FORNITURA DI UNA PIATTAFORMA DI SORVEGLIANZA ATTIVA PER RIORIENTAMENTO DEL PROGETTO SISTEMA INFORMATIVO CURE PRIMARIE A SUPPORTO DELLA GESTIONE DELL'EMERGENZA SANITARIA COVID-19

ATS SARDEGNA

Data:	05-06-2020
Autore:	Piergiorgio Annicchiarico (ATS) Alessandro Pala (ATS) Daniela Mura (ATS)
Versione-Variante	001-C
Rivisto:	Piergiorgio Annicchiarico Alessandro Pala
Approvato:	Piergiorgio Annicchiarico Alessandro Pala
Distribuito:	Distribuzione esclusivamente interna

UNIONE EUROPEA
Fondo europeo di sviluppo regionale

REPUBBLICA ITALIANA

POR FESR SARDEGNA 2014-2020

ELEMENTI DI CONTROLLO DEL DOCUMENTO

Sintesi: Il presente documento descrive i requisiti per la fornitura di Servizi di tipo SaaS relativi ad una Piattaforma di Sorveglianza Attiva Pazienti COVID-19 sul Territorio della Regione Sardegna

Codice	SCSAN-COVID19-CT-001.C
Tipo	Capitolato Tecnico
Data	05-06-2020
Versione	001
Variante	C
Stato	FINALE
Pagine	37
Altri documenti correlati	• Legge Regionale 17 novembre 2014 n. 23 *Norme urgenti per la riforma del sistema sanitario regionale. Modifiche alle leggi regionali n. 23 del 2005, n. 10 del 2006 e n. 21 del 2012* • Delibera della Giunta Regionale n. 44/13 del 07.11.2014 • Delibera della Giunta Regionale n. 60/2 del 02.12.2015 *Sistema Regionale delle Cure Territoriali. Linee di indirizzo per la riqualificazione delle cure primarie* • Delibera della Giunta Regionale n. 17/14 del 04.04.2017 POR FESR 2014-2020 – Programmazione integrata interventi in ambito sanitario. • Delibera della Giunta Regionale n. 17/10 del 01.04.2020 – Emergenza Covid-19. Riorganizzazione delle attività assistenziali ospedaliere e territoriali.
Moduli	Non applicabile
Parole Chiave	▪ Piattaforma Sorveglianza Attiva COVID-19 ▪ Capitolato Tecnico
File Name	SICP_SORVEGLIANZA ATTIVA COVID-19_CT_v1C_rev05_06_2020.pdf

Evoluzione modifiche apportate:

Data	Versione/Variante	Descrizione
22-04-2020	A	Versione iniziale
07-05-2020 12-05-2020 14-05-2020	B	Revisione
15-05-2020 29-05-2020 05-06-2020	C	Versione finale

INDICE

1. INTRODUZIONE

1.1. SCOPO E ORGANIZZAZIONE DEL DOCUMENTO

Il presente documento costituisce il Capitolato Tecnico che descrive i requisiti per la **fornitura di una piattaforma applicativa di sorveglianza attiva** per i pazienti COVID-19 e altri pazienti ritenuti ad alto rischio (p.es. pazienti cronici con comorbilità e con problematiche respiratorie pre-esistenti, per BPCO, asma, etc.).

Nel contesto dell'emergenza sanitaria legata al diffondersi del virus COVID-19, **l'obiettivo della presente iniziativa è infatti quello di rendere disponibile**, attraverso l'attivazione dell'architettura applicativa richiesta, **una piattaforma che supporti le attività territoriali di sorveglianza attiva sui pazienti COVID-19**, o altre tipologie di pazienti individuate come a rischio, **attraverso appositi piani di monitoraggio e sorveglianza individuali.**

In coerenza con lo scopo del documento i contenuti esposti sono così organizzati:

- Il capitolo 2 fornisce una panoramica del contesto di riferimento e inquadra la fornitura oggetto del presente capitolato;
- Il capitolo 3 descrive l'oggetto della fornitura definendone: obbiettivi, orizzonte temporale, requisiti, servizi richiesti ed elementi economici;
- Il capitolo 4 espone le specifiche di gestione del progetto richieste;
- Il capitolo 5 riporta i livelli di servizio che verranno monitorati nel corso della fornitura;
- Il capitolo 6 riporta i requisiti ai quali il Fornitore deve attenersi e/o implementare allo scopo di preservare l'integrità, la disponibilità e la riservatezza delle informazioni nell'ambito dell'erogazione della presente fornitura.

Di seguito, nel paragrafo successivo, il glossario.

1.2. GLOSSARIO

ATS	Azienda per la Tutela della Salute della Sardegna
AFT	Aggregazioni Funzionali Territoriali
CA	Continuità Assistenziale
CCM	Cronich Care Model
CCP	Cartella Clinica delle Cure Primarie
CDI-COVID	Cure Domiciliari Integrate con specializzazione COVID-19
CDR	Clinical Document Repository
CdS	Case della Salute
COT	Centrale Operativa Territoriale
CCP	Cartella clinica delle Cure Primarie
ESB	Enterprise Service Bus
COVID-19	Malattia respiratoria acuta da SARS-CoV-2
PDTA	Percorso Diagnostico Terapeutico Assistenziale
FSE	Fascicolo Sanitario Elettronico
SISaR	Sistema Informativo Sanitario Regionale
IoT	Internet of Things
MCA	Medici di Continuità Assistenziale
MMG	Medici di Medicina Generale
PDTA	Percorso Diagnostico Terapeutico Assistenziale
PLS	Pediatri di Libera Scelta
SISP	Servizio di Igiene e Sanità Pubblica
SICP	Sistema Informativo delle Cure Primarie
UCCP	Unità Complessa di Cure Primarie
USCA	Unità Speciali di Continuità Assistenziale

2. CONTESTO DI RIFERIMENTO

L'Azienda per la Tutela della Salute della Sardegna (ATS) rappresenta uno dei principali soggetti erogatori dei servizi sanitari pubblici nel territorio regionale e costituisce un punto di riferimento privilegiato nell'ambito dell'attuale fase di organizzazione dell'assistenza sanitaria regionale.

La ATS Sardegna a seguito della L.R. n. 17 del 27 luglio 2016 è impegnata in un profondo processo di riorganizzazione, razionalizzazione e centralizzazione che tiene conto del profondo cambiamento in corso nel SSR; sono stati avviati dei percorsi di riorganizzazione complessiva della Sanità Regionale, dei Presidi Ospedalieri, dei processi di Presa in Carico dei Pazienti, di centralizzazione dei processi amministrativi, di acquisto e dei processi Clinico-Sanitari. L'obiettivo fondamentale che si intende raggiungere è quello di rimettere il Paziente al centro dei processi assistenziali, di cura e prevenzione, con la certezza della sostenibilità finanziaria del sistema.

In questo contesto l'innovazione digitale è una leva strategica per l'ATS Sardegna, che sta affrontando un cambiamento epocale e una profonda trasformazione dei processi di erogazione dei propri servizi sanitari.

Nel corso degli anni, l'informatizzazione della Sanità Regionale si è sviluppata nelle differenti ex-ASL regionali che attualmente sono divenute le ASSL (Area Socio Sanitaria Locale) della ATS Sardegna, in base alle priorità che all'epoca ciascuna singola azienda ASL aveva, allo scopo di dotarsi degli strumenti più idonei per l'espletamento di funzioni amministrative o altri specifici adempimenti.

Successivamente, il Dipartimento ICT, costituito con la Deliberazione del Direttore Generale N. 373 del 09/03/2018, si è impegnato nello sviluppo dei processi di informatizzazione dei servizi anche alla luce delle nuove esigenze riguardanti l'intera ATS Sardegna considerando anche la forte disomogeneità presente nell'ambito delle singole ASSL.

Nello specifico, la ATS Sardegna intende ottimizzare il complesso dei sistemi informativi sanitari regionali, tramite l'implementazione dei Servizi di Interoperabilità fra i Sistemi Informativi realizzati e in fase di realizzazione, consentendo la condivisione dei dati clinici dei pazienti e intervenendo sull'orchestrazione e sulla Cooperazione Applicativa nell'ambito delle Cure Primarie, ponendo le basi per il passaggio da un modello "ospedale-centrico", verso uno più territoriale.

La Scheda Progetto "Sistema Informativo per le Cure Primarie", allegata alla Convenzione sottoscritta tra ATS e Assessorato Sanità (Deliberazione del Direttore Generale n. 534 del 18/04/2018: "Recepimento del Finanziamento Regionale per la realizzazione del sistema informativo per le Cure Primarie della Sardegna e contestuale approvazione della relativa convenzione tra Regione Autonoma della

Sardegna - RAS e l'Azienda Tutela della Salute – ATS"), definisce l'oggetto di massima dell'intervento ed i principi strategici per la sua realizzazione operativa.

Nella strategia di attuazione l'intervento è strutturato in maniera articolata, configurandosi come un'aggregazione di più sotto-progetti che concorrono all'attuazione degli obiettivi generali:

1. **Attivazione sperimentale del Servizio 116117**: costituisce il sotto-progetto inerente al riordino della Medicina di Continuità Assistenziale con particolare riferimento all'attivazione del Servizio 116117, anche quale "step" intermedio verso il modello a regime delle Cure Primarie.
2. **CDR-XDS di Servizi Interoperabilità del SICP**: costituisce il sotto-progetto inerente alla costruzione del **sistema infrastrutturale di interoperabilità dei dati** e di **cooperazione applicativa** a supporto della implementazione del SICP.
3. **Realizzazione del Portale di Accesso alle Cure Primarie**: Realizzazione di soluzioni software di supporto alle Cure Primarie, PDTA e telemedicina. Prevede la realizzazione di un Portale delle Cure Primarie, quale portale di accesso e di gestione dei pazienti arruolati nei vari percorsi di diagnosi in un definito contesto organizzativo di sperimentazione (p.es. Case della Salute, PDTA Workflow).

In particolare, il sotto-progetto 3 è inerente al progressivo riordino delle attività assistenziali con particolare riferimento all'attivazione del Portale e dei servizi on line per le Unità Complesse di Cure Primarie (UCCP – Case della Salute) e per i Percorsi Diagnostici Terapeutici ed Assistenziali (PDTA), basato sui servizi di interoperabilità per i dati e la cooperazione applicativa.

Esso costituisce un importante step a supporto di una transizione graduale verso un modello a regime delle Cure Primarie, che concorre per la propria parte al raggiungimento degli obiettivi strategici nell'insieme dei sotto-progetti indicati.

In questo contesto, alla luce dell'emergenza sanitaria in corso legata al diffondersi del virus COVID-19 è stato definito uno scenario di riorientamento di alcune delle attività previste dal progetto "Sistema Informativo delle Cure Primarie", in piena compatibilità con i contenuti e gli obiettivi generali già stabiliti per gli interventi e fissati dal POR FESR 2014-2020 che finanzia il progetto.

In particolare, sono state definite approvate le attività necessarie al riorientamento dei servizi e sistemi relativi al sotto-progetto 1 (Attivazione del servizio sperimentale 116117), per l'attivazione di una Centrale Operativa Territoriale (COT) che abiliti servizi aggiuntivi di monitoraggio anche attraverso chiamate *outbound* (es. registro contatti, registro chiamate, rilevazione parametri sanitari) valorizzando i sistemi di gestione delle schede di contatto sviluppate e in corso di completamento da parte di Sardegna IT.

Inoltre, quale fase ulteriore dello sviluppo di servizi a supporto della sorveglianza attiva

dei pazienti, è stata definita una proposta di riorientamento dei servizi e sistemi del sotto-progetto 3 (Realizzazione del Portale di Accesso alle Cure Primarie) attraverso l'attivazione di una **piattaforma di sorveglianza attiva** che abiliti ad una gestione integrata, tramite la definizione e la verifica dell'attuazione di piani di monitoraggio e sorveglianza individuali, delle attività di monitoraggio tra gli attori coinvolti nel processo (es. operatori della COT, MMG, SISP, USCA, CDI-COVID, Unità Regionali di dimissione post-ospedaliera, Distretti sanitari).

Si specifica che, nelle attività di riorientamento del sotto-progetto 1, sono in valutazione le tempistiche necessarie all'attivazione di una seconda Centrale Operativa Territoriale a supporto della sorveglianza attiva dei pazienti COVID.

Il riorientamento dei servizi e sistemi del sotto-progetto 3 per servizi e sistemi a supporto dell'emergenza sanitaria, presentato in questo paragrafo, **è oggetto della presente fornitura**.

La presente fornitura è quindi limitata all'approvvigionamento delle componenti e dei servizi necessari a fornire un valido supporto nella sorveglianza dei pazienti COVID-19 nel contesto dell'emergenza sanitaria in atto.

Restano validi, anche alla luce dei riorientamenti in corso, gli obiettivi inizialmente previsti dal progetto "Sistema Informativo delle Cure Primarie" già stabiliti per gli interventi e fissati dal POR FESR 2014-2020.

3. CARATTERISTICHE DELLA FORNITURA

3.1. OGGETTO DELLA FORNITURA

L'iniziativa ha l'obiettivo di rendere disponibile ad ATS una piattaforma a supporto della sorveglianza attiva dei pazienti COVID-19 e altri pazienti ritenuti a rischio, come meglio specificato di seguito.

In coerenza con gli obiettivi generali è **oggetto della presente iniziativa la fornitura delle componenti e dei servizi necessari, nel contesto dell'attuale emergenza sanitaria, per implementare, diffondere e gestire una piattaforma di sorveglianza attiva per i pazienti COVID-19** e altri pazienti ritenuti ad alto rischio (p.es. pazienti cronici con comorbilità e co problematiche respiratorie pre-esistenti per BPCO, asma, etc.).

La piattaforma dovrà supportare un servizio di sorveglianza attiva che ha l'obiettivo di consentire il monitoraggio, sulla base di piani di sorveglianza e monitoraggio individuali, **dei pazienti al domicilio** e al contempo consentire agli operatori delle Centrali Operative Territoriali, ai MMG, alle USCA, al SISP e ad altri attori coinvolti di **ridurre il numero di contatti con i pazienti ad alto rischio**, riducendo allo stesso tempo la possibilità da parte dei pazienti di entrare in contatto, proprio presso le strutture di assistenza, con il virus e quindi con forme di contagio.

Il servizio in questa fase di emergenza sanitaria risponde alle **esigenze di sorveglianza attiva dei seguenti pazienti**:

- **Pazienti sospetti, probabili e confermati COVID-19** in isolamento domiciliare obbligatorio e fiduciario;
- **Pazienti COVID 19 dimessi** dalle strutture ospedaliere gestibili al domicilio;
- **Pazienti cronici e fragili** che potrebbero, in caso di contagio, vedere aggravarsi la propria condizione di salute (es. BPCO).

La fornitura **comprende l'erogazione dei servizi professionali** atti a supportare l'attivazione del servizio, nonché orientati alla efficace operatività della soluzione stessa e all'exit management a conclusione del contratto.

La Piattaforma dovrà essere messa a disposizione di ATS e degli altri attori coinvolti nella sorveglianza dei pazienti come MMG, SISP, USCA, operatori delle COT e pazienti.

La piattaforma dovrà essere **implementata sulle risorse infrastrutturali rese disponibili da ATS nel contesto dei servizi Cloud previsti dalla Gara SPC Cloud**

Lotto 1. Il Fornitore dovrà quindi garantire la compatibilità della propria soluzione ai requisiti definiti nel relativo Contratto Quadro.

L'implementazione della piattaforma sulle risorse infrastrutturali rese disponibili da ATS è quindi da considerarsi a carico del Fornitore che dovrà inoltre garantire la fornitura di tutte le necessarie licenze software relative ai sistemi operativi, ai database e alle componenti software necessarie all'esecuzione della piattaforma.

La fornitura si inserisce nel contesto del **riorientamento di alcune delle attività previste dal progetto "Sistema Informativo delle Cure Primarie" (SICP)** definito alla luce dell'emergenza sanitaria in corso legata al diffondersi del virus COVID-19, in **piena compatibilità con i contenuti e gli obiettivi generali già stabiliti per gli interventi e fissati dal POR FESR 2014-2020** che finanzia il progetto.

Per il raggiungimento degli obiettivi descritti **si ritiene fondamentale il coordinamento e l'integrazione con i servizi e sistemi che saranno messi a disposizione dal riorientamento del sotto-progetto 1 e con eventuali altri progetti già in essere** (es. Progetto COVID-19 – Sistema Gestione casi e contatti COVID-19- Sardegna IT); questo per evitare dinamiche contrastanti e gestire possibili interrelazioni reciproche.

3.2. ESTENSIONE COMPLESSIVA E ORIZZONTE TEMPORALE

La fornitura prevede **una durata del contratto di 6 (sei) mesi** dall'avvio delle attività.

Si consideri che tenuto conto della situazione emergenziale si potrà procedere alla consegna anticipata dei lavori prima della stipula del contratto.

In funzione dell'evoluzione epidemica e dello stato di emergenza, si prevede l'esercizio dell'opzione di **rinnovo della durata del contratto per ulteriori 6 mesi, alle medesime condizioni contrattuali**.

L'avvio dell'erogazione del servizio dovrà avvenire entro 10 (dieci) giorni solari dalla comunicazione formale di inizio attività da parte di ATS.

Seppur non soggetti a valutazione per quanto sopra stabilito, il Fornitore è comunque tenuto a presentare in sede di offerta, pena non validità della stessa:

- Un **piano operativo** descrittivo in modo dettagliato di tempi e modalità operative di attivazione ed erogazione del servizio per le componenti previste dal progetto;
- Il **modello organizzativo** comprensivo di **gruppi di lavoro e professionalità;**
- Una **descrizione esaustiva dell'architettura e la dotazione dell'infrastruttura fisica necessaria al funzionamento compiuto della propria soluzione**, indicando tutti i requisiti, i vincoli e le informazioni in termini di hardware e

software richieste per la fornitura di servizi cloud tramite la gara SPC Cloud Lotto 1.

La **strategia di realizzazione** prevede la selezione di un **Fornitore** a cui affidare l'erogazione del servizio nel suo complesso che possa dimostrare di possedere i requisiti tecnici e di esperienza specifica maturata e di essere in grado di attivare immediatamente il servizio.

Il Fornitore dovrà garantire la capacità di scalare l'erogazione dei propri servizi qualora necessario a fronte dell'evolversi dell'emergenza sanitaria.

3.3. DIMENSIONAMENTO ED ELEMENTI ECONOMICI

Si riporta di seguito una stima inerente al dimensionamento del servizio. Si precisa che tutte le informazioni fornite sono da considerarsi indicative e non vincolanti per la Stazione Appaltante.

Si specifica che **la stima di seguito riportata del numero di pazienti potenzialmente convolti è stata determinata in considerazione dei seguenti elementi**:

- **Stato attuale della diffusione del virus Covid-19** e numero di pazienti possibili, probabili e confermati Covid-19;
- **Numerosità di pazienti cronici e/o fragili presenti sul territorio regionale e potenzialmente ad alto rischio** in caso di contagio Covid-19 e con affezioni che possono generare evoluzioni critiche della malattia (p.es. BPCO);
- **Orizzonte temporale massimo della fornitura** (6 mesi + 6 mesi);

In coerenza con le valutazioni e gli elementi considerati **si stima un numero di pazienti che necessiterebbero della sorveglianza attiva sulla piattaforma pari a 15.000 pazienti nell'arco di 12 mesi**.

L'ipotesi di distribuzione dei costi prevede:

a) Oneri di progetto per l'esecuzione delle attività necessarie all'avvio del progetto;
b) Oneri per la gestione operativa del servizio;
c) Oneri per l'esecuzione delle attività di integrazione opzionali.

In coerenza con l'ipotesi di distribuzione dei costi di seguito i corrispettivi previsti:

	Corrispettivo	€ (IVA esclusa)
1	**Corrispettivo *una tantum* al termine del collaudo e avvio della piattaforma applicativa richiesta**	**50.000 €**

2	**Corrispettivo *una tantum* per ogni paziente per cui viene attivata la sorveglianza attiva sulla piattaforma**	**18 €/paziente configurato e attivato**
3	**Corrispettivo *una tantum* al termine dell'esito positivo dei collaudo dell'integrazione opzionale**	**15.000 €**

Si precisa quanto segue:

a) Il costo di cui al punto 1 (*una tantum* al temine del collaudo e avvio della piattaforma) corrisponde al corrispettivo per **oneri di progetto per l'esecuzione delle attività necessarie all'avvio del progetto**, comprese le attività necessarie alla declinazione nel contesto specifico, all'installazione, collaudo e messa in produzione, all'addestramento e formazione del personale e alle attività di integrazione con altri sistemi. Si specifica che si intendono comprese anche le attività di integrazione obbligatorie, che si potranno rendere necessarie anche in seguito all'avvio del servizio; inoltre comprende **la produzione – alla fine del contratto – della base dati** (in formato opportunamente concordato in fase esecutiva), corredata della relativa documentazione di dettaglio, **per la consegna dei dati alla Stazione Appaltante** e/o per la migrazione degli stessi dati su una eventuale altra piattaforma gestionale; non sono compresi oneri derivanti dall'esercizio di piattaforme infrastrutturali; la piattaforma applicativa dovrà comunque essere implementata sulle risorse rese disponibili da ATS nel contesto dei servizi Cloud previsti dalla Gara SPC Cloud Lotto 1.

b) Il costo di cui al punto 2 (tariffa di 18€/paziente *una tantum* per ogni paziente per cui viene attivata la sorveglianza attiva sulla piattaforma) corrisponde al corrispettivo per gli **oneri necessari per la gestione operativa del servizio applicativo**, comprese le attività necessarie all'attivazione della sorveglianza sui pazienti, al project management e all'assistenza e manutenzione della piattaforma applicativa per tutta la durata del contratto. **Si specifica che per attività necessarie all'attivazione della sorveglianza sui pazienti si intendono tutte le attività necessarie alla configurazione dell'utenza per lo specifico paziente e l'associazione agli operatori e strutture dedicate alla sorveglianza** sulla base delle richieste di attivazione che saranno fornite in coerenza con i protocolli clinico-sanitari definiti. In coerenza con gli stati del paziente definiti in relazione al processo di sorveglianza, descritti in dettaglio nel paragrafo 3.4, l'attivazione di un paziente sulla piattaforma corrisponderà all'associazione del paziente allo stato "Reclutato".

c) Il costo di cui al punto 3 (*una tantum* al temine del collaudo con esito positivo dell'integrazione) corrisponde al corrispettivo per **oneri di progetto per l'esecuzione delle attività necessarie all'integrazione della piattaforma con il FSE di Regione Sardegna**. Come specificato le attività di integrazione con il

FSE, dettagliata al paragrafo 3.5, sono **da intendersi come opzionali**, non comprese quindi nei corrispettivi di cui ai punti precedenti, e **potranno essere richieste da ATS nel corso del progetto, per tutta la durata del contratto, al verificarsi dell'effettiva esigenza**.

La base d'asta ed il conseguente valore di contrattualizzazione calcolato sulla base di quanto stabilito dal Codice dei Contratti vigente, **è definito** – oltre che tenendo conto del corrispettivo *una tantum previsto* al temine del collaudo e avvio della piattaforma - **su un numero di pazienti stimato in 7.500 nei sei mesi successivi alla stipula contrattuale**, ferma restando la possibilità per ATS Sardegna di esercitare l'opzione di estensione al verificarsi di una delle due seguenti condizioni:

1. Esigenza di **incrementare il numero dei pazienti** per cui si rende necessaria la sorveglianza attiva già all'interno dell'arco temporale dei sei mesi originari;
2. Esigenza di **estendere temporalmente la durata dei servizi** al termine dei sei mesi originari. L'esercizio di tale opzione sarà comunicato da ATS all'aggiudicatario almeno 20 giorni solari prima della scadenza contrattuale.

La base d'asta soggetta a ribasso è pertanto pari a 185.000,00 € (IVA esclusa).

La Stazione Appaltante **si riserva inoltre la facoltà di incrementare la fornitura dei servizi, agli stessi patti e condizioni, fino a concorrenza del limite di un quinto dell'importo complessivo aggiudicato**, al netto di Iva e/o di altre imposte e contributi di legge, nonché degli oneri per la sicurezza dovuti a rischi da interferenze, e fino al raggiungimento del medesimo.

In coerenza con le valutazioni sopra esposte il **valore massimo stimato dell'Appalto**, definito all'articolo 35 comma 4 del Codice dei Contratti Pubblici**, è pari a 372.000,00 € (IVA esclusa).**

Il Valore massimo stimato dell'Appalto non sarà soggetto a ribasso. Lo sconto offerto dai concorrenti sulla base d'asta sarà applicato in maniera lineare ai prezzi unitari.

L'utilizzo della piattaforma su ogni specifico paziente reclutato per cui viene attivata la sorveglianza **dovrà essere garantito fino al venir meno delle esigenze di monitoraggio**, per tutta la durata contrattuale.

Si precisa che in caso di estensione della durata dei servizi per ulteriori sei mesi, l'utilizzo della piattaforma per i pazienti attivi al termine dei sei mesi originari dovrà essere garantito, senza ulteriori corrispettivi, fino al venir meno delle esigenze di monitoraggio.

In coerenza con gli stati del paziente definiti in relazione al processo di sorveglianza, descritti in dettaglio nel paragrafo 3.4, il venir meno delle esigenze di monitoraggio corrisponderà all'associazione del paziente allo stato "Disattivato".

Resta inteso che **i servizi richiesti dovranno essere garantiti non oltre il termine della durata definita per il contratto**, al netto di eventuali rinnovi così come precedentemente descritti.

In coerenza con l'ipotesi di distribuzione dei costi è stato definito il seguente **piano dei corrispettiv**i:

- Un **corrispettivo una tantum al termine del collaudo e avvio della piattaforma applicativa richiesta**. Il corrispettivo comprende tutte le attività necessarie all'avvio di progetto definite nel presente capitolato comprese le attività di integrazione obbligatorie definite al paragrafo 3.5.
- Un **corrispettivo una tantum per ogni paziente per cui viene attivata la sorveglianza attiva**. Il corrispettivo una tantum comprende tutte le attività necessarie all'attivazione della sorveglianza attiva su un paziente e alla gestione operativa del servizio comprese le attività di assistenza, manutenzione e project management.
- Un **corrispettivo una tantum al termine del positivo collaudo dell'integrazione con il FSE di Regione Sardegna**, qualora tale attività opzionale sia richiesta formalmente da ATS.

Il corrispettivo una tantum previsto per l'esecuzione delle attività necessarie all'avvio del progetto verrà riconosciuto con la prima fattura, relativa al primo trimestre di attività, in seguito al positivo collaudo e conseguente avvio della piattaforma applicativa richiesta, ad eccezione di una riserva pari al 5% dell'importo previsto, da corrispondere con l'ultima fattura alla fine del contratto, in corrispondenza della realizzazione della componente di Exit Management.

Il corrispettivo una tantum previsto per l'attivazione e configurazione di ogni paziente sulla piattaforma verrà riconosciuto trimestralmente. Per il calcolo del corrispettivo trimestralmente saranno conteggiati i pazienti attivati sulla piattaforma e verrà calcolato il complessivo previsto per i mesi di riferimento moltiplicando il corrispettivo *una tantum* previsto per ogni paziente attivato e configurato sulla piattaforma.

Il **corrispettivo una tantum previsto per l'attività opzionale di integrazione con il FSE di Regione Sardegna verrà riconosciuto alla prima fatturazione trimestrale prevista seguente al positivo collaudo** dell'integrazione stessa.

3.4. REQUISITI FUNZIONALI

In questo paragrafo vengono illustrate le **caratteristiche funzionali previste per la piattaforma di sorveglianza attiva** oggetto del presente capitolato.

Le funzionalità rese disponibili dalla piattaforma dovranno consentire il supporto ad un servizio di sorveglianza attiva da parte dei MMG-PLS, operatori delle COT e degli altri soggetti territoriali coinvolti (es. SISP, USCA, Distretti, Medici Competenti, CDI-Covid, MCA, etc.).

Il servizio è rivolto alle categorie di pazienti individuate nel precedente paragrafo 3.1.

Le funzionalità a supporto del servizio di sorveglianza attiva **dovranno essere fruibili via Internet, dai principali browser di mercato** (Internet Explorer, Chrome, Firefox e Safari), **da qualsiasi dispositivo connesso ad Internet** (PC, tablet, smartphone, ecc.) e **tramite app mobile per i sistemi iOS e Android**.

Di seguito le funzionalità che dovranno essere garantite.

ID	Requisito	Descrizione
1.1	Profilazione Utenze	La soluzione deve prevedere utenze profilate e relativi meccanismi di autenticazione per l'utilizzo da parte dei diversi possibili attori coinvolti (es. Paziente, MMG, Medico Ospedaliero, erogatore CDI Covid, operatore USCA, operatore SISP, Medici competenti, operatori Centrale Operativa Territoriale).
1.2	Piano di monitoraggio	Possibilità di impostare da parte del MMG e/o altro operatore incaricato un piano di monitoraggio su base singolo Paziente (il piano di monitoraggio dovrà consentire di definire la tipologia e la frequenza delle misurazioni da raccogliere e le condizioni di allarme sui valori rilevati).
1.3	Piano di sorveglianza	Possibilità di impostare da parte del MMG e/o altro operatore incaricato un piano di sorveglianza su base singolo Paziente (il piano di sorveglianza dovrà consentire di definire il numero di chiamate di sorveglianza al Paziente e le fasce temporali di esecuzione delle chiamate).

ID	Requisito	Descrizione
1.4	Raccolta dati clinici	Raccolta e inserimento, secondo piano di monitoraggio e piano di sorveglianza definiti, dei dati clinici del Paziente. I dati potranno essere raccolti in modalità manuale, tramite inserimento in specifiche maschere di caricamento dei valori autonomamente rilevati, e/o in modalità automatica, tramite integrazione con appositi dispositivi. La soluzione dovrà garantire la possibilità di guidare la raccolta dei dati clinici da parte degli operatori anche tramite schemi di valutazione e triage definiti dai protocolli clinico-sanitari.
1.5	Visualizzazione temporale	Consentire la visualizzazione e l'analisi dell'andamento nel tempo dei piani di monitoraggio e sorveglianza definiti sulla base dei contatti e dei dati clinici raccolti.
1.6	Alert	Possibilità di configurare una serie di alert specifici sul singolo paziente al verificarsi di determinate condizioni definite.
1.7	Generazione elenco pazienti	Supporto alla sorveglianza attiva tramite la generazione automatica dell'elenco dei Pazienti da contattare, comprensivo anche di eventuali segnalazioni inerenti al corretto svolgimento dell'attività di sorveglianza.
1.8	Esportazione Dati	Dovrà essere prevista la possibilità di esportare i dati gestiti (es. elenco pazienti) secondo un formato definito.
1.9	Tracciamento comunicazioni	Il sistema dovrà garantire il tracciamento delle comunicazioni da e verso il Paziente e, tramite l'integrazione con i servizi resi disponibili dal riorientamento del sotto-progetto 1, il registro dei contatti telefonici.
1.10	Notifica comunicazioni	Il sistema dovrà consentire di impostare notifiche automatiche al MMG o ad altri operatori dei contatti e comunicazioni avvenute con il paziente.
1.11	Importazione Dati	Possibilità di importare dati da piattaforme applicative di altri Fornitori secondo formati predefiniti (es. schede contatto, esito tampone, elenco pazienti da contattare, etc.).
1.12	Archiviazione Dati	Archiviazione su proprio repository dei dati trattati.
1.13	Creazione worklist	Il sistema deve generare, sulla base del piano di monitoraggio e di sorveglianza definito, work list ad uso degli operatori che si occupano della sorveglianza attiva.
1.14	Gestione consensi	Il sistema deve garantire l'eventuale gestione consensi: raccogliere, consultare, aggiornare e gestire i consensi che potranno essere previsti per l'esecuzione della sorveglianza attiva.

ID	Requisito	Descrizione
1.15	Gestione anagrafica paziente	Possibilità di inserire e/o completare le informazioni anagrafiche del paziente anche attraverso una chiamata verso banca dati esterna.
1.16	Produzione report e indicatori	Il sistema deve consentire la produzione di reportistica ad hoc su richiesta e il monitoraggio, anche tramite cruscotti appositamente definiti, di specifici indicatori che verranno determinati. In particolare, dovranno essere previsti una serie di indicatori che consentano di misurare il livello di attuazione di quanto definito nei piani di monitoraggio e sorveglianza.
1.17	Supervisione del servizio	Il Fornitore dovrà mettere a disposizione un ambiente di supervisione del funzionamento del servizio in grado di presentare, tramite cruscotti in tempo reale, l'andamento del servizio a titolo di esempio: numero pazienti in carico, dove, di che tipologia, eventuale strumentazione in uso, planning delle attività, ecc.
1.18	Connessione sicura Audio/ Video	Il sistema dovrà garantire soluzioni di videochiamata per limitare i contatti allo stretto necessario e abilitare un colloquio diretto tramite connessione audio/video sicura tra operatore e paziente.
1.19	Gestione stato paziente	Il sistema dovrà garantire la possibilità di gestire gli stati del paziente in relazione al processo di sorveglianza attiva. La soluzione dovrà in particolare garantire la gestione dei seguenti stati del paziente: • **Reclutato**: corrisponde all'attivazione e configurazione del paziente sulla piattaforma di sorveglianza; • **Sospeso**: si riferisce ad un paziente clinicamente guarito (o negativizzato) per cui viene sospeso il monitoraggio; • **Riattivato**: si riferisce ad un paziente precedentemente sospeso e su cui, a fronte di una ricaduta o di una nuova infezione, viene riattivato il monitoraggio; • **Disattivato**: corrisponde al venir meno delle esigenze di monitoraggio del paziente; la disattivazione in corso di contratto potrà avvenire o per decesso del paziente, o per altri motivi di natura amministrativa e/o sanitaria (es. paziente che si trasferisce ad altra Regione, etc.).

3.5. INTEGRAZIONI

Al fine di garantire un supporto completo al servizio di sorveglianza attiva, il sistema dovrà garantire una serie di integrazioni che dovranno essere oggetto di approfondimenti specifici.

Di seguito viene presentata la **lista delle integrazioni prioritarie obbligatorie richieste**:

ID	Requisito	Descrizione
1.1	Anagrafiche	Il sistema deve garantire l'integrazione con il sistema anagrafico regionale degli assistibili ANAGS. Le specifiche di integrazione sono riportate nei documenti *"ANAGS-IS-Scarico Variazioni"* e *"ANAGS-IS-Anonimizzazione"* allegati al presente capitolato.
1.2	Sistemi di gestione casi e contatti	Il sistema dovrà integrarsi con il sistema di gestione casi e contatti. Le caratteristiche del sistema sono dettagliate nel documento "*E-HEALTH-2020 - Analisi Funzionale Sistema Gestione casi e contatti COVID-19"* allegato al presente capitolato.
1.3	Strumenti di diagnostica	Il sistema dovrà prevedere eventuali possibili integrazioni con i sistemi e strumenti di diagnosi per il monitoraggio dei sintomi e dello stato di salute al domicilio, costituiti da dispositivi elettromedicali che verranno fornititi da ATS Sardegna.

Tutte le attività necessarie alle integrazioni comprese nella tabella precedente sono da intendersi come obbligatorie e sono quindi ricomprese nel corrispettivo definito per l'avvio del servizio (descritto al paragrafo 3.3), a valle del superamento del collaudo della piattaforma.

ATS, nel corso del progetto e per tutta la durata del contratto, potrà richiedere le attività opzionali necessarie a garantire l'integrazione della piattaforma oggetto del presente capitolato con l'FSE regionale. Le specifiche di integrazione attuali sono riportate nei documenti "E-HEALTH-2020_D5.1.2.15_Soluzione semplificata di accesso al FSE tramite viewer" e "EXE-DES-Integration_Services" allegati al presente capitolato. **L'attivazione di tale opzione**, per cui è previsto un corrispettivo specifico descritto al paragrafo 3.3, **dovrà avvenire tramite richiesta formale di ATS**.

Si specifica che per le ulteriori integrazioni che si rederanno necessarie nel corso della fornitura, non riconducibili alle tre famiglie di integrazioni specificate in tabella, potrà essere stabilito un ulteriore corrispettivo, anche attraverso il ricorso all'incremento del valore contrattuale in fase esecutiva per un importo non superiore al 20% della base d'asta.

3.6. INTEROPERABILITÀ E REQUISITI NON FUNZIONALI

La soluzione, anche successivamente all'attivazione, ma su richiesta della Stazione Appaltante, dovrà garantire i seguenti requisiti non funzionali:

- **Coerenza con il contesto** del Servizio Sanitario di Regione Sardegna;
- **Scalabilità**, ovvero capacità della soluzione di distribuire la logica applicativa e i dati su più nodi fisici in caso di crescita degli utenti o picchi di utilizzo;
- **Correttezza del dimensionamento** del sistema;
- **Affidabilità**, ovvero capacità della soluzione di garantire un funzionamento continuativo e senza degradazioni delle prestazioni;
- **Disponibilità**, per ciascun utente abilitato, delle informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti anche in mobilità;
- **Manutenibilità**, ovvero garantire limitata complessità e oneri di manutenzione della soluzione erogata secondo il modello proposto, anche in relazione alle frequenti evoluzioni normative tipiche del contesto sanitario regionale;
- **Semplificazione e standardizzazione dell'acceso ai servizi** offerti dalla soluzione proposta;
- **Integrità dei dati**, ovvero la capacità di garantire sia l'integrità logica del dato in seguito a transazioni non andate a buon fine, sia l'integrità fisica del dato in caso di blocco del sistema;
- **Sicurezza e rispetto della privacy**, come descritto nel Capitolo 6;
- **Conformità**, ovvero aderenza allo standard di comunicazione HL7 e coerenza con i profili IHE (Integrating Healthcare Enterprise).

3.7. ARCHITETTURA FISICA

La piattaforma dovrà essere **implementata sulle risorse infrastrutturali rese disponibili da ATS Sardegna nel contesto dei servizi Cloud previsti dalla Gara SPC Cloud Lotto 1**.

Il Fornitore dovrà quindi garantire la compatibilità della propria soluzione ai requisiti definiti nel relativo Contratto Quadro SPC Cloud Lotto 1 di cui alle URL:

- https://www.cloudspc.it/ContrattoQuadro.html;
- https://www.consip.it/attivita/gara-spc-cloud-disponibile-la-documentazione.

Sarà onere del Fornitore l'implementazione e la messa in esercizio della piattaforma applicativa proposta, comprensiva delle necessarie licenze relative ai sistemi operativi, ai database e alle componenti software necessarie all'esecuzione della piattaforma, sulle risorse infrastrutturali Cloud messe a disposizione dalla Amministrazione contraente, in coerenza con il Piano Operativo proposto.

Al fine di garantire l'approvvigionamento corretto delle risorse da parte di ATS, il Fornitore è tenuto a descrivere in maniera esaustiva l'architettura e la dotazione dell'infrastruttura fisica necessaria al funzionamento compiuto della propria soluzione, indicando tutti i requisiti e le informazioni in termini di hardware richieste per la fornitura di servizi cloud tramite la gara SPC Cloud Lotto 1.

3.8. SERVIZI PROFESSIONALI

La fornitura prevedere l'erogazione dei seguenti servizi professionali atti a supportare l'attivazione del servizio, nonché orientati alla efficace operatività della soluzione stessa:

- **Analisi funzionale di dettaglio (specifiche funzionali) e delle procedure operative**. Rientrano in queste attività: la progettazione, la realizzazione e declinazione nel contesto specifico dei servizi e soluzioni applicative facenti parte della soluzione.
- **Installazione, configurazione, collaudo e messa in produzione**. Rientrano in queste attività tutti quei servizi di supporto alla fase di attivazione e del governo complessivo del sistema. Tra cui il supporto alla gestione della domanda e alla pianificazione delle evoluzioni.
- **Addestramento e formazione del personale**. Rientrano in queste attività i servizi per la gestione del cambiamento e la formazione e supporto tecnico-specialistico agli operatori coinvolti. Particolare attenzione dovrà essere riservata al supporto dei singoli operatori nella fase di avvio del sistema.
- **Assistenza e manutenzione correttiva ed evolutiva**: rientrano in queste attività i servizi di manutenzione (correttiva, perfettiva, adeguativa, normativa) del software in esercizio e l'assistenza a tutti gli utenti della soluzione.
  Si intendono comprese anche tutte le attività necessarie alla configurazione dell'utenza per l'avvio della sorveglianza attiva su un paziente.
  Il servizio di assistenza dovrà essere operante dalle 8.00 alle 20.00, 7 giorni su 7, e operare a supporto degli Operatori della COT, MMG, USCA, CDI-COVID, Distretti e gli altri attori coinvolti nel processo di sorveglianza attiva.
  Il servizio dovrà erogare, gestire e manutenere la piattaforma applicativa, con caratteristiche aderenti alle normative vigenti in materia di protezione dei dati personali/sicurezza delle informazioni e fornire assistenza tecnica tramite Help Desk per l'utilizzo della piattaforma applicativa.
- **Program e Project Management**: rientrano in queste attività il coordinamento gestionale e amministrativo dell'iniziativa complessiva ed il supporto ad ATS Sardegna e agli operatori coinvolti.
- **Exit management**: alla scadenza del contratto il Fornitore dovrà garantire i servizi necessari a trasferire le competenze e i dati gestiti durante la fornitura al Committente o ad una terza parte da esso eventualmente individuata per il periodo successivo, e secondo le modalità che verranno definite.

Come definito al paragrafo 3.3, gli oneri relativi ai seguenti servizi saranno remunerati con il corrispettivo *una tantum* al termine del collaudo e all'avvio operativo della piattaforma applicativa richiesta (ad eccezione di una riserva pari al 5% dell'importo previsto, da corrispondere alla fine del contratto, in corrispondenza della realizzazione della componente di Exit Management):

- Analisi funzionale di dettaglio (specifiche funzionali) e delle procedure operative
- Installazione, configurazione, collaudo e messa in produzione;
- Addestramento e formazione del personale;
- Exit management.

Saranno invece remunerati attraverso il corrispettivo *una tantum* per ogni paziente per cui viene attivata la sorveglianza attiva i servizi di:

- Assistenza e manutenzione correttiva ed evolutiva
- Program e Project management.

La fatturazione di tali corrispettivi verrà effettuate su base trimestrale.

4. SPECIFICHE DI GESTIONE DEL PROGETTO

Le indicazioni fornite nelle prossime sezioni dovranno essere considerate mandatarie dal Fornitore, il quale dovrà organizzare le proprie attività nel rispetto dei vincoli e delle modalità di azione descritte.

Il **Fornitore è tenuto a presentare** in sede di offerta, **pena non validità della stessa**, un **piano operativo** descrittivo in modo dettagliato di tempi e modalità operative di attivazione ed erogazione del servizio per le componenti previste dal progetto. Il Piano, seppur non oggetto di valutazione, dovrà essere allegato, **pena esclusione**, come offerta tecnica.

Il Fornitore è altresì tenuto a presentare unitamente al piano **operativo il modello organizzativo previsto** per il supporto all'attivazione e gestione delle componenti di progetto, descrivendo in particolare la **composizione dei gruppi di lavoro e professionalità** coinvolti nell'erogazione del servizio.

Dovrà essere indicato un referente unico dell'intero servizio oltre che i referenti operativi specifici. Le risorse individuate dovranno essere descritte in termini di profilo professionale, da esplicitare nominativamente in sede di contratto e dovranno corrispondere in termini di qualità e professionalità a quanto indicato nel piano operativo.

A questo proposito, dato il contesto dinamico e la complessità dell'intervento, **il Proponente dovrà dare evidenza della propria flessibilità organizzativa**, ovvero di aver predisposto adeguate risorse, processi organizzativi e meccanismi di coordinamento al fine di poter gestire efficacemente non solo l'erogazione dei servizi richiesti, ma anche variazioni di contesto.

Come definito nel paragrafo 3.8, il Fornitore è tenuto a **descrivere in maniera esaustiva l'architettura e la dotazione dell'infrastruttura fisica necessaria al funzionamento compiuto della propria soluzione**, indicando tutti i requisiti e le informazioni in termini di hardware richieste per la fornitura di servizi cloud tramite il Contratto Quadro CONSIP SPC Cloud Lotto 1.

Come già specificato al paragrafo 3.2, **l'avvio dell'erogazione del servizio dovrà avvenire entro 10 (dieci) giorni solari dalla comunicazione formale di inizio attività da parte di ATS**.

Per il raggiungimento degli obiettivi descritti si ritiene fondamentale il coordinamento con eventuali altri progetti già in essere, allo scopo di evitare dinamiche contrastanti e gestire possibili interrelazioni reciproche.

Il Fornitore dovrà garantire, fino al termine dell'incarico, tutte quelle attività e servizi necessari ad assicurare il corretto funzionamento della soluzione, nel rispetto degli opportuni Livelli di servizio come descritto nel Capitolo 5.

5. LIVELLI DI SERVIZIO RICHIESTI

In questa parte del documento si definiscono gli indicatori atti a descrivere i livelli di qualità dei servizi, che verranno applicati alle forniture oggetto dell'Appalto.

Il Fornitore, durante l'intera durata dell'incarico, dovrà periodicamente produrre (con una periodicità mensile) specifici report contenenti i livelli di servizio di seguito riportati.

La struttura dei report dovrà essere prodotta dal Fornitore secondo uno schema condiviso e approvato da ATS Sardegna e condivisi su base mensile, e potranno essere utilizzati per verificare la correttezza dei report dei Livelli di Servizio.

L'ATS Sardegna si riserva comunque la più totale autonomia nell'esecuzione delle verifiche dei Livelli di Servizio. A tale scopo dovranno essere fornite opportune credenziali di tipo Amministratore sulla piattaforma applicativa fornita, allo scopo di analizzare i dati in essa presenti.

Il non rispetto dei Livelli di Servizio in seguito alla rilevazione del superamento dei valori di soglia crea le condizioni per azioni contrattuali specifiche, sulla base anche del Capitolato Generale dei Contratti di Appalto dell'ATS Sardegna.

Indipendentemente dal periodo di consuntivazione (variabile in relazione allo specifico indicatore) il Fornitore è tenuto ad uno stretto controllo dell'andamento dei livelli qualitativi dei servizi offerti (LdS) per intervenire tempestivamente nel ripristino dei valori target non appena si rilevino deviazioni significative.

Di seguito sono riportate le schede dei Livelli di Servizio (LdS) della fornitura che verranno applicati alla fornitura del presente Appalto.

5.1. DISPONIBILITÀ DELLA PIATTAFORMA

Titolo del LdS	Disponibilità della piattaforma
Descrizione	Misura della disponibilità della Piattaforma Applicativa
Unità di misura	Percentuale
Periodo di riferimento	Settimana solare precedente la rilevazione
Frequenza di misurazione	Settimanale
Dati da rilevare	Tr_i = tempo di indisponibilità espresso in ore solari causato dal i-esimo malfunzionamento applicativo Td = tempo di disponibilità prevista nel periodo di riferimento espresso in ore solari N = numero di malfunzionamenti applicativi
Formula	LdS = $\frac{Td - \sum_{i=1}^{N} Tri}{Td}$ (trasformato in percentuale, ad esempio 0,964 equivale a 96,4%)

Valore di soglia	LdS ≥ 99,99%
Tipo Sanzione	Applicazione di una penale pari allo 0,3‰ dell'ammontare netto contrattuale al primo scostamento al di sotto della soglia e per ogni scostamento pari al 0,01% fino ad un massimo di 5 scostamenti.
Note	

5.2. TEMPO DI RISPOSTA SERVIZIO DI ASSISTENZA E MANUTENZIONE

Titolo del LdS	Tempo di risposta del servizio di Assistenza e Manutenzione
Descrizione	Misura il tempo richiesto per la risposta da parte servizio di Assistenza e Manutenzione ad una richiesta di assistenza
Unità di misura	Minuti lavorativi
Periodo di riferimento	Giorno lavorativo precedente la rilevazione
Frequenza di misurazione	Giornaliera
Dati da rilevare	Tr_i = tempo di risposta alla richiesta di assistenza N = numero di richieste di assistenza ricevuto nel periodo di riferimento
Formula	LdS = $\frac{\sum_{i}^{N}{}_{=1} Tri}{N}$
Valore di soglia	LdS ≤ 5 minuti lavorativi
Tipo Sanzione	Applicazione di una penale pari allo 0,3‰ dell'ammontare netto contrattuale al primo scostamento al di sopra della soglia e per ogni scostamento pari a 1 minuto lavorativo fino ad un massimo di 5 scostamenti
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio

5.3. TEMPO DI RISOLUZIONE RICHIESTE DI ASSISTENZA

Titolo del LdS	Tempo di risoluzione delle richieste di assistenza
Descrizione	Rispetto del tempo di risoluzione delle richieste di assistenza da parte del servizio di Assistenza e Manutenzione
Unità di misura	Percentuale
Periodo di riferimento	Giorno lavorativo precedente la rilevazione
Frequenza di misurazione	Giornaliera

Dati da rilevare	NcOK = numero di ticket chiusi nella tempistica prevista nel periodo di riferimento NcT = numero di ticket chiusi nel periodo di riferimento
Formula	LdS = $\frac{NcOK}{NcT}$ (trasformato in %, ad es. 0,855 corrisponde a 85,5%)
Valore di soglia	LdS ≥ 90,00% Tempistiche previste per la chiusura dei ticket: max. 4 ore lavorative
Tipo Sanzione	Applicazione di una penale pari allo 0,3‰ dell'ammontare netto contrattuale al primo scostamento al di sotto della soglia e per ogni scostamento pari al 2% fino ad un massimo di 5 scostamenti
Note	Oggetto di registrazione giornaliera dei dati elementari necessari al calcolo del Livello di Servizio

5.4. PRODUZIONE DEI RAPPORTI DI DETTAGLIO DEI LIVELLI DI SERVIZIO

Titolo del LdS	Produzione dei rapporti di dettaglio dei Livelli di Servizio erogati
Descrizione	Misura in tempo intercorrente tra la consegna del rapporto di dettaglio la cui produzione è in capo al Fornitore e il termine del relativo periodo di riferimento
Unità di misura	Giorni lavorativi
Periodo di riferimento	Settimana lavorativa precedente la rilevazione
Frequenza di misurazione	Settimanale
Dati da rilevare	Tr_i = tempo dalla data di termine del periodo di riferimento del rapporto i-esimo e la sua data di consegna da parte del Fornitore N = numero di rapporti previsti nel periodo di riferimento
Formula	LdS = $\frac{\sum_{i}^{N=1} Tri}{N}$
Valore di soglia	LdS ≤ 1 giorno lavorativo
Tipo Sanzione	Applicazione di una penale pari allo 0,3‰ dell'ammontare netto contrattuale al primo scostamento al di sotto della soglia e per ogni scostamento pari a un giorno solare
Note	

5.5. SLITTAMENTO DELLA CONCLUSIONE DI UNA ATTIVITÀ DELL'INIZIATIVA

Titolo del LdS	Rispetto delle tempistiche di programmazione attività
Descrizione	Ritardo, per cause imputabili al Fornitore, nella conclusione delle attività di progetto rispetto ai tempi-limite massimi definiti nel Capitolo 4 o ai tempi definiti nel Piano Operativo o comunque rispetto all'ultima pianificazione approvata da ATS. Il ritardo è considerato tale anche nei seguenti casi: • Collaudo/approvazione della consegna o del completamento dell'attività con esito negativo; • Non completezza della consegna o delle attività, anche per quanto riguarda la documentazione richiesta.
Unità di misura	Giorni lavorativi
Periodo di riferimento	Settimanale
Frequenza di misurazione	Ad ogni conclusione definita per le attività di progetto
Dati da rilevare	▪ Data di consegna effettiva (*Dc*) ▪ Data di consegna pianificata (*Dp*)
Formula	$LdS = Dc - Dp$
Valore di soglia	LdS ≤ 1 giorno lavorativo
Tipo Sanzione	Applicazione di una penale pari all'1‰ dell'ammontare netto contrattuale al primo scostamento al di sotto della soglia e per ogni scostamento pari a un giorno solare
Note	

6. GESTIONE DELLA PRIVACY E DELLA SICUREZZA DELLE INFORMAZIONI

Di seguito vengono definiti i requisiti ai quali il Fornitore deve attenersi e/o implementare allo scopo di preservare l'integrità, la disponibilità e la riservatezza delle informazioni nell'ambito dell'erogazione della presente fornitura.

La sicurezza delle informazioni rappresenta un obiettivo di primaria importanza per ATS. Al fine di consentire un'efficace ed efficiente gestione della sicurezza delle informazioni sotto tutti gli aspetti, il Fornitore si impegna a rispettare:

- Le prescrizioni normative in materia di protezione dei dati personali (D.Lgs. 196/03 successivamente rivisto con D.Lgs. 101/18, provvedimenti emanati dal Garante della Privacy);
- Quanto previsto dal Regolamento UE 2016/679 (Regolamento Europeo in materia di protezione dei dati personali, di seguito GDPR);
- Gli standard di settore, in particolare quelle richieste dalla ISO 27001/27002.

Il Fornitore si impegna a fornire tutto il supporto necessario per la risoluzione di eventuali incidenti o situazioni di crisi per la sicurezza delle informazioni in relazione all'oggetto del contratto. In particolare, il Fornitore dovrà comunicare immediatamente a ATS qualsiasi incidente occorso alle informazioni.

Tutto quanto definito e richiesto dal presente Capitolato Tecnico in materia di gestione della sicurezza delle informazioni e privacy dovrà essere garantito dal Fornitore stesso e dai suoi eventuali sub fornitori.

6.1. GESTIONE DELLA PRIVACY

Il D.Lgs. 196/03 successivamente rivisto con D.Lgs.101/18 e il Regolamento UE 2016/679 (Regolamento Europeo in materia di protezione dei dati personali, di seguito GDPR), nonché i Provvedimenti emanati dall'Autorità Garante per la Protezione dei dati personali (di seguito Garante Privacy), si prefiggono di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Con "trattamento dei dati personali" s'intende nel seguito qualunque operazione (ad es.: consultazione, elaborazione, conservazione, ecc.) svolta con o senza l'ausilio di mezzi elettronici riguardante dati concernenti persone fisiche, giuridiche o enti.

Il D.Lgs. 196/03 successivamente rivisto con D. Lgs.101/18 stabilisce in particolare:

- La necessità di strutturare e mettere in atto un'organizzazione specifica per la Privacy attraverso l'identificazione di opportuni ruoli e le relative procedure di

nomina;

- Un insieme di misure di sicurezza che devono essere applicate con lo scopo di assicurare un livello adeguato di protezione dei dati.

Il Garante Privacy ha inoltre espresso misure e accorgimenti specifici per i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (Provvedimento del 27 novembre 2008 e s.m.i.).

Nei paragrafi successivi vengono descritti, secondo l'ordine logico appena definito, i requisiti relativi alla normativa della privacy che il Fornitore dovrà rispettare.

6.1.1. Misure di sicurezza

L'articolo 5, par. 2 del Regolamento 679/2016/UE ("Principio di responsabilizzazione") impone che è responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare tale conformità delle attività di trattamento. Tali misure dovrebbero tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Quando il titolare del trattamento decide di affidarsi a soggetti esterni e questi, per poter svolgere l'attività, devono trattare dati personali di cui la titolarità è del titolare i soggetti esterni devono essere nominati quali responsabili del trattamento ex articolo 28 del Regolamento 679/2016/UE. Tale nomina a responsabile del trattamento impone che quest'ultimo svolga l'analisi dei rischi ex articolo 32 Regolamento 679/2016/UE anche sui trattamenti di dati personali svolti per conto del titolare del trattamento.

Il Fornitore verrà individuato quale responsabile del trattamento ex articolo 28 e riceverà dal titolare del trattamento la lettera di nomina contente tutte le indicazioni dell'articolo 28 del Regolamento 679/2016/UE.

Oltre all'applicazione delle misure di sicurezza, il trattamento dei dati personali, da parte del Fornitore, dovrà sempre ispirarsi al rispetto dei principi generali del D.Lgs. 196/03 successivamente rivisto con D.Lgs.101/18 e del GDPR e quindi avvenire in modo lecito e secondo correttezza, valutando la pertinenza, la completezza e la non eccedenza dei dati rispetto alle finalità dei trattamenti in funzione delle attività assegnate.

In particolare, si evidenzia il principio di minimizzazione (ex articolo 5, par. 1, lett. c del regolamento 679/2016/UE) che prevede che gli strumenti elettronici siano configurati in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite possano essere realizzate mediante altri strumenti quali dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità.

L'evoluzione della normativa sulla privacy, mediante la pubblicazione di provvedimenti, regolamenti, ecc. ad hoc da parte del Garante Privacy, ha richiesto e potrebbe richiedere in futuro, l'implementazione di misure di sicurezza specifiche. Si chiede quindi al Fornitore di considerare e applicare ogni ulteriore misura che potrà derivare dall'evoluzione normativa.

Inoltre, come previsto dal GDPR, deve essere adottato un approccio basato sulla *Security* e *Privacy by Design* e *by Default* che prevede l'adozione di adeguate misure di sicurezza a tutela di tutto il ciclo di vita del trattamento dei dati personali. Tali misure non sono definite puntualmente dalla normativa, ma devono essere selezionate dal Titolare e Responsabili attraverso opportune attività di analisi e verifica dei trattamenti e dei potenziali impatti in termini di privacy. Il Fornitore dovrà pertanto garantire il rispetto di tali misure e, al contempo, impegnarsi al rispetto delle misure di sicurezza identificate come necessarie ed opportune per il servizio.

In particolare, il servizio:

- Tenendo conto dello stato dell'arte nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, deve mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento UE 2016/679 e tutelare i diritti degli interessati;
- Deve prevedere che la soluzione metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo deve valere per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In apposito registro dovranno essere tenuti aggiornati i referenti incaricati al trattamento e detto registro deve essere reso disponibile online dall'affidatario del servizio.

6.1.2. Provvedimento sugli Amministratori di Sistema

Il Garante Privacy ha stabilito specifiche misure di sicurezza e di verifica relativamente alle attività svolte da parte degli Amministratori di Sistema sui sistemi da loro gestiti.

Si rimanda al Provvedimento del Garante Privacy e s.m.i per la descrizione completa delle misure che il Fornitore è tenuto ad implementare nell'ambito oggetto del contratto. Di seguito si riportano i punti principali che il Fornitore è tenuto a rispettare:

- Identificare come Amministratori di Sistema le figure professionali finalizzate

alla gestione ed alla manutenzione degli impianti di elaborazione e sue componenti e altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali;

- Attribuire le funzioni di Amministratore di Sistema previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- Effettuare la designazione quale Amministratore di Sistema individualmente, allegando l'elenco analitico degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- Riportare in un apposito documento, da mantenere aggiornato e disponibile ai diversi Titolari in caso di loro richiesta e al Garante Privacy in caso di accertamenti, gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite. Detto registro deve essere consultabile dalle funzioni preposte dall'affidatario del servizio ed aggiornato on line a cura del fornitore;
- Adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema e degli utenti che accedono direttamente ai sistemi, ai database e alle console applicative dei sistemi, ai sistemi di virtualizzazione, dei dispositivi di rete, dei database ed alle applicazioni complesse. In particolare, le registrazioni degli accessi devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;
- Conservare le registrazioni degli accessi per un congruo periodo, non inferiore a sei mesi, rendendole accessibili alla consultazione da parte dei Titolari e degli organi giuridici che ne possono fare richiesta;
- Effettuare ogni 6 mesi (o in un periodo che potrà essere variato durante l'applicazione del contratto) una verifica delle attività svolte dagli Amministratori di Sistema, fornendo a tal fine evidenze a chi ha la titolarità delle banche dati e dei sistemi informatici.

Il Fornitore dovrà comunicare tempestivamente le nomine tramite apposita comunicazione a ATS dove saranno inserite tutte le informazioni che garantiscono il rispetto degli aspetti richiesti dalla Normativa in vigore.

6.1.3. Data Breach

Il Fornitore dovrà garantire la comunicazione al Titolare (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali al fine di consentire al Titolare stesso il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del regolamento. La comunicazione da parte del Fornitore dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC istituzionale e dovrà contenere almeno i seguenti punti:

- Natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni;
- Descrivere le probabili conseguenze della violazione dei dati personali

Descrivere le misure adottate da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Il responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite.

6.1.4. Cancellazione Dati Personali e Sensibili

Si evidenzia che l'articolo 28 del Regolamento 679/2016/UE indica che il Fornitore deve cancellare e/o restituire al titolare tutti i dati personali una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il titolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione.

6.1.5. Trasferimento e Trattamento dei Dati all'Estero

Nel caso in cui, per l'erogazione del servizio si dovesse configurare la necessità di trasmettere dati personali degli interessati in Paesi al di fuori dell'Unione Europea, il Fornitore si impegna a comunicare al titolare questo obbligo normativo, come imposto dall'articolo 28, par. 3, lett. a) del Regolamento 679/2016/UE, i Paesi nei quali i dati potranno essere comunicati al fine di poter idoneamente informare l'interessato. Al fine di rendere lecita la trasmissione il Titolare e il Fornitore concordano che le prescrizioni normative di riferimento sono quelle previste dagli articoli 44, 45, 46, 47, 48, 49, 50 del Regolamento 679/2016/UE; quindi qualora la trasmissione avvenisse in Paesi nei confronti dei quali non sussistessero decisioni di adeguatezza della Commissione Europea (ex. articolo 45 del Regolamento 679/2016/UE) e non sussistessero le garanzie adeguate di cui all'articolo 46 del Regolamento 679/2016/UE, il trasferimento potrà

essere effettuato solamente sulla base di apposito consenso dell'interessato ai sensi dell'articolo 49, comma 1, lettera a) del Regolamento 679/2016/UE.

6.2. GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

6.2.1. Requisiti generali

Il Fornitore deve:

- Garantire il rispetto della normativa vigente (Leggi sul copyright, ecc.), anche attraverso l'implementazione di procedure appropriate;
- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite nell'ambito di tutte le attività ad esso affidate;
- Nell'ambito del trattamento, comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, rispettare il principio di:
    - Minimo privilegio;
    - Necessità;
    - Separazione dei compiti.
- Verificare con regolarità la conformità dei servizi erogati agli standard di sicurezza e ai requisiti richiesti da ATS;
- Garantire la redazione di tutta la documentazione richiesta da ATS in conformità agli standard definiti da ATS;
- Raccogliere le evidenze, a seguito di un incidente di sicurezza, conservarle e presentarle qualora sussista la necessità di azioni legali di natura civile o penale;
- Impegnarsi formalmente a gestire in modo riservato e sotto la propria responsabilità le informazioni e i dati di cui viene a conoscenza. Al termine del contratto, salvo diverse disposizioni, le informazioni e i dati devono essere distrutti con modalità sicure o restituiti fornendo le relative evidenze a ATS;
- Garantire che tutti gli strumenti di lavoro eventualmente introdotti in ATS, come ad esempio laptop e dispositivi di memorizzazione, siano stati preventivamente autorizzati da ATS e dotati di tutte le misure di sicurezza ritenute necessarie e adeguate (come nel caso dei gestori ed assistenti);
- Garantire che tutti gli strumenti di lavoro forniti da ATS non siano modificati e la documentazione sia custodita con cura;
- Utilizzare sistemi antivirus, controllo malware e meccanismi di sicurezza per i media rimovibili, per tutte le postazioni e reti coinvolti nello svolgimento di attività

per ATS.

- È vietata l'estrazione e il trasferimento di dati e/o di ogni altra informazione dalle basi dati e dai sistemi di ATS, salvo espressa e preventiva autorizzazione da parte di ATS.

6.2.2. Requisiti di sicurezza fisica

Il Fornitore, al fine di garantire a tutte le informazioni gestite per conto di ATS adeguati livelli di tutela, deve definire, implementare e mantenere opportune soluzioni di sicurezza relativamente a: sicurezza perimetrale, controllo degli accessi fisici, sicurezza di uffici, locali tecnici ed attrezzature e quanto necessario: ad esempio l'alimentazione elettrica e la sicurezza dei cablaggi, i supporti di memorizzazione in ingresso e in uscita, lo smaltimento e il riutilizzo delle apparecchiature stesse. Nei prossimi paragrafi vengono illustrati i requisiti di sicurezza fisica che il Fornitore dovrà soddisfare in termini di: sicurezza delle postazioni di lavoro e delle reti e di infrastruttura del Fornitore.

Sicurezza delle postazioni di lavoro e delle reti: Il Fornitore, allo scopo di proteggere l'integrità, la disponibilità dei dati e di prevenire la divulgazione non autorizzata o l'utilizzo improprio delle informazioni, deve:

- Identificare e includere in qualunque tipo di accordo sui servizi di rete affidati all'esterno, le caratteristiche di sicurezza, i Livelli di servizio e i requisiti gestionali dei servizi di rete autorizzati;
- Garantire che i dati siano protetti contro il rischio di intrusione e dell'azione di software dannosi, mediante l'attivazione di idonei strumenti elettronici (es.: antivirus) curandone l'aggiornamento periodico.

Sicurezza dell'infrastruttura del fornitore: Il Fornitore, in funzione delle attività assegnate, deve implementare sulla propria infrastruttura e sulle proprie postazioni le opportune regole di sicurezza in funzione della criticità del servizio e/o dell'informazione trattata. Nel dettaglio il Fornitore deve:

- Controllare e monitorare, tramite appostiti strumenti quali ad esempio firewall, IDS, i "punti di contatto" tra le reti interne del Fornitore e la rete di ATS;
- Dotare le postazioni utilizzate dal Fornitore per accedere alla rete e ai sistemi di ATS di opportuni meccanismi di sicurezza (antivirus, patch di sicurezza, etc);
- Prevedere con cadenza periodica, al fine di garantire efficienza e livelli di sicurezza adeguati alle postazioni e alle reti utilizzati:

- Attività di hardening;
- Attività di patching;
- Vulnerability/assessment/penetration test.

6.2.3. Requisiti di Sicurezza Organizzativa e Logica

I requisiti di sicurezza organizzativa e logica che il Fornitore deve rispettare contribuiscono alla corretta gestione della sicurezza stessa all'interno dell'organizzazione, essendo finalizzati a prevenire ed impedire la perdita, il danneggiamento o il furto di beni/informazioni e l'interruzione dei servizi erogati. Nei prossimi paragrafi vengono illustrati i requisiti di sicurezza organizzativa e logica che il Fornitore dovrà soddisfare in termini di requisiti per la firma digitale, requisiti di gestione delle risorse umane, requisiti di erogazione di servizi di fornitori terzi, controllo degli accessi e analisi e gestione dei rischi.

Requisiti per la firma digitale: Il Fornitore deve garantire che il proprio personale (Dipendenti, Collaboratori e fornitori terzi) coinvolto con i servizi oggetto della fornitura abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni e applichi le norme di sicurezza.

Nel dettaglio il Fornitore per il personale coinvolto con la fornitura deve:

- Durante il proprio processo di ingaggio del personale, valutare i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza in funzione delle attività che dovranno essere svolte;
- Prevedere un processo disciplinare formale relativo agli eventuali casi di violazione della sicurezza;
- Erogare un'adeguata e periodica formazione inerente le tematiche di sicurezza;
- Rimuovere, alla conclusione del rapporto di lavoro, tutti i diritti di accesso utilizzati per accedere alle reti, alle postazioni ed alle informazioni funzionali ai servizi oggetto della fornitura.

Requisiti per la sicurezza delle risorse umane: Il Fornitore deve garantire che il proprio personale (Dipendenti, Collaboratori e fornitori terzi) coinvolto con i servizi oggetto della fornitura abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni e applichi le norme di sicurezza.

Nel dettaglio il Fornitore per il personale coinvolto con la fornitura deve:

- Durante il proprio processo di ingaggio del personale, valutare i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza in funzione delle

attività che dovranno essere svolte;

- Prevedere un processo disciplinare formale relativo agli eventuali casi di violazione della sicurezza;
- Erogare un'adeguata e periodica formazione inerente le tematiche di sicurezza;
- Rimuovere, alla conclusione del rapporto di lavoro, tutti i diritti di accesso utilizzati per accedere alle reti, alle postazioni ed alle informazioni funzionali ai servizi oggetto della fornitura.

Requisiti di erogazione dei servizi di fornitori terzi: Ove il Fornitore si avvalga di fornitori terzi per l'erogazione dei servizi oggetto della fornitura dovrà, come imposto dall'articolo 28, par. 2 e 4 del Regolamento 679/2016/UE, nominare tali fornitori terzi come sub-responsabili. Ai sensi dell'art.28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Fornitore di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub-responsabili". A fronte di tale autorizzazione, si richiede al Fornitore di comunicare alla scrivente l'elenco di tutti gli eventuali soggetti individuati in qualità di sub-responsabili (fornitori terzi). La scrivente provvederà a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla scrivente al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.

Si precisa come è obbligo del Responsabile del trattamento individuare e nominare in forma scritta i propri sub-responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del sub- responsabile i medesimi obblighi posti a carico del responsabile e specificati nel presente documento, in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.

Si evidenza come il Responsabile conservi nei confronti della scrivente, Titolare del trattamento, ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal sub-responsabile.

Controllo degli accessi: Il Fornitore deve garantire sia sugli ambienti di ATS sia sui propri che l'accesso alle informazioni, servizi e sistemi di ATS avvenga in modo sicuro per prevenire l'accesso da parte di utenti che non hanno i necessari diritti e pertanto impedire trattamenti non autorizzati, tenuto conto che il ciclo di vita delle utenze è completamente in carico a ATS.

Nel caso di accesso ad ambienti di ATS, il Fornitore deve:

- Richiedere in forma scritta la creazione di una nuova utenza che deve contenere l'identificativo della persona a cui verrà assegnata, l'ambito di utilizzo, il ruolo e l'ambiente. Le utenze richieste devono essere univoche, personali e utilizzate in modo che l'accesso alle informazioni da parte di ogni singolo utente sia limitato alle sole (principio del "minimo privilegio") informazioni di cui necessita (principio del "need-to-know") per lo svolgimento dei propri compiti;
- Inviare una tempestiva comunicazione a ATS in caso di variazione delle mansioni o delle attività in modo che il profilo venga adeguato alle effettive nuove esigenze;
- Effettuare una revisione periodica delle utenze al fine di individuare le utenze inattive e quelle che necessitano di una modifica di privilegi da comunicare a ATS;
- Richiedere immediatamente la disabilitazione di un'utenza assegnata ad un suo dipendente o collaboratore nei seguenti casi:
    - Interruzione del rapporto di lavoro con il Fornitore;
    - Cambio di mansione che non necessita dell'accesso ai servizi applicativi di ATS;
    - Utenze inattive emerse nella revisione periodica.

L'accesso deve essere effettuato con autenticazione forte: smart card operatore oppure OTP.

Analisi e Gestione dei Rischi: Il fornitore è tenuto a svolgere attività di analisi dei rischi rispetto alla sicurezza delle informazioni sull'intero oggetto del contratto. In particolare, l'analisi deve essere svolta almeno annualmente. I risultati dell'analisi dei rischi devono essere presentati a ATS dal Fornitore nei tempi e nei modi che saranno concordati opportunamente tra le parti e devono almeno prevedere:

- L'identificazione e la descrizione del rischio;
- Il livello di gravità del rischio;
- L'eventuale impatto sui servizi;
- Indicazioni sulle possibili soluzioni congiuntamente alle relative stime sui tempi e costi.

Il Fornitore, condividendolo con ATS, definirà, ove necessario, le modalità di gestione del rischio (ovvero mitigazione, esternalizzazione ed accettazione) e sarà responsabile della redazione di un Piano di Trattamento dei Rischi da attuare nei tempi concordati con ATS.

6.3. GESTIONE DELLA CONFORMITÀ

6.3.1. Report da parte del Fornitore

Entro trenta giorni dalla stipula del contratto, il Fornitore dovrà predisporre una proposta di documento di autocertificazione periodica delle regole e delle policy relative alla sicurezza delle informazioni.

In particolare, tale documentazione dovrà includere:

- La descrizione delle azioni implementate e delle regole definite;
- Il risultato dei test effettuati atti a garantire l'effettivo rispetto di tali regole.

Una volta approvato il documento da parte di ATS, il Fornitore dovrà, mediante lo stesso, autocertificare annualmente o su richiesta di ATS. Questa documentazione è considerata parte del sistema complessivo di monitoraggio della fornitura.

6.3.2. Attività di verifica e controllo

ATS, avrà facoltà di effettuare o fare effettuare, eventualmente anche da terze parti, attività di verifica e controllo sull'applicazione, da parte del Fornitore ed eventualmente dei Subfornitori, di quanto sopra esposto e di qualsiasi altra misura di sicurezza che dovrà essere implementata a fronte di nuove politiche definite da ATS. La verifica può essere effettuata sia tramite visita presso il Fornitore o congiuntamente presso il suo SubFornitore, sia tramite richiesta di idonea documentazione attestante la conformità alla normativa, a regolamenti o a certificazioni. A fronte di difformità rilevate, il Fornitore si impegna ad eseguire gli interventi per il superamento delle stesse previa validazione da parte di ATS delle soluzioni identificate.