool ITSM

Il sistema ITSM deve soddisfare in generale le seguenti funzionalità trasversali:

Caratteristiche minime:

Codice	Descrizione
CRM-M-1	Installazione On-prem con possibilità di passaggio a SaaS.

CRM-M-2	Il tool ITSM selezionato deve soddisfare gli standard ITIL v4, assicurando la conformità alle migliori pratiche internazionali nella gestione dei servizi IT.
CRM-M-3	Integrazione con sistemi periferici (cloud/On-prem): Il sistema ITSM deve offrire API per la creazione automatica ed il tracciamento di ticket ITSM da sistemi esterni come, ad esempio, Dynamics Customer Service 365, mantenendo le informazioni del sistema originante per una tracciabilità bilaterale. I ticket devono includere l'insieme di informazioni necessari per rintracciare e riconciliare case generati su CRM e relativi ticket ITSM. Il sistema deve fornire aggiornamenti asincroni riguardo lo stato e l'avanzamento del ticket tramite API, con attivazioni nei momenti chiave del ciclo di vita del ticket (assegnazione, inizio lavorazione, aggiornamenti, risoluzione). L'integrazione deve utilizzare protocolli di comunicazione sicuri e crittografia dei dati per proteggere le informazioni sensibili. Deve inoltre essere possibile scalare il sistema orizzontalmente per aggiungere risorse, e deve integrarsi senza interruzioni con l'infrastruttura IT esistente. Oltre all'integrazione del ciclo di vita ed eventi ticket ITSM con sistemi periferici, è richiesto anche l'accesso in lettura e potenzialmente anche in scrittura al Knowledge Base del sistema ITSM tramite API.
CRM-M-4	Accesso in Near-Real-Time ai Dati: Il sistema ITSM deve fornire accesso in near-real-time ai dati grezzi e strutturati, tramite interfacce moderne quali webservice / API REST, per alimentare e aggiornare i modelli e gli algoritmi di IA con dati accurati e affidabili.
CRM-M-5	Integrazione di Webapp Esterne: Le interfacce del sistema ITSM devono permettere l'integrazione di webapp esterne (es. Chat), facilitando l'usabilità e l'esperienza degli utenti attraverso funzionalità e interazioni offerte dagli strumenti di IA.
CRM-M-6	Gestione dell'Identità e Accesso: Utilizzo di funzioni di Single-Sign-On e autenticazione multifattore per l'accesso alle risorse e funzionalità cloud. Servizi di gestione delle identità per garantire l'accesso sicuro e configurabile agli utenti, con possibilità di configurare una matrice RBAC con almeno 5 ruoli personalizzabili.
CRM-M-7	Funzionalità Self-Service e Mobilità: Strumenti self-service da app mobili e web based per gli utenti, con accesso attraverso un portale web sicuro per l'accesso utente e amministrativo.
CRM-M-8	Gestione dei Dati e Conformità: Conformità completa alla normativa sulla protezione dei dati dell'UE, con certificazioni ISO 27001.
CRM-M-9	Reporting e Analisi: Funzionalità avanzate di reportistica e analisi, inclusi report standard e personalizzati. Integrazione con strumenti di Business Intelligence come SAP SAC e Microsoft Power BI per analisi approfondite.
CRM-M-10	Tutti i moduli dovranno essere disponibili via web attraverso le ultime versioni dei seguenti browser: Google Chrome, Mozilla Firefox, Microsoft Edge.
CRM-M-11	Field Support Manager in modalità offline per i tecnici sul campo.
CRM-M-12	Scalabilità del sistema.
CRM-M-13	Multi-tenant.
CRM-M-14	La soluzione deve garantire la disponibilità di un'API RESTful che permetta l'accesso e la gestione dei dati attraverso operazioni CRUD (Create, Read, Update, Delete). L'API deve essere sicura e supportare l'autenticazione e l'autorizzazione degli utenti. Devono essere previste endpoint per l'inserimento di nuovi dati, la lettura di dati esistenti, l'aggiornamento di record e la loro

	eliminazione. La documentazione dell'API deve essere completa e includere esempi di utilizzo per ciascuna operazione.
CRM-M-15	15.000 utenti nominati (utenti Fulfiller).
CRM-M-16	Motore BPMN2 come base per le definizioni dei processi.
CRM-M-17	CRM, funzionalità di Service to Offer.
CRM-M-18	Sviluppo AI in-house in ambiente On-prem, garantendo che non ci sia fuga di dati verso Open AI o altri.
CRM-M-19	Gestione finanziaria (pianificazione e calcolo dei servizi, nonché loro allocazione dei costi per causa).
CRM-M-20	Gestione completa delle licenze inclusa l'ottimizzazione SaaS, l'ottimizzazione Oracle e le funzioni di ottimizzazione SAP.
CRM-M-21	Nel caso di eventuale utilizzo in cloud, funzionalità che consente il monitoraggio dei costi.
CRM-M-22	Possibilità di personalizzazione approfondita tramite wizards.
CRM-M-23	Possibilità di integrazione con sistemi di Endpoint Management (distribuzione di software).

Caratteristiche ulteriori:

Codice	**Descrizione**
CRU-M-1	Advanced ChatBot: Il sistema ITSM dovrebbe includere un AdvancedChatBot configurabile sia in termini di knowledge-base che di modello LLM di riferimento, senza pre-set-up. Questo ChatBot dovrebbe supportare gli utenti di back-office nella ricerca di soluzioni per i clienti e assistere i cittadini nella auto-risoluzione dei problemi IT, migliorando la velocità e l'efficacia delle risoluzioni.

4.1.2 Caratteristiche macroaree funzionali

4.1.2.1 Asset e configuration management

L'asset e configuration management si occupa di registrare, tracciare e gestire tutti gli asset IT, delle loro relazioni e le configurazioni presenti nell'infrastruttura aziendale. Questo include hardware, software, documentazione e altre risorse critiche. La gestione accurata di questi elementi è fondamentale per garantire la trasparenza, la sicurezza e l'efficienza operativa. Inoltre, il configuration management assicura che tutte le configurazioni siano conosciute e gestite in modo coerente, permettendo un controllo completo sull'infrastruttura IT e facilitando la gestione dei cambiamenti.

Caratteristiche minime:

Codice	**Descrizione**
ACM-M-1	Registrazione e tracciabilità degli asset e delle loro relazioni attraverso il loro ciclo di vita.
ACM-M-2	Personalizzazione delle tipologie di asset con attributi e relazioni custom.
ACM-M-3	Gestione delle configurazioni degli asset IT.

Caratteristiche ulteriori:

Codice	Descrizione
ACM-U-1	Auditing e tracciabilità delle modifiche.
ACM-U-2	Automazione e integrazione dei processi di gestione degli asset IT.
ACM-U-4	Integrazione con altri processi ITSM.

4.1.2.2 Change management

Il change management si occupa di gestire tutte le modifiche all'infrastruttura IT in modo controllato e documentato, minimizzando i rischi e l'impatto sugli utenti finali. Questo processo include la gestione delle richieste di cambiamento (RFC), la pianificazione, l'approvazione, la comunicazione e l'implementazione delle modifiche.

Caratteristiche minime:

Codice	Descrizione
CHM-M-1	Registrazione e gestione dei cambiamenti.
CHM-M-2	Workflow di approvazione configurabili.
CHM-M-3	Strumento per l'analisi dei rischi e dell'impatto delle modifiche.

Caratteristiche ulteriori:

Codice	Descrizione
CHM-U-1	Integrazione con altri processi ITSM.
CHM-U-2	Auditing e tracciabilità delle modifiche.
CHM-U-3	Gestione delle emergency change.

4.1.2.3 Financial management

Il financial management per i servizi IT si occupa della gestione dei costi e dei budget relativi all'IT. Questo include la pianificazione finanziaria, il monitoraggio delle spese e la reportistica. È essenziale per garantire che le risorse IT siano utilizzate in modo efficiente e che i costi siano tenuti sotto controllo.

Caratteristiche minime:

Codice	Descrizione
FIM-M-1	Gestione dei costi e dei budget IT.
FIM-M-2	Reportistica finanziaria.
FIM-M-3	Tracciamento delle spese operative e capitali.

Caratteristiche ulteriori:

Codice	Descrizione
FIM-U-1	Strumenti per l'analisi dei costi-benefici delle iniziative IT.
FIM-U-2	Gestione dei contratti di fornitori (ciclo passivo).

4.1.2.4 Incident management

L'incident management ha il compito di gestire gli incidenti che possono verificarsi nell'infrastruttura IT, con l'obiettivo di ripristinare il normale funzionamento dei servizi il più

rapidamente possibile e minimizzare l'impatto sugli utenti finali. Questo processo include la rilevazione, la registrazione, la classificazione, l'indagine e la risoluzione degli incidenti.

Caratteristiche minime:

Codice	Descrizione
IDM-M-1	Registrazione e tracciamento degli incidenti.
IDM-M-2	Automazione del flusso di lavoro per la risoluzione degli incidenti.
IDM-M-3	Reportistica sugli incidenti.
IDM-M-4	Gestione degli SLA.
IDM-M-5	Integrazione con una knowledge base per la gestione delle conoscenze che contribuisce ad una risoluzione più rapida.
IDM-M-6	Integrazione con altri processi ITIL.

Caratteristiche ulteriori:

Codice	Descrizione
IDM-U-1	Strumento per l'analisi delle cause principali degli incidenti.
IDM-U-2	Integrazione con la gestione degli eventi e degli incidenti.
IDM-U-3	Funzionalità di matching di incident per identificare casi simili e risolverli rapidamente. Machine learning per la classificazione e il raggruppamento logico degli incident.

4.1.2.5 Knowledge management

Il knowledge management si occupa di creare, condividere, utilizzare e gestire la conoscenza e le informazioni all'interno dell'organizzazione IT. Questo processo supporta la risoluzione rapida dei problemi, la formazione degli utenti e la gestione efficace delle informazioni.

Caratteristiche minime:

Codice	Descrizione
KBM-M-1	Creazione e gestione di una base di conoscenze per l'archiviazione di qualsiasi tipo di documento desiderato (errori noti, soluzioni alternative, istruzioni, soluzioni, checklist, ecc.).
KBM-M-2	Accesso rapido alle soluzioni e alle best practice.
KBM-M-3	Integrazione con altri processi ITSM.

Caratteristiche ulteriori:

Codice	Descrizione
KBM-U-1	Strumento per l'analisi dell'utilizzo delle conoscenze.
KBM-U-2	Strumenti di collaborazione per la condivisione delle conoscenze.

4.1.2.6 Self-Service Portal

Il portale Self-Service serve agli utenti per richiedere in autonomamente servizi IT, accedere alla knowledge base, segnalare incidenti e accedere a risorse informative.

Caratteristiche minime:

Codice	Descrizione
SSP-M-1	Accesso tramite un interfaccia web accessibile con i web-browser richiesti.

Caratteristiche ulteriori:

Codice	Descrizione
SSP-U-1	Chat-bot integrato.

4.1.2.7 Problem management

Il problem management si concentra sull'identificazione e la risoluzione delle cause profonde degli incidenti. L'obiettivo è prevenire la ricorrenza degli incidenti, migliorando la stabilità e la performance dei servizi IT.

Caratteristiche minime:

Codice	Descrizione
PLM-M-1	Registrazione e tracciamento dei problemi.
PLM-M-2	Strumenti avanzati per l'analisi delle cause "root".
PLM-M-3	Tracciamento delle azioni correttive.

Caratteristiche ulteriori:

Codice	Descrizione
PLM-U-1	Integrazione con altri processi ITSM.
PLM-U-2	Integrazione con un Known Error Database.

4.1.2.8 Release management

Il release management si occupa di pianificare, programmare e controllare il movimento delle release verso l'ambiente di produzione. Il suo obiettivo è garantire che le release vengano distribuite in modo sicuro e che siano ben integrate con l'infrastruttura esistente.

Caratteristiche minime:

Codice	Descrizione
RLM-M-1	Pianificazione e gestione delle release software.
RLM-M-3	Tracciamento delle versioni e delle modifiche.
RLM-M-4	Integrazione con la gestione delle configurazioni.

Caratteristiche ulteriori:

4.1.2.9 License management

Il License management gestisce il ciclo di vita delle risorse software all'interno di un'organizzazione. Questo include la gestione delle licenze, il monitoraggio delle installazioni e l'ottimizzazione dell'utilizzo delle risorse software.

Caratteristiche minime:

Codice	Descrizione

SAM-M-1	Gestione delle licenze/sottoscrizionin software On-Prem e Cloud.
SAM-M-2	Tracciamento delle installazioni e dell'utilizzo delle licenze.
SAM-M-3	Reportistica sulla conformità delle licenze.

Caratteristiche ulteriori:

Codice	Descrizione
SAM-U-1	Ottimizzazione delle licenze.
SAM-U-2	Strumento per l'analisi dei costi del software.
SAM-U-3	Gestione dei costi cloud.

4.1.2.10 IT Service portfolio / IT Service catalog management

Il Service portfolio / Service catalog management gestisce l'intero portafoglio dei servizi IT offerti dall'organizzazione. Questo include la creazione, la gestione e la comunicazione del catalogo dei servizi disponibili per gli utenti finali.

Caratteristiche minime:

Codice	Descrizione
SSM-M-1	Creazione e gestione di un catalogo dei servizi IT.
SSM-M-2	Descrizione dettagliata dei servizi offerti.
SSM-M-3	Accesso self-service ai servizi per gli utenti.

Caratteristiche ulteriori:

Codice	Descrizione
SSM-U-1	Integrazione con altri processi ITSM.
SSM-U-2	Strumento per l'analisi dell'utilizzo dei servizi.

4.1.2.11 Service level management

Il Service level management si occupa di definire, monitorare e gestire gli accordi sui livelli di servizio (SLA) tra il fornitore di servizi IT e i clienti. L'obiettivo è garantire che i servizi IT erogati soddisfino le aspettative e i requisiti dei clienti.

Caratteristiche minime:

Codice	Descrizione
SLM-M-1	Definizione e gestione degli SLA (Service Level Agreements).
SLM-M-2	Monitoraggio delle performance dei servizi rispetto agli SLA.
SLM-M-3	Reportistica sugli SLA.

Caratteristiche ulteriori:

Codice	Descrizione
SLM-U-1	Strumento per l'analisi delle deviazioni dagli SLA.
SLM-U-2	Strumenti di miglioramento continuo per i servizi.

4.1.2.12 Contract management

Il Contract management è una funzione fondamentale all'interno del sistema ITSM che consente di gestire e tracciare l'intero ciclo di vita dei contratti sia passivi che attivi. Questo include la creazione, la gestione, la revisione, il rinnovo e la chiusura dei contratti. La funzionalità di Contract Management deve garantire che tutti i contratti siano gestiti in modo efficiente e conforme alle normative, migliorando la trasparenza e riducendo i rischi associati alla gestione contrattuale.

Caratteristiche minime:

Codice	Descrizione
CTM-M-1	Tracciamento del ciclo di vita dei contratti: creazione, approvazione, revisione, rinnovo e chiusura dei contratti.
CTM-M-2	Gestione dei contratti attivi e passivi con tracciabilità e gestione delle obbligazioni contrattuali.
CTM-M-3	Archiviazione e accesso sicuro ai contratti da parte degli utenti autorizzati.
CTM-M-4	Funzionalità di time sheet per la registrazione e il monitoraggio del tempo impiegato su progetti e servizi.
CTM-M-5	Processi end-to-end per i contratti attivi: dalla richiesta di preventivo, al preventivo, al contratto, fino alla fatturazione.
CTM-M-6	Automazione dei flussi di lavoro contrattuali per approvazioni, revisioni e rinnovi.
CTM-M-7	Integrazione con sistemi di fatturazione per generazione e gestione dei pagamenti e delle fatture.
CTM-M-8	Gestione delle risorse e allocazione dei costi associati ai contratti.

Caratteristiche ulteriori:

Codice	Descrizione
CTM-U-1	Notifiche e avvisi automatici per scadenze contrattuali e rinnovi imminenti.
CTM-U-2	Strumento per l'analisi e reportistica avanzata per monitorare le performance contrattuali e identificare rischi.

4.1.3 Multilinguismo

Il prodotto deve supportare pienamente la lingua italiana, tedesca ed inglese.

In particolare:

1. **Interfaccia Utente**: L'interfaccia utente del prodotto deve essere disponibile nelle tre lingue sopra menzionate. L'utente deve poter selezionare la lingua preferita attraverso le impostazioni del prodotto.
2. **Reportistica**: I report prodotti deve essere disponibile nelle tre lingue sopra menzionate; la lingua del report deve essere selezionabile e potrebbe differire dalla lingua in uso per l'interfaccia utente.
3. **Documentazione**: Tutta la documentazione relativa al prodotto, inclusi manuali d'uso, guide rapide, e documenti di supporto tecnico, deve essere fornita nelle tre lingue specificate.

4. **Supporto Tecnico**: Il servizio di assistenza clienti e supporto tecnico deve essere disponibile in italiano o tedesco e inglese, sia per quanto riguarda l'assistenza telefonica che per quella via e-mail.
5. **Aggiornamenti e Comunicazioni**: Tutti gli aggiornamenti del prodotto, le note di rilascio e le comunicazioni ufficiali devono essere tradotti e distribuiti in italiano, tedesco e inglese.

4.2 Manutenzione

Il fornitore si impegna a mantenere il software, inclusa la correzione degli errori, l'adattamento a nuove esigenze, l'ottimizzazione delle prestazioni e le misure preventive per garantire la stabilità. Gli aggiornamenti e le patch saranno forniti regolarmente. Il supporto sarà fornito tramite un helpdesk, disponibile durante gli orari di servizio stabiliti. Gli interventi di manutenzione pianificati dovranno essere annunciati in anticipo, e i costi dovranno essere indicati in modo trasparente.

4.3 Servizi Professionali

I servizi professionali necessari per garantire una corretta implementazione del tool ITSM includono:

4.3.1 Servizi di Installazione e Preparazione dell'Infrastruttura

Il fornitore dovrà collaborare strettamente con i team IT di SIAG per assicurare che l'hardware e il software siano adeguatamente configurati per supportare il nuovo sistema. Questo comprende la verifica delle prestazioni, la sicurezza della rete e la compatibilità con i dispositivi e le applicazioni esistenti.

4.3.2 Analisi di Business, Disegno Architetturale e Analisi Funzionale

Prima dell'implementazione del tool, sarà condotta un'analisi di business per definire i requisiti specifici e le aspettative di SIAG. L'analisi funzionale seguirà per dettagliare come le funzionalità del tool ITSM dovranno essere configurate per incontrare queste esigenze. Inoltre, verrà realizzato il disegno architetturale della soluzione per garantire che il sistema sia scalabile, sicuro e integrato con l'infrastruttura IT esistente. Queste analisi garantiranno che il tool sia personalizzato per massimizzare l'efficacia e l'efficienza dei processi IT gestiti da SIAG.

4.3.3 Implementazione e Testing

Dopo l'installazione e la configurazione iniziali, il tool ITSM verrà sottoposto a una serie di test rigorosi per verificare che tutte le funzionalità operino come previsto e che siano pienamente operative senza interruzioni per gli utenti finali. I test includeranno scenari di uso reale per assicurare che il tool risponda adeguatamente alle esigenze operative di SIAG.

4.3.4 Go-Live e Supporto Post-Go-Live

Una volta completati i test e ottenuta la convalida finale, il tool ITSM verrà messo in produzione. Durante la fase di go-live, sarà fornito un supporto intensivo per assicurare una transizione fluida. Il supporto post-go-live include assistenza immediata per eventuali problemi, formazione degli utenti e ottimizzazione continua del sistema in base al feedback ricevuto.

4.3.5 Migrazione dei Dati e Integrazione con Altri Sistemi

Una parte fondamentale del progetto sarà la migrazione dei dati dal vecchio sistema al nuovo tool ITSM. Questo processo dovrà essere gestito con la massima attenzione per garantire l'integrità dei dati. Inoltre, il tool dovrà integrarsi in modo sincrono ed asincrono tramite p. es. API con altri sistemi periferici, in cloud e/o On-prem, in uso presso SIAG.

4.3.6 Formazione

Il fornitore dovrà erogare un minimo di 5 corsi di formazione per il personale IT e per gli utenti finali di SIAG. La formazione dovrà coprire l'uso delle funzionalità del tool ITSM, le procedure operative standard e le best practice per garantire un'adozione efficace del nuovo sistema. La formazione potrà avvenire anche in modalità remota.

4.3.7 Modalità di Erogazione dei Servizi Professionali

SIAG si aspetta che le attività vengano svolte con modalità agile Scrum, che prevede un approccio iterativo e incrementale per l'introduzione della soluzione ITSM. Questo metodo agile consente di suddividere il progetto in sprint di durata fissa, durante i quali il team di progetto sviluppa e rilascia incrementi funzionali del sistema.

L'adozione di Scrum garantisce:

1. Iterazioni brevi e frequenti: Ogni sprint, della durata di 2-4 settimane, si conclude con la consegna di una parte funzionante del sistema ITSM, permettendo una revisione regolare e l'adattamento delle priorità in base ai feedback ricevuti.
2. Collaborazione continua: Il fornitore lavorerà a stretto contatto con i team di SIAG, partecipando a riunioni quotidiane (daily stand-up), pianificazioni degli sprint (sprint planning) e revisioni degli sprint (sprint review) per assicurare che le esigenze e le aspettative siano costantemente allineate.
3. Flessibilità e adattabilità: L'approccio Scrum permette di rispondere rapidamente ai cambiamenti delle esigenze e delle priorità, migliorando continuamente il sistema in base al feedback degli utenti e all'evoluzione del contesto operativo.

Questo approccio iterativo e collaborativo assicurerà che la soluzione ITSM venga implementata in modo efficace, con un focus costante sul miglioramento dell'efficienza operativa e sulla soddisfazione degli utenti finali.

4.4 Licenze

La politica di licenze richiesta dovrà avere le seguenti caratteristiche:

- licenza d'uso perpetua a fronte di un'istallazione on-prem dell'applicativo per utenti illimitati, numero illimitato di installazioni proprie (partner SIAG);
- trasferimento gratuito delle licenze software da un eventuale partner al cliente SIAG;
- canone annuale di manutenzione con orizzonte temporale garantito di 10 anni.

5 Durata del contratto

La durata del contratto sarà composta da un periodo necessario per le attività di migrazione e implementazione del tool (Fase 1) più il periodo di utilizzo dell'applicativo a regime (Fase 2).

Nel dettaglio:

- Fase 1: in via di definizione.
- Fase 2: 12 mesi dalla conclusione della Fase 1. Dalla scadenza della Fase 2, la stazione appaltante si riserva la facoltà di prorogare il contratto per 9 volte di durata pari a 12 mesi ciascuna.

6 Importo a base di gara

Da definire a fronte della consultazione di mercato.

7 Esecuzione della fornitura/del servizio

L'operatore economico aggiudicatario è tenuto a seguire le istruzioni e le direttive fornite da IAA per l'avvio dell'esecuzione del contratto; qualora l'operatore economico aggiudicatario non adempia, IAA ha facoltà di procedere alla risoluzione del contratto.
Qualora circostanze particolari impediscano temporaneamente la regolare esecuzione delle prestazioni oggetto del contratto, il RUP/DEC ne ordina la sospensione, indicando le ragioni e l'imputabilità delle medesime. È ammessa la sospensione anche parziale della prestazione, ordinata dal RUP/DEC nei casi di forza maggiore o di altre circostanze speciali che impediscano la esecuzione o la realizzazione a regola d'arte della prestazione

7.1 Modalità di esecuzione della fornitura/del servizio

L'operatore economico aggiudicatario deve garantire l'esecuzione di tutte le prestazioni a perfetta regola d'arte, nel rispetto delle normative vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel presente capitolato, nell'offerta tecnica, nell'offerta economica e nel successivo contratto di appalto.

L'operatore economico aggiudicatario si obbliga, infine, a dare immediata comunicazione ad IAA di ogni circostanza influente sull'esecuzione del servizio.

Nel caso di fornitura di servizi cloud, l'aggiudicatario dovrà:

- informare IAA, con un preavviso minimo di 10 gg, di qualsiasi attività di modifica all'infrastruttura oggetto del servizio che abbia un potenziale impatto sui Servizi IT di IAA. Contestualmente all'avviso della pianificazione degli interventi, l'operatore economico aggiudicatario dovrà fornire una descrizione dettagliata della modifica proposta e la classificazione della criticità. Nel corso dell'intervento, qualora dovessero comparire problematiche impreviste potenzialmente impattanti sui sistemi o sul servizio, IAA dovrà essere tempestivamente avvisata, costantemente informata sulle attività messe in campo per risolvere il problema e allineata sugli sviluppi della risoluzione. Al temine dei lavori l'operatore economico aggiudicatario avviserà IAA del completamento delle attività inviando, se necessario, un report contenente la descrizione dei cambiamenti implementati;
- fornire a IAA indicazioni sulla procedura di dismissione del servizio. Nello specifico, il documento dovrà descrivere la modalità di chiusura e di restituzione degli asset (compresi i dati), la rimozione/cancellazione sicura degli asset e di eventuali copie dai

sistemi del CSP ed elencare gli asset e i tempi entro i quali questi devono essere dismessi/ritornati.

8 Livelli di servizio/SLA e penali

8.1 SLA e corrispondenti penali

Da definire.

9 Pianificazione delle attività e pacchetti di lavoro

Le attività inerenti allo svolgimento delle prestazioni oggetto del contratto dovranno essere pianificate dettagliatamente in accordo con IAA. Esse saranno suddivise in appositi pacchetti di lavoro, se previsto.

10 Verifiche di conformità della fornitura del servizio

IAA monitorerà costantemente l'erogazione dei servizi attraverso controlli incrociati tra l'andamento dei ticket e la reportistica prodotta dall'Aggiudicatario. Verrà inoltre periodicamente verificato il livello di soddisfazione dell'utente finale.

11 Condizioni di fatturazione e pagamento

Da definire a fronte della consultazione di mercato.

Ai sensi dell'art. 3, c. 1, lett. e) dell'allegato I.1 del D.lgs. n. 36/2023, art. 2359 co.1 c.c. e dell'art. 17-ter del DPR 633/1972 I.A.A. in quanto società controllata dalla PAB, rientra nell'ambito di applicazione della "scissione dei pagamenti (c.d. split payment).

Dal 01-01-2019 la legge di Bilancio 2018 nr. 205 del 27.12.2017 ha introdotto l'obbligo della fatturazione elettronica. Le fatture elettroniche dovranno pertanto essere trasmesse dai propri fornitori residenti, stabiliti ed indentificati in Italia, attraverso il Sistema di Interscambio (SDI) nel formato XML. Il Codice Destinatario Univoco per l'invio delle fatture è **XL13LG4**.

Il pagamento del corrispettivo avverrà, dietro presentazione di regolare fattura, entro 30 giorni dalla data di ricezione della medesima, fatte salve le verifiche di legge, nonché dell'eventuale ulteriore documentazione prevista dal contratto, a mezzo bonifico bancario, mediante accredito sul c/c dedicato che verrà indicato dal fornitore.

Le fatture devono essere indirizzate ad Informatica Alto Adige S.p.A., via Siemens 29, 39100 Bolzano e devono contenere le seguenti indicazioni: oggetto del contratto, n. ordine/contratto, nr. CIG e il nome del RUP. Nelle singole posizioni della fattura inserire le seguenti indicazioni: descrizione posizione, unità/pezzi, prezzo unitario, totale ed inoltre il riferimento alla copertura temporale della singola posizione

12 Penali

Nel caso in cui il Responsabile Unico del Procedimento, anche a mezzo di suo incaricato, rilevasse inadempienze nell'esecuzione dell'appalto o, comunque, inottemperanze agli

obblighi contrattuali, l'Impresa aggiudicataria potrà incorrere nel pagamento di penalità, fatta salva la risoluzione contrattuale nei casi previsti.
In caso di inadempimento degli obblighi contrattuali le penali dovute sono calcolate in misura compresa tra lo 0,3 per mille e l'1 per mille dell'ammontare netto contrattuale, da determinare di volta in volta in relazione all'entità del danno arrecato e della gravità dell'inadempimento. Nel caso in cui l'applicazione delle penali superi il limite del 10% dell'importo contrattuale o qualora l'inadempimento integri un'ipotesi di colpa grave nell'esecuzione di obblighi e condizioni contrattuali l'ente committente procederà con la risoluzione del contratto in danno dell'affidatario nonché all'affidamento a terzo operatore economico dell'esecuzione delle prestazioni contrattuali residue, con oneri a carico dell'operatore economico aggiudicatario.

Non danno luogo a responsabilità per la ditta le interruzioni dovute a cause di forza maggiore intendendosi per forza maggiore qualunque fatto eccezionale, imprevedibile e al di fuori della normale conduzione dell'appalto, che l'Impresa non possa evitare con l'esercizio della normale diligenza.

È sempre salvo il risarcimento del maggior danno.

13 Varianti

Ai sensi dell'art. 120, co. 9 del D.lgs. n. 36/2023 e ss.mm.ii., IAA si riserva la facoltà, con semplice preavviso scritto, di apportare variazioni alla fornitura/servizio oggetto dell'appalto, in aumento o in diminuzione, fino al massimo di 1/5 dell'ammontare complessivo previsto dall'appalto. Tali variazioni seguiranno comunque gli stessi prezzi, patti e condizioni definiti nell'appalto.
Nel caso di necessità motivata di variazioni in aumento delle prestazioni oggetto del contratto di oltre 1/5 del prezzo complessivo contrattuale, si procederà ai sensi del co. 1 e 13 dell'art. 120 del D.lgs. n. 36/2023 e ss.mm.ii., previo consenso da parte del contraente, alla stipulazione di un atto aggiuntivo al contratto, alle medesime condizioni del contratto principale ove applicabili. È fatta salva la possibilità di recesso da parte dell'appaltatore qualora le diminuzioni superino il quinto dell'importo contrattuale, da esercitarsi non oltre il trentesimo giorno successivo alla comunicazione di variazione da parte di IAA. In caso di recesso, l'appaltatore dovrà garantire i servizi oggetto dell'appalto fino all'individuazione, da parte dell'Ente, del nuovo contraente.

Qualora si rendano necessarie eventuali forniture o servizi supplementari, non programmabili e non compresi nel presente appalto, troverà applicazione quanto previsto dall'art. 120, co 1. Lett. b) del D.lgs. n. 36/2023.

In ogni caso, qualsiasi fornitura o servizio aggiuntivo e/o supplementare dovrà essere eseguito solo in seguito ad autorizzazione da parte del RUP che, accertata la disponibilità di budget nel bilancio di IAA, indicherà i tempi e le modalità di intervento, provvedendo ai necessari controlli sulla prestazione richiesta. Nessun servizio aggiuntivo e/o supplementare, se non previamente autorizzato, potrà essere addebitato a IAA in sede di fatturazione.

L'operatore economico aggiudicatario comunque non potrà introdurre varianti alla fornitura oggetto del contratto, salvo previo accordo scritto con IAA. Ogni contravvenzione a questa disposizione sarà a completa responsabilità dello stesso. Le modifiche non in precedenza autorizzate non danno titolo a pagamenti o rimborsi di sorta e, ove il RUP lo giudichi opportuno, comportano la rimessa in pristino, a carico del contraente, della situazione originaria preesistente.

È fatta salva, comunque, l'applicazione dell'art. 120 del D.lgs. n. 36/2023 e ss.mm.ii..

14 Divieto di cessione del contratto e subappalto

Ai sensi dell'art. 119, co.1 del D.lgs. n. 36/2023 e ss.mm.ii., è vietata, a pena di nullità, la cessione del contratto.
Per quanto riguarda il subappalto, si applicano le disposizioni di cui all'art. 119, co. 2 e seguenti del D.lgs. n. 36/2023 con le esclusioni previste dall'art. 225 co. 2 dello stesso.

Qualora autorizzato il subappalto, i sub fornitori dovranno presentare garanzie in termini di conoscenza specialistica, affidabilità e risorse, sufficienti per mettere in atto misure tecniche e organizzative che soddisfino anche i requisiti previsti dalle norme in materia di protezione dei dati personali e di tutela dei diritti dell'interessato.

L'operatore economico aggiudicatario si impegna a mettere a disposizione di IAA l'elenco aggiornato dei propri sub fornitori informandola di tutte le modifiche riguardanti l'aggiunta o la sostituzione di eventuali sub fornitori, nei limiti in cui ciò sia consentito, in modo che essa possa eventualmente opporsi a tali modifiche.

L'operatore economico aggiudicatario si impegna ad imporre ai sub fornitori, ulteriori responsabili esterni (ovvero sub responsabili), con contratto o atto giuridico analogo, le stesse obbligazioni in materia di protezione dei dati gravanti sull'Operatore economico aggiudicatario. A dimostrazione dell'adempimento dell'obbligo posto a suo carico, l'Operatore economico aggiudicatario provvede a comunicare a IAA una copia del contratto concluso con i sub responsabili.

Qualora il sub fornitore/sub responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'operatore economico aggiudicatario risponde verso IAA dell'inadempimento di quest'ultimo.

La violazione del divieto di cessione del contratto o degli obblighi nascenti dall'eventuale subappalto comporta la risoluzione anticipata del contratto per grave inadempienza contrattuale.

15 Risoluzione e recesso

Trovano applicazione per la risoluzione ed il recesso del contratto le disposizioni previste dagli articoli 122 e 123 del D.lgs. 36/2023 e ss.mm.ii.

IAA può recedere dal contratto, in qualunque tempo e fino al termine della prestazione, secondo la procedura prevista dall'articolo 123 del D.lgs. 36/2023. Tale facoltà è esercitata per

iscritto mediante comunicazione da inviare all'operatore economico aggiudicatario a mezzo Posta Elettronica Certificata con un preavviso minimo di 60 (sessanta) giorni dalla data di effettivo recesso.

È causa di risoluzione del contratto di appalto, oltre a quelle cause già espressamente previste all'interno del presente capitolato:

- applicazione di penali di importo complessivo superiore al 10% del valore del contratto;
- cessazione dell'attività, fallimento, altra procedura concorsuale, liquidazione, IAA controllata, concordato preventivo o qualsiasi altra situazione equivalente;
- commissione di atti, connessi all'esecuzione del contratto, rilevanti ai fini penali, accertati da IAA con ogni mezzo e oggetto di eventuale denuncia o querela;
- grave violazione della riservatezza di dipendenti o altri soggetti i cui dati sono oggetto di trattamento;
- violazione degli obblighi attinenti alla sicurezza sul lavoro;
- violazione grave o reiterata dei principi contenuti nel Codice Etico; di IAA
- l'accertamento in capo all'operatore economico aggiudicatario di una delle cause interdittive di cui all'art. 67 ovvero dell'art. 84, comma 4 del D.Lgs. 159/2011;
- il mancato utilizzo nelle transazioni derivanti dal contratto del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010, n. 136;
- la sospensione senza giustificato motivo, anche di un giorno, dell'attività;
- lo smarrimento o rovina del materiale di IAA per un importo superiore a € 5.000,00, oltre al risarcimento del danno;
- in base alla gravità del fatto, il mancato rispetto del segreto d'ufficio e di riservatezza su documenti, fatti e/o dati concernenti l'organizzazione e l'andamento di IAA.

In caso di risoluzione anticipata del contratto e fino all'esperimento di nuova gara, IAA addebiterà all'operatore economico aggiudicatario il maggior onere derivante dalla necessità di affidare il servizio ad altro operatore.

Il contratto è sottoposto a condizione risolutiva nel caso di intervenuta disponibilità di convenzioni Consip e/o della centrale di committenza regionale che prevedano condizioni di maggior vantaggio economico, così come previsto ai sensi dell'art. 1, co. 13, del D.L. n. 95 2012, come convertito in L. 7 n. 35 2012. IAA rileva la presenza di condizioni economiche migliorative rispetto al contratto nelle convenzioni Consip e/o nella centrale di committenza regionale e le comunica all'operatore economico aggiudicatario con i mezzi previsti dal contratto. L'operatore economico aggiudicatario, entro quindici giorni dal ricevimento della comunicazione, esprime esplicitamente e incondizionatamente la volontà di adeguare i corrispettivi previsti nel contratto a quelli inseriti nelle convenzioni Consip e/o della centrale di committenza regionale. IAA non considera efficaci, eccezioni o contestazioni connesse alle diverse condizioni previste nelle citate convenzioni, alle quali l'operatore economico aggiudicatario deve incondizionatamente aderire. Decorso il termine di cui sopra ed in assenza di positivo riscontro, IAA recede dal contratto senza ulteriore comunicazione ed il compenso

per l'operatore economico aggiudicatario è quello previsto dalla normativa di riferimento. Anche in questa ipotesi, l'operatore economico aggiudicatario è tenuto ad assicurare lo svolgimento della prestazione per il tempo necessario a IAA a formalizzare la sottoscrizione della convenzione con Consip e/o con la centrale di committenza regionale

La risoluzione non si estende alle prestazioni già eseguite.

Per qualsiasi ragione si addivenga alla risoluzione del contratto, l'operatore economico aggiudicatario, oltre all'immediato incameramento della garanzia definitiva, sarà tenuto al risarcimento di tutti i danni, diretti ed indiretti ed alla corresponsione delle maggiori spese alle quali IAA dovrà andare incontro per il rimanente periodo contrattuale.

16 Rispetto delle norme di assicurazione sociale e sicurezza sul lavoro

1. L'operatore economico aggiudicatario è tenuto a:
   a. osservare le norme e le prescrizioni dei contratti collettivi sulla tutela, sicurezza, salute, assicurazione ed assistenza dei lavoratori. In particolare, curerà tutti gli adempimenti previsti dal D.lgs. 81/2008;
   b. rispettare tutte le norme in materia retributiva, contributiva, previdenziale, assistenziale, assicurativa e sanitaria;
   c. applicare integralmente tutte le norme contenute nei contratti collettivi dei lavoratori e negli accordi integrativi per il settore di attività.
2. In caso di violazione degli obblighi di cui sopra, previa contestazione all'operatore economico aggiudicatario delle inadempienze ad essa denunciate dai preposti, IAA effettuerà trattenute su qualsiasi credito maturato a favore dell'operatore economico aggiudicatario per l'esecuzione della prestazione e procederà, in caso di crediti insufficienti allo scopo, all'escussione della garanzia fideiussoria.
3. Per le detrazioni e sospensioni dei pagamenti di cui sopra, l'operatore economico aggiudicatario non potrà opporre eccezioni a IAA a titolo di risarcimento dei danni.
4. In caso di ripetute infrazioni alle norme in materia retributiva, contributiva, previdenziale, assistenziale, assicurativa e/o sanitaria, IAA provvederà a risolvere il contratto e ad effettuare le dovute comunicazioni alle competenti Autorità.

17 Garanzie

A partire dal rilascio del certificato di regolare esecuzione e per tutto il periodo di garanzia come indicato nell'offerta, l'operatore economico aggiudicatario si impegna ad assicurare che i servizi di assistenza e manutenzione siano conformi agli specifici livelli qualitativi (SLA) indicati nell'offerta stessa e/o nel presente capitolato.

18 Messa a disposizione e utilizzo di apparecchiature

1. L'operatore economico aggiudicatario dovrà richiedere per iscritto a IAA l'autorizzazione all'utilizzo di propri prodotti software negli ambienti informatici messi a disposizione da

IAA, indicando il tipo di prodotto e il motivo del suo utilizzo. L'uso di prodotti software non autorizzati costituirà grave inadempienza contrattuale a tutti gli effetti di legge.

2. In ogni caso l'operatore economico aggiudicatario garantisce di aver adottato tutte le opportune cautele e che i prodotti software utilizzati sono esenti da virus.
3. Prima del loro utilizzo negli ambienti di IAA, e se da quest'ultima ritenuto opportuno, l'operatore economico aggiudicatario è obbligato a sottoporre i supporti magnetici e ottici alle verifiche richieste da IAA, o a far operare il proprio personale esclusivamente sulle apparecchiature messele a disposizione.
4. L'operatore economico aggiudicatario garantisce che le apparecchiature, i materiali e i supporti sui quali sono caricati i documenti e i programmi sono esenti da vizi derivanti dalla progettazione o cagionati da errata esecuzione o da deficienze dei materiali impiegati, che ne diminuiscono il valore e/o che li rendano inidonei, anche solo parzialmente, all'uso cui sono destinati.
5. Ferma restando la facoltà di IAA di risolvere il contratto per inadempimento delle obbligazioni, l'operatore economico aggiudicatario è obbligata al risarcimento di qualsiasi danno, in forma specifica o per equivalente.

19 Revisione prezzi

1. Ai sensi del art. 60 del D.lgs n.36/2023 i prezzi sono aggiornati, in aumento o in diminuzione, sulla base dei seguenti indici sintetici elaborati dall'ISTAT: con riguardo ai contratti di servizi e forniture, gli indici dei prezzi al consumo, dei prezzi alla produzione dell'industria e dei servizi e gli indici delle retribuzioni contrattuali orarie.
   La revisione dei prezzi è riconosciuta se le variazioni accertate risultano superiori al 5 per cento dell'importo complessivo e opera nella misura dell'80 per cento della variazione stessa, in relazione alle prestazioni da eseguire.
2. L'eventuale revisione del prezzo sarà valutata sulla base di una istruttoria condotta dal RUP, coadiuvato dal DEC, se esistente, e approvata da IAA.

20 Obblighi dell'Operatore economico aggiudicatario

1. L'operatore economico aggiudicatario si obbliga a eseguire a regola d'arte tutte le prestazioni ad esso affidate. A tal proposito, l'operatore economico aggiudicatario dichiara di aver preso conoscenza delle prestazioni da eseguire, dei luoghi e delle modalità di esecuzione e di disporre dei mezzi tecnici, organizzativi e finanziari per far fronte agli impegni assunti. Dichiara, altresì, di conoscere e osservare tutte le leggi, i regolamenti e le disposizioni vigenti, in particolare al settore tecnico di riferimento.
2. Oltre a tutti gli obblighi derivanti dal presente capitolato, dalle leggi e dai regolamenti, sono a carico dell'operatore economico aggiudicatario:
   a) L'organizzazione e l'esecuzione della prestazione in conformità all'offerta e, in ogni caso, secondo le modalità impartite da IAA, nel rispetto di norme e indicazioni sulla qualità dei materiali e dei servizi e sulle regole di buona esecuzione;
   b) L'utilizzo, nel rispetto delle norme vigenti, di personale adeguato, per numero e per competenza, alle prestazioni da eseguirsi;

c) L'assunzione di ogni responsabilità per i danni eventualmente cagionati a IAA e/o a terzi durante l'esecuzione del servizio, dichiarando fin d'ora di tenere IAA sollevata e indenne da qualsiasi obbligo di risarcimento;
d) Il rispetto della pianificazione delle attività e dei pacchetti di lavoro nonché il rispetto delle SLA se previste.

21 Misure di gestione ambientale

L'offerente deve essere in grado di applicare misure di gestione ambientale, durante l'esecuzione del contratto, in modo da arrecare il minore impatto possibile sull'ambiente, attraverso l'adozione di un sistema di gestione ambientale, conforme ad una norma tecnica riconosciuta (EMAS, ISO 14001).

L'offerente deve operare in conformità alle disposizioni normative vigenti in materia di tutela dell'ambiente in relazione alla fornitura, alla messa a disposizione, alla manutenzione e allo smaltimento o riciclaggio dei materiali, inclusi gli imballaggi ed altri materiali di supporto.

22 Obblighi di riservatezza

1. L'operatore economico aggiudicatario tutelerà la piena riservatezza delle informazioni acquisite nell'esecuzione del contratto, rispettando le seguenti clausole di riservatezza ed in particolare si obbliga a:
   a. considerare e trattare in maniera strettamente riservata tutte le informazioni, dati o documenti ricevuti o resi accessibili da IAA e ad attuare tutte le cautele e le misure di sicurezza necessarie e opportune, secondo i migliori standard professionali, al fine di mantenere riservate tali informazioni e prevenire accessi non autorizzati, la sottrazione e la manipolazione delle stesse;
   b. non divulgare e/o comunque a non rendere note a Terzi le informazioni, intendendosi per "Terzi" tutti i soggetti diversi dagli amministratori, dipendenti, intermediari o consulenti ("Persone Collegate") di IAA, a cui l'operatore economico aggiudicatario potrà comunicare le informazioni nella misura in cui ciò sia necessario al fine di consentirgli di svolgere le attività affidategli sulla base del principio del need to know;
   c. dare istruzioni ai propri tecnici circa l'obbligo del più assoluto riserbo nell'ipotesi in cui, accidentalmente dovessero avere notizia di dati o informazioni di titolarità di IAA o di terzi contenuti in cartelle elettroniche, con divieto di diffusione o comunicazione di qualsivoglia notizia e/o dato dei quali dovessero venire a conoscenza.
2. In ogni caso, i documenti e i dati trattati dall'Operatore economico aggiudicatario non potranno essere neanche parzialmente duplicati, riprodotti, esportati, comunicati a terzi, né diffusi o trasferiti all'estero e sempre e comunque dovranno essere trattati nell'esatta osservanza degli obblighi contrattuali e delle finalità ricomprese nelle obbligazioni assunte dall'operatore economico aggiudicatario con il contratto.
3. In caso di inosservanza degli obblighi di riservatezza e segretezza, IAA si riserva la facoltà di dichiarare risolto di diritto il contratto, fermo restando l'obbligo del risarcimento di tutti i danni che dovessero derivare a carico di IAA e/o del fruitore finale.

23 Rispetto del codice etico e del Modello di Organizzazione e Gestione ai sensi del Decreto Legislativo 231/2001

1. L' operatore economico aggiudicatario è a conoscenza che IAA ha adottato ed attua un Modello di Organizzazione, Gestione e Controllo ai sensi del D.lgs. 231/01, con i relativi Codice Etico e Sistema Disciplinare, che dichiara di aver letto dal sito aziendale e che dichiara di aver compreso.
2. L' operatore economico aggiudicatario aderisce ai principi al succitato Modello di organizzazione, gestione e controllo nonché ai suoi allegati e si impegna a rispettarne i contenuti, i principi, e le procedure e in generale ad astenersi da qualsivoglia comportamento atto a configurare le ipotesi di reato indicate nel D.lgs. 231/01 e riportate nel predetto Modello di organizzazione, gestione e controllo.
3. Si impegna altresì a rispettare e a far rispettare ad eventuali suoi collaboratori, tutti i principi contenuti nella suddetta documentazione ed i Protocolli comportamentali previsti da IAA ai sensi del D.lgs. 231/2001 ed allegati al presente contratto. La violazione delle regole previste dai sopraccitati documenti rappresenta grave inadempimento contrattuale.
4. L' operatore economico aggiudicatario dichiara che nell'ambito degli ordinari contatti con IAA e/o con il cliente e/o con il fruitore finale, non si sono verificati da parte di chicchessia episodi che anche ipoteticamente appaiano riconducibili o comunque rilevanti ai sensi del D.lgs. 231/01 in qualunque forma, finalizzati a compensare il responsabile di illeciti comportamenti, volti a produrre un vantaggio per IAA.

24 Sicurezza dati

24.1 Regole generali

1. L'operatore economico aggiudicatario si impegna ad adottare tutte le misure idonee a garantire la sicurezza, l'integrità e la disponibilità di ogni dato e informazione, di qualsivoglia natura di cui è venuta a conoscenza in occasione del rapporto instaurato e per lo svolgimento dell´ incarico rispettando eventuali ed ulteriori disposizioni e regolamenti di in materia di sicurezza, riservatezza, integrità e disponibilità date da IAA. Il rispetto di tutte le prescrizioni non deve causare ulteriori spese a IAA.
2. L'operatore economico aggiudicatario ha l'obbligo di mantenere riservati i dati e le informazioni, di non divulgarli né di farne oggetto di comunicazione o trasmissione nonché di uso per scopi diversi da quelli oggetto del contratto o senza l'espressa autorizzazione di IAA.
3. Tutti i sistemi tecnologici messi a disposizione e/o utilizzati dall'operatore economico aggiudicatario nell'esecuzione del contratto devono garantire preventive misure di sicurezza, volte a minimizzare i rischi di sicurezza connessi al trattamento dei dati.
4. Sono vietate a norma di legge e per vincolo contrattuale tutte le operazioni fisiche, logiche e di rete non strettamente pertinenti all'oggetto del contratto.
5. I terminali ed i dispositivi utilizzati per la connessione devono venir collocati in aree sicure ad accesso controllato. Nel caso di utilizzo di strumenti portatili, devono essere adottate regole comportamentali che diminuiscano il rischio di sottrazione o accesso abusivo.

6. Tutti i sistemi tecnologici messi a disposizione e/o utilizzati dall'operatore economico aggiudicatario nell'esecuzione del contratto non devono essere utilizzati per erogare contemporaneamente servizi a terzi e servizi relativi al contratto. Devono essere altresì assicurate tutte le contromisure volte ad evitare qualsivoglia collegamento logico tra realtà tecnologiche distinte, fatto salvo il collegamento minimo necessario ai sistemi dell'operatore economico aggiudicatario per l'accesso ai sistemi di cui al contratto e all'erogazione dei servizi previsti.
7. L'operatore economico aggiudicatario dichiara che, su richiesta di IAA, eventuali copie od originali di informazioni in suo possesso, e di cui IAA e/o il Cliente e/o il fruitore finale siano titolari, siano distrutte con procedure idonee e documentate.
8. Una volta terminato il rapporto contrattuale con IAA, l'operatore economico aggiudicatario si impegna alla restituzione di ogni dato e/o informazione acquisiti durante il periodo di vigenza contrattuale.
9. Relativamente a misure di sicurezza organizzativa l'operatore economico aggiudicatario deve garantire:
   a. tutte le cautele per non lasciare incustodito ed accessibile il terminale durante una sessione di connessione;
   b. tutte le precauzioni per assicurare la segretezza della password utilizzata;
   c. che l'utilizzo degli strumenti IAA (connessioni, sistemi, banche dati) avvenga solo per necessità e nel rispetto di quanto previsto dai rapporti contrattuali in essere;
   d. che ogni attività sui sistemi e sui dati sia svolta solo se espressamente concordata con IAA.
10. L'operatore economico aggiudicatario è responsabile dell'esatta osservanza da parte dei propri dipendenti e consulenti nonché dei propri eventuali subappaltatori, degli obblighi anzidetti.

24.2 Misure specifiche e requisiti di sicurezza

Le misure di sicurezza che l'operatore economico aggiudicatario dovrà adottare nell'ambito del servizio o della fornitura oggetto del capitolato tecnico, sono definite nelle matrici del presente paragrafo (Matrice 1 – Requisiti di sicurezza obbligatori, Matrice 2 – Requisiti di sicurezza facoltativi) e si riferiscono alle linee guida AGID per la sicurezza nel procurement ICT. L'elenco specifico dei "Requisiti di sicurezza" da applicare (rappresentati attraverso un codice la cui descrizione è riportata nella Tabella 4 si evince incrociando, all'interno della Matrice 1, la "Tipologia di contratto" ed il "Livello di Criticità Complessiva (LCC)" identificati per l'acquisto e di seguito riportati (Tabella 3).

Per la fornitura di sole licenze software e relativo supporto tali misure non sono da considerarsi.

Tipologia di contratto	☐	a) contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche
	☒	b) contratti di acquisizione di prodotti (hardware o software)
	☐	c) contratti per attività di operation e conduzione
	☐	d) contratti per servizi diversi da a) e c) (es. supporto specialistico, formazione, help desk, ecc.)
Livello di Criticità Complessiva (LCC)	☐	BASSO
	☐	MEDIO
	☒	ALTO

Tabella 3 - Parametri per identificazione Requisiti sicurezza

- Matrice di identificazione dei requisiti **obbligatori.**
  In evidenza, la cella o le celle relative alle misure da applicare per il servizio o la fornitura in oggetto.

		Livello di Criticità Complessiva (LCC)		
		BASSO	**MEDIO**	**ALTO**
Tipologia di contratto	**a) contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche**	R6, R11, R13, R14, R15, R17, R18, R19, R20, R21, R22, R23	R1, R6, R11, R12, R13, R14, R15, R17, R18, R19, R20, R21, R22, R23	R1, R6, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R20, R21, R22, R23
	b) contratti di acquisizione di prodotti (hardware o software)	R6, R11, R13, R14, R15, R17, R18, R19, R24, R25, R26, R27, R28, R29, R30, R31, R32, R33	R1, R6, R11, R12, R13, R14, R15, R17, R18, R19, R24, R25, R26, R27, R28, R29, R30, R31, R32, R33	R1, R6, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R24, R25, R26, R27, R28, R29, R30, R31, R32, R33
	c) contratti per attività di operation e conduzione	R6, R11, R13, R14, R15, R17, R18, R19, R34, R35, R36, R37, R42, R43, R44	R1, R6, R11, R12, R13, R14, R15, R17, R18, R19, R34, R35, R36, R37, R38; R40, R41, R42, R43, R44, R45	R1, R6, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R34, R35, R36, R37, R38, R39; R40, R41, R42, R43, R44, R45
	d) contratti per servizi diversi da a) e c) (es. supporto specialistico, formazione, help desk, ecc.)	R6, R11, R13, R14, R15, R17, R18, R19	R1, R6, R11, R12, R13, R14, R15, R17, R18, R19	R1, R6, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19

Matrice 1 – Requisiti di sicurezza obbligatori

- Matrice dei requisiti **facoltativi.**
  Eventuali ulteriori requisiti assimilabili come elementi migliorativi del servizio o della fornitura che l'operatore economico aggiudicatario può offrire senza oneri aggiuntivi da parte di IAA.

		Elementi migliorativi (EM)
Tipologia di contratto	**a) contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche**	R2, R3, R4, R5, R7
	b) contratti di acquisizione di prodotti (hardware o software)	R2, R3, R4, R5, R7
	c) contratti per attività di operation e conduzione	R2, R3, R4, R5, R7
	d) contratti per servizi diversi da a) e c) (es. supporto specialistico, formazione, help desk, ecc.)	R2, R3, R4, R5, R7

Matrice 2 – Requisiti di sicurezza facoltativi

- Tabella dei Requisiti
  Elenco dei requisiti, e loro descrizione, ai quali le matrici 1 e 2 fanno riferimento.

Requisito	**Descrizione**
R1	Il fornitore deve adottare al proprio interno le procedure e politiche di sicurezza definite dall'amministrazione committente, con particolare riferimento alle modalità di accesso ai sistemi dell'amministrazione, all'hardening (esempio installazione di soluzioni di end point security) dei dispositivi utilizzati dal fornitore, alla gestione dei dati dell'amministrazione.
R2	Il fornitore deve possedere la certificazione ISO/IEC 27001 e mantenerla per tutta la durata della fornitura.
R3	(alternativo al precedente) Anche se il fornitore non è certificato ISO/IEC 27001, almeno deve usare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) aggiornato nel tempo e/o predisporre un piano di qualità secondo lo standard ISO 10005
R4	Il fornitore deve far eseguire annualmente un audit sul proprio sistema di sicurezza, a proprie spese e da una società specializzata scelta previa approvazione della stazione appaltante. NB: Qualora applicabile, tale attività si incrocia con il requisito R2 (le verifiche dell'Ente Certificatore hanno cadenza pressoché annuale).
R5	L'amministrazione può, con un preavviso di 20 giorni solari, richiedere ulteriori attività di auditing secondo modalità concordate con il fornitore. Le risultanze di tali audit verranno comunicate all'amministrazione.
R6	L'amministrazione, direttamente o tramite terzi incaricati, può eseguire verifiche relative alla conformità della prestazione dei servizi rispetto a quanto stabilito nel capitolato tecnico oltre che nell'offerta tecnica se migliorativa.

R7	Il personale del fornitore che presta supporto operativo nell'ambito dei servizi di sicurezza dovrà possedere certificazione su specifici aspetti della sicurezza.
R8	Il fornitore deve disporre di una struttura per la prevenzione e gestione degli incidenti informatici con il compito d'interfacciarsi con le analoghe strutture dell'amministrazione e con le strutture centrali a livello governativo.
R9	Il fornitore deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici
R10	Il SOC del fornitore deve sovrintendere alla gestione operativa e continuativa degli incidenti informatici sui servizi erogati nell'ambito della fornitura.
R11	Il fornitore deve garantire il rispetto di quanto richiesto dalla normativa vigente in materia di sicurezza cibernetica, anche in riferimento ai contenuti del GDPR, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, e adottando procedure tecniche e organizzative volte alla gestione di eventuali violazioni di dati personali
R12	Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise).
R13	Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati.
R14	Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
R15	Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE. Eventuali eccezioni dovranno essere preventivamente discusse ed autorizzate dall'amministrazione.
R16	Il fornitore deve dare disponibilità a far parte di un Comitato di Direzione Tecnica, eventualmente aperto anche a soggetti terzi, che tratti il tema della sicurezza, sia nell'ottica di favorire la risoluzione di temi aperti sia per introdurre eventuali varianti al contratto per fronteggiare nuove minacce o altro.
R17	Il fornitore deve condividere le informazioni necessarie al fine di garantire il corretto monitoraggio della qualità e della sicurezza, eventualmente pubblicando le stesse nel portale della fornitura.
R18	Il fornitore si impegna a sottoscrivere una clausola di non divulgazione (NDA) sui dati e sulle informazioni dell'amministrazione.
R19	Le soluzioni e i servizi di sicurezza proposti dal fornitore devono essere aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato; devono essere conformi alle normative e agli standard di riferimento applicabili; devono venire adeguati nel corso del contratto, senza oneri aggiuntivi, alle normative che l'UE o l'Italia rilasceranno in merito a servizi analoghi.
R20	l fornitore deve attenersi alla politica di sicurezza dell'amministrazione committente, con particolare riferimento all'accesso ai dati dell'amministrazione, che avverrà esclusivamente sui sistemi di sviluppo e test. Eventuali eccezioni dovranno essere preventivamente autorizzate dall'amministrazione.

R21	In fase di analisi, il fornitore deve definire le specifiche di sicurezza (non funzionali) a partire dai requisiti espressi dall'amministrazione.
R22	In fase di progettazione codifica, il fornitore deve implementare le specifiche di sicurezza nel codice e nella struttura della base dati.
R23	Al termine del progetto, il fornitore deve rilasciare tutta la documentazione necessaria all'amministrazione per gestire correttamente quanto rilasciato anche sotto l'aspetto della sicurezza.
R24	Deve essere previsto l'utilizzo di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.).
R25	Deve essere possibile, in caso di necessità di accesso alla rete, il filtraggio di indirizzi IP.
R26	Deve essere supportato l'utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.).
R27	Deve essere possibile la gestione di più profili con privilegi diversi.
R28	Deve essere presenta la funzionalità di "richiesta creazione o cambio della password al primo accesso".
R29	Blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso.
R30	Gli accessi amministrativi degli utenti devono essere registrati su un archivio (log) non cancellabile con il reset, per almeno sei mei, o, in alternativa deve essere possibile forwardare i dati su di un server esterno.
R31	Deve essere possibile gestire i log di sistema (accessi, allarmi, ecc.).
R32	Il fornitore (anche in collaborazione con il produttore della tecnologia) deve offrire processi, unità organizzative e strumenti dedicati alla gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura. Il rientro da queste vulnerabilità, a carico del fornitore, deve avvenire in tempi congrui alla severità della vulnerabilità) e senza compromettere la fornitura stessa.
R33	Per gli apparati proposti deve essere disponibile documentazione tecnica (schede tecniche, manuali, guide operative) relativa alla corretta configurazione e gestione degli aspetti di sicurezza.
R34	I meccanismi di autenticazione devono essere basati su meccanismi di crittografia asimmetrica, a chiave pubblica; la lunghezza delle chiavi va impostata sulla base della criticità della comunicazione da cifrare (ad esempio 256 bit per le meno critiche, 512 bit per le più critiche). La gestione e distribuzione delle chiavi e dei certificati è a carico del fornitore. L'aggiudicatario dovrà fornire a IAA informazioni sulle procedure di gestione del ciclo di vita delle chiavi di crittografia [generate, change, store, retrieve, retain and destroy], in modo da potere verificare la conformità rispetto ai propri requisiti; Vengono richieste le informazioni sulle procedure raccomandate di gestione (best practice). Al fornitore del servizio è inoltre vietato memorizzare e gestire le chiavi utilizzate da IAA direttamente o indirettamente tramite terzi incaricati.
R35	Autorizzazione: sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni.
R36	Confidenzialità nella trasmissione dei dati: le comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'amministrazione devono essere cifrate.
R37	Fornire meccanismi che permettano di garantire l'integrità di quanto trasmesso (ad esempio meccanismi di hashing).

R38	Il fornitore deve descrivere nel dettaglio le soluzioni tecniche utilizzate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza, …) per soddisfare i requisiti di sicurezza dell'amministrazione committente.
R39	In fase di attivazione del servizio, il fornitore deve concordare con l'amministrazione le modalità operative e le politiche di sicurezza, i livelli di gravità degli incidenti, le attività e le contromisure che dovranno essere svolte per contrastare le minacce.
R40	Il fornitore dovrà attenersi alle politiche di sicurezza definite dalla committente, con particolare riferimento alla definizione di ruoli e utenze per l'accesso ai sistemi gestiti.
R41	In caso di necessità, da parte degli operatori, di accesso a Internet, il fornitore deve utilizzare un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'amministrazione.
R42	In caso di rilevazione di un incidente di gravità elevata (con scala da definire a inizio fornitura), il fornitore deve dare immediata notifica, tramite canali concordati con l'amministrazione, dell'incidente rilevato e delle azioni da intraprendere, al Responsabile della Sicurezza indicato dall'amministrazione e agli organismi individuati dal legislatore a presidio della sicurezza cibernetica.
R43	Per ogni incidente di sicurezza, il fornitore s'impegna a consegnare all'amministrazione, entro il giorno successivo, un report che descriva la tipologia di attacco subito, le vulnerabilità sfruttate, la sequenza temporale degli eventi e le contromisure adottate.
R44	Su richiesta dell'amministrazione, il fornitore deve consegnare i log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT. Tali log dovranno essere inviati all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta.
R45	Il fornitore deve monitorare la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite. Entro il giorno successivo al rilascio dell'upgrade/patch/hotfix, il fornitore deve avviare una valutazione, da rilasciarsi entro un numero giorni da stabilirsi, propedeutica all'installazione delle stesse sui dispositivi di sicurezza, che ad esempio identifichi la possibilità di applicare la patch immediatamente, o la necessità di apportare MEV o integrazioni prima di procedere alle installazioni.

Tabella 4 – Requisiti di sicurezza

25 Verifica di conformità

1. Entro 20 giorni dall'ultimazione delle prestazioni previste in contratto, il DEC o, in mancanza, il RUP avvia le attività necessarie per l'emissione del certificato di verifica di conformità delle prestazioni.
2. Il certificato è rilasciato previo accertamento che tutte le condizioni, obblighi e prestazioni richieste dal contratto siano stati effettivamente rispettati e forniti in conformità alle pattuizioni contrattuali e a regola d'arte, presentino i requisiti richiesti dalla documentazione contrattuale e dalle leggi di settore in vigore al momento del rilascio del certificato, che siano state consegnate all'operatore economico aggiudicatario tutte le certificazioni e dichiarazioni di conformità prescritte dalla legge e dal contratto e che i dati contabili corrispondano ai dati di fatto.
3. Esaminati i documenti acquisiti ed accertatane la completezza, il soggetto incaricato della verifica di conformità fissa il giorno del controllo definitivo e ne informa il RUP.

Quest'ultimo ne dà tempestivo avviso all'operatore economico aggiudicatario, affinché la stessa possa intervenire.

4. In casi particolari, che non consentono il collaudo o la verifica sulla totalità delle prestazioni, le stesse sono eseguite a campione, con modalità idonee a garantire la verifica dell'esecuzione delle prestazioni contrattuali.
5. Il certificato dovrà contenere l'indicazione degli eventuali giorni di ritardo e l'eventuale importo totale della penale da applicarsi. IAA trasmette il certificato all'operatore economico aggiudicatario, che lo deve accettare entro 15 gironi dal ricevimento.
6. Il soggetto incaricato della verifica di conformità riferisce al RUP su eventuali contestazioni fatte dall'operatore economico aggiudicatario. Il RUP si esprime sulle risultanze della verifica di conformità e sulle eventuali contestazioni dell'operatore economico aggiudicatario.
7. Il certificato deve essere emesso entro 60 giorni dall'inizio delle operazioni di verifica.
8. Il soggetto che procede alla verifica di conformità indica se le prestazioni sono o meno collaudabili, ovvero, riscontrandosi difetti o mancanze di lieve entità riguardo all'esecuzione, collaudabili previo adempimento delle prescrizioni impartite all'operatore economico aggiudicatario, con assegnazione di un termine per adempiere. In tal caso il termine previsto per l'emissione del certificato di conformità è interrotto fino alla completa rimozione ed eliminazione dei difetti e mancanze riscontrate. Nel caso di mancata rimozione dei difetti, IAA si riserva la facoltà di emettere il certificato di collaudo applicando le detrazioni previste o facendo rimuovere i difetti con una esecuzione d'ufficio e oneri a carico dell'operatore economico aggiudicatario.
9. È fatta salva la responsabilità dell'operatore economico aggiudicatario per eventuali vizi o difetti anche in relazione a parti, componenti o funzionalità non verificabili in sede di verifica di conformità.
10. A seguito dell'emissione del certificato IAA provvede al pagamento dei crediti residui e allo svincolo della cauzione definitiva.
11. Sono a carico dell'operatore economico aggiudicatario gli oneri relativi all'esecuzione delle verifiche e agli accertamenti eseguiti per il rilascio del certificato di conformità. Se l'operatore economico aggiudicatario non dovesse ottemperare a siffatti obblighi, le relative spese verranno detratte dal credito residuo o dalla cauzione definitiva.

26 Certificato di regolare esecuzione

A seguito dell'intervenuta comunicazione dell'ultimazione delle prestazioni, il RUP effettua i necessari accertamenti e rilascia il certificato di regolare esecuzione o di collaudo da far sottoscrivere all'operatore economico aggiudicatario.

27 Proprietà, qualità e sicurezza del SW sviluppato e dei prodotti in genere

27.1 Proprietà e riuso

1. Nel caso in cui oggetto del contratto sia l´acquisto di SW e/o di un programma elaborato per IAA, quest´ultima acquisisce il diritto di proprietà e dei diritti derivanti di tutto quanto

realizzato dall´operatore economico aggiudicatario in esecuzione del contratto (a titolo meramente esemplificativo e non esaustivo, trattasi dei prodotti SW e dei sistemi sviluppati, degli elaborati, delle procedure SW e, in più genericamente, di creazioni intellettuali e opere dell´ingegno), dei relativi materiali e documentazione creati, inventati, ideati e predisposti o realizzati dall´operatore economico aggiudicatario nell´ambito o in occasione dell´esecuzione del contratto.

2. Pertanto, IAA potrà, senza restrizione alcuna, utilizzare, pubblicare, diffondere, duplicare o cedere anche solo parzialmente detti materiali o opere dell'ingegno, essendone la titolare esclusiva.
3. I diritti di cui sopra devono intendersi acquisiti da IAA in modo perpetuo, illimitato e irrevocabile.
4. L'operatore economico aggiudicatario si obbliga a fornire a IAA tutta la documentazione e il materiale necessari all'effettivo esercizio dei predetti diritti di titolarità esclusiva, nonché a sottoscrivere tutti i documenti necessari all'eventuale trascrizione di detti diritti in favore di IAA in eventuali registri o elenchi pubblici.
5. Tutti i report e, comunque tutta la documentazione di rendicontazione e di monitoraggio del contratto fornita e/o predisposta e/o realizzata dall´operatore economico aggiudicatario in esecuzione degli adempimenti contrattuali, tutti i dati e le informazioni ivi contenute nonché la documentazione di qualsiasi tipo derivata dall´esecuzione del contratto sono e rimarranno di esclusiva titolarità di IAA che potrà disporne, senza alcuna restrizione, la pubblicazione, la diffusione, l'utilizzo per le proprie finalità istituzionali.
6. Quale titolare esclusiva del SW, del programma e dei relativi prodotti, IAA potrà concederne il riuso ai sensi e nelle modalità limiti previste dalla legge in vigore in materia.

27.2 Qualità

Gli artefatti software sviluppati ad-hoc o le modifiche apportate su programmi già esistenti e il cui codice sorgente appartiene ad IAA o alla Pubblica Amministrazione o la cui proprietà sarà ad essi conferita, nonché la documentazione tecnica quali l'analisi di sistema, i component diagram, i deployment diagram, la documentazione di progetto, la documentazione delle API, ecc., dovranno essere realizzati a regola d'arte, seguendo le linee guida pubblicate da Informatica Alto Adige presso l'indirizzo https://servicemanual.services.siag.it/#/ e rispettando la normativa ISO 25010 e successivi aggiornamenti. Eventuali integrazioni, variazioni o deroghe dovranno essere esplicitamente concordate tra IAA e l'operatore economico prima dell'avvio dei lavori esecutivi o, in caso di eventi non predicibili che portino alla necessità di integrazione, variazione o deroga, in corso d'opera.

27.3 Sicurezza

La realizzazione dei software, o parte di essi, dovrà seguire le buone pratiche per lo sviluppo di software sicuro facendo riferimento a quanto indicato dalle linee guida AGID. IAA si riserva la facoltà di richiedere comprova dell'applicazione di tali pratiche ossia di dimostrare la rispondenza alle linee guida richiedendo specifici report che contengano l'esito dell'analisi statica del codice, di test di sicurezza effettuati sia sul codice che sull'intero applicativo, eventuali web-application scan e/o penetration test esplicitamente richiesti e quant'altro si riveli necessario. Tali report potranno essere richiesti da IAA anche in seguito al rilascio del prodotto nel periodo di vigenza della garanzia.

28 Brevetti industriali e diritti d'autore

1. L'operatore economico aggiudicatario assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, d'autore ed in genere di privativa altrui.
2. Qualora venga promossa nei confronti di IAA un'azione giudiziaria da parte di terzi che vantino diritti su beni acquistati o in licenza d'uso, l'operatore economico aggiudicatario manleverà e terrà indenne IAA, assumendo a proprio carico tutti gli oneri conseguenti, inclusi i danni verso terzi, le spese giudiziali e legali a carico di IAA stessa.
3. Nell'ipotesi di azione giudiziaria di cui al precedente paragrafo 2, fermo restando il diritto al risarcimento del danno nel caso in cui la pretesa azionata sia fondata, IAA ha facoltà di dichiarare la risoluzione di diritto del contratto, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per l'avvenuto uso, salvo che l'operatore economico aggiudicatario ottenga il consenso alla continuazione dell'uso delle apparecchiature e dei programmi il cui diritto di esclusiva è giudizialmente contestato.

29 Accesso agli atti, accesso civico e trasparenza

1. Tutti gli atti connessi al contratto saranno accessibili nei modi e con le limitazioni previsti dalla L. 241/1990 seguenti, dall'art. 53 del Codice e seguenti.
2. In ottemperanza alle prescrizioni di cui al D.lgs. n. 33/2013 in materia di obblighi di accesso civico e trasparenza:
   a. gli atti connessi al contratto potranno essere resi accessibili ai sensi dell'art. 5 del D.lgs. 33/2013;
   b. IAA pubblica sul proprio sito web, in un'apposita sezione denominata "Società Trasparente", liberamente consultabile da tutti i cittadini, tutte le informazioni relative alle procedure di scelta del contraente per l'affidamento di lavori, servizi e forniture, anche con riferimento alla modalità di selezione prescelta ai sensi del Codice.

30 Foro competente

Per tutte le controversie derivanti dall'esecuzione del contratto, comprese quelle non oggetto di transazione ai sensi dell'art. 212 del Dlgs 36/2023 e ss.mm.ii., sarà competente in via esclusiva il Foro di Bolzano.

31 Disposizioni in tema di Trattamento dei dati personali (art. 28 del General Data Protection Regulation (GDPR) 2016/679)

Se le attività previste dal presente capitolato e dal successivo contratto comportano il trattamento, da parte dell'operatore economico aggiudicatario, di dati per i quali IAA svolge il ruolo di Titolare o di Responsabile del trattamento, varrà quanto segue:

1. l'operatore economico aggiudicatario dovrà limitarsi alle operazioni strettamente necessarie allo svolgimento delle attività previste dal contratto. I dati saranno trattati, all'interno dell'impresa, soltanto dai soggetti che dovranno utilizzarli per l'esecuzione delle prestazioni oggetto del contratto. Sarà cura dell'esecutore autorizzare i suddetti soggetti

al trattamento dei dati ed istruirli, per iscritto, circa un trattamento dei dati conforme alle norme vigenti ed alle direttive impartite.
Il personale dipendente o i collaboratori/collaboratrici che saranno incaricati di svolgere le prestazioni oggetto del contratto dovranno assicurare la massima riservatezza;

2. l'operatore economico aggiudicatario si impegna a conservare una lista aggiornata degli estremi identificativi delle persone fisiche individuate quali amministratori di sistema, che IAA si riserva di richiedere, le quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. L'esecutore si impegna altresì a svolgere un'attività di verifica dell'operato degli amministratori di sistema con cadenza almeno annuale;
3. nell'ambito del trasferimento di dati verso paesi extra UE l'operatore economico aggiudicatario si impegna a:
   a) non trasferire dati personali al di fuori dello Spazio Economico Europeo, a meno che lo Stato destinatario dei dati non sia oggetto di una decisione di adeguatezza della Commissione europea ai sensi dell'articolo 45 del GDPR;
   b) non avvalersi altresì di subfornitori che a loro volta possano trasferire i dati personali oggetto della fornitura al di fuori dello Spazio Economico Europeo, fermo restando quanto previsto sub a), quali fornitori di un servizio di supporto al fornitore primario (per esempio attività di manutenzione). In questo ultimo caso infatti si concretizzerebbe un accesso da Paesi terzi extra-SEE, che risulta equivalente ad un trasferimento di dati in paesi extra-SEE, che deve essere scongiurato inserendo nell'incarico la clausola che tale previsione prevale su qualsiasi altra disposizione potenzialmente contrastante del contratto (ad esempio una descrizione standard dei servizi);
4. nell'ambito dell'attività svolta in adempimento agli obblighi contrattualmente assunti, l'operatore economico aggiudicatario è, inoltre, tenuto a compiere tutto quanto necessario per il rispetto delle vigenti disposizioni di legge in materia di trattamento di dati personali. In particolare, deve:
   a) adottare le misure di sicurezza previste in questo capitolato che tengono conto di quanto disposto dall'articolo 28 con rinvio all'articolo 32 del Regolamento UE 2016/679;
   b) provvedere a nominare un/una responsabile della protezione dei dati (Data Protection Officer) nei casi previsti dalla normativa vigente e comunicare tale nominativo nonché i relativi dati di contatto a IAA al momento della sottoscrizione del presente atto;
   c) tenere in forma scritta un registro delle categorie di attività svolte quale Responsabile del trattamento dei dati nonché mettere a disposizione di IAA l'estratto delle attività di trattamento effettuate per conto di IAA, ove richiesto;
   d) permettere, previo congruo preavviso, lo svolgimento dei controlli previsti dall'articolo 28, par. 3 lett. h) del Regolamento UE 2016/679 da parte di IAA o da altro soggetto da quest'ultima incaricato; in tali controlli rientrano le attività di auditing privacy da parte di IAA, a cui il fornitore si impegna a partecipare;
   e) assistere, per quanto di competenza, tenuto conto delle attività di trattamento affidate, IAA nell'adozione delle misure atte ad eliminare/ridurre i rischi, qualora il trattamento richieda da parte di IAA l'esecuzione della valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA);

f) informare entro 24 h la IAA di qualsiasi violazione dei dati (Data Breach) sia venuta a conoscenza inviando una mail agli indirizzi dpo@siag.it e privacy@siag.it nonché contattando contestualmente il referente del contratto e completando tempestivamente, e comunque in modo da garantire il rispetto tempi previsti dalla normativa vigente per l´eventuale notifica al Garante, tutta la documentazione che verrà sottoposta da IAA;
g) interagire tempestivamente con IAA in caso di richieste di informazioni od effettuazione di controlli e accessi da parte dell'Autorità, anche fornendo la documentazione richiesta da IAA per ottemperare alle richieste dell'Autorità;
h) assistere, per quanto di competenza, tenuto conto delle attività di trattamento affidate, IAA in tutte le questioni rilevanti ai fini di legge, fornendole supporto e accesso a tutte le informazioni necessarie a dar seguito:
    i. alle richieste di esercizio dei diritti da parte degli interessati,
    ii. alla segnalazione delle violazioni dei dati personali,
    iii. alla valutazione d'impatto sulla protezione dei dati,
    iv. alla consultazione preventiva,
    v. cancellare, ovvero riconsegnare i dati personali a IAA, secondo le indicazioni impartite dalla stessa, alla cessazione del trattamento, a meno che non sia previsto per legge un termine di conservazione dei dati;

5. l'esecutore non ricorre ad altro responsabile o sub-responsabile del trattamento, senza autorizzazione, puntuale o generale, di IAA, in conformità all'art. 28, par. 2 e 4, del Regolamento. Individua, altresì, in ossequio al principio di accountability, misure organizzative volte a garantire a IAA idonei strumenti di controllo delle attività di trattamento effettuate sotto la propria responsabilità;
6. ove il ricorso a sub-responsabili sia stato autorizzato da IAA nelle modalità previste al punto n.5, l'esecutore si impegna ad imporre ad eventuali sub fornitori, contratto o atto giuridico analogo, le stesse obbligazioni in materia di protezione dei dati gravanti sull'esecutore stesso. A dimostrazione dell'adempimento dell'obbligo posto a suo carico, l'esecutore provvederà ad inviare a IAA una copia del contratto concluso con i sub fornitori, ogni suo eventuale aggiornamento nonché la nomina ai sensi dell'art.28 del Regolamento UE 2016/679 gestita nei confronti dei sub fornitori e sottoscritta da entrambe le parti;
7. se presente, il responsabile della protezione dei dati dell'esecutore (responsabile o sub responsabile del trattamento) oltre all' ottemperare a quanto previsto all'interno dell'art.39 del GDPR, è tenuto a segnalare a IAA (titolare o responsabile del trattamento) eventuali inadempienze riscontrate, lato esecutore, sia nella fase preliminare al processo di acquisizione che nell'ambito delle azioni da svolgere dopo la stipula del contratto;
8. nei termini e nelle condizioni contrattuali per la fornitura di servizi cloud, l'aggiudicatario deve garantire che il CSP cancelli in modo sicuro e irrevocabile i supporti dati in cloud, prima di considerare un riuso dei supporti.

Resta inteso che le obbligazioni a carico dell'esecutore decadranno in qualunque caso di cessazione del rapporto contrattuale, con effetto dalla data di tale cessazione.

32 Disposizioni in tema di misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi

Se le attività previste dal presente capitolato e dal successivo contratto comporteranno la gestione, diretta e/o indiretta, di servizi legati all'Azienda Sanitaria dell'Alto Adige, l'esecutore, in ottemperanza alla Direttiva (UE) 2016/1148 del Parlamento europeo, dovrà garantire il rispetto di quanto previsto all'interno dell'articolo 14 "Obblighi in materia di sicurezza e notifica degli incidenti" della suddetta direttiva e sue eventuali successive modificazioni che dovessero insorgere posteriormente alla data di stipulo del contratto.

Inoltre, laddove dovessero sussistere anche gli obblighi derivanti dalle disposizioni in tema di trattamento dati personali, l'esecutore dovrà garantire entrambi gli adempimenti e, in caso di sovrapposizioni, prediligere il livello di copertura migliore.

Informatica Alto Adige Spa
Il RUP
(firmato digitalmente)

Firmato digitalmente dall'Operatore Economico per presa visione ed accettazione.