

Procedura di acquisto di un servizio in modalità SaaS per la registrazione degli accessi del personale, anche in sedi non collegate alla rete dati aziendale - virtualizzazione dei terminali di rilevazione presenze

## **Capitolato Tecnico Prestazionale**

## Sommario

0.	INTRODUZIONE	4
0.1	Premessa	4
0.2	Glossario e Acronimi	4
1.	SCOPO E OGGETTO DELL'INTERVENTO	6
1.1	Il contesto regionale	6
1.2	Scopo	6
1.3	Oggetto della fornitura	6
1.3.1	Stato dell'arte	7
1.3.2	Perimetro di intervento	7
2.	DURATA E IMPORTO	8
3.	AMBITO SOGGETTIVO DELLA FORNITURA (coordinamento del progetto)	9
4.	CARATTERISTICHE DELLE SOLUZIONI OFFERTE IN FORNITURA	11
4.1	Architettura della Soluzione	11
4.2	Requisiti Piattaforma timbratura digitale	13
4.3	Interoperabilità	14
4.4	Gestione della privacy e della sicurezza delle informazioni	14
4.5	Integrità	15
4.6	Configurabilità e adattabilità al contesto	15
4.7	Accessibilità, usabilità e portabilità	15
4.8	Modularità e Scalabilità	16
4.9	Tracciabilità ed esibizione	17
4.10	Gestione utenze	17
4.11	Statistiche e reportistica	17
4.12	Acquisizione dati pregressi	18
4.13	Quadro normativo di riferimento	18
4.14	Integrazioni previste	19
5.	CARATTERISTICHE DEI SERVIZI IN FORNITURA	20
5.1	Servizio di Manutenzione Evolutiva di Applicazioni Esistenti (MEV)	20
5.2	Servizio di Manutenzione Adeguativa e Migliorativa (MAD)	21
5.3	Servizio di Manutenzione Correttiva SW "pregresso e non in garanzia" (MAC)	21
5.4	Help Desk ed assistenza di I° e II° livello e sistema di tracking	21
5.5	Formazione	22
5.6	Attività iniziale per il dispiegamento della soluzione	23
6.	GESTIONE DELLA PRIVACY E DELLA SICUREZZA DELLE INFORMAZIONI	23
6.1	Obblighi generali del Fornitore in materia di protezione dei dati personali	26
6.2	Previsioni specifiche in materia di protezione dei dati personali	27

7.	TEMPI E DELIVERABLES	30
8.	GESTIONE DELLA FORNITURA	32
8.1	Governo della Fornitura	32
8.2	Gestione del contratto con il Fornitore e relative tempistiche	32
8.3	Entry Strategy, Exit Strategy	33
9.	LIVELLI DI SERVIZIO	34
9.1	IMP – Rispetto Impegni in Offerta Tecnica	34
9.2	RSC – Rispetto Scadenza da Capitolato.	35
9.3	TIP – Tempestività nell’inserimento del personale	35
9.4	TINT – Tempo di esecuzione di interventi di manutenzione evolutiva	36
9.5	DIC – Numero difetti bloccanti in collaudo	37
9.6	GSC – Giorni di sospensione in collaudo	37
9.7	TRAA – Tempo di risoluzione Anomalia in Avvio e post erogazione in garanzia	37
9.8	TPI – Tempestività di presa in carico anomalia in avvio e post erogazione in garanzia	38
9.9	NAR – Numero anomalie recidivanti in avvio e post erogazione in garanzia	38
10.	GARANZIA DEI SERVIZI/PRODOTTI FORNITI	39
11.	ELEMENTI DIMENSIONALI DI PROGETTO	39
11.1	Numero di utenti dipendenti per Azienda	39
12.	PARAMETRI PER LA VALUTAZIONE DELL’OFFERTA	41
12.1	Criterio di ripartizione qualità/prezzo	41
12.2	Criteri di valutazione dell’offerta tecnica	41

## 0. INTRODUZIONE

### 0.1 Premessa

Il presente Capitolato Tecnico Prestazionale ha lo scopo di illustrare agli operatori economici offerenti l'oggetto e l'articolazione della fornitura richiesta dall'Azienda Regionale della Salute della Sardegna (ARES Sardegna).

### 0.2 Glossario e Acronimi

Definizione	Significato
ACN	Agenzia Cyber Sicurezza Nazionale
AGENAS	Agenzia Nazionale per la Gestione dei Servizi Sanitari Regionali
AgID	Agenzia per l'Italia Digitale
AO	Azienda Ospedaliera
AOU	Azienda Ospedaliera Universitaria
AQ	Accordo Quadro
ARES	Azienda Regionale per la Salute della Sardegna (ente appaltante e committente, amministrazione)
AREUS	Azienda Regionale Emergenza Urgenza Sardegna
ARNAS	Azienda di Rilievo Nazionale ed Alta Specializzazione
B.I.	Business Intelligence
CIE	Carta d'Identità Elettronica
CNS	Carta Nazionale dei Servizi
CTP	Capitolato Tecnico Prestazionale (il presente documento)
DGR	Delibera di Giunta regionale
D.Lgs	Decreto Legislativo
eIDAS digital	Electronic IDentification, Authentication and trust Services
GDPR	General Data Protection Regulation
OT	Offerta Tecnica
PEP	Piano Esecutivo di Progetto (documento che il Fornitore è chiamato a redigere in fase esecutiva del presente Capitolato, in modo tale da descrivere in dettaglio la soluzione proposta nonché le tempistiche per la relativa implementazione)

Definizione	Significato
<b>RAS</b>	Regione Autonoma Sardegna
<b>SA</b>	Sistema applicativo
<b>SaDIT</b>	Dipartimento per la Sanità Digitale e l’Innovazione Tecnologica di ARES
<b>SaaS</b>	Software as a Service
<b>SI</b>	Sistema Informativo ASL/AO/IRCCS (il complesso dell’architettura hardware e software di supporto ai processi clinico-scientifici ed amministrativi all’interno dell’ASL/AO/IRCCS)
<b>SLA</b>	Service Level Agreement
<b>SPID</b>	Sistema pubblico di identità digitale
<b>SSR</b>	Sistema Sanitario Regionale

# 1. SCOPO E OGGETTO DELL'INTERVENTO

## 1.1 Il contesto regionale

La natura atipica di diverse sedi di lavoro, sia di ARES sia delle AA.SS.LL., richiede l'adozione di modalità differenti e più innovative per la rilevazione delle presenze del personale aziendale.

Alla luce di tali considerazioni, si intende procedere all'acquisizione di un'infrastruttura tecnologica in cloud, basata anche sull'uso di APP, che consenta la timbratura elettronica da cellulare, anche in assenza di connessione alla rete aziendale.

## 1.2 Scopo

L'obiettivo della fornitura è dotare l'Amministrazione di uno strumento che consenta il tracciamento delle presenze e delle assenze indipendentemente dalla connettività dati aziendale e che assicuri la corretta alimentazione dei sistemi di gestione del personale.

L'implementazione di tale Sistema Informativo rappresenta un elemento strategico rilevante in termini di:

- Fornire un miglioramento tecnologico e funzionale dei sistemi;
- Fornire una tecnologia che limiti i costi non trascurabili relativi alla gestione dei TRP;
- Fornire la rilevazione della presenza in qualsiasi sede;
- Miglioramento delle procedure di timbratura e accesso;

Tale procedura ha come fine ultimo quello di accelerare il processo di trasformazione digitale in ambito sanitario.

## 1.3 Oggetto della fornitura

La presente gara d'appalto ha per oggetto la fornitura di una piattaforma software, con i correlati servizi di personalizzazione, parametrizzazione, formazione e manutenzione, finalizzata alla registrazione delle presenze del personale.

La piattaforma offerta deve essere in grado di gestire l'intero processo di acquisizione delle timbrature del personale delle Aziende ARES e AA.SS.LL., in continuità funzionale con quanto già reso disponibile dal sistema attualmente in uso.

Nello specifico, sono da intendersi compresi nell'affidamento:

- fornitura di una componente client (APP) user-friendly, disponibile sia per dispositivi Android (scaricabile dal Play Store) sia per dispositivi iOS (scaricabile dall'Apple Store), ad uso dei dipendenti;

- configurazione e avvio, personalizzazione, formazione, assistenza a utenti e amministratori, nonché i servizi di manutenzione ordinaria e straordinaria;
- integrazione applicativa con i sistemi di rilevazione presenze in uso presso le aziende (SISaR HR);
- architettura cloud, senza installazione di software o hardware nei data center delle Aziende sopra citate;
- la piattaforma deve essere disponibile per il periodo indicato al capitolo 2 . “Durata e importo” e per il numero iniziale di utenti indicato al capitolo 11 “Elementi dimensionali di progetto”;
- un'area di "back office" o area di configurazione per gli amministratori della piattaforma;

L'operatore economico offerente deve descrivere nell'Offerta Tecnica le modalità con cui intende implementare la Soluzione, specificando le tecnologie da utilizzare ed eventuali migliorie rispetto alle caratteristiche minime richieste nel presente Capitolato.

Costituisce elemento premiante l'integrazione con metodi di riconoscimento basati su standard di identità digitale federata (quali SPID, CIE, OpenID Connect, ecc.), in alternativa all'utilizzo di credenziali locali.

### **1.3.1 Stato dell'arte**

L'attuale piattaforma consente l'erogazione del servizio di acquisizione delle timbrature elettroniche. Attualmente l'APP installata sul dispositivo mobile del dipendente consente le seguenti funzionalità:

- timbrature ingresso e uscita;
- visualizzazione dello storico delle timbrature;
- inserimento giustificativo di timbratura;
- timbrature off-line;
- personalizzazione del font dell'APP;

Ogni dipendente accede alla piattaforma autenticandosi con un proprio account (login e password). L'APP installata sul dispositivo mobile consente la registrazione delle presenze secondo le regole di configurazione previste.

### **1.3.2 Perimetro di intervento**

Ai fini del raggiungimento degli obiettivi l'operatore economico offerente potrà pertanto:

- prevedere soluzioni tecniche che soddisfino, in modo almeno equipollente, le specifiche indicate nel presente CTP. Di tale equipollenza dovrà essere fornita adeguata e oggettiva evidenza;
- escludere ogni aggravio diretto/indiretto per l'Amministrazione;
- essere motivata da oggettiva valutazione di opportunità;

Il progetto proposto dovrà chiaramente illustrare il perimetro di intervento e l'articolazione delle scelte.

## **2. DURATA E IMPORTO**

La durata del contratto è stabilita secondo il modello 3+3: tre anni iniziali, con possibilità di estensione per ulteriori tre anni.

La base d'asta stimata è pari a euro 150.000,00 annui, IVA esclusa (circa euro 10,00/utente IVA esclusa), per un totale di euro 450.000,00 IVA esclusa nel triennio, calcolata su una platea stimata di circa 15.000 utenti.

Si specifica che il numero di timbrature effettuate non dovrà influire sul costo della fornitura.

Ai sensi dell'art. 41, comma 14, del D.Lgs. 36/2023, l'importo dell'appalto comprende i costi della manodopera, che la stazione appaltante ha stimato in euro 67.500,00, con un'incidenza di circa il 15% sull'importo complessivo triennale posto a base di gara.



### 3. AMBITO SOGGETTIVO DELLA FORNITURA (coordinamento del progetto)

L'organizzazione centrale di ARES, ed in particolare il Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica, sarà responsabile della gestione delle attività trasversali e della gestione complessiva degli investimenti. A questo livello saranno oggetto di declinazione:

- le attività di supporto alla gestione complessiva della procedura ed alla definizione delle strategie di intervento;
- le attività di configurazione dei sistemi;
- gli aspetti infrastrutturali dell'intervento.

Le già menzionate attività verranno dettagliate all'interno del Piano Esecutivo di Progetto.

L'aggiudicatario dovrà rendersi disponibile a incontri programmati, concordati con l'ente appaltante, al fine di monitorare le fasi di lavorazione, evidenziare eventuali criticità e condividere le relative azioni correttive.

Il servizio comprenderà le attività di progettazione, realizzazione e collaudo del Sistema nel rispetto dei requisiti definiti.

L'attività di implementazione dell'applicazione software terminerà con la fase di collaudo e dovrà essere completata entro 4 mesi, secondo un piano di rilasci definito al **Cap. 7 "Tempi e Deliverables"**.

Per ciascuna fase di rilascio, dovrà esserci un'attività di collaudo e verrà verificata la congruenza di quanto realizzato con le specifiche dei requisiti e con le specifiche tecniche approvate e il rispetto degli standard della qualità.

L'attività di progettazione avrà inizio a seguito dell'avvio delle attività contrattuali e dovrà concludersi con l'approvazione da parte di ARES Sardegna.

Ai fini del raggiungimento degli obiettivi progettuali nei tempi e nei modi previsti, l'Operatore aggiudicatario sarà tenuto a collaborare con ARES e a garantire tutta la disponibilità necessaria per eventuali approfondimenti tecnico-organizzativi.

L'aggiudicatario dovrà garantire la continuità dell'attuale servizio in uso in tutte le sedi già configurate (QR code, coordinate GPS, Beacon) oppure proporre una soluzione ex novo che assicuri almeno il medesimo livello di servizio.

Per ridurre il rischio di lock-in, al termine del contratto il fornitore dovrà garantire la completa portabilità dei dati, che dovranno essere esportabili in formati standard, aperti e documentati.

La documentazione delle API e Web Services deve essere resa disponibile.

Il passaggio ad eventuale fornitore subentrante deve avvenire senza costi aggiuntivi per l'amministrazione.

## 4. CARATTERISTICHE DELLE SOLUZIONI OFFERTE IN FORNITURA

Le caratteristiche richieste sono espressive delle necessità del committente e devono essere interpretate in coerenza con i principi del D.Lgs. 36/2023.

Gli operatori economici offerenti sono pertanto liberi di proporre i prodotti ed i servizi, di livello almeno pari o superiore, che riterranno meglio rispondenti alle finalità dell'appalto, rimanendo salva ed impregiudicata la facoltà di scelta dell'ente appaltante in coerenza con i criteri di aggiudicazione.

L'offerente deve provare, con qualsiasi mezzo appropriato, che le soluzioni da lui proposte ottemperano in maniera almeno equivalente ai requisiti definiti nelle specifiche tecniche di cui al presente capitolato Tecnico Prestazionale.

### 4.1 Architettura della Soluzione

Dal punto di vista infrastrutturale, la Soluzione dovrà essere resa disponibile in modalità Software as a Service (SaaS), su Cloud Provider certificato ACN, con risorse adeguatamente dimensionate rispetto ai carichi attesi.

Tutti i costi relativi all'utilizzo del servizio SaaS devono essere ricompresi nell'offerta economica, nessun ulteriore costo dovrà essere sostenuto dalla Stazione Appaltante.

La fornitura dovrà prevedere la fornitura dei seguenti ambienti/aree tecnologiche:

- 1) PRODUZIONE (PR): Ambiente operativo di erogazione del servizio, utilizzato H24 dagli operatori;
- 2) AMMINISTRATORE (Back Office) per consentire:
  - a) inserimento, modifica e cancellazione degli utenti, anche mediante importazione massiva;
  - b) creazione di QR code senza limiti, da associare univocamente ai vari luoghi e al relativo codice terminale, secondo il tracciato record previsto;
  - c) realizzazione di un file di testo secondo il seguente tracciato personalizzato, al fine di consentire l'esportazione e la messa a disposizione delle timbrature nel sistema di rilevazione presenze SISaR HR attualmente in uso, come di seguito definito:

CAMPI	LUNGHEZZA	VALORI AMMESSI
TERMINALE	3	001-999
VERSO	1	E (Entrata) U (Uscita)
FILLER	6	0X6 (Sei volte zero)

CAUSALE	3	001-999
BADGE	13	Preceduto da zeri valore badge a destra
DATA	8	GGMMAAAA
ORA	2	HH
MINUTI	2	MM
SECONDI	2	SS
TOTALE	40	

esempio: 014E000000025000000003056508102024143136

suddivisione:

TRP	VERSO	FILLER	CAUSALE	BADGE	DATA	HH	MM	SS
014	E	000000	025	0000000030565	08102024	14	31	36

Il file incrementale realizzato dovrà essere nominato secondo il seguente pattern: 2024-11-01\_8\_00\_APP.txt (data\_ora\_APP.txt), con invio di tre tracciati giornalieri per Azienda; il numero dei tracciati giornalieri potrà essere ridefinito in fase esecutiva senza oneri aggiuntivi per l'Amministrazione.

L'Aggiudicatario, nell'ambito della presente fornitura e senza alcun onere a carico dell'Amministrazione, dovrà farsi carico di:

- eseguire tutte le attività e i servizi professionali necessari per la configurazione e parametrizzazione degli ambienti sopra elencati;
- aggiornare obbligatoriamente tutti gli ambienti sopra elencati in relazione all'evoluzione della normativa vigente e alle disposizioni aziendali, per tutta la durata contrattuale, nonché eseguire gli aggiornamenti software necessari al corretto funzionamento della soluzione;

Dal punto di vista architetturale, l'operatore economico offerente deve descrivere nell'Offerta Tecnica le modalità di implementazione della Soluzione, le tecnologie utilizzate e le eventuali migliorie rispetto alle caratteristiche minime richieste.

La soluzione dovrà prevedere un cloud server certificato, come descritto nel Decreto ACN n. 29 e successive integrazioni, dedicato su web farm di un provider nazionale, con capacità di traffico adeguata al numero di utenti previsto.

La gestione sistemistica e l'ottimizzazione del server sono a carico del fornitore.

Il fornitore dovrà garantire:

- backup del server e di ogni altro aspetto relativo all'archiviazione dei dati;

- la possibilità di progettare implementazioni in alta affidabilità e procedure di disaster recovery allineate al progetto regionale;
- qualità della connessione rete;
- modalità di recupero e migrazione dati;
- gestione della sincronizzazione delle timbrature offline;
- adeguati livelli di ridondanza e sicurezza applicativa e risk management;
- alta disponibilità della piattaforma SaaS ( $\geq 99,8\%$ );
- alte performance di risposta app ( $\leq 2$  secondi);
- configurazione e personalizzazione grafica integrale del portale; ove possibile, è preferibile il ricorso a soluzioni software caratterizzate da supporto a lungo termine;

## 4.2 Requisiti Piattaforma timbratura digitale

La Soluzione dovrà possedere le seguenti caratteristiche. Tutti i requisiti richiesti, funzionali e non funzionali, si intendono obbligatoriamente compresi nell'offerta:

COD.	DESCRIZIONE REQUISITI DEL SISTEMA INFORMATIVO	Tipologia
R-01	Ambiente Back-End Amministratori	Funzionale
R-02	Gestione della profilazione degli utenti in base al ruolo di amministratore e utente finale (creazione, modifica, disattivazione).	Funzionale
R-03	Utilizzo di tecnologie di geolocalizzazione tramite QRcode, GPS, Bluetooth (BEACON o tecnologie equivalenti), Tag NFC (nel rispetto della normativa a tutela del lavoratore);	Funzionale
R-04	Creazione di punti di rilevazione presenze senza limiti da associare univocamente ai vari luoghi con codice univoco per terminale.	Funzionale
R-05	Realizzazione secondo specifiche (par. 4.1 del CTP) di un file di testo esportabile compatibile con le specifiche del sistema di Rilevazione Presenze SISaR HR attualmente in uso	Funzionale
R-06	Compatibilità con il sistema di rilevazione presenze virtuale attualmente in uso (integrazione con SISaR HR mediante scambio file secondo il tracciato record indicato nel presente capitolato oppure mediante utilizzo di web services o API REST documentate, concordate con l'Amministrazione) o eventuale produzione di una soluzione ex-novo a garanzia dell'attuale servizio i cui costi devono essere compresi nella fornitura in oggetto	Funzionale

<b>R-07</b>	Servizio di Timbratura per modalità Lavoro Agile	Funzionale
<b>R-08</b>	Servizio di reminder integrato (Timer/Sveglia) configurabile dall'utente	Non Funzionale
<b>R-09</b>	Gestione del Workflow richiesta/autorizzazione assenza da App	Funzionale
<b>R-10</b>	Visualizzazione Cartellino collegato a sisar HR da App	Funzionale
<b>R-11</b>	Integrazione dei metodi di riconoscimento attraverso gli standard di Identità digitale federata (SPID, CIE, OpenID Connect, dati biometrici, ecc) in alternativa alle credenziali rilasciate dall'amministratore in fase di registrazione/recupero credenziali.	Premiante
<b>R-12</b>	Dashboard statistiche e reportistica avanzata	Funzionale
<b>R-13</b>	Gestione timbrature off-line.	Funzionale
<b>R-14</b>	Funzionalità antifrode timbrature ( protezione contro generazione coordinate GPS false e il rapporto dispositivi/utenze dovrà essere di 1 a 1)	Funzionale

### 4.3 Interoperabilità

L'anagrafica degli utenti dovrà essere unica a livello regionale e dovrà essere garantita attraverso l'integrazione con il modulo SISAR attualmente in uso in tutte le aziende sanitarie denominato "Gestione Risorse Umane" (HR)

Si sottolinea l'importanza che il sistema dimostri ampie capacità di integrazione, basate su protocolli e metodologie riconosciuti come standard di mercato. È essenziale che il sistema sia in grado di interoperare con piattaforme regionali, aziendali e nazionali, secondo modalità documentate e sicure.

Il sistema deve consentire la definizione di tempi e modalità di integrazione in base alla tipologia di comunicazione, permettendo sia un approccio asincrono in risposta a variazioni dei dati, sia un approccio sincrono con una cadenza prefissata e configurabile.

### 4.4 Gestione della privacy e della sicurezza delle informazioni

È richiesta obbligatoriamente, a pena di esclusione dalla procedura di gara, la conformità della soluzione proposta al quadro normativo di riferimento riportato nel paragrafo 4.13 e a quanto descritto nel capitolo 6 del presente Capitolato.

Sarà necessario prevedere sistemi di crittografia dei dati in transito e a riposo.

## **4.5 Integrità**

L'obiettivo dell'integrità è la tutela dall'alterazione di dati, informazioni e/o risorse informatiche. L'integrità comprende quindi differenti tipologie di interventi per evitare la perdita, la modifica (paradossalmente anche la generazione ex novo di dati errati), la cancellazione di dati e informazioni, non autorizzata e non voluta.

L'integrità dei dati contenuti in questo contesto si declina in diversi modi:

- i dati inseriti corrispondano effettivamente all'utente al quale si riferisce;
- i singoli documenti inseriti siano effettivamente integri e vengano mantenuti tali secondo il quadro normativo vigente.

Oltre ad eventuali errori nel trattamento, si richiede siano gestite anche le seguenti casistiche:

- la violazione dell'integrità del dato derivata dall'accesso di utenti con privilegi amministrativi;
- la violazione dell'integrità del dato derivata da una azione volontaria per modificare o omettere le informazioni.

Per garantire l'integrità del dato, l'applicativo non dovrà consentire a più operatori di modificare contemporaneamente le informazioni riferite al medesimo utente e dovrà visualizzare appositi avvisi in caso di accesso concorrente.

## **4.6 Configurabilità e adattabilità al contesto**

Il sistema oggetto della fornitura dovrà possedere caratteristiche di elevata configurabilità e adattabilità al contesto.

## **4.7 Accessibilità, usabilità e portabilità**

La Soluzione dovrà garantire, in linea generale e per quanto riguarda la portabilità, l'adozione delle Linee Guida AgID sull'accessibilità agli strumenti informatici, con particolare riferimento agli strumenti web e mobile.

Relativamente all'accessibilità e usabilità è richiesto all'operatore economico offerente di garantire:

- navigazione intuitiva della piattaforma che assicuri un utilizzo semplice da parte degli utenti;
- rapidità di accesso alle funzioni chiave del sistema (ad es. presenza di menù generale con le aree applicative principali);
- la gestione dettagliata e flessibile della profilazione degli utenti. In particolare, per ogni modulo o ambito di utilizzo della Soluzione dovrà essere possibile definire gli operatori abilitati a svolgere le diverse operazioni previste (ad es. creazione, modifica, visualizzazione, ecc.). I profili individuati dovranno poter essere applicabili a livello di operatori, gruppo di operatori, ecc.;

- una grafica semplice, leggibile e caratterizzata da combinazioni cromatiche idonee a favorire il comfort visivo. Attraverso un'unica interfaccia, l'utente dovrà poter presidiare l'intero processo e reperire rapidamente le informazioni necessarie;
- un'organizzazione dei singoli inserimenti in più campi, suddivisi in base alla sezione del documento, strutturati ad es. tramite checkbox, menu a tendina, ecc. per facilitare la manipolazione ed il riuso successivo delle informazioni;
- visualizzazione efficace e immediata delle informazioni ritenute più rilevanti, quali: eventi critici occorsi, allarmi, fase corrente di lavorazione dell'unità;
- interfacce responsive, tali da garantire una fruizione efficace ed efficiente della soluzione anche tramite dispositivi mobili (ad esempio smartphone e tablet);
- l'accesso tramite standard W3C;
- la visualizzazione delle informazioni circoscritte all'ambito operativo dell'utente, con la possibilità sia di limitare i dati modificabili o inseribili, sia di facilitare la compilazione dei campi di testo libero mediante valori preimpostati o suggerimenti contestuali;
- la configurazione di meccanismi per il log-out dell'operatore nel caso in cui non effettui transazioni, di tipologie definite, per un tempo stabilito. Questi meccanismi dovranno essere configurabili per la definizione del tempo di inattività e per la definizione delle tipologie di transazioni che, se eseguite, azzerano il tempo di inattività;
- funzioni di assistenza e supporto per agevolare gli utenti affetti da deficit visivi e/o uditivi nella fruizione del sistema e nella compilazione di eventuali questionari o moduli;

#### **4.8 Modularità e Scalabilità**

La Soluzione proposta deve soddisfare il requisito di modularità in modo da permettere l'estensione delle funzionalità attraverso l'implementazione o l'integrazione di moduli aggiuntivi anche in tempi differenti. La soluzione sarà costituita da un certo numero di sottosistemi, ciascuno dei quali svolge un compito ben definito ed è in relazione con gli altri secondo semplici interdipendenze. Ciascun sottosistema dovrà essere il più possibile indipendente dagli altri al fine di rendere più facile la sua modifica e il suo riuso.

La Soluzione proposta deve soddisfare il requisito di scalabilità, ossia deve essere capace di aumentare il throughput applicativo in proporzione all'incremento delle risorse hardware impiegate per ospitare l'applicazione. Tale requisito dovrà essere garantito senza degrado significativo delle prestazioni percepite dagli utenti.

In termini di estendibilità la Soluzione dovrà essere in grado di supportare la crescita nel tempo delle esigenze operative degli ES: dovrà essere possibile estendere di volta in volta la Soluzione con le funzionalità in base alle necessità degli organici degli ES.



## 4.9 Tracciabilità ed esibizione

La Soluzione dovrà consentire la completa tracciabilità delle operazioni effettuate (es. inserimento, modifica, cancellazione, note integrative o correzioni), al fine di renderle fruibili in ogni momento attraverso apposite funzioni di consultazione e audit.

## 4.10 Gestione utenze

Deve essere prevista, in ottemperanza al D.Lgs. 196/2003, al Regolamento (UE) 2016/679 e al D.Lgs. 101/2018, la possibilità di estrarre in ciascun sistema l'elenco dei profili attivi e delle relative autorizzazioni.

- profilo;
- funzioni autorizzate extra profilo;
- per ogni funzione autorizzata le modalità di accesso ai dati (lettura, inserimento, modifica, etc.).

Tale elenco o matrice deve essere accessibile in tempo reale dai Responsabili di procedura e/o del trattamento dei dati, per avere sempre sotto controllo le relative abilitazioni.

La funzione deve disporre di un layout facilmente consultabile dagli operatori, con possibilità di drill down o di esplosione dell'elenco (ad es. per vedere le singole funzioni previste dal profilo).

La definizione dei profili di accesso per gli utenti deve prevedere a titolo di esempio non esaustivo, almeno le seguenti categorie:

- utente interno amministratore di sistema: gestore di tutti i permessi;
- utente interno dei servizi abilitato alla fruizione del servizio;

Il sistema deve permettere di configurare gli utenti, i gruppi di utenti e i relativi profili ai quali devono poter essere assegnati in maniera configurabile sia le funzionalità consentite sia le modalità di accesso e i dati consultabili.

## 4.11 Statistiche e reportistica

Il sistema deve essere di facile utilizzo e dotato delle funzionalità necessarie alla produzione di reportistica su diverse parametrizzazioni e indicatori specifici delle attività svolte. Dovrà, quindi, essere possibile:

- produrre report statistici prefissati e interrogare la base dati su tutti i dati inseriti;
- elaborare dati utili per la valutazione economica dell'attività della Fornitura;
- creare reportistica specifica;
- esportare porzioni di data base per analisi con strumenti esterni al sistema;
- statistiche di utilizzo dell'applicativo;
- richiedere gestione audit e logging amministrativo;

- prevedere conservazione log per almeno 24 mesi.

#### **4.12 Acquisizione dati pregressi**

La Ditta aggiudicataria dovrà garantire l'acquisizione e/o la migrazione degli archivi storici pregressi nel nuovo sistema offerto; il costo delle attività di elaborazione e importazione degli archivi sarà interamente a carico dell'aggiudicatario.

L'aggiudicatario dovrà garantire la continuità dell'attuale servizio in tutte le sedi già configurate (QR code, coordinate GPS, Beacon) oppure proporre una soluzione ex novo in grado di assicurare la medesima continuità operativa.

È da considerarsi parte integrante del servizio l'attività di import dei dati dal sistema attualmente in uso. È fondamentale garantire la continuità del servizio anche qualora si renda necessario effettuare una migrazione progressiva.

I costi delle attività di import dati e della documentazione faranno parte integrante dell'offerta.

Sarà necessario prevedere un ambiente di test su cui effettuare la verifica del buon esito della migrazione dei dati, prima di passare in produzione.

#### **4.13 Quadro normativo di riferimento**

Relativamente all'implementazione della Soluzione, l'operatore economico offerente dovrà attenersi agli standard, alle linee guida nazionali ed europee di riferimento e alla normativa vigente, al fine di garantire il corretto esercizio del servizio.

Di seguito si fornisce, in maniera esemplificativa ma non esaustiva, il quadro di riferimento delle principali norme e linee guida da tenere in considerazione:

- Decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (in breve CAD);
- Decreto Legislativo 30 giugno 2003, n.196 (art. 18): Codice in materia di protezione dei dati personali e Regolamento UE 2016/679 - GDPR e D.Lgs. 101/2018;
- Linee Guida AgID sull'accessibilità degli strumenti informatici (2023);
- Linee Guida AgID di design per i siti internet e i servizi digitali della PA (2022);
- Linee Guida AgID per il Software Sicuro per lo sviluppo(2020);
- Determinazioni 306/2022 e 307/2022 di ACN.
- NIST Cybersecurity Framework (CSF) versione 2.0

Regolamento AgID/ACN, recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione 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 (2022).

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (così modificato in base al provvedimento del 25 giugno 2009);
- D.Lgs. n. 36/2023 e s.m.i.

L'Aggiudicatario avrà l'obbligo di recepire e applicare gli aggiornamenti dei riferimenti normativi rilevanti ai fini della presente fornitura per tutta la durata contrattuale.

#### 4.14 Integrazioni previste

La Soluzione dovrà integrarsi con i Sistemi Informativi già operativi nella Regione Sardegna. Poiché i sistemi oggetto del presente Capitolato dovranno interoperare con i sistemi esistenti, il Fornitore dovrà descrivere puntualmente nell'Offerta Tecnica le modalità di integrazione previste.

Le attività relative alle integrazioni con i sistemi attualmente in uso lato Soluzione sono da intendersi incluse nella base d'asta.

Sarà compito dell'OE aggiudicatario collaborare con i vendor esterni per definire le modalità tecniche di integrazione e i relativi cronoprogrammi da includere nella progettazione esecutiva.

A titolo esemplificativo e non esaustivo si elencano le possibili integrazioni suddivise per contesto aziendale, regionale e nazionale. Si precisa, inoltre, che quanto dettagliato, potrebbe subire variazioni a seguito di eventuali attività evolutive o di aggiornamento/sostituzione del sistema applicativo.

Sistema	Contesto (Regionale/Nazionale)
Anagrafe SISAR HR	Regionale

## 5. CARATTERISTICHE DEI SERVIZI IN FORNITURA

I servizi offerti dovranno essere finalizzati al raggiungimento degli obiettivi di progetto e risultare complementari, sufficienti e funzionali alla completa messa in esercizio dei sistemi, componenti e moduli software inclusi nella fornitura.

I servizi richiesti sono:

- Manutenzione Evolutiva di Applicazioni Esistenti (MEV);
- Manutenzione Adeguativa e Migliorativa (MAD);
- Manutenzione Correttiva SW “pregresso e non in garanzia” (MAC);
- Help Desk ed assistenza di I° e II° livello e sistema di tracking;
- Formazione;
- Attività iniziale per il dispiegamento della soluzione.

Gli eventuali servizi di integrazione necessari al raggiungimento degli obiettivi di progetto si intendono interamente a carico dell'aggiudicatario.

### 5.1 Servizio di Manutenzione Evolutiva di Applicazioni Esistenti (MEV)

Il servizio di manutenzione evolutiva del software comprende gli interventi volti ad arricchire le applicazioni esistenti e/o fornite con nuove funzionalità, nonché quelli finalizzati a modificare o integrare le funzionalità già disponibili.

Rientrano in questo servizio tutti i progetti di reingegnerizzazione parziale di applicazioni esistenti e/o fornite, specificatamente richiesti dalla Amministrazione e per questa specificatamente sviluppati, che pur modificando l'architettura applicativa, la gestione dei dati e il modello di interazione con l'utente/sistemi esterni non realizzano una applicazione completamente differente da quella di partenza.

Sono compresi anche gli adeguamenti dovuti a modifiche normative o organizzative che richiedano variazioni della logica applicativa e comportino un impatto sulle funzionalità disponibili agli utenti superiore a 8 ore/uomo.

I servizi MEV forniti ai fini di:

- migliorare e/o integrare le funzionalità del software tramite rilascio sistematico di ogni nuova versione commerciale del medesimo prodotto offerto (major/minor release);
- risolvere e correggere errori software, siano essi di minore o maggiore criticità, inclusi i rilasci di patch e soluzioni operati come azione correttiva di sicurezza;
- adeguare il software a norme e leggi nazionali e/o internazionali applicabili.

I servizi MEV specificatamente finalizzati ad azioni correttive di sicurezza devono essere tempestivamente forniti per tutto il periodo di vita del prodotto senza alcun onere a carico della Amministrazione.

Deve essere incluso nell'offerta un numero minimo annuo di almeno 20 giornate/uomo di MEV gratuite; costituirà elemento premiante la proposta di un numero di giornate superiore incluse nell'offerta.

## **5.2 Servizio di Manutenzione Adeguativa e Migliorativa (MAD)**

Il servizio comprende l'attività volta ad assicurare la costante aderenza delle procedure e dei programmi all'evoluzione dell'ambiente tecnologico del sistema informativo. Comprende tutti gli interventi sul software che non rientrano nella correttiva e nella evolutiva, conseguenti a cambiamento dei requisiti (organizzativi, normativi, d'ambiente, di prodotto-tecnologia-ambienti-piattaforma) che non richiedano una variazione dei requisiti funzionali.

A partire dalle attività di presa in carico del parco applicativo il fornitore deve predisporre il Piano di Adeguamento che evidenzia l'analisi dei rischi correlata alla inadeguata qualità intrinseca del software, all'evoluzione delle piattaforme tecnologiche e dei prodotti, all'utilizzo delle applicazioni ed al livello di raggiungimento dei limiti di fruizione ottimale.

## **5.3 Servizio di Manutenzione Correttiva SW “pregresso e non in garanzia” (MAC)**

Il servizio viene attivato da una segnalazione di malfunzionamento da parte dell'Amministrazione, che deve contenere tipicamente le informazioni necessarie alla riproduzione del malfunzionamento, i danni causati alle basi dati nonché la categoria del malfunzionamento.

Ogni segnalazione di malfunzionamento costituisce richiesta di intervento di Manutenzione Correttiva attraverso il processo di gestione delle segnalazioni ed il relativo sistema di front-end verso gli utenti adottato dall'Amministrazione (Call Center, Service Desk, Help Desk).

## **5.4 Help Desk ed assistenza di I° e II° livello e sistema di tracking**

Tale assistenza sarà erogata mediante un servizio di supporto telefonico e un help desk online, al quale dovranno essere dedicate risorse professionali adeguatamente qualificate. Per questo servizio potrà essere richiesta la messa a disposizione di un sistema di ticketing.

I contenuti del servizio in oggetto possono essere così riassunti:

- Assistenza telefonica e help desk online per la diagnosi ed il superamento di eventuali difetti o malfunzionamenti riscontrati nell'utilizzo standard del software applicativo;

- Assistenza nel caso di gravi anomalie o malfunzionamenti del sistema che, pur non derivanti da errori del software, possano compromettere la continuità del servizio;
- Consulenza organizzativa per un utilizzo ottimale del sistema;
- Controlli sulla corretta parametrizzazione del sistema.

Il sistema, inoltre, deve prevedere una modalità di gestione delle segnalazioni/richieste di assistenza che assicuri la tracciabilità dei ticket ricevuti. Nello specifico, dovrà avere le seguenti caratteristiche:

- Sistema di tracciatura delle chiamate con evidenza di tutti i passaggi con accesso riservato al RUP/DEC, finalizzato ad agevolare il controllo tecnico contabile ed avere contezza di eventuali “reclami” dell’utenza;
- Modalità di contabilizzazione dei tempi di intervento;
- Accesso globale al database in termini di consultazione al fine di analizzare problemi e soluzioni ricorrenti da parte dei RUP/DEC, prevedendo anche report specifici finalizzati ad individuare i percorsi di miglioramento, sia in termini di sviluppo che di formazione;
- Il sistema di registrazione dei ticket deve consentire di poter riaprire, anche parzialmente, assegnando una percentuale di risoluzione, un ticket considerato precedentemente come chiuso e quindi cumulare i tempi di risoluzione, eventualmente abbattuti per la percentuale residua.

Il servizio dovrà essere disponibile dalle ore 8.:00 alle ore 18:00, dal lunedì al venerdì, con esclusione dei giorni festivi infrasettimanali, e dovrà garantire tempi di risposta inferiori a 24 ore.

## **5.5 Formazione**

Sono richieste specifiche sessioni formative per complessive 10 ore, nonché attività di assistenza all’avvio, riguardanti l’utilizzo del back office e dell’APP da parte degli utenti amministratori. La formazione deve includere:

- piano di formazione per gli amministratori di sistema;
- calendarizzazione delle sessioni di formazione.

Inoltre:

- tutta la documentazione fornita a supporto del funzionamento e dell’utilizzo della piattaforma applicativa rivolta agli utenti (ad esempio: manuali utente, materiali didattici per la formazione e materiali informativi) dovrà essere redatta in lingua italiana, salvo diversa autorizzazione dell’Amministrazione;
- dovrà essere predisposto e mantenuto aggiornato, con le evoluzioni e le correzioni apportate al software in corso d’opera, il manuale operativo, sia in formato PDF sia in

versione fruibile online, comprensivo della sequenza delle attività e delle relative istruzioni operative.

## 5.6 Attività iniziale per il dispiegamento della soluzione

Nell'ambito del servizio di supporto per il dispiegamento della soluzione, rientra il supporto nella messa in esercizio delle applicazioni fornite e presa in carico delle stesse.

Deve inoltre essere prevista una pianificazione dettagliata di tutte le attività di avvio del sistema.

## 6. GESTIONE DELLA PRIVACY E DELLA SICUREZZA DELLE INFORMAZIONI

Il trattamento dei dati personali derivante dalla prestazione dei servizi di cui al presente affidamento dovrà svolgersi nel rispetto della normativa vigente in materia di protezione dei dati personali (di seguito, complessivamente, "Normativa Privacy").

Inoltre, il fornitore dovrà essere in possesso della certificazione di sicurezza ISO/IEC 27001 o di certificazione equivalente.

A titolo meramente esemplificativo, si richiamano:

- Norme fondamentali comunitarie e nazionali in materia di data protection:
  - Regolamento UE 2016/679, recante «Regolamento Europeo in materia di protezione dei dati personali»;
  - o Decreto Legislativo n. 196/2003, recante il «Codice in materia di Protezione dei dati personali», come novellato dal D.Lgs. 101/2018;
- Provvedimenti e prassi Ue in materia di data protection (a titolo esemplificativo):
  - «Guidelines 9/2022 on personal data breach notification under GDPR» dell'European Data Protection Board;
  - «Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement» dell'European Data Protection Board;
  - «Guidelines 01/2022 on data subject rights - Right of access», adottate dall'European Data Protection Board il 18 gennaio 2022;
  - «Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali», adottate dall'European Data Protection Board il 14 dicembre 2021;
  - Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni «relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale»;
  - Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, recante «Una strategia europea per i dati» (COM/2020/66/final del 19 febbraio 2020);
  - Raccomandazione della Commissione Europea dell'8 aprile 2020, recante «on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data»;

- «Linee Guida 4/2019 in materia di Protezione dei dati fin dalla progettazione e per impostazione predefinita» adottate dall'European Data Protection Board il 20 ottobre 2020;
- «Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19», adottate dall'European Data Protection Board il 21 aprile 2020;
- «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679», adottate dal WP29 il 4 aprile 2017 e modificate il 4 ottobre 2017;
- «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679», adottate dal WP29 il 28 novembre 2017 e modificate il 10 aprile 2018;
- «Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679», adottate dal WP29 il 3 ottobre 2017 e modificate il 6 febbraio 2018;
- Provvedimenti e prassi nazionali in materia di data protection (a titolo esemplificativo):
  - Provvedimento del 30 luglio 2019, adottato dall'Autorità Garante per la protezione dei dati personali, sulla notifica delle violazioni dei dati personali (data breach);
  - Provvedimento del 7 marzo 2019, adottato dall'Autorità Garante per il trattamento dei dati personali, recante «Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019»;
  - Provvedimento n. 146 del 5 giugno 2019, adottato dall'Autorità Garante per il trattamento dei dati personali, recante le «prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101»;
  - Provvedimento dell'11 ottobre 2018, adottato dall'Autorità Garante per il trattamento dei dati personali, recante «Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679»;
  - Provvedimento del 29 aprile 2021, adottato dall'Autorità Garante per il trattamento dei dati personali, recante il «Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico»;
  - Provvedimento n. 393 del 2 luglio 2015, adottato dall'Autorità Garante per il trattamento dei dati personali, recante «Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche»;
  - Provvedimento del 27 novembre 2008, adottato dall'Autorità Garante per il trattamento dei dati personali, recante prescrizioni «ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema»;



- Fonti regolatorie in materia di digitalizzazione (a titolo esemplificativo):
  - Decreto Legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»;
  - «Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022», approvato con D.P.C.M. 17 luglio 2020;
  - «Piano Nazionale di Ripresa e Resilienza», approvato con Decisione di esecuzione del Consiglio dell'Unione europea del 13 luglio 2021;
  - Determinazione AgID n. 628/2021 del 15 dicembre 2021, recante «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»;
  - Circolare AgID 18 aprile 2017, n. 2/2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni»;
  - Legge 9 gennaio 2004, n. 4, recante «Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici»;
  - Circolare del 9 aprile 2018, n. 2, adottata dall'Agenzia per l'Italia Digitale, e avente ad oggetto «Criteri per la qualificazione dei Cloud Service Provider per la PA»;
  - Circolare AgID del 1° ottobre 2018, n. 3, avente ad oggetto «Responsabile per la transizione digitale - art. 17 decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale"»;
  - «Linee guida AgID sull'accessibilità degli strumenti informatici», adottate il 23 luglio 2020;
  - «Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici», adottate a settembre 2020 e modificate a maggio 2021;
  - Determinazione AgID n. 455/2021 del 25 giugno 2021, recante «Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici».

Si precisa che il Fornitore, nel corso dell'intera durata del Contratto Esecutivo, dovrà garantire pieno rispetto anche delle norme, dei provvedimenti e delle prassi in materia di data protection che dovessero intervenire nel tempo.

Fermo quanto sopra, nei sottoparagrafi successivi si descriveranno alcuni degli obblighi generali (connessi alla Normativa Privacy) e specifici (individuati sulla base delle peculiarità degli appalti oggetto di affidamento con la presente procedura) che il Fornitore dovrà rispettare ai fini della protezione dei dati personali.

Tutto quanto definito e richiesto dal presente Capitolato Tecnico dovrà essere garantito dal Fornitore e dai suoi eventuali subappaltatori/subcontraenti.

## 6.1 Obblighi generali del Fornitore in materia di protezione dei dati personali

Il Fornitore verrà nominato responsabile del trattamento dei dati personali (di seguito, anche solo «Responsabile») dal titolare del trattamento (di seguito, anche «Titolare»), e dovrà, pertanto, operare in conformità alle prescrizioni di cui all'art. 28 del GDPR, alle previsioni afferenti alla data protection che saranno contenute nel Contratto Esecutivo e alle istruzioni che saranno impartite dal Titolare medesimo nel corso dell'esecuzione dell'appalto.

In ragione di quanto sopra e a titolo esemplificativo, il Fornitore dovrà:

- sul piano organizzativo, strutturare e mettere in atto un'organizzazione specifica per la protezione dei dati personali attraverso la definizione di un modello privacy, con individuazione di ruoli, funzioni e responsabilità, procedendo alla predisposizione delle necessarie policy e al conferimento delle nomine.
  - In tal senso, procederà ad individuare: (i) i soggetti “delegati” e i soggetti “autorizzati al trattamento”, ai sensi dell'art. 2-quaterdecies del Codice Privacy; (ii) gli “Amministratori di sistema” per le attività legate al presente appalto (v. Provvedimento del 27 novembre 2008);
  - Il Fornitore avrà facoltà di avvalersi di sub-fornitori nelle modalità previste dall'art. 28 Reg. UE 2016/679 e dal Contratto Esecutivo;
- sul piano delle misure di sicurezza: il Fornitore dovrà adottare un approccio basato sul principio di Privacy by Design e by Default di cui agli artt. 25 e 32 del GDPR e alle «Guidelines 4/2019 on Article 25 Data Protection by Design and by Default», adottate dall'European Data Protection Board (EDPB) il 20 ottobre 2020. Di conseguenza, il Fornitore dovrà:
  - da un lato, predisporre fin dalla progettazione misure tecniche e organizzative adeguate (data protection by design), volte (i) ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e (ii) ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del GDPR e a tutelare i diritti e le libertà fondamentali degli interessati;
  - dall'altro, dare effettiva attuazione alle suddette misure nell'ambito del trattamento, affinché siano trattati, per impostazione predefinita, solo i dati personali necessari alla specifica finalità perseguita (data protection by default);
  - In tal senso, il Fornitore, nel valutare l'adeguato livello di sicurezza, dovrà tenere conto dei rischi presentati dal trattamento, in particolare di quelli che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

In caso di violazione dei dati personali, nel rispetto del GDPR e del Contratto Esecutivo, il Fornitore dovrà:

- darne comunicazione al Titolare, immediatamente e, in ogni caso, non oltre le 24 ore, da quando il Fornitore medesimo, o un suo Sub-Responsabile, ha avuto conoscenza della violazione o ha avuto elementi per sospettare che sia avvenuta una violazione;
- collaborare con il Titolare, anche al fine di consentire il completamento del processo di notifica all'Autorità Garante, nelle (i) attività di indagine, al fine rilevare tutte le

evidenze necessarie a valutare le cause, la natura e gli effetti della violazione dei dati personali, nonché (ii) nell'adozione delle azioni necessarie a mitigare qualsivoglia danno o conseguenza lesiva per i diritti e delle libertà degli Interessati e (iii) nella predisposizione e implementazione, previa approvazione del Titolare, di un piano di misure per la riduzione tempestiva delle probabilità che una violazione dei dati personali simile a quella occorsa possa ripetersi in futuro.

## 6.2 Previsioni specifiche in materia di protezione dei dati personali

A specificazione e in aggiunta rispetto agli obblighi generali di cui al paragrafo precedente, il Fornitore dovrà:

- (a) garantire il pieno coordinamento con gli altri soggetti coinvolti nel trattamento dei dati personali – quali, ad esempio, Regione, Ministero della Salute, Aziende Sanitarie, Operatori e Strutture sanitarie, la Società Polo Strategico Nazionale S.p.A. – proponendo misure tecnico-giuridiche finalizzate alla integrazione e alla sinergia con gli stessi (ad es., procedure, protocolli operativi).

Tali strumenti dovranno assicurare la conformità dei trattamenti alla Normativa Privacy nel corso dell'intero ciclo di vita dei dati personali ed efficaci policy in materia di privacy, ad esempio con riferimento alla gestione degli eventi di *data breach*, in modo da consentire al Titolare di porre in essere le attività previste dalla Normativa Privacy medesima;

- (b) garantire il rispetto della *data protection* nell'ambito dell'intero ciclo di vita dei dati personali, anche mediante misure tecnico-organizzative differenziate a seconda del soggetto di volta in volta coinvolto (ad es., *team* operativo e dipendenti del Fornitore, dipendenti di Ares Sardegna, ecc.).

A tal fine, il Fornitore dovrà tra l'altro garantire adeguata formazione nei confronti di ciascuna tipologia di soggetti coinvolti nei processi di digitalizzazione e predisporre apposite linee guide, manuali, moduli, flussi relativi ai processi e al ciclo di vita del dato;

- (c) individuare una figura che ricopra il ruolo di Privacy & Security Manager, che gestirà nel corso dell'esecuzione contrattuale tutte le tematiche di Sicurezza e di Privacy afferenti alla commessa e che costituirà il referente unico per l'Azienda in merito alle suddette materie, coordinandosi con il DPO dell'Azienda medesima e del Fornitore;
- (d) effettuare, in fase di avvio delle attività progettuali, un'analisi dei rischi privacy (sulla base del principio di *privacy by design*), al fine di segnalare al Titolare rischi verso l'Azienda, verso gli utenti e verso ulteriori soggetti terzi connessi al trattamento e di individuare misure tecniche ed organizzative da adottare, anche ai fini di una effettiva tutela dei diritti e delle libertà delle persone fisiche. Le metodologie di analisi del rischio dovranno essere preventivamente condivise con l'Azienda;
- (e) garantire il rispetto della normativa in materia di digitalizzazione (ad es., CAD e Linee

Guida AgID), quali, ad esempio, le «*Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici*» di settembre 2020/maggio 2021; la Determinazione AgID n. 628/2021 del 15 dicembre 2021 in materia di «*Cloud della PA*» e il Provvedimento del Garante n. 393 del 2 luglio 2015, in materia di «*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche*»;

- (f) supportare sul piano tecnico il Titolare nelle interlocuzioni con l'Autorità garante per la protezione dei dati personali (i.e., tematiche di data protection), l'Agenzia per l'Italia Digitale (i.e., tematiche di digitalizzazione), il Ministero della Salute (i.e., tematiche di governance sanitaria), l'Agenzia per la Cybersicurezza Nazionale (i.e., tematiche di sicurezza dei dati), la Società Polo Strategico Nazionale S.p.A. e ogni altra Autorità coinvolta nell'ambito dell'attuazione dell'appalto in questione;
- (g) adottare misure per l'acquisizione e la conservazione dei consensi (ove necessari in ragione degli specifici trattamenti, alla luce dei «*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*» resi dal Garante in data 7 marzo 2019) nel rispetto del GDPR (i.e., art. 7) e delle prassi UE e nazionali;
- (h) garantire che i dati personali siano trattati esclusivamente su infrastrutture localizzate all'interno dell'Unione europea, salvo documentate e motivate ragioni di natura normativa o tecnica, che dovranno essere preventivamente approvate dal Titolare e fermo, in ogni caso, il rispetto degli artt. 45 e ss. del GDPR;
- (i) garantire sistemi di autenticazione per il riconoscimento dei soggetti che utilizzano gli applicativi, con profili per gestire livelli differenziati di accesso alle informazioni e la tracciabilità delle attività e delle modifiche tramite produzione di log specifici;
- (j) garantire il rispetto del principio di minimizzazione del trattamento dei dati personali, ai sensi del combinato disposto di cui agli artt. 5 e 6 del GDPR, rispondente alla necessità che i dati personali vengano raccolti per finalità determinate, esplicite e lecite nei limiti di quanto necessario per il raggiungimento dello scopo per i quali sono stati raccolti.

Con riferimento alla presa in carico e messa in esercizio delle architetture e infrastrutture (*hardware* e *software*), finalizzata alla gestione tecnica di rilascio in termini di nuove applicazioni nonché di modifiche delle applicazioni già in esercizio, l'operatore economico dovrà inoltre adottare misure specifiche volte a garantire la conformità alla normativa in materia di data protection, quali:

- a) svolgimento di analisi dei rischi privacy necessarie ad individuare misure specifiche che possano ridurre i rischi connessi al trattamento dei dati personali, secondo metodologie preventivamente condivise con l'Azienda. Tali analisi dovranno essere espletate in fase di progettazione, in fase di consegna di ciascun singolo modulo/parte consegnata, in fase di consegna finale del prodotto e in ogni altro momento indicato dall'Azienda nel corso dello svolgimento del contratto;
- b) progettazione, definizione e sviluppo degli applicativi con modalità coerenti rispetto alle risultanze delle analisi di cui al punto precedente e alle conseguenti indicazioni

dell'Azienda;

- c) svolgimento *ex ante* di tutte le analisi tecnico-funzionali volte a consentire al titolare di elaborare valutazioni d'impatto sulla protezione dei dati personali (o «**DPIA**») conformemente all'articolo 35 del Regolamento (UE) n. 2016/679 e alle migliori prassi UE e nazionali;
- d) progettazione e adozione di misure idonee ad assicurare la conformità del software alla disciplina in materia di data protection, garantendo *inter alia*: (i) la sicurezza dei dati e la riservatezza delle informazioni (i.e., mediante misure di continuità operativa e disaster recovery, conservazione dei dati, tracciabilità degli eventi relativi alla sicurezza, crittografia, pseudonimizzazione e di anonimizzazione in linea con le best practices di settore o con i codici di condotta approvati dall'Autorità Garante); (ii) la "qualità ed esattezza del dato" (ossia la completezza, accuratezza, tempestività, coerenza, univocità, integrità, conformità dello stesso); (iii) la definizione di una durata predefinita della conservazione dei dati e modalità di cancellazione selettiva al termine del trattamento;
- e) adozione di misure necessarie a garantire la certificabilità secondo le migliori metodologie internazionali;
- f) monitorare costantemente i flussi relativi ai processi e al ciclo di vita dei dati, segnalando immediatamente con appositi alert qualsiasi anomalia effettiva o potenziale e prevedendo misure di prevenzione rispetto ad eventi dannosi (i.e., data leak e data loss);
- g) In ogni caso, nel corso dell'esecuzione del Servizio, il Titolare avrà facoltà di effettuare attività di verifica e controllo (o «**audit**»), previo preavviso e anche presso i locali del Fornitore, sulla corretta esecuzione, da parte del Fornitore ed eventualmente dei sub-fornitori, delle prestazioni inerenti al trattamento dei dati personali.

## 7. TEMPI E DELIVERABLES

Si richiede all'offerente di elaborare una proposta di cronoprogramma progettuale ottimizzato, dall'avvio dei lavori sino alla messa in produzione e a regime di tutti i sistemi offerti. Tale proposta dovrà:

- tassativamente rispettare il termine temporale ultimo di progetto;
- contemplare, quantunque riarrangiate, tutte le fasi di seguito descritte rispettando le percentuali di progressione (SAL%) per le relative scadenze.

Sono altresì possibili approcci di tipo iterativo-incrementale con l'aggiunta di servizi/funzioni aggiuntive.

Eventuali proposte migliorative sui tempi di messa in produzione/regime e su eventuali diversi e motivati approcci di dispiegamento saranno considerate come elemento premiante della proposta progettuale.

Ulteriori deliverables di progetto potranno essere concordati tra ARES ed il Fornitore nel corso del contratto.

Il Fornitore dovrà redigere un Piano di lavoro generale che rappresenti l'insieme dei servizi richiesti.

Inoltre, il Fornitore dovrà trasmettere il Piano della Qualità specifico, entro 10 giorni lavorativi dalla stipula del contratto esecutivo.

Fase	Timing	Attività	Deliverables
	(mesi dal T0)		
T0	0	Avvio lavori	Verbale di avvio lavori
1	1	<p>Assessment dei sistemi informativi coinvolti e definizione delle specifiche di integrazione. Tale attività, che dovrà essere svolta in stretta collaborazione e condivisione con i referenti di ARES e concludersi con un Documento di Assessment che riporti:</p> <ul style="list-style-type: none"> <li>- mappatura ed analisi dei processi che interessano l'introduzione della soluzione, con il coinvolgimento di tutti gli stakeholder nei relativi ambiti di competenza;</li> <li>- mappa delle integrazioni necessarie e relative specifiche;</li> <li>- mappa dei dati da importare (acquisizione e/o migrazione degli archivi storici pregressi);</li> <li>- descrizione della modalità di introduzione dei moduli funzionali della soluzione oggetto del presente capitolato.</li> </ul> <p>Formalizzazione di un Piano Esecutivo di Progetto (da concertare con le Direzioni di ARES) che contempli il cronoprogramma degli interventi, gli attori, milestones e target, il piano di subentro e presa in carico (Entry Strategy), le modalità di gestione delle fasi transitorie sia dal punto di vista tecnico che dei processi e dei servizi sanitari, l'organizzazione per il governo ed il coordinamento dell'intero progetto ed i relativi strumenti di monitoraggio.</p>	<ul style="list-style-type: none"> <li>-Documento di assessment</li> <li>-Piano Esecutivo di Progetto</li> </ul>

2	3	Configurazione iniziale dell'ambiente per eseguire i test di collaudo inclusivo delle integrazioni necessarie. Redazione del Piano di Collaudo dell'ambiente di test. Collaudo dell'ambiente di test.	-Piano di Collaudo -Report di Collaudo
3	4	Dispiegamento della soluzione in ambiente di produzione. Dovranno essere: - realizzato il porting e la relativa validazione di dati (dati storici) necessari all'avvio dei sistemi; - realizzate le configurazioni iniziali e delle integrazioni necessarie; - redatto il piano di Collaudo; - conclusi i test ed i collaudi con esito positivo; - redatto il piano di Formazione per gli utenti amministratori di sistema; - completata la formazione per gli utenti amministratori di sistema; - avvio dei servizi (avvio del periodo di garanzia)	-Piani di Collaudo -Report di Collaudo -Piani di Formazione -Registrazioni della avvenuta formazione degli utenti
4	5	Accettazione definitiva della soluzione	SAL periodici

## 8. GESTIONE DELLA FORNITURA

L'impianto contrattuale con il Fornitore prevederà un contratto esecutivo stipulato tra ARES e il Fornitore aggiudicatario. ARES eserciterà funzioni di monitoraggio-dell'esecuzione del servizio al fine di garantirne il corretto andamento.

### 8.1 Governo della Fornitura

Fatte salve le specifiche e le caratteristiche di cui al presente CTP ed a quelle offerte, nonché per ciò che concerne Competenze/Ruoli chiave, non verranno imposti vincoli sull'organizzazione che il Fornitore vorrà dare alle proprie risorse.

A questo proposito, sarà onere del Proponente fornire evidenza della qualità dell'organizzazione e delle figure proposte.

ARES si riserva di valutare e segnalare eventuali incompatibilità del personale messo a disposizione dal Fornitore per l'erogazione della fornitura e di richiederne la sostituzione con motivata istanza.

In caso di variazione al gruppo di lavoro, il Fornitore dovrà assicurare alle nuove risorse un periodo di affiancamento come da Livelli di servizio, senza ulteriori oneri.

Al fine di esercitare il controllo sull'attuazione generale del Servizio, ARES avrà facoltà di definire all'occorrenza un Comitato di Direzione.

Il Comitato di Direzione eserciterà il controllo strategico sul Servizio e sarà incaricato della valutazione dello stato di avanzamento complessivo.

### 8.2 Gestione del contratto con il Fornitore e relative tempistiche

I momenti di controllo e verifica dell'andamento della fornitura dovranno essere costanti per tutta la durata del contratto esecutivo e garantire una visibilità completa e dettagliata dell'avanzamento delle attività. In particolare, dovranno riguardare:

- monitoraggio attività operative;
- controllo costi e attestazione di consegna dei rilasci;
- controllo della qualità della fornitura e del rispetto degli SLA definiti;
- verifica costi, consumi e andamento generale del contratto.

Il Fornitore dovrà mantenere aggiornata la sezione relativa allo stato di avanzamento dei lavori contenuta nel Piano Esecutivo di Progetto e nel Piano Esecutivo Aziendale approvati, fornendo sulla base della tempistica di aggiornamenti definita nel Piano di Qualità e dalle necessità del singolo intervento o ciclo di vita, o su richiesta dell'Amministrazione, indicazioni sulle attività concluse ed in corso, esplicitando la percentuale di avanzamento, su eventuali rischi/criticità/ritardi, su eventuali impatti dei rischi/criticità, su azioni di recupero e razionali dello scostamento, sulle attività in servizio esteso ed in reperibilità.



Il Fornitore dovrà individuare un proprio Responsabile del Contratto che costituirà il suo punto di riferimento nei confronti di ARES per tutte le necessità di governo del contratto.

Il Fornitore dovrà indicare la figura del Project Manager di cantiere quale referente operativo per la realizzazione di quanto previsto contrattualmente.

### 8.3 Entry Strategy, Exit Strategy

Al fine di garantire la corretta pianificazione di questa fase, dovrà essere redatto dal Fornitore ed approvato da ARES il Piano di trasferimento (PTF).

Al fine di garantire la corretta pianificazione di tali fasi, dovranno essere redatti dal Fornitore e approvati da ARES il Piano di Presa in Carico e subentro (PPC) e il Piano di Trasferimento (PTF).

Con riferimento alla Entry Strategy, gli operatori offerenti, in considerazione del contesto operativo, infrastrutturale, applicativo e sistemistico in cui si opera e delle scelte progettuali proposte, dovranno descrivere le modalità di presa in carico del servizio.

Detto documento dovrà:

- proporre il dettaglio delle attività da espletare all'inizio del contratto, la relativa tempificazione, le stime di impegno, le risorse professionali coinvolte e il loro successivo impiego nei servizi, nonché le attività, i tempi e le responsabilità connesse al subentro;
- esplicitare metodi e soluzioni atti a minimizzare gli impatti sul SSR, con particolare riguardo alla continuità dei servizi e delle attività clinico-assistenziali.

Di seguito si riporta una traccia dei contenuti e delle caratteristiche qualificanti dell'attività di Exit, che dovranno essere progettate e gestite di concerto con il Committente:

- **Piano di Trasferimento:** Le attività di affiancamento e rilascio sono specificate e governate dal PTF, in cui saranno riportate tutte le attività previste in termini di tempi, risorse impiegate, punti di verifica e controllo dei risultati attesi, criteri di accettazione, i rischi, la cadenza degli incontri per la verifica dello stato di avanzamento delle attività;
- **Responsabilità:** durante il periodo di affiancamento e migrazione al termine del Contratto, la responsabilità del Servizio viene mantenuta dal Fornitore fino al termine previsto contrattualmente.
- **Governo del processo:** il Fornitore assicura tutte le attività finalizzate a coordinare e verificare la corretta ed efficace esecuzione delle attività di Affiancamento e Rilascio nel rispetto dei termini concordati nonché la coerenza con i requisiti, i vincoli ed i termini stabiliti nei documenti contrattuali; a tale scopo viene individuata una figura unica per il Fornitore (Project Manager) che coordinerà tutte le attività e che interfacerà il Committente ovvero l'eventuale Fornitore terzo subentrante;
- **Continuità dei servizi:** al fine di garantire al Committente il mantenimento dei livelli di servizio richiesti anche da parte del subentrante, nel Piano di Transizione dovranno essere previste specifiche fasi di verifica e validazione del trasferimento delle conoscenze e delle componenti operative;

- **Risorse professionali:** un gruppo di risorse del Fornitore appositamente designato affiancherà le risorse del Committente e/o del Fornitore subentrante per il trasferimento delle conoscenze sui servizi e sulle relative attività di gestione.
- **Procedure tecniche:** insieme delle procedure necessarie al trasferimento dei dati verso eventuali nuove tecnologie e/o diversi fornitori.

## 9. LIVELLI DI SERVIZIO

Il presente documento descrive il livello minimo di qualità atteso nell'erogazione dei servizi oggetto della fornitura.

Gli indicatori di qualità nell'ambito della presente iniziativa vengono descritti con il seguente dettaglio:

- la fase di riferimento: ovvero, in quale macro-attività di progetto ricade la rilevazione e l'attinenza dell'indicatore;
- l'ID indicatore: ovvero il codice identificativo dell'indicatore; il periodo di riferimento su cui calcolare l'indicatore;
- il titolo Indicatore;
- la descrizione Indicatore;
- i dati elementari o i sub-indicatori da rilevare per la misura;
- l'unità di misura;
- le formule di calcolo e gli arrotondamenti da adottare;
- gli obiettivi che l'indicatore deve soddisfare espressi tramite valori soglia;
- la penale correlata al non rispetto dell'obiettivo/valore soglia.

In fase di erogazione, il fornitore deve mantenere costantemente adeguato il livello di qualità, tenendo conto della disponibilità di nuove versioni di standard, best practice e linee guida applicabili.

### 9.1 IMP – Rispetto Impegni in Offerta Tecnica

<b>Fase di Riferimento</b>	Gestione Complessiva di Progetto
<b>ID Indicatore</b>	<b>IMP</b>
<b>Titolo Indicatore</b>	Rispetto Impegni in Offerta Tecnica
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare la coerenza tra quanto espresso in offerta tecnica, in termini di impegni, con il numero impegni non rispettati in fase esecutiva

<b>Dati da rilevare</b>	- requisiti funzionali/funzionalità previsti in offerta tecnica (RFot); - requisiti funzionali soddisfatti (RSot)
<b>Unità di misura</b>	Requisiti funzionali presenti in offerta tecnica
<b>Valore Soglia</b>	VS = 0
<b>Formula</b>	$VS = RFot - RSot$
<b>Penale</b>	0,05% del valore contrattualizzato per ogni impegno non rispettato

## 9.2 RSC – Rispetto Scadenza da Capitolato.

<b>Fase di Riferimento</b>	Gestione Complessiva di Progetto
<b>ID Indicatore</b>	<b>RSC</b>
<b>Titolo Indicatore</b>	Rispetto Scadenza da Capitolato
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare i giorni di ritardo rispetto ai target definiti all'Interno del Capitolato Tecnico (paragrafo "Tempi e deliverables")
<b>Dati da rilevare</b>	- data Prevista per il target (DPTt); - data Effettiva per il target (DETt).
<b>Unità di misura</b>	Giorno Solare
<b>Valore Soglia</b>	VS = 0
<b>Formula</b>	$VS = DETt - DPTt$
<b>Penale</b>	0,05% del valore contrattualizzato per ogni giorno oltre il VS

## 9.3 TIP – Tempestività nell’inserimento del personale

<b>Fase di Riferimento</b>	Gestione Complessiva di Progetto
----------------------------	----------------------------------

<b>ID Indicatore</b>	<b>TIP</b>
<b>Titolo Indicatore</b>	Tempestività nell’inserimento di personale
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare la tempestività nell’inserimento/sostituzione delle risorse impiegate nella fornitura, compresi i referenti.
<b>Dati da rilevare</b>	- data richiesta inserimento/sostituzione risorsa (DTIr); - data effettiva inserimento nuova risorsa (DTIe)
<b>Unità di misura</b>	Giorno Lavorativo
<b>Valore Soglia</b>	VS = 3
<b>Formula</b>	$VS = DTIe - DTIr$
<b>Penale</b>	0,05% del valore contrattualizzato per ogni tripla di giorni lavorativi oltre il valore soglia

#### 9.4 TINT – Tempo di esecuzione di interventi di manutenzione evolutiva

<b>Fase di Riferimento</b>	Fase di Realizzazione, parametrizzazione e configurazione
<b>ID Indicatore</b>	<b>TINT</b>
<b>Titolo Indicatore</b>	Tempo di esecuzione di interventi di manutenzione evolutiva
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare l'efficacia della pianificazione degli interventi e la loro conclusione entro i termini previsti dal Piano di dettaglio delle attività e dei task da produrre in fase esecutiva
<b>Dati da rilevare</b>	- giorni previsti da pianificazione (GP <sub>a</sub> ); - data inizio attività effettiva (DTI <sub>a</sub> ); - data fine attività effettiva (DTF <sub>a</sub> );
<b>Unità di misura</b>	Giorno Solare
<b>Valore Soglia</b>	VS = GP <sub>a</sub>
<b>Formula</b>	$VS \Rightarrow DTI_a - DTF_a$

<b>Penale</b>	0,08% del valore contrattualizzato per ogni giorno solare oltre il valore soglia
---------------	--

### 9.5 DIC – Numero difetti bloccanti in collaudo

<b>Fase di Riferimento</b>	Fase di Collaudo
<b>ID Indicatore</b>	<b>DIC</b>
<b>Titolo Indicatore</b>	Numero difetti bloccanti in collaudo
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare l'efficacia delle attività in fase di collaudo con l'individuazione delle non conformità bloccanti*
<b>Dati da rilevare</b>	numero totale non conformità bloccanti
<b>Unità di misura</b>	Rilievo sulla non conformità bloccanti
<b>Valore Soglia</b>	VS = 3
<b>Formula</b>	
<b>Penale</b>	0,03% del valore contrattualizzato per ogni non conformità bloccante oltre il valore soglia

### 9.6 GSC – Giorni di sospensione in collaudo

<b>Fase di Riferimento</b>	Fase di Collaudo
<b>ID Indicatore</b>	<b>GSC</b>
<b>Titolo Indicatore</b>	Giorni di sospensione in collaudo
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare l'efficienza nelle procedure di collaudo effettuate dal fornitore sulla piattaforma, definendo il numero di giorni di sospensione dell'attività di collaudo
<b>Dati da rilevare</b>	- Tempo previsto in giorni, per l'attività di collaudo così come da Piano Attività redatto dal fornitore e approvato dall'Amministrazione (GPc); - Numero giorni di sospensione del collaudo (GSc)
<b>Unità di misura</b>	Giorno Lavorativo
<b>Valore Soglia</b>	VS = 10%
<b>Formula</b>	$VS = (GSc/GPc) * 100$
<b>Penale</b>	0,003% del valore contrattualizzato per ogni punto percentuale oltre il valore soglia

### 9.7 TRAA – Tempo di risoluzione Anomalia in Avvio e post erogazione in garanzia

<b>Fase di Riferimento</b>	Fase di Avvio e Post-erogazione
<b>ID Indicatore</b>	<b>TRAA</b>
<b>Titolo Indicatore</b>	Tempo di risoluzione Anomalia in Avvio e post erogazione in garanzia

<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare il tempo di risoluzione di una anomalia in avvio secondo una categorizzazione delle anomalie in: - bloccanti; - non bloccanti
<b>Dati da rilevare</b>	- data e ora (hh:mm) della presa in carico dell'anomalia (DTPa); - data e ora (hh:mm) della risoluzione dell' anomalia (DTRa);
<b>Unità di misura</b>	Ora solare
<b>Valore Soglia</b>	Per le anomalie bloccanti: $VS < 2$ ore solari; Per le anomalie non bloccanti $VS < 8$ ore solari;
<b>Formula</b>	$VS = DTRa - DTPa$
<b>Penale</b>	- 0,002% del valore contrattualizzato per ogni ora oltre il valore soglia per le anomalie bloccanti; - un rilievo ogni 4 ore oltre il valore soglia, 0,01% del valore contrattualizzato oltre il terzo rilievo effettuato

### 9.8TPI – Tempestività di presa in carico anomalia in avvio e post erogazione in garanzia

<b>Fase di Riferimento</b>	Fase di Avvio e Post-erogazione
<b>ID Indicatore</b>	<b>TPI</b>
<b>Titolo Indicatore</b>	Tempestività di presa in carico anomalia in avvio e post erogazione in garanzia
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare i tempi di presa in carico delle richieste effettuate dagli utenti finali in merito a malfunzionamenti e anomalie
<b>Dati da rilevare</b>	- data e ora (hh:mm) della richiesta d'intervento (DTRi); - data e ora (hh:mm) di presa in carico della richiesta (DTPI)
<b>Unità di misura</b>	Minuti
<b>Valore Soglia</b>	$VS = 60$
<b>Formula</b>	$VS = DTPI - DTRi$
<b>Penale</b>	0,003% del valore complessivo contrattualizzato ogni 60 minuti successivi al valore soglia

### 9.9NAR – Numero anomalie recidivanti in avvio e post erogazione in garanzia

<b>Fase di Riferimento</b>	Fase di Avvio e Post-erogazione
<b>ID Indicatore</b>	<b>NAR</b>
<b>Titolo Indicatore</b>	Numero anomalie recidivanti in avvio e post erogazione in garanzia
<b>Descrizione Indicatore</b>	Tale indicatore mira a valutare l'efficacia degli interventi corretti su anomalie e malfunzionamenti recidivanti una stessa funzionalità o modulo di sistema

<b>Dati da rilevare</b>	-numero anomalie e malfunzionamenti recidivanti sulla stessa funzionalità/modulo;
<b>Unità di misura</b>	Anomalie verificate sulla stessa funzionalità o modulo di sistema
<b>Valore Soglia</b>	VS = 3
<b>Formula</b>	
<b>Penale</b>	0,05% del valore contrattualizzato per ogni anomalia recidiva sullo stesso modulo oltre il valore soglia

## 10. GARANZIA DEI SERVIZI/PRODOTTI FORNITI

I nuovi prodotti, sistemi e le nuove funzionalità dovranno essere coperti da garanzia post -collaudo per dodici mesi.

## 11. ELEMENTI DIMENSIONALI DI PROGETTO

Le informazioni di seguito riportate hanno lo scopo di fornire una descrizione di maggior dettaglio del contesto oggetto dell'intervento e di supportare gli operatori economici offerenti nella predisposizione della proposta.

Si precisa che tali informazioni sono da considerarsi non vincolanti per l'Amministrazione e potranno essere oggetto di aggiornamento in sede di avvio e durante l'esecuzione contrattuale.

### 11.1 Numero di utenti dipendenti per Azienda

Il numero complessivo dei dipendenti del SSR riportato nella tabella seguente rappresenta esclusivamente la platea potenziale del personale delle Aziende sanitarie. Il servizio oggetto della presente gara riguarda il personale effettivamente abilitato all'utilizzo della soluzione di timbratura elettronica tramite applicazione mobile, stimato in circa 15.000 utenti, con possibilità di estensione fino a 30.000 utenti, corrispondenti all'intera platea potenziale, senza modifiche architetturali.

ENTE SANITARIO	TOTALE per AS
ARES	680
ASL SASSARI	2.811
ASL GALLURA	1.691
ASL NUORO	2700
ASL OGLIASTRA	876
ASL ORISTANO	2169
ASL MEDIO CAMPIDANO	1193
ASL SULCIS	1.834
ASL CAGLIARI	4882
AOU CAGLIARI	1837
AOU SASSARI	3221
AREUS	557
ARNAS BROTZU	3360
<b>TOTALE</b>	<b>27811</b>

Numero di TRP attualmente in uso (e locazione)

Azienda	TRP Fisici	TRP Virtuali
ARES	2	3
ASL 31	54	21
ASL 32	25	13
ASL 33	51	29
ASL 34	16	7
ASL 35	33	44
ASL 36	18	12
ASL 37	32	12
ASL 38	99	46
ARNAS Brotzu	16	0
AOU Cagliari	10	0
AOU Sassari	15	0
AREUS	2	0



## 12. Parametri per la Valutazione del' Offerta

### 12.1.Criterio di ripartizione qualità/prezzo

L'Appalto verrà aggiudicato in base al criterio dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo, ai sensi dell'art. 108, commi 1 e 2, del Codice, secondo la ripartizione tra punteggio tecnico ed economico indicata di seguito.

La valutazione dell'offerta tecnica e dell'offerta economica sarà effettuata in base ai seguenti punteggi.

	PUNTEGGIO MASSIMO
Offerta tecnica	80
Offerta economica	20
<b>TOTALE</b>	<b>100</b>

### 12.2.Criteri di valutazione dell'offerta tecnica

La valutazione sarà effettuata sulla base dell'allegato al presente capitolato tecnico prestazionale denominato "Tabella Criteri di Valutazione" e meglio disciplinata all'interno del "CAPITOLATO D'ONERI".

P.I Nicolò Cadeddu

---

Dott. ssa Anna Girau

---

P.I. Andrea Orrù

---

P.I. Cristian Tuvoni

---

Dott.ssa Gigliola Zaniboni

---

Il Segretario Tiziana Usai

---