CAPITOLATO TECNICO

sistema integrato per la gestione delle prestazioni Neurofisiopatologiche (NIS)

Sistema informatico e servizi per il supporto per il sistema di Neurofisiologia (NIS – Neurophysiology Information System)

Sommario

1. SCOPO E ORGANIZZAZIONE DEL DOCUMENTO

Il presente documento ha lo scopo di presentare al Proponente l'oggetto e l'articolazione della fornitura richiesta dalla Fondazione IRCCS Istituto Neurologico Carlo Besta (di seguito anche Istituto), nonché gli elementi per strutturare l'offerta tecnica richiesta per l'aggiudicazione della procedura di gara.

Nel presente documento vengono illustrati: il contesto e gli obiettivi dell'iniziativa, la nuova soluzione richiesta, i correlati servizi professionali di supporto - sia in sede progettuale sia in fase di esercizio a regime - e l'organizzazione complessiva per il governo dell'iniziativa.

Seguendo questa logica, nella prima parte del documento (Capitolo 2) viene illustrato il contesto di riferimento in cui l'iniziativa si colloca.

Vengono poi specificate (Capitolo 3) le generalità della fornitura, evidenziandone in particolare oggetto, luogo, e durata.

In seguito (Capitolo 4 e Capitolo 5) viene delineato il modello di riferimento che dovrà indirizzare la proposta di Sistema NIS – Neurophysiology Information System da parte del Proponente in termini di requisiti funzionali e non funzionali, esigenze di supporto ai processi e vincoli tecnologici che dovranno essere rispettati per garantire le integrazioni necessarie con il resto del Sistema Informativo dell'Istituto.

Successivamente (Capitolo 6) vengono elencati i requisiti e i processi che il Fornitore dovrà eseguire al fine di garantire la privacy e la sicurezza delle informazioni.

Vengono poi descritte (Capitolo 7) le specifiche di gestione di progetto (avvio, manutenzione, livelli di servizio, penali, …) e i servizi professionali compresi all'interno del perimetro di gara.

Viene, infine, descritto (Capitolo 8) il piano dei corrispettivi che sarà messo in atto durante il progetto.

2. CONTESTO DI RIFERIMENTO

L'Istituto ha deciso da tempo di intervenire sul **proprio sistema informativo ospedaliero**, finalizzato a favorire una integrazione per processi basata sulla centralità del paziente e sulla condivisione delle informazioni come supporto alle decisioni cliniche e come punto di partenza per la definizione di obiettivi e strategie di programmazione sanitaria e sociale.

L'Istituto vuole, in sintesi, perseguire i seguenti **obiettivi strategici**:

- Porre il paziente al centro del sistema organizzativo e informativo passando anche attraverso la re-ingegnerizzazione dei processi clinico-sanitari e la realizzazione di un sistema informativo sanitario di eccellenza che abiliti, nel medio termine la dematerializzazione dei processi;
- Introdurre una forte componente di innovazione tecnologica sul punto di cura come reale contributo alle attività cliniche e terapeutiche, per la condivisione delle informazioni tra i professionisti sanitari, a supporto delle decisioni, della diagnosi e del percorso terapeutico;
- Migliorare in modo decisivo l'efficienza dei processi sanitari ed ottenere impatti positivi in termini di efficacia delle cure, gestione del rischio e qualità complessiva del servizio;
- Migliorare l'efficacia e l'efficienza dei processi amministrativi e gestionali interni.

In tale prospettiva l'Istituto intende utilizzare il sistema informativo come leva di cambiamento, facendo coincidere la riprogettazione del supporto digitale con una ottimizzazione dei processi organizzativi interni. Questo permetterà al sistema informativo di diventare una leva di attuazione della strategia aziendale e un essenziale sostegno a tutte le attività e processi della catena del valore dell'Istituto, siano esse attività di tipo primario o di supporto.

In coerenza con tale percorso, si è manifestata l'esigenza di introdurre un Sistema NIS – Neurophysiology Information System, tale sistema è oggetto del presente documento.

3. CARATTERISTICHE DELLA FORNITURA

3.1. Obiettivi generali dell'iniziativa

Scopo del presente documento consiste nell'approvvigionamento di un Sistema NIS – Neurophysiology Information System e relativi servizi di implementazione ed esercizio. Il sistema dovrà disporre dei requisiti, funzionali e non, descritti nei Capitoli 4 e 5.

3.2. Oggetto della fornitura

È oggetto della presente gara l'acquisizione, l'attivazione e la diffusione presso l'Istituto di un Sistema NIS – Neurophysiology Information System. Più specificatamente costituiscono oggetto della gara:

- **La soluzione applicativa,** comprensiva delle eventuali licenze d'uso del software comprensiva delle eventuali licenze d'uso del software per il seguente dimensionamento, sotto rappresentanti al fine di dare un dimensionamento della struttura, fermo restando che sono indicativi ed oggetto di conferma in sede di progetto esecutivo:
  ;
- **Una serie di servizi professionali specialistici e di processo** connessi alla gestione del Sistema;
- **14 monitor** + PdL a supporto delle refertazione./

Non è ricompresa nel perimetro di fornitura la componente hardware lato server per il sistema in quanto si utilizzerà la componente di infrastruttura hardware già utilizzata dall'Istituto. In particolare, per quanto concerne gli ambienti software di sviluppo e test verrà utilizzata l'infrastruttura presente in Istituto; per quanto riguarda, invece, gli ambienti software di produzione verrà utilizzata l'infrastruttura regionale (gestita da ARIA s.p.a.) secondo quanto previsto dalla DGR XI/1726/ del 10/06/2019. Si richiede al fornitore di rispettare la compliance con le caratteristiche dell'infrastruttura hardware aziendale e regionale, di seguito descritte:

- Infrastruttura dell'Istituto:
  L'infrastruttura presente presso l'Istituto si compone di un ambiente di virtualizzazione basato su un'architettura WMWare Essential Plus composta da 3 server PowerEdge R640 in Cluster e da 1 vCenter Server virtuale. I nodi VMWare proposti vengono connessi agli Storage Huawei dell'Ente (1 Storage Huawei e 1 server di Management Huawei RH128 v3) attraverso 2 Switch Fiber Channel Connectrix DS-6505.
  L'ambiente di backup risulta composto da un Data Domain DD3300 e dal software di backup Veeam Backup & Replication.
- Infrastruttura Regionale:

L'infrastruttura regionale messa a disposizione da ARIA s.p.a. si basa su una soluzione USC Blade Server – CISCO con servizio di Disaster Recovery SAN based. La reference architecture prevede come standard: virtualizzazione VMWare vCloud Suite 6 o superiore e vCenter 6 o superiore; sistemi operativi Linux (RedHat Enterprise Linux 6.x o 7.x e Oracle Linux 5.11 o superiore) o Microsoft (Windows Server 2016 o superiore e Windows Client 10); Data Layer Oracle Database (Oracle DB Server 12c o 18g) o Microsoft SQL Server (MS SQL 2014 o 2016); Oracle Java JDK 1.8 o 1.9; Application server RedHat JBOSS Enterprise 7.x o Tomcat LISPA 3.6 o Microsoft IIS 10; Web Server Apache Enterprise Web Server 2.4 o Microsoft IIS 10.

L'oggetto della fornitura sopra citato è descritto nel dettaglio all'interno delle relative sezioni del presente Documento Tecnico.

3.3. Luogo della Fornitura

I servizi oggetto della fornitura, che verranno dettagliati nel prosieguo di questo documento, saranno erogati:

- Presso la Fondazione IRCCS Istituto Neurologico Carlo Besta;
- Presso le sedi del Fornitore per le attività a suo carico di gestione e coordinamento funzionali al servizio.

3.4. Orizzonte temporale dell'iniziativa

Il progetto ha una **durata complessiva di 5 anni** (**60 mesi**) per la diffusione ed erogazione del servizio. Si ipotizza un **periodo iniziale di massimo 60 giorni** a partire dalla sottoscrizione del contratto per la predisposizione dei servizi applicativi, l'applicazione della struttura organizzativa di supporto e l'avviamento del servizio.

4. REQUISITI FUNZIONALI

Il sistema NIS dovrà disporre delle seguenti funzionalità:

- **Gestione delle richieste di esami per pazienti esterni** tramite integrazione con l'applicativo CUP secondo le specifiche SISS ;
- **Gestione delle richieste di esami da reparto per i pazienti interni**, in termini di:
  - Gestione di ordini semplici e di ordini ciclici;
  - Funzioni di workflow applicativo che consentano di supportare il processo di preparazione dell'ordine: ad esempio: preparazione di una bozza, firma dell'ordine, autorizzazione, ecc.;
  - Alimentazione modulo di tracciamento delle attività di avanzamento per ogni singola richiesta;
  - Funzioni di monitoring e visualizzazione degli ordini e dei risultati che consentono di seguire l'avanzamento dello stato di un ordine e di visualizzare i risultati delle prestazioni sanitarie richieste;
  - Selezione della scheda erogatore tramite opportuni filtri;
  - Pianificazione dell'esecuzione degli ordini in funzione delle disponibilità;
  - Validazioni richieste;
  - Fruizione delle funzionalità di esecuzione degli ordini;
- **Interfacciamento con gli strumenti** di EEG/PE ed EMG e con le Workstation utilizzate in UOC Neuro7 - reparto di Neurologia B (per i dettagli fare riferimento al paragrafo 4.1) in modo tale che i segnali siano associati al referto;
- **Gestione del processo di refertazione** in termini di:
  - Utilizzo di liste di lavoro ordinabili per sala/medico esecutore/date e orario/tipologia della prestazione/ecc.;
  - Stato esame – consente di visualizzare lo stato dell'esame (prenotato, accettato, eseguito, refertato);
  - Gestione delle varie fasi del processo: referto provvisorio, validato, firmato, stampato, consegnato;
  - Chiusura referto con firma digitale con la possibilità di gestire le tematiche di anonimizzazione ed oscuramento secondo regole SISS;
  - Funzionalità di firma multipla;
  - Gestire con firma digitale anche per referti sostitutivi o integrativi.

Il sistema dovrà, inoltre, prevedere le seguenti integrazioni con i differenti moduli del Sistema Informatico dell'Istituto:

- **BAC**: per quanto di pertinenza tramite i servizi di cooperazione applicativa relativi ad identificazione assistito ed allineamento anagrafiche e codifiche utilizzate;
- **CUP**: per la gestione delle richieste di esami relative a pazienti esterni;

- **Gestionale di reparto e CCE** (attualmente ruolo svolto dall'applicativo Medical Tutorial): integrazione tramite passaggio di contesto (utente e paziente) al modulo dell'applicativo per l'emissione ordini e la visualizzazione degli stessi;
- **Repository aziendale**: per l'archiviazione dei referti prodotti dal sistema (eventualmente sia come repository interno Medical Tutorial sia come repository verso l'esterno di piattaforma SISS);
- Piattaforma aziendale di **conservazione digitale a norma dei documenti informatici**.

All'interno della fornitura dovranno essere inclusi **14 workstation comprensive di monitor** a supporto delle postazioni di refertazione, dotati delle seguenti caratteristiche: **Monitor LCD/LED non inferiore a 27"** ad alta risoluzione in grado di visualizzare più tracce contemporaneamente.

Le workstation dovranno essere coperte da manutenzione per l'intera durata contrattuale.

4.1. Caratteristiche degli strumenti di EEG/PE e EMG

Come specificato sopra, il sistema dovrà garantire l'interfacciamento con gli strumenti di EEG/PE e EMG. Di seguito vengono riportate le caratteristiche di tali strumenti.

Sezione EEG/PE
Server: Unità di elaborazione di tipo Server, linea HP Proliant, SO Microsoft Windows Server 2016, RAM 16 GB e Unita RAID 5 con dimensione totale 12 TB
n. 3 VideoEEG a 48 canali, produttore Micromed, codice BRAIN QUICK DT RSCH V EEG E
n. 3 VideoEEG a 48 canali, produttore Micromed, codice BRAIN QUICK DT RSCH V EEG E
n. 1 EEG portatile carrellato, produttore Micromed, BRAIN QUICK NS FLXI V EEG E
n. 6 PdL con software per la revisione e l'elaborazione dei segnali e per la gestione del processo di produzione referti.

Le unità di Elaborazione sono basate su Processori Intel e sistema operativo Microsoft Windows 7 PRO 64 Bit: Ambiente Operativo Micromed System Plus Evolution rel. 1.04.197 o Superiore.
n. 2 EEG dinamici Holter, produttore Micromed, KIT MORPHEUS AMB

Sezione EMG/PE
La strumentazione sarà sostituita. Saranno acquisiti:
N. 1 Elettromiografo completo di stimolatori e moduli per l'esecuzione di test di Potenziali Evocati; con unità di elaborazione rappresentata da PC desktop di ultima generazione con sistema operativo Windows 7 o 10, in versione Professional. Software per l'acquisizione, la revisione e l'elaborazione dei segnali e per la gestione del processo di produzione referti
N. 2 Elettromiografi con unità di elaborazione rappresentata da PC desktop di ultima generazione con sistema operativo Windows 7 o 10, in versione Professional. Software per l'acquisizione, la revisione e l'elaborazione dei segnali e per la gestione del processo di produzione referti.

Il sistema comprenderà un database centralizzato di archiviazione di segnali, tracciati e referti, con le
Il database sarà implementato sull'infrastruttura tecnologica per l'archiviazione iperconvergente virtuale di cui dispone il Servizio Informativo Aziendale.

UOC Neuro7 - reparto di Neurologia B
Di seguito sono riportate le caratteristiche delle Workstation e delle apparecchiature utilizzate nell' UOC Neuro7 - reparto di Neurologia B con cui il nuovo sistema dovrà interfacciarsi.

- **Workstation:**
  - n. 3 Workstation HP Z240 Tower con CPU i5 3.2GHz; RAM 8GB; OS Win 10 Pro 64bit;
  - n. 1 Workstation HP Z240 Tower con CPU i7 3.6GHz; RAM 8GB; OS Win 10 Pro 64bit.
- **Apparecchiature:**
  - n. 1 Video-EEG a 128 canali (composta da n. 2 testine da 64 canali) con telecamera infrarossi per monitoraggio a lungo termine (LTM), produttore MICROMED, modello VIDEO-EEG BQ3200 DV/128 LTM;
  - n. 3 Video-EEG a 32 canali con telecamera infrarossi per monitoraggio a lungo termine (LTM), produttore MICROMED, modello VIDEO-EEG BQ3200 DV/32 LTM;
  - n. 1 Video-EEG a 32 canali con telecamera, per monitoraggio sala operatoria/terapia intensiva e registrazioni polisonnografiche, produttore MICROMED, modello VIDEO-EEG LTM EXPRESS 2016;
  - n. 1 Video-EEG a 32 canali telecamera, infrarossi, produttore MICROMED, modello VIDEO-EEG HANDY DV;
  - n. 1 Holter EEG a 32 canali, produttore MICROMED. modello MORPEHUS;
  - n. 1 Stazione di archiviazione NAS, modello NAS RAID.

Monitoraggio intraoperatorio

2 strumenti AXON intraoperatori con EEG EMG PE

una stazione di lettura.

È importante sottolineare, che le apparecchiature potranno essere oggetto di aggiornamento o sostituzione, in questo caso le modalità di interfacciamento saranno riviste in sede di definizione del progetto per la realizzazione dell'iniziativa.

Il sistema inoltre dovrà garantire le seguenti caratteristiche:

- Possibilità di refertazione a distanza, cioè di visualizzazione e refertazione dei tracciati su postazioni diverse da quelle d'acquisizione.
- Possibilità di salvare i referti anche formato PDF;
- Gestione e controllo degli accessi tramite profilo utente nominativo integrato con Active Directory.

5. REQUISITI NON FUNZIONALI

5.1. Interfaccia applicativa

- **Interfaccia orientata alla rappresentazione grafica e auto-referenziata**

Tale funzione assume aspetti particolarmente rilevanti in quanto deve permettere all'utente finale un uso dei dati facile e intuitivo, in particolar modo in un ambiente sanitario dove il dato assume aspetti molto importanti in termini di urgenza, qualità del dato, sicurezza e privacy. Inoltre visto che i dati disponibili sono sempre più rilevanti occorre rappresentarli in forma e struttura in funzione del loro utilizzo ed in relazione all'operatore che ne ha bisogno, superando l'impatto uomo-macchina attraverso un costante adeguamento di queste funzioni.

- **Accessibilità e usabilità**

Per accessibilità si intende l'inserimento e la consultazione agevole e leggibile delle informazioni gestite dall'applicativo, attraverso un accesso configurato al sistema (sistema adattativo), anche per mezzo di aree di sintesi o evidenza. Con il termine usabilità, più in generale, ci si riferisce al grado di facilità e soddisfazione con cui l'interazione uomo-strumento si compie.

Per garantire l'accessibilità del sistema da parte di tutti gli utenti, le informazioni devono essere facilmente reperibili, esplicitate in modo chiaro e rese di indubbia interpretazione. Per favorire la leggibilità e l'immediatezza nel reperimento delle informazioni può inoltre essere utile poter visualizzare le informazioni in forma cronologica e sintetica, dando poi la possibilità di accedere al dettaglio di ciascun evento.

Il sistema deve essere adattativo, ovvero deve visualizzare solamente le informazioni circoscritte all'ambito operativo dell'utente (reparto/ambulatorio/amministrazione/…) e quindi limitare i dati modificabili/inseribili a seconda dei diritti dell'operatore che si autentica al sistema, facilitando nel contempo la compilazione attraverso l'introduzione di frasi standardizzate nei campi di testo libero (è auspicabile che, dove possibile queste siano collegate a sistemi di codifica dei contenuti – es. ICD9).

Affinché lo strumento sia usabile, è importante che la grafica sia semplice e con combinazioni di colori "comode" per la vista. È inoltre importante valutare con attenzione il rispetto degli standard W3C esistenti al fine di garantire la fruibilità del sistema anche da parte di soggetti con discapacità fisica. Ciò, unito a una strutturazione delle informazioni logica, semplice ed intuitiva, permette all'utente di prendere rapidamente dimestichezza con lo strumento e quindi di ridurre notevolmente i tempi di formazione del personale, e di ridurre la probabilità di errori di inserimento.

5.2. Interoperabilità e aderenza a standard

Le integrazioni interne al **sistema informativo clinico-sanitario** dovranno essere realizzate secondo lo standard di comunicazione HL7 e rispondere ai profili IHE (lntegrating Healthcare Enterprise), ove specificato (es. sistemi RIS;LIS).

Nel contesto Sanitario si sono affermati diversi standard che forniscono dei riferimenti specifici ai diversi livelli:

- Funzionali (codifiche, profili di cura, ecc);
- Di Integrazione (HL7, DICOM, ecc);
- Tecnologici (Sistemi, tablet ecc).

Risulta importante che ogni applicazione sia aderente a questi standard e che sia in grado, in modo semplice, di adattarvisi.

L'aderenza a standard internazionali - in termini funzionali, sintattici e semantici - è una caratteristica necessaria.

Per gli standard sintattici, oltre alle differenti componenti di HL7 che supportano la messaggistica tra applicazioni sanitarie presenti in azienda, è utile considerare lo standard DICOM (Digital Imaging and COmmunications in Medicine) per i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni ed oggetti multimediali di tipo biomedico.

5.3. Patrimonio Informativo

Nel seguito si descrivono le principali caratteristiche che deve possedere il "Patrimonio Informativo" aziendale nel più generale contesto dei principi peculiari di un Sistema Informativo Ospedaliero.

- **Alta Disponibilità**

Il sistema deve rendere disponibili a ciascun utente abilitato (interno od esterno) le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.

La soluzione proposta deve garantire per gli utenti autorizzati la disponibilità h 24 di tutte le funzioni applicative e dei Componenti applicativi Trasversali. In questo contesto l'architettura disegnata deve esprimere condizioni di load balancing elaborativo tra i nodi server e opzioni di failover integrate. Nell'elaborato l'Offerente deve evidenziare le disposizioni che puntano a garantire l'alta disponibilità della soluzione anche a fronte del verificarsi di gravi emergenze.

Rientrano nelle contromisure per diminuire il rischio di indisponibilità delle informazioni, le tematiche di back up, di ridondanza, di Business Continuity e di Disaster Recovery. In particolare a

questo proposito verrà valutata la coerenza delle soluzioni proposte e documentate rispetto al piano di Continuità ed Emergenza ed al Piano di Disaster Recovery che verranno presentati.

- **Unicità dell'informazione**

L'unicità delle informazioni presenti nel sistema è un requisito imprescindibile: dati replicati e ridondati incrementano pericolosamente la possibilità di propagazione degli errori all'interno di processi operativi "information intensive", tipici dell'ambito sanitario.

Dal punto di vista operativo tale assioma si traduce nella necessità di inserire i dati una e una sola volta e di renderli utilizzabili in tutti i contesti in cui se ne presenti la necessità.

- **Integrità**

Il sistema deve impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali. Anche la perdita di dati (per esempio a seguito di cancellazione o danneggiamento), viene considerata come alterazione.

5.4. Requisiti di conformità tecnica

Rientrano nelle ordinarie attività di progetto gli adeguamenti applicativi che dovessero rendersi necessari per l'integrazione dei sistemi e l'implementazione di specifici workflow in conformità alle regole/specifiche tecniche del SISS, fino al momento del go-live della soluzione. Rientrano invece nelle attività di manutenzione evolutiva eventuali aggiornamenti al funzionamento dei sistemi applicativi a fronte di un cambiamento delle regole/specifiche tecniche del SISS notificate a valle del momento del go-live di ogni singola soluzione applicativa fornita.

Dovranno essere rispettate tutte le disposizioni attualmente vigenti, ad esempio:

- Requisiti per i videoterminali indicati nella circolare 71911/10.0.296;
- Requisiti indicati dal D.Lgs. 19 settembre 1994 N. 626;
- Requisiti di ergonomia riportati nella direttiva CEE 90/270 recepita dalla legislazione italiana nella legge N. 142 del 19 febbraio 1992;
- Requisiti di sicurezza I.M.Q. (Istituto Marchio di Qualità) e di emissione elettromagnetica F.C.C. (Federal Communications Commission); in alternativa dovranno almeno rispettare analoghi requisiti certificati da altri Enti riconosciuti a livello europeo, nel qual caso la Società dovrà allegare una descrizione delle prove effettuate e dei risultati ottenuti;
- Norme di sicurezza CEI 74/2 (EN 60950/IEC 950);
- Norme di sicurezza CEI 110/5 (EN 55022 / CISPR 22)
- Linee guida europee e nazionali per software medicali e certificazione CE (Direttiva 95/42/CC e nuovo regolamento dispositivi medici (MDR) 2017/745)

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 l'Istituto. 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 all'Istituto 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.

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;
- 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 all'Istituto 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 dei 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 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 dall'Istituto;
- Garantire la redazione di tutta la documentazione richiesta dall'Istituto in conformità agli standard definiti dall'Istituto;
- 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 all'Istituto;
- Garantire che tutti gli strumenti di lavoro eventualmente introdotti nell'Istituto, come ad esempio laptop e dispositivi di memorizzazione, siano stati preventivamente autorizzati dall'Istituto 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 dall'Istituto 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 l'Istituto.

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

6.2.2. Requisiti di sicurezza fisica

Il Fornitore, al fine di garantire a tutte le informazioni gestite per conto dell'Istituto 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 dell'Istituto;
- Dotare le postazioni utilizzate dal Fornitore per accedere alla rete e ai sistemi dell'Istituto 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 Sistema deve consentire la gestione di documenti (caricamento, conservazione, ….) in formato PDF firmati digitalmente (standard PAdES).

Il caricamento di ciascun documento, quando firmato digitalmente, deve essere condizionato all'esito positivo delle necessarie verifiche per l'accettabilità dello stesso (corrispondenza tra l'identità dell'utente loggato e quella del firmatario, validità del certificato utilizzato per la firma, …).

Deve, inoltre, essere consentita la firma digitale anche massiva di documenti.

Requisiti di gestione 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 di 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 dell'Istituto sia sui propri che l'accesso alle informazioni, servizi e sistemi dell'Istituto 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 all'Istituto:

Nel caso di accesso ad ambienti dell'Istituto, 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 all'Istituto 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 all'Istituto;
- 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 dell'Istituto;
    - 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 all'Istituto 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 l'Istituto, 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 l'Istituto.

6.3. Verifica 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 dell'Istituto, il Fornitore dovrà, mediante lo stesso, autocertificare annualmente o su richiesta dell'Istituto. Questa documentazione è considerata parte del sistema complessivo di monitoraggio della fornitura.

6.3.2. Attività di verifica e controllo

L'Istituto, avrà facoltà di effettuare o fare effettuare, eventualmente anche a 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 dall'Istituto. 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 fronte di difformità rilevate, il Fornitore si impegna ad eseguire gli interventi per il superamento delle stesse previa validazione da parte dell'Istituto delle soluzioni identificate.

7. SPECIFICHE DI GESTIONE DEL PROGETTO

7.1. Fase preliminare

Il Fornitore nominerà un Responsabile Tecnico Unico che dovrà rimanere in carica per tutta la durata del contratto, eccetto diversi accordi con il Servizio Informativo Aziendale e sarà la figura che:

- Si interfaccerà con l'Istituto per verificare l'esecuzione delle attività indicate secondo il presente capitolato;
- Dovrà organizzare e supervisionare l'attività del personale del Fornitore;
- Dovrà inoltre garantire che i tempi di fornitura siano sempre rispettati;
- Sarà il riferimento per il Servizio Informativo Aziendale sugli aspetti tecnico e organizzativi della fornitura e dei servizi manutentivi correlati.

Dalla firma del contratto è concesso un periodo di tempo (fase preliminare: max 30 gg) in cui il Fornitore provvederà ad allestire tutto il necessario, prendendo visione dei locali, delle infrastrutture e degli strumenti dell'Istituto.

In tale periodo inoltre l'Istituto provvederà ad una breve presentazione degli strumenti applicativi con cui il Fornitore dovrà integrarsi. La durata (in termini di ore) e la modalità (lezione frontale, manuali eccetera) di tale presentazione sarà a discrezione dell'Istituto.

Al termine della fase preliminare il Fornitore dovrà fornire il progetto esecutivo dell'architettura completa di tutte le integrazioni e posizionando con date reali il piano temporale sottodescritto.

In particolare dovrà essere formalizzato e maggiormente dettagliato con diagrammi di Gantt il piano sotto descritto.

Piano di formazione e assistenza all'avvio

Il piano di formazione deve comprendere tutte le attività di formazione e avvio all'utilizzo del nuovo sistema. Il piano di formazione deve includere almeno i seguenti dati:

1. La metodologia adottata, tenendo conto che la formazione deve necessariamente essere erogata on-site presso l'Istituto;
2. La descrizione dei corsi, con evidenza in dettaglio dei rispettivi contenuti, della durata, del numero minimo e massimo di partecipanti e degli obiettivi formativi;
3. Il numero di giornate e ore erogate (complessivamente e per ciascuna sessione di ciascun corso);

4. L'evidenza della documentazione, della manualistica, del materiale informativo distribuito durante i corsi;
5. L'evidenza della documentazione disponibile online;
6. Il curriculum del personale impiegato.

ll piano di assistenza all'avvio deve includere almeno i seguenti dati:

- La metodologia adottata;
- Il numero di risorse impiegate con relativi curricula;
- Il numero di giornate impiegato (per risorsa e complessivo).

Il piano di formazione e assistenza dovrà essere parte integrante del piano di avvio.

Il piano di formazione deve prevedere uno spazio, per la formazione sui sistemi di integrazione (es. anagrafe centrale, sistema repository, sistema CUP eccetera) per un impegno complessivo di un'ora per ogni sessione.

Se il personale tecnico proposto sarà ritenuto inidoneo alle attività programmate (es. mancata conoscenza dei sistemi informatici forniti, inesperienza in progetti di informatizzazione di grandi realtà...) dal Servizio Informativo Aziendale; l'Istituto si riserva la richiesta di sostituzione di tale personale, senza oneri a carico dell'Istituto.

Il Fornitore dovrà comunque impegnarsi al massimo al fine di permettere la continuità operativa dell'Istituto. La copertura 24/24h sarà garantita dalla reperibilità del personale il Fornitore per problemi bloccanti.

7.2. Fase di collaudo

Al termine della fase preliminare il Fornitore dovrà predisporre (entro max 90 gg dalla sottoscrizione del contratto) una versione stabile della soluzione che sarà oggetto di collaudo da parte dell'Istituto.

Il collaudo racchiude tutte le attività di verifica funzionale e tecnica della soluzione predisposta. Nella tabella sotto riportata sono indicati i test che il Fornitore dovrà svolgere e il deliverable che dovrà produrre in seguito alle attività. Le attività di test dovranno riguardare tutte le funzionalità della nuova soluzione. Il Fornitore, prima di iniziare la fase di collaudo, dovrà produrre un **Piano di Collaudo** contenente modalità e tempistiche per ogni tipologia di test, i casi d'uso coperti dal test e le funzionalità impattate. Il Piano di Collaudo dovrà essere preventivamente consegnato all'Istituto che ne validerà il contenuto e ne autorizzerà l'esecuzione secondo i tempi e i modi indicati. Il Piano di Collaudo dovrà contemplare almeno i test riassunti nella tabella seguente.

Tipo di test	Deliverable
Funzionali	Verbale di esecuzione dei test funzionali con il relativo esito
Di unità	Verbale di esecuzione dei test di unità
Di Sicurezza	Verbale di esecuzione dei test di sicurezza
Di integrazione	Verbale di esecuzione dei test di integrazione
Test di non regressione	Verbale di esecuzione dei test di non regressione
Test del modello fisico della base dati	Verbale di esecuzione dei test del modello fisico della base di dati

Tabella 1. Elenco dei test minimi che devono essere compresi nel Piano di Collaudo

Il collaudo sarà effettuato con la partecipazione dei Referenti operativi dell'Istituto e del Fornitore.

Tutti i verbali prodotti a seguito delle diverse sessioni di test andranno consegnati all'Istituto. Eventuali test con esito negativo (problema funzionale, valore sopra soglia, etc.) dovranno essere ripetuti fino al completo successo di tutti i test definiti.

L'avvio della gestione a regime del Servizio sarà subordinato al superamento del collaudo della soluzione, nonché alla verifica dell'adempimento degli obblighi amministrativi ed organizzativi.

L'esito del collaudo sarà oggetto di un verbale riportante le prove superate e gli eventuali fallimenti riscontrati, firmato dai Referenti operativi coinvolti.

7.3. Fase di gestione a regime

A seguito della fase di collaudo avrà avvio la fase di gestione a regime. In questa fase, il Fornitore dovrà fornire il servizio di assistenza e manutenzione post-avvio. Il servizio erogato dal Fornitore dovrà tenere conto di quanto segue:

- Deve essere garantita la continuità operativa e funzionale delle attività dell'Istituto e degli utenti che vi lavorano in relazione al loro profilo, agli ambienti e agli strumenti disponibili;
- Dovrà essere messo a disposizione dell'Istituto un Single Point of Contact (SPOC) volto a erogare help desk di secondo livello;
- Il servizio di gestione, manutenzione e assistenza dell'applicativo dovrà prevedere i seguenti Service Level Agreement:
  - **DIS1 Disponibilità del sistema automatico in linea >= 99,5%**
  - Assistenza e manutenzione per ogni tipologia di problema dal lunedì al venerdì dalle 7:30 alle 18:00 e il sabato dalle 7:30 alle 13:30 (esclusi i festivi);
  - Assistenza e manutenzione per i problemi bloccanti o alta criticità in H24;
  - Presa in carico dei problemi: **immediata**;

- Risoluzione di problemi bloccanti: **entro e non oltre 2 ore solari** dalla presa in carico;
- Risoluzione di problemi non bloccanti di alta criticità **entro e non oltre 4 ore solari** dalla presa in carico;
- Risoluzione di problemi non bloccanti a media criticità o installazione di sistemi di backup: **entro e non oltre 8 ore solari** dalla presa in carico;
- Risoluzione di problemi non bloccanti a bassa criticità: **entro e non oltre 12 ore lavorative** dalla presa in carico.

Per tutta la durata del contratto dovrà essere garantito il supporto tecnico, con gli SLA sopra descritti, sia lato applicativo che lato database al fine di garantire la risoluzione dei problemi indicati. A titolo di esempio dovranno essere garantite le seguenti tipologie di attività sistemistiche:

- Verifiche sul web server per problematiche legate a blocchi o rallentamenti
- Verifiche sul database server per problematiche legate a backup falliti, rallentamenti legati a indici o query lunghe, corruzione dei dati sia livello logico che fisico ed eventuale ripristino da un backup e gestione spazi tablespace.

La manutenzione dovrà ricomprendere tutti gli aggiornamenti disponibili sul sistema fornito (anche major release) compresi quelli derivanti da normative nuove o modificate. In particolare il costo manutentivo dovrà garantire l'adeguamento del sistema informatico derivanti da inserimenti o aggiornamenti di normative europee, nazionali o regionali. Gli adeguamenti normativi potranno essere sia di carattere clinico-organizzativo, sia di carattere informativo (es. variazioni sui tracciati dei flussi informativi) che tecnico (es. nuove specifiche sulla validità della firma digitale).

Per ogni aggiornamento il servizio di manutenzione deve comprendere l'attività di test (system test o unit test), successiva ai test di versione effettuati in laboratorio, da effettuare nell'impianto dell'Istituto e che comprende le integrazioni esistenti con i restanti sistemi informatici.

I test debbono comprendere tutti i casi d'uso e ad ogni test deve seguire una scheda di test riportante l'esito degli stessi. Nel caso si evidenzino problematiche, nell'ambito della stessa manutenzione, debbono trovare risoluzione prima dell'installazione della nuova versione.

Il servizio di assistenza dovrà comprendere un'attività di assistenza on site per i successivi 5 anni volta a massimizzare l'utilizzo dello strumento e che dovrà svolgere, a titolo esemplificativo e non esaustivo, le seguenti attività da effettuarsi in accordo al Servizio Informativo Aziendale:

- Supporto all'utilizzo del sistema informatico;
- Configurazioni specifiche, realizzazioni stampe, estrazioni, report eccetera in funzione dell'estensione e della necessità dell'Istituto;
- Formazione agli utenti e agli operatori in generale dell'Istituto;
- Realizzazioni di configurazioni sui profili e abilitazioni particolari in funzione delle necessità aziendali;

- Supporto per eventuali progetti di estensione dello strumento informatico.

Il servizio di presidio dovrà avvenire attraverso l'esecuzione di circa 150 giornate professionali presso la sede dell'Istituto in orario d'ufficio concordando con il Servizio Informativo Aziendale i periodi di effettiva erogazione. Il personale coinvolto dovrà conoscere dettagliatamente il sistema informatico oggetto di fornitura oltre che disporre di una buona preparazione informatica.

La fornitura dovrà prevedere la manutenzione per i 5 anni successivi all'avvio.

Il mancato rispetto degli SLA richiesti comporterà l'applicazione delle opportune penali e nel caso degli sforamenti degli SLA perdurassero per più di 5 eventi l'Istituto si riserva la facoltà di risolvere il contratto con oneri aggiuntivi a carico del Fornitore.

7.4. Servizi di exit management

Il Fornitore dovrà dichiarare la propria disponibilità a prestare il massimo supporto all'Istituto o all'Istituto che potrà subentrare nella fornitura del sistema informatico oggetto della fornitura, al termine del periodo contrattuale, fornendo tutte le informazioni, le conoscenze maturate e le indicazioni utili alla continuità operativa del servizio e mettendo a disposizione il proprio personale per un affiancamento della durata massima di 60 giorni al fine di mantenere un adeguato livello del servizio.

Il Responsabile Tecnico dovrà coordinare il personale, gestire il trasferimento delle informazioni e garantire il corretto funzionamento del servizio, senza interruzioni o peggioramenti.

7.5. Penali e sanzioni per eventuali inadempimenti

L'importo complessivo delle penali irrogate non può superare il 10 % dell'importo contrattuale. Qualora il ritardo nell'adempimento determini un importo massimo della penale superiore al 10% dell'ammontare netto contrattuale, il Responsabile del procedimento promuove l'avvio delle procedure per la risoluzione del contratto.

Per ogni giorno solare di ritardo rispetto alla data fissata per la consegna, per il collaudo o per l'installazione, sarà dovuta una penalità in misura giornaliera pari al 0.5% dell'ammontare netto contrattuale.

L'applicazione delle penali di cui al presente articolo non pregiudica il risarcimento di eventuali danni o ulteriori oneri sostenuti dalla Stazione appaltante a causa dei ritardi. L'Istituto si riserva la facoltà di applicare le seguenti penali per ogni singolo caso di inadempienza riferito all'importo di aggiudicazione. Numero di ore di ritardo rispetto agli SLA indicati

<30min	<2ore	<3ore	>3
0.03%	0.06%	0.09%	0,1%

Numero di interventi nel mese effettuati senza rispetto delle SLA

<10	<15	<20	>20
0.03%	0.06%	0.09%	0.1%

Le penali saranno applicate tenendo in considerazione il valore massimo dato dalla due tabelle soprastanti per singolo caso di inadempienza riferito all'importo di aggiudicazione.

Per quanto riguarda le workstation si richiede 4x8x NBD con 0.1 % di applicazione di penale rispetto all'importo di aggiudicazione per ciascun ora di ritardo.

8. PIANO DEI CORRISPETTIVI

La fatturazione, per la parte di licenze e servizi di avvio e beni dovrà avvenire in seguito alla fase di collaudo descritta nel paragrafo dedicato.

I pagamenti saranno disposti come indicato nella Lettera Invito.