



La tua
Campania
cresce in
Europa

CAPITOLATO SPECIALE

**Piano di azione per la Ricerca & Sviluppo,
l'Innovazione e l'ICT (D.G.R. n. 180 del 29/04/2011)**

**Procedura aperta per l'appalto della realizzazione di una
piattaforma software di Circolarità anagrafica**

Interventi

**Realizzazione della piattaforma SOA regionale
Integrazione del servizio di comunicazione in
Cooperazione applicativa SPICCA
Realizzazione della piattaforma data hub
regionale per la circolarità anagrafica**

CIG 4010070E6F

CUP B22E11000080009



SOMMARIO

1	PREMESSA	4
2	DESCRIZIONE DEL CONTESTO E DELLE PREESISTENZE.....	4
2.1	COOPERAZIONE APPLICATIVA IN CAMPANIA (SPICCA)	4
2.2	COLLEGAMENTO ALL'INDICE NAZIONALE DELLE ANAGRAFI (INA – SAIA)	4
2.3	DATA CENTER REGIONALE.....	5
2.4	SISTEMA INFORMATIVO REGIONALE.....	5
3	DESCRIZIONE DELLA FORNITURA.....	6
3.1	FINALITA'.....	6
3.2	OGGETTO.....	6
3.3	DURATA.....	7
4	SPECIFICHE TECNICHE DELL'INTERVENTO	7
4.1	SERVICE ORIENTED ARCHITECTURE (SOA).....	7
4.1.1	ESB (ENTERPRISE SERVICE BUS).....	8
4.1.2	SOA GOVERNANCE.....	9
4.1.3	BAM (BUSINESS ACTIVITY MONITORING)	10
4.1.4	SISTEMA IAM	10
4.1.4.1	INTEGRAZIONE TRA IAM E IDENTITÀ FEDERATA SPICCA.....	12
4.1.4.2	SPERIMENTAZIONE n. 1 – INTEGRAZIONE DELLO IAM CON UN APPLICATIVO REGIONALE	13
4.1.5	DIMENSIONAMENTO MINIMO DELLA PIATTAFORMA SOA.....	13
4.2	DATA HUB REGIONALE PER LA CIRCOLARITÀ ANAGRAFICA E PER L'IDENTITÀ DIGITALE.....	14
4.2.1	REALIZZAZIONE DI DATA HUB E ID REPOSITORY	14
4.2.2	SPERIMENTAZIONE N. 2 - CIRCOLARITÀ ANAGRAFICA.....	17
4.3	START-UP DEL SISTEMA.....	17
4.3.1	PROFILI PROFESSIONALI RICHIESTI	19
5	ELENCO DELLE ATTIVITÀ E TEMPI.....	21
6	MODALITÀ DI SVOLGIMENTO DEL CONTRATTO	22
6.1	DIREZIONE DELL'ESECUZIONE DEL CONTRATTO	22
6.2	COMUNICAZIONI.....	23
6.3	PIANIFICAZIONE DELLE ATTIVITÀ.....	23
6.3.1	PIANO DI LAVORO GENERALE.....	23
6.3.2	PIANO DELLA QUALITÀ	24
6.3.3	PIANO DI SICUREZZA INFORMATICA.....	24
6.3.4	PIANI DI LAVORO DI OBIETTIVO	24
6.4	ESECUZIONE DELLA FORNITURA.....	25
6.4.1	OBIETTIVI E CLASSI DI FORNITURA.....	25
6.4.1.1	CICLO DI VITA DEGLI OBIETTIVI PROGETTUALI A CORPO	26

6.4.1.2	CICLO DI VITA DEGLI OBIETTIVI SVILUPPO DI COMPONENTI SOFTWARE	26
6.4.2	LUOGO DI LAVORO ED AMBIENTI PER LE VERIFICHE DI CONFORMITA' E MESSA IN ESERCIZIO	27
6.5	GESTIONE DELLA FORNITURA	28
6.5.1	GESTIONE DEGLI OBIETTIVI A CORPO	28
6.5.2	GESTIONE DEGLI OBIETTIVI DI SVILUPPO SOFTWARE	28
6.5.3	RIDEFINIZIONE DEGLI OBIETTIVI DI SVILUPPO SOFTWARE.....	28
6.6	CONSUNTIVAZIONE DELLE ATTIVITA'.....	29
6.7	VERIFICHE DI CONFORMITA'.....	29
6.7.1	VERIFICA DI CONFORMITÀ DELL'OBIETTIVO.....	30
6.7.2	VERIFICA DI CONFORMITÀ INTERMEDIA.....	30
6.7.3	VERIFICA DI CONFORMITÀ FINALE.....	31
6.7.4	STANDARD DELLA DOCUMENTAZIONE FORNITA.....	31
6.8	RILIEVI E PENALI.....	31
6.9	GARANZIA.....	32
7	INDICATORI DI QUALITA' E LIVELLI DI SERVIZIO.....	32
7.1	REVISIONE DEGLI INDICATORI DI QUALITÀ	32
8	INADEMPIMENTI	32
9	RESPONSABILE OPERATIVO DELL'APPALTO PER IL FORNITORE.....	33
10	VARIANTI.....	33
11	CORRISPETTIVI	33
12	ESECUZIONE IN DANNO	34
13	OBBLIGHI A CARICO DEL FORNITORE.....	34
14	OBBLIGAZIONI DERIVANTI DAL RAPPORTO DI LAVORO	34
15	RESPONSABILITÀ CIVILE.....	34
16	SICUREZZA	35
17	OBBLIGHI DI RISERVATEZZA.....	35
18	TRATTAMENTO DEI DATI	35
19	MANLEVA, BREVETTI E DIRITTI D'AUTORE.....	36
20	PROPRIETA'.....	36
21	DIVIETO DI CESSIONE DEL CONTRATTO E CESSIONE DEL CREDITO.....	36
22	DIVIETO DI SOSPENSIONE DEL SERVIZIO	37
23	CAUSE DI RISOLUZIONE DEL CONTRATTO	37
24	RECESSO	38
25	TRACCIABILITA' DEI PAGAMENTI.....	38
26	NORME - RINVIO	38
27	STAZIONE APPALTANTE E RIFERIMENTI.....	38
28	ALLEGATI.....	38

1 PREMESSA

Il “Piano di azione per la Ricerca & Sviluppo, l’Innovazione e l’ICT” della Regione Campania (approvato con Delibera di Giunta regionale n. 180 del 29/04/2011) ha come obiettivo la realizzazione del sistema Informativo integrato regionale (SIIR) finalizzato allo sviluppo della cittadinanza digitale sul territorio campano e per sostenere una partecipazione attiva alla Società dell’Informazione di tutte le componenti del proprio tessuto socio-economico.

Per lo sviluppo della cittadinanza digitale è però necessario garantire, in prima istanza, tutti gli interventi finalizzati alla realizzazione e al potenziamento delle infrastrutture telematiche, dei sistemi informatici e delle piattaforme applicative idonee all’erogazione multicanale di servizi al cittadino e, infine, attuare il monitoraggio continuo dei servizi erogati per garantire la qualità dei risultati attesi: gli obiettivi riguardano, quindi:

1. la realizzazione di una piattaforma che sia conforme ai dettami del Sistema pubblico di connettività (SPC), della cooperazione applicativa (SpCoop) e dell’approccio architetturale orientato ai servizi,
2. la promozione dell’identità digitale dei cittadini mediante la quale avere credenziali digitali sicure per accedere ai servizi o essere riconosciuti in un sistema federato come responsabile di specifiche funzioni.

L’oggetto di questo capitolato è quello di attuare gli interventi infrastrutturali software volti al soddisfacimento degli obiettivi indicati ai precedenti 2 punti.

2 DESCRIZIONE DEL CONTESTO E DELLE PREESISTENZE

In questo capitolo vengono riportate tutte le informazioni utili relative al contesto e agli asset tecnologici della Regione Campania su cui dovrà integrarsi tutto quanto è oggetto del presente capitolato.

2.1 COOPERAZIONE APPLICATIVA IN CAMPANIA (SPICCA)

In base a quanto previsto dal Codice dell’Amministrazione Digitale (CAD), la Cooperazione applicativa deve avvenire secondo le specifiche del Sistema Pubblico di Connettività e cooperazione (SPC) in conformità alle regole tecniche e di sicurezza SPC emanate con il Decreto del Presidente del Consiglio dei Ministri del 1 aprile 2008 e nelle specifiche e requisiti funzionali di SpCoop pubblicate dal Cnipa / Digit PA.

La Regione Campania, ha realizzato il Sistema di Interoperabilità e Cooperazione applicativa in Campania (di seguito SPICCA) nel pieno rispetto delle specifiche tecniche emanate a livello nazionale in materia (la porta di dominio di SPICCA ha superato positivamente i test di verifica funzionale e congruità tecnica ed è qualificata secondo gli standard definiti da DigitPA nell’ambito dei servizi infrastrutturali di interoperabilità, di cooperazione e di accesso; il Centro Gestione SICA di DigitPA ha emesso il certificato digitale per la Porta di dominio di SPICCA). Con delibera n. 1328 del 31 luglio 2009, la Regione Campania ha reso disponibile SPICCA a tutte le Pubbliche Amministrazioni presenti sul territorio campano al fine di favorire la realizzazione della rete dei servizi telematici (sul B.U.R.C. n. 63 del 19/10/2009 sono state pubblicate le *Regole tecniche per l’utilizzo di SPICCA*): tutta la documentazione e le specifiche tecniche relative alla piattaforma SPICCA è liberamente disponibile e scaricabile al seguente link: www.innovazione.regione.campania.it/content/cooperazione-applicativa.

Si sta, inoltre, procedendo all’adeguamento di SPICCA alle ultime specifiche DigitPA “Modello di Gestione Federata Delle Identità Digitali (GFID)”, versione 1.5.1 del 26/07/2011, che porteranno alla realizzazione di un **ALD** (Autorità Locale di Dominio), di un **Federation Gateway** e di una **Porta di Dominio** conformi a tali specifiche, oltre che all’adeguamento allo standard **SAML 2.0**. Alla conclusione di tali attività, prevista per settembre 2012, verrà resa disponibile l’ulteriore documentazione tecnica.

2.2 COLLEGAMENTO ALL’INDICE NAZIONALE DELLE ANAGRAFI (INA – SAIA)

L’Indice Nazionale delle Anagrafi (INA), istituito presso il CNSD del Dipartimento per gli affari interni e territoriali - Direzione centrale per i servizi demografici, consente l’individuazione del comune che detiene i dati anagrafici dei cittadini iscritti in Anagrafe della Popolazione Residente (APR) ed Anagrafe degli Italiani

Residenti all'Estero (AIRE), per un migliore esercizio della funzione di vigilanza e di gestione dei dati anagrafici e di stato civile. Esso si compone di:

- INA - infrastruttura tecnologica che garantisce l'esercizio dei processi di interscambio e cooperazione, in attuazione delle finalità suddette, tra i comuni, il Ministero dell'interno e gli altri soggetti autorizzati;
- SAIA (Sistema di Accesso e Interscambio Anagrafico) - componente che consente l'aggiornamento telematico dell'INA e permette di inviare le comunicazioni di variazione anagrafica contemporaneamente all'Anagrafe Tributaria (in caso di nascite, decessi, variazioni di residenza o domicilio), alla Motorizzazione Civile (in caso di variazioni di residenza), all'INPS (in caso di decessi) e al Ministero dell'Interno (per l'aggiornamento dell'INA).

Il coordinamento tecnico ed il relativo sviluppo delle azioni inerenti il sistema di accesso ed interscambio anagrafico di INA-SAIA è in capo al CISIS¹: la soluzione infrastrutturale realizzata nell'ambito del progetto ICAR² (task AP2 – Consultazione Anagrafica Interregionale) è interamente basato sullo standard SPCoop e serve per erogare, in cooperazione applicativa, il flusso Comuni-Ministero dell'Interno e il flusso Regione-Ministero dell'Interno. Per consentire il collegamento in sicurezza Regione-Ministero, oltre che l'utilizzo delle **porte di dominio su SPC** (che, nel caso di Regione Campania, è la **Porta di dominio di SPICCA**), è stato sviluppato dall'Università di Tor Vergata un **modulo software**, denominato **SS_BKPDD** (o più comunemente **plug-in**) che ha la funzione di gestire la sicurezza nell'erogazione e fruizione dei servizi applicativi esposti sia dal Ministero dell'Interno (CNSD), sia dagli Enti ad esso connessi. Le caratteristiche tecniche di tale plug-in sono descritte nell'Allegato Tecnico della Convenzione scaricabile al seguente link: **<http://www.innovazione.regione.campania.it/sites/default/files/Indicazioni-tecniche-connessione-regione-CNSD.pdf>**

La Regione Campania:

1. ha sottoscritto, in data 22/12/2010, il Protocollo di Intesa con il Ministero dell'Interno per il collegamento all'INA,
2. ha installato, configurato ed integrato (in SPICCA) il plug-in da Tor Vergata ed ha concluso, con esito positivo, i test di interoperabilità.

2.3 DATA CENTER REGIONALE

La Regione Campania ha realizzato nel 2011 un moderno Data Center eco-compatibile (Green IT) in grado sia di accogliere tutte le applicazioni informatiche, presenti e future, dell'ente Regione Campania che di ospitare servizi in modalità "cloud computing".

Contestualmente alla realizzazione del nuovo Data Center si è anche effettuato l'ammodernamento delle componenti impiantistiche a supporto (impianto elettrico, gruppo di continuità e impianti di condizionamento ambientale) che ha permesso di assicurare livelli di consumo energetico e livelli di affidabilità conformi alle specifiche internazionali previste per tali strutture

Il *core* IT del Data Center, l'isola Green, è stata sviluppata attraverso le tecnologie di virtualizzazione dei server (basata sulla piattaforma di virtualizzazione VMware vSphere), delle reti (networking a 10 Gb) e dello storage (con soluzioni EMC ed ha una capacità di oltre 100 TB); ciò consente di ospitare e gestire fino a 1000 server virtuali interconnessi e collegati ad Internet alla Intranet Regionale e alla Extranet (SPC) delle Pubbliche Amministrazioni del territorio.

Inoltre è attivo un sistema di gestione centralizzata delle risorse degli utenti attraverso un Active Directory Domain Services 2008.

2.4 SISTEMA INFORMATIVO REGIONALE

Il sistema informativo regionale è composto da applicativi implementati nel corso degli anni in funzione dell'esigenza di informatizzare procedimenti e attività; esso può suddividersi in due grosse categorie di applicativi:

- applicativi di tipo **orizzontale**, utilizzati da tutti i dipendenti di Regione Campania (ad esempio il Sistema Informativo di Gestione e Rilevamento delle Presenze, SIGREP),

¹ Il CISIS è l'organo tecnico della Conferenza delle Regioni e delle Province autonome in materia di sistemi informatici, geografici e statistici ed opera per le singole materie di competenza esclusiva e congiunta

² ICAR (Interoperabilità e Cooperazione Applicativa fra le Regioni) è l'azione interregionale promossa dal CISIS finalizzata al coordinamento dello sviluppo in tutti i territori regionali della cooperazione applicativa secondo le specifiche SPCoop

- applicativi di tipo **verticale**, utilizzati in un determinato ambito amministrativo (ad esempio SisteMA61, per il monitoraggio POR FESR 2007/2013 Obiettivo Operativo 6.1 “Sviluppo Urbano Sostenibile...”).

Gli asset tecnologici (sia hardware che software) che compongono l'intero sistema informativo regionale di Regione Campania devono essere tenuti in debita considerazione nello sviluppo della progettazione e la successiva realizzazione della piattaforma SOA.

La tabella nell'**Allegato PREESISTENZE** elenca i principali applicativi che compongono il Sistema informativo regionale. In tale tabella sono riportati i valori degli indicatori relativi a:

- carichi sul sistema informativo attuale (in termini di accesso degli utenti e di richiesta di spazio di memorizzazione dei dati e di banda impiegata);
- tecnologie utilizzate (piattaforma software, DBMS, standard e framework di sviluppo)

che vanno considerati elementi sostanziali al fine di garantire che la scelta delle componenti tecnologiche della SOA siano idonee al dimensionamento ottimale degli interventi oggetto del presente capitolato e garantiscano.

- l'integrazione con il preesistente sistema informativo,
- l'interoperabilità tra i servizi (sia quelli esistenti che quelli che si andranno ad implementare successivamente).

3 DESCRIZIONE DELLA FORNITURA

3.1 FINALITA'

L'implementazione della piattaforma infrastrutturale regionale per l'attuazione della circolarità anagrafica nell'ambito dell'Obiettivo Strategico regionale denominato SIIR (Sistema Informativo Integrato Regionale) è una delle azioni individuate nella sezione ICT del “Piano di azione per la Ricerca & Sviluppo, l'Innovazione e l'ICT” (approvato con DGR n. 180 del 29/04/2011).

Tale intervento si innesta nella più ampia strategia nazionale di eGovernment e attraverso esso ci si propone di realizzare l'infrastruttura abilitante per:

- garantire l'interoperabilità dei sistemi informativi (regionali e non),
- l'inoltro delle informazioni alle PP.AA. abilitate alla ricezione automatica dei dati di interesse,
- la cooperazione applicativa in sicurezza orientata ai servizi per garantire lo scambio di informazioni anagrafiche certificate.

Stante quanto premesso, le **finalità dell'intervento** da porre in essere sono le seguenti:

1. realizzazione di un'architettura software di tipo Services Oriented Architecture (SOA), finalizzata al riuso e all'integrazione delle applicazioni (esistenti e a realizzarsi) della Regione Campania, anche in ambito SPCoop,
2. promozione di interventi finalizzati allo sviluppo della circolarità anagrafica,
3. creazione di un sistema di Identità Digitale (ID) rivolto ai cittadini della Campania,

3.2 OGGETTO

Oggetto della presente procedura di gara è l'affidamento delle attività di:

1. analisi di dettaglio, progettazione, realizzazione, test, rilascio e messa in esercizio e successive attività di start-up relative a:
 - a. piattaforma software SOA della Regione Campania,
 - b. integrazione della realizzanda SOA con la preesistente piattaforma SPICCA,
 - c. servizio di data hub per la circolarità anagrafica,
 - d. integrazione dei servizi di Identità Digitale e Identità Federata SPICCA,
 - e. esposizione dei servizi di interoperabilità propedeutici alla fruizione dell'Identità Digitale,
 - f. predisposizione di appositi scenari di sperimentazione per l'utilizzo di tale piattaforma,
2. addestramento del personale dell'Amministrazione regionale o dei terzi dalla stessa indicati

3. affiancamento per il subentro, al termine dell'appalto, al soggetto indicato dall'Amministrazione.

Le specifiche tecniche della piattaforma, dei suoi componenti e delle azioni oggetto del presente capitolato sono dettagliate al capitolo 4; le modalità di sviluppo dell'intervento ed i tempi correlati sono riportati ai capp. 5, 6 e 7.

3.3 DURATA

La durata complessiva del progetto dovrà essere pari, al massimo, a ventiquattro (24) mesi con le modalità specificate al successivo capitolo 5 – **Elenco delle attività e tempi**.

4 SPECIFICHE TECNICHE DELL'INTERVENTO

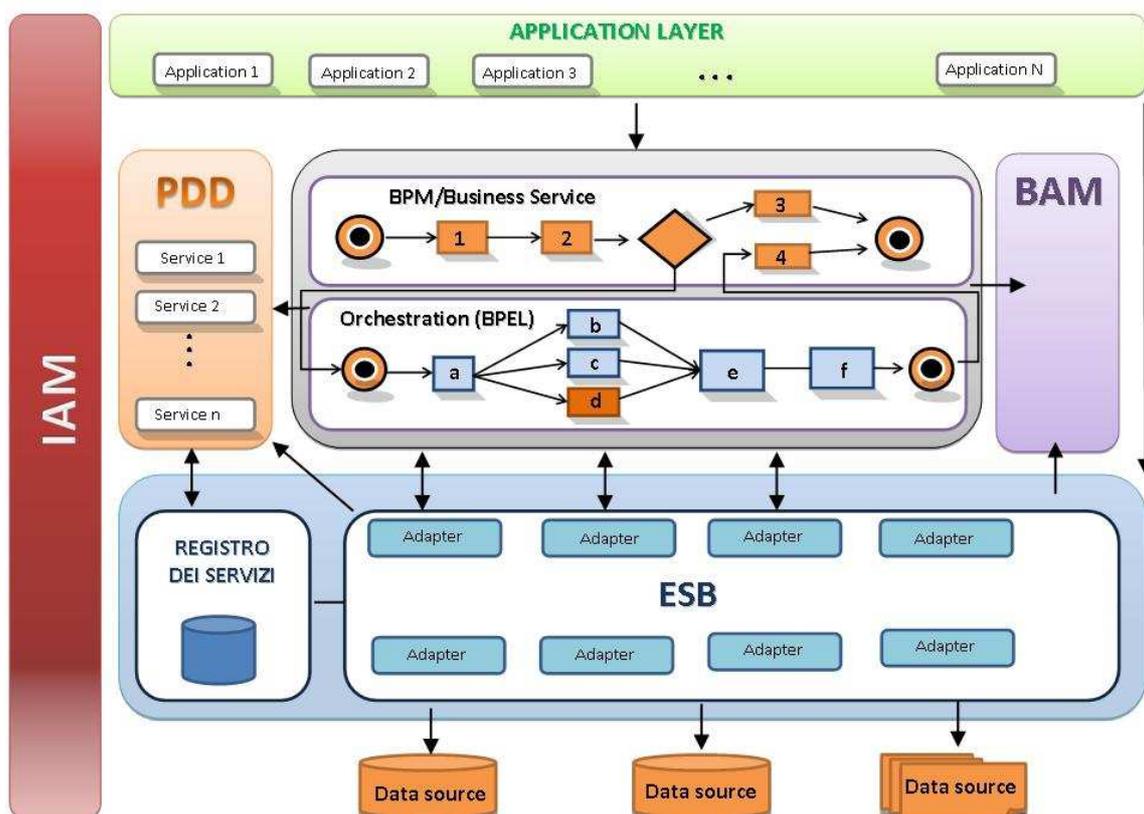
4.1 SERVICE ORIENTED ARCHITECTURE (SOA)

Si richiede la **fornitura e la messa in esercizio di un'architettura software di tipo Services Oriented Architecture (SOA)**; gli elementi essenziali dell'architettura SOA oggetto della fornitura saranno:

- **servizi di ESB** con adattatori per i principali database e sistemi verticali interni (si faccia riferimento al par. 4.1.1 - **ESB (ENTERPRISE SERVICE BUS)**),
- **componenti di governance** (si faccia riferimento al par. 4.1.2 – **SOA Governance**),
- **servizi di orchestrazione e workflow** (si faccia riferimento al par. 4.1.2 – **SOA Governance**),
- **servizi di management & monitoring (BAM)** (si faccia riferimento al par. 4.1.3 – **BAM (Business Activity Monitoring)**),
- sistema **IAM** (si faccia riferimento al par. 4.1.4 – **Sistema IAM**).

Quanto oggetto della fornitura andrà installato interamente sul preesistente hardware in dotazione presso il Data Center regionale (cfr. par. 2.3 - **DATA CENTER REGIONALE**).

Si riporta lo schema di architettura generale e, successivamente, il dettaglio dei componenti sopra elencati.



Il componente Registro dei Servizi ³ andrà ad integrare il preesistente Registro SICA.

Il **Registro SICA** e la **PDD** (Porta di dominio) sono asset regionali (SPICCA) descritti nel par. 2.1 – **Cooperazione applicativa in Campania (SPICCA)**.

Si fa presente che:

- pur non prevedendo, quindi, alcuna fornitura di hardware, **la proposta tecnica dovrà essere corredata anche di una sezione nella quale siano definite l'architettura e il dimensionamento delle risorse necessarie (cpu, ram, storage, network, etc.)** per implementare nel Data Center regionale la soluzione proposta;
- la soluzione offerta per la piattaforma SOA dovrà avere un'architettura modulare e altamente scalabile e flessibile in termini di performance e affidabilità,
- stante il rispetto dei requisiti minimi richiesti, nel processo di selezione della piattaforma infrastrutturale di circolarità anagrafica verranno privilegiate le proposte tecniche che massimizzeranno l'utilizzo di soluzioni a codice sorgente aperto (open source);
- per ciascuna ulteriore requisito proposto (previa presentazione di adeguata documentazione) sarà valutata la caratteristica migliorativa.

Nel seguito si riportano le specifiche di tutti i citati componenti della piattaforma SOA.

4.1.1 ESB (ENTERPRISE SERVICE BUS)

Deve prevedersi la fornitura di un componente ESB che abbia almeno i requisiti minimi elencati nel seguito:

- **composizione di servizi ad accoppiamento debole;**
- **gestione dei messaggi** mediante:
 - routing basato sugli **attributi** del messaggio,
 - **arricchimento** informativo dei messaggi e **trasformazione dei dati** veicolati,
 - **trasformazione del formato** dei dati e dei messaggi, anche mediante IDE,
 - **validazione e normalizzazione** (e.g. XML) del messaggio, anche mediante IDE,
 - **codifica del messaggio** in funzione delle specifiche del servizio, anche mediante IDE,
 - **cifratura del messaggio**, con la possibilità, fra l'altro, di apporre la firma digitale al messaggio o alle sue parti designate e di poterla verificare,
 - il **pattern publish/subscribe** quale modalità di scambio, necessario anche al fine di integrare correttamente la componente Porta di Dominio,
 - supporto per un'**architettura event-driven (EDA)**;
- **gestione delle interruzioni** di servizio a causa di errori e successivo **ripristino con garanzia di transazionalità**;
- presenza di strumenti di gestione avanzata di **integrazione dati** con:
 - interfacciamento a diversi data source anche in modalità transazionale,
 - invocazione di stored procedure/stored function,
 - operazioni transazionali su database eterogenei;
- predisposizione degli **adapter** che garantiscano l'integrazione con gli applicativi facenti capo al sistema informativo regionale;
- supporto per l'**integrazione con LDAP e Active Directory**;
- **indipendenza da application server e/o ambienti di runtime proprietari**;

Elemento migliorativo sarà considerato l'uso di un **framework OSGi** (Open Standard Gateway initiative framework) al fine di gestire automaticamente le dipendenze tra componenti delle applicazioni e controllare il ciclo di vita del codice (configurazione e distribuzione dinamica).

³ Tutta la documentazione tecnica relativa al Registro dei Servizi SPICCA è disponibile al seguente link:
<http://www.innovazione.regione.campania.it/content/cooperazione-applicativa>

4.1.2 SOA GOVERNANCE

Al fine di garantire il controllo effettivo dell'intero ciclo di vita delle attività realizzate in seno alla SOA la fornitura dovrà includere quell'insieme di **funzionalità che permettono il governo dei processi (SOA Governance)** e si compone dei seguenti moduli:

- **Orchestrazione**, per integrare web services di sistemi differenti,
- **Process Management (BPM)**, per la gestione dei processi.

Nella tabella seguente si riporta l'elenco dei **requisiti minimi richiesti** dei diversi componenti della realizzanda SOA Governance regionale, con evidenza degli asset regionali preesistenti per i quali dovrà garantirsi l'integrazione.

Registro dei servizi e repository	Tra gli assets della Regione Campania è già presente il Registro dei Servizi SPICCA (UDDI based) in grado di gestire la pubblicazione dei servizi e il ciclo di vita dell'Accordo di Servizio (vedere specifiche CNIPA/DigitPA). Questo registry espone web service per l'inquiry e per la creazione e cancellazione di un servizio e relativi accordi di servizio nelle sue componenti Specifica e Generale. Il Registry della SOA e gli altri moduli della piattaforma tra cui il BAM e il BPM dovranno essere integrati con il registro SPICCA esistente (ad es. mediante l'elevazione di un web service puro in un web service nella versione SPICCA/SPCOOP).
Orchestrazione e Process Management (BPM)	I moduli di Orchestrazione e Process Management (BPM) dovranno fortemente interagire secondo gli standard di riferimento più accreditati (XML, WSDL, BPEL4WS, WSCI, BPML, BPEL4People, XPDL). Entrambi i moduli dovranno essere strettamente integrati con il modulo BAM per il monitoraggio dei processi e per la gestione del ciclo di vita.
Requisiti del modulo di Orchestrazione	I <u>requisiti minimi</u> del modulo di Orchestrazione sono i seguenti: <ul style="list-style-type: none"> • descrivere il processo in termini di logica del flusso di esecuzione controllato; • controllare i flussi di esecuzione in ogni singola parte; • definire interazioni (scambi di messaggi) ed ordine di esecuzione che vi possono essere fra i servizi web da orchestrare; • invocare i servizi in modalità asincrona; • gestire eccezioni ed integrità delle transazioni; • gestire gli errori e/o la mancata risposta di un servizio invocato; • garantire la separazione della logica del processo dai web service che lo realizzano; • garantire anche l'orchestrazione dei servizi esposti su SPICCA/SPCOOP.
Requisiti del modulo BPM	Il modulo di Business Process Management (BPM) dovrà avere i seguenti <u>requisiti minimi</u> : <ul style="list-style-type: none"> • offrire un'interfaccia grafica per la definizione di processi, stati ed azioni, • permettere l'integrazione con qualsiasi applicazione esterna nel caso di attività svolte da "umani" mediante scambio di dati di contesto di riferimento, • offrire meccanismi di assegnazione di attività per utente/ruolo di business, • supportare "stati di attesa" ed attendere un evento esterno per la riattivazione di un processo, • permettere di fruire di servizi di orchestrazione mediante scambio di dati di contesto di riferimento, • offrire un tool grafico che visualizzi lo stato del processo, • fornire un meccanismo di "task manager" per garantire, agli utenti "umani" coinvolti, uno strumento per accedere alle attività ad essi assegnate. <p>Elemento migliorativo sarà considerato la fornitura di un Motore di regole (Rules engine). Tale componente avrà lo scopo di disaccoppiare fortemente le regole di business (che soprattutto per applicazioni "datate" sono tipicamente "sepolte" nel codice) dal codice applicativo.</p> <p>I principali requisiti che il Rules Engine dovrà implementare sono:</p> <ul style="list-style-type: none"> • repository centralizzato delle regole, • editor visuale (anche non web) per la creazione, modifica, cancellazione, deploy, undeploy di una regola • integrazione con il BAM, • esposizione di un set di API di facile utilizzo per l'integrazione in applicazioni terze tecnologicamente omogenee, • esposizione di Decision Service per l'integrazione anche in applicazioni terze tecnologicamente non omogenee o per l'integrazione in processi WS-BPEL.

4.1.3 BAM (BUSINESS ACTIVITY MONITORING)

Il modulo **Business Activity Monitoring (BAM)** deve consentire agli utenti/operatori autorizzati di acquisire in tempo reale lo stato generale della piattaforma. Dovrà, inoltre, integrarsi completamente con il modulo di BPM (si veda par. 4.1.2) nel tracciare i processi ed effettuare analisi per l'identificazione della causa che porta alla violazione degli SLA.

I requisiti minimi che dovranno essere garantiti dal modulo BAM sono i seguenti:

- **gestione dei log** attraverso interfaccia utente in grado visualizzarli con filtro a livello di servizio, sistema, componente etc;
- **monitoraggio delle risorse del sistema** (cpu, code, thread etc.);
- creazione di **report sulle attività dell'ESB** con dati aggregati sull'esecuzione dei servizi (tempo minimo, massimo medio etc di esecuzione);
- **versioning del deploy** dei servizi con possibilità di ripristino di versioni precedenti;
- **reload a caldo di servizi** senza necessità di riavviare l'engine;
- **monitoraggio delle risorse assegnate al singolo servizio** in modo da poterne definire le modalità di funzionamento rispetto ad altri servizi (es. caching, pooling etc);
- capacità di **aggregazione dei dati e delle informazioni** ottenute dalle varie sorgenti dati in metriche di alto livello (es. media dei tempi di risposta delle transazioni, ecc.);
- definizione delle **soglie di variazioni di misurazione** per la segnalazione attraverso alert e notifiche di vario genere;
- definizione di **KPI** (Key Performance Indicator) personalizzati attraverso l'utilizzo delle metriche definite nel sistema;
- **modifica della configurazione di controllo** di un servizio;
- **integrazione con i componenti** della piattaforma quali ESB, Registry e PDD, **BPM, Orchestrator e IAM** (locale e federato), in particolare integrazione in **modalità Event-Driven con l'ESB**,
- componenti di **monitoraggio** e di **reportistica** (su piattaforma nativa web e facilmente estendibili) mediante **dashboard**; in particolare la parte di reportistica dovrà essere corredata di un **tool** (anche non web) **per il design e il deploy** di nuovi report;
- **definizione delle regole di correlazione tra eventi e generazione di allarmi** (da inviare a destinatari preconfigurati e/o per automatizzare l'innesco di processi correlati) attraverso **motore ad eventi**;
- **presenza di un modulo software integrato con la Porta di Dominio** per la gestione dei livelli di servizio secondo gli standard più accreditati (WSLA, Ws-Agreement,...) e per tracciare sul BAM i tempi ed il livelli di servizio anche dei servizi esposti in cooperazione applicativa.

Per tutti i moduli integrati sarà necessario poter visualizzare lo stato dei diversi processi monitorati.

Elementi migliorativi saranno considerati:

- la gestione del ciclo di vita completo dei servizi per i vari moduli: start, stop, suspend, resume (dove applicabile);
- la capacità del modulo BAM di essere basato su o lavorare con la tecnologia Complex Event Processing (CEP).

4.1.4 SISTEMA IAM

La fornitura prevede la realizzazione di un sistema di **Identity and Access Management (IAM)** al fine di definire un processo di applicazione di policy appropriate per gestire le informazioni riguardanti le identità degli utenti e controllare l'accesso alle risorse informatiche. Dovrà quindi prevedersi la fornitura di un software di gestione di identità, accesso, autenticazione, federazione e servizi correlati.

Il Sistema da realizzare dovrà prevedere:

- il **rispetto delle specifiche di autenticazione** come da documentazione nazionale e regionale (SpCoop, Spicca, DigitPa, Icar), integrandosi con quanto già realizzato (si veda il cap. 2 – Descrizione del contesto e delle preesistenze), conformemente alle specifiche DigitPA - per la Gestione Federata delle Identità Digitali (GFID);

- un sistema per la gestione delle identità digitali e di autenticazione di:
 - utenti di questa Amministrazione,
 - cittadini fruitori dei servizi on-line disponibili,
 - utenti di Enti, federati in ambito regionale, che intendano esporre servizi con un'unica credenziale di autenticazione;
- di garantire, ove possibile, il web Single Sign-On (wSSO) ovvero l'autenticazione unica per le applicazioni web, evitando all'utente il reinserimento della propria credenziale di accesso qualora già collegato;
- la gestione di diversi tipi di credenziali di autenticazione (deboli, forti, riconoscimento tramite carta dei servizi, etc.).

La componente funzionale IAM deve consentire la completa gestione degli accessi e del ciclo di vita delle identità digitali, dal processo di creazione e organizzazione fino all'eliminazione dell'identità digitale. Ogni singolo utente, dipendente o utente esterno, è oggetto di un processo di assegnazione della propria identità digitale.

Le principali macro-funzionalità che il sistema di Identity and Access Management deve garantire sono:

1. Access Control,
2. Identity Administration
3. Provisioning/Deprovisioning;
4. Auditing & Reporting.

La soluzione proposta dovrà presentare specifiche di scalabilità, rispetto degli standard (de jure e de facto), flessibilità, affidabilità, basso impatto per l'utente finale e a livello applicativo.

Nella tabella seguente si riporta l'elenco dei **requisiti minimi richiesti** dei diversi componenti dello IAM, con evidenza degli asset regionali preesistenti per i quali dovrà garantirsi l'integrazione.

Access Control	<p>Devono essere forniti i meccanismi di:</p> <ol style="list-style-type: none"> 1. Autenticazione, prevedendo la possibilità di utilizzare, a seconda dei casi, meccanismi di autenticazione forte (ad es. CNS) e/o debole. 2. Autorizzazione. 3. Single Sign On.
Identity Administration	<p>Deve consentire:</p> <ol style="list-style-type: none"> 1. la gestione del ciclo di vita delle identità; 2. la gestione di gruppi e ruoli (Profilation).
Provisioning & Deprovisioning	<p>Deve consentire:</p> <ol style="list-style-type: none"> 1. la rappresentazione del processo di autorizzazione di una richiesta; 2. la propagazione della richiesta alle strutture e ai responsabili di competenza.
Auditing & Reporting	<p>Deve consentire di</p> <ol style="list-style-type: none"> 1. registrare tutte le transazioni e le attività degli utenti; 2. generare report relativi a tutte le attività di gestione delle identità; 3. visualizzare/generare report per: <ul style="list-style-type: none"> • tutte le fasi delle richieste per i diritti di accesso; • richieste di modifiche dei diritti di accesso; • dettagli sull'accesso degli utenti alle applicazioni. 4. monitorare gli accessi; 5. segnalare in modo automatico la presenza di anomalie e/o falle di sicurezza legate a statistiche di comportamento degli utenti e/o a policy di sicurezza predefinite. <p>Deve anche prevedersi la generazione di un log contenente i dati relativi al controllo degli accessi. Inoltre il sistema deve includere modelli di report che siano facilmente personalizzabili in base alle esigenze di Regione Campania, inclusi i riepiloghi delle attività, delle eccezioni, degli eventi, ecc..</p>

<p>Identity Management (per la gestione del ciclo di vita delle identità)</p>	<p>Deve consentire:</p> <ul style="list-style-type: none"> • la creazione, la modifica, la disabilitazione e la cancellazione degli account attraverso sistemi eterogenei, • il Self Provisioning con innesco di processi autorizzativi basati su workflow che prevedano eventualmente anche l'ausilio di eventuali policy, • la gestione delle identità in accordo con eventuali modelli di amministrazione decentrata, • servizi di password management (update, reset,...), • servizi di auditing e reporting, • possibilità di interoperare mediante WS-* interfacciandosi con altri componenti che supportino l'architettura WS-* utilizzando le specifiche di federazione definite WS-Federation; • possibilità di supportare client passivi e smart, garantendo la comunicazione federata tra ogni tipologia di terminale WS-enabled endpoints, includendo comunicazioni tra server e client passivi, come i browser; • possibilità di estendere l'architettura supportando vari tipi di security-token, inclusa Security Assertion Markup Language (SAML) e autenticazione Kerberos, • separazione tra logica applicativa e sicurezza nei servizi, abilitando così l'interoperabilità sicura tra applicativi ed utenti e consentendo di effettuare autenticazione basata su certificate per multifactor authentication e per siti web basati su SSL.
<p>Access Management (per il controllo degli accessi alle risorse IT, web e non, interne o esterne alla Regione Campania)</p>	<p>Devono essere forniti:</p> <ul style="list-style-type: none"> • strumenti per la verifica centralizzata delle identità degli utenti; • strumenti per la verifica dei privilegi di accesso alle applicazioni o alle funzioni che le compongono (autorizzazione); • Single Sign On (SSO); • federazione delle identità (SSO fra domini di sicurezza diversi e condivisione degli attributi di identità dell'utente); • servizi di auditing e reporting. <p>Ulteriore requisito: il sistema IAM va integrato con il sistema di Identità Federata realizzato nell'ambito del Progetto SPICCA; in tal modo:</p> <ul style="list-style-type: none"> • gli utenti regionali gestiti dallo IAM potranno accedere a <ul style="list-style-type: none"> ○ applicazioni rese disponibili dall'ente regionale; ○ applicazioni rese disponibili in modalità federata da soggetti esterni alla Regione; • gli utenti esterni al dominio Regione Campania potranno accedere ad applicazioni del sistema informativo regionale rese disponibili in modalità federata. <p>Per il soddisfacimento di tale ulteriore requisito si faccia anche riferimento al cap. 4.1.4.1 – Integrazione tra IAM e Identità Federata SPICCA</p>
<p>Requisiti ulteriori</p>	<ol style="list-style-type: none"> 1. Le componenti di Identity and Access Management devono garantire la sincronizzazione, la trasformazione e la distribuzione delle informazioni tra applicazioni, database e servizi di directory al fine di condividere le informazioni dei dati relativi alle diverse identità digitali create. 2. Lo IAM deve garantire l'integrazione con i repository di sicurezza dei prodotti e applicazioni specificati al cap. 2 – Descrizione del contesto e delle preesistenze

4.1.4.1 INTEGRAZIONE TRA IAM E IDENTITÀ FEDERATA SPICCA

L'obiettivo primario del Sistema di Identità Federata è quello di garantire la circolarità all'autenticazione permettendo che l'identità digitale venga riconosciuta da più sistemi interoperanti, in conformità alle ultime

specifiche DigitPA “Modello di Gestione Federata Delle Identità Digitali (GFID)”, versione 1.5.1 del 26/07/2011.

E' quindi richiesta l'integrazione tra la componente IAM della SOA e la componente di Identità federata di SPICCA in maniera tale da:

1. garantire agli utenti regionali l'accesso alle applicazioni esposte da soggetti terzi appartenenti alla federazione SPICCA;
2. controllare gli accessi ai servizi del sistema informativo regionale che si renderanno disponibili in modalità federata ad Enti terzi appartenenti alla federazione SPICCA.

Tale integrazione deve avvenire secondo le seguenti modalità:

<p>Accesso alle applicazioni esposte da soggetti terzi appartenenti alla federazione SPICCA</p>	<p>I componenti dell'Identità Federata genereranno dei Token di autenticazione per gli utenti gestiti dallo IAM; ciò richiede di integrare:</p> <ul style="list-style-type: none"> • il modulo ALD (Autorità Locale di Dominio) dell'Identità Federata SPICCA ⁴, per i servizi di tipo web, • gli opportuni handler della Porta di Dominio (porta delegata), per i servizi di tipo xml-based, • lo IAM, <p>per consentire la creazione delle opportune asserzioni SAML a partire dalle informazioni utente gestite dallo IAM e dai relativi directory utente.</p>
<p>Controllo degli accessi ai servizi del sistema informativo regionale che si renderanno disponibili in modalità federata ad Enti terzi appartenenti alla federazione SPICCA</p>	<p>Garantire per il corretto mapping degli attributi e delle informazioni utente provenienti dalla federazione con attributi interni all'Ente attraverso l'integrazione dei componenti sviluppati per il controllo degli accessi di tipo federato ⁵ e lo IAM. In tal modo la componente di controllo degli accessi relativa all'Identità Federata renderà disponibili allo IAM le informazioni sull'utente che sta provando ad accedere ai servizi interni e lo IAM, in base alle informazioni ricevute ed eventualmente mappate su attributi locali, deciderà se abilitare o meno l'accesso alle risorse.</p>

4.1.4.2 SPERIMENTAZIONE n. 1 – INTEGRAZIONE DELLO IAM CON UN APPLICATIVO REGIONALE

Per verificare la corretta attuazione di tale piattaforma, a titolo di **sperimentazione del modulo IAM**, sarà richiesta l'attuazione dello scenario di integrazione dello IAM con uno dei repository delle credenziali di un applicativo interno preesistente (ad es. SIGREP, CEDEL).

4.1.5 DIMENSIONAMENTO MINIMO DELLA PIATTAFORMA SOA

Ferme restando:

- le richieste caratteristiche di scalabilità per tutti i componenti del sistema,
- le specifiche qualitative e quantitative sulle transazioni (che verranno stabilite, nel corso della Fase A, all'interno del Piano della Qualità),

⁴ Il componente **ALD** (Autorità Locale di Dominio) dell'Identità Federata SPICCA è un asset regionale ed è composto dall'IdP (Identity Provider), dalla PA (Profile Authority) e dalla AA (Attribute Authority) ed i principi e le logiche di funzionamento sono regolate da DigitPA

⁵ I componenti per il controllo degli accessi di tipo federato sono denominati Federation gateway per i servizi di natura web e corrispondono a opportuni moduli della Porta di Dominio per i servizi di natura xml-based.

dovrà essere presentata una soluzione in cui ogni componente della SOA assicuri, quale volume minimo di traffico gestito nella configurazione di base, quello generato dal parco applicativi specificato in Allegato PREESISTENZE.

4.2 DATA HUB REGIONALE PER LA CIRCOLARITÀ ANAGRAFICA E PER L'IDENTITÀ DIGITALE

Uno degli obiettivi dell'intervento è la **realizzazione di un data hub** in grado, da un lato di garantire l'esercizio dei processi afferenti alla circolarità anagrafica (es. servizi INA/SAIA) e dall'altro di fornire servizi informativi elementari sulle informazioni, presenti nell'archivio regionale delle Identità Digitali, basate su dati anagrafici provenienti da fonti eterogenee. In particolare dovranno essere realizzate varie attività distinte collocate a diversi livelli nella architettura SOA da realizzare:

1. realizzazione di un **ID repository** contenente tutte le utenze potenzialmente destinatarie dei servizi applicativi messi a disposizione dal Sistema informativo della Regione Campania e dagli altri enti federati; in aggiunta il data hub deve avere:
 - a. interfacce pubbliche che garantiscano l'interrogazione dell'ID repository,
 - b. modulo per la gestione dei profili utente
 - c. componenti per il monitoraggio delle attività di alimentazione, di accesso e di arricchimento (incrocio) dei dati disponibili, con gestione del disallineamento delle fonti (attraverso un sistema di alert);
2. sperimentazione ai fini sanitari dell'integrazione dei servizi esposti da INA/SAIA.

Tutti gli interventi sono dettagliati nel seguito.

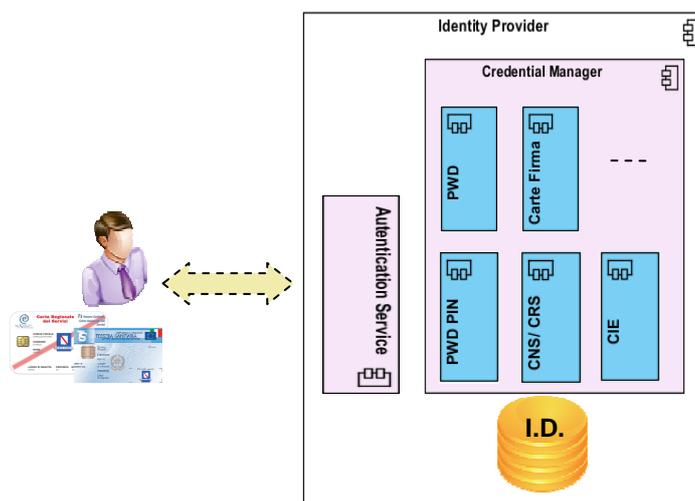
4.2.1 REALIZZAZIONE DI DATA HUB E ID REPOSITORY

La Regione Campania intende offrire un servizio centralizzato di identificazione, predisponendo una base dati per la realizzazione di un sistema di Identità digitale (ID repository) per i cittadini della Regione Campania;

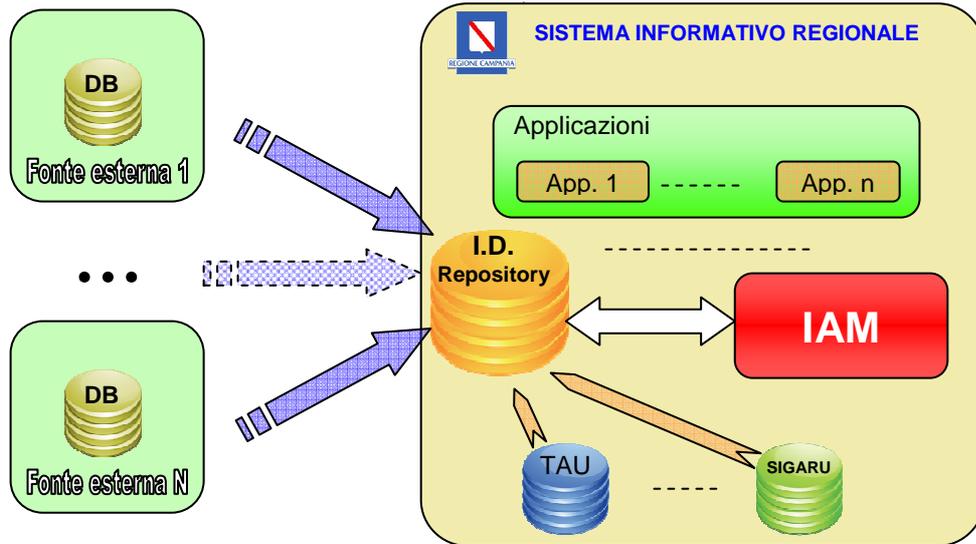
Oggetto della fornitura è la realizzazione di tale repository che:

- verrà utilizzato dallo IAM in ambito SOA;
- verrà alimentato ed aggiornato, a partire da fonti disponibili tracciate, sia per le proprie esigenze interne (statistiche, servizi integrati per i tributi, gestione dei finanziamenti, ecc.) sia per l'intero patrimonio informativo regionale, al fine di evitare la presenza di più fonti dati relative ai dati identificativi dei cittadini non allineate e/o aggiornate.

Lo schema di principio del processo di **autenticazione** è rappresentato nella figura successiva.



La logica di **popolamento del ID repository** è riportata nella figura seguente.



Il dataset minimo dell'ID Repository sarà il seguente:

	Nome	Descrizione
1	Cf	Codice Fiscale
2	Nome	Nome
3	Cognome	Cognome
4	Data di nascita	Data di nascita del titolare della CNS, nel formato YYYYMMDD
5	Luogo di nascita	Luogo di nascita
6	Provincia di nascita	Provincia della città di nascita
7	Sesso	Sesso
8	Residenza	Città di residenza
9	Provincia	Provincia della città di residenza
10	CAP	Codice di avviamento postale del comune di residenza
11	Email	Indirizzi di posta elettronica
12	ASL di appartenenza	Specifica della ASL di appartenenza
13	Tessera sanitaria	Numero di tessera sanitaria
14	Fonte di provenienza	Specifica della fonte di provenienza del dato e della data di

Tale dataset dovrà essere ulteriormente arricchito da parte del Fornitore, a seguito delle risultanze di analisi delle specifiche, di tutte le informazioni:

- necessarie alla gestione di un'anagrafe regionale sanitaria integrata, sulla base delle specifiche normative regionali e nazionali in materia e nel rispetto della privacy,
- relative ad altre specifiche esigenze applicative individuate da questa Amministrazione (es. anagrafe degli studenti universitari, ...).

Dovranno, inoltre, essere forniti i seguenti **strumenti**:

<p>Modulo per la gestione dei profili utente</p>	<p>Il data hub dovrà interagire con la componente Profilation dello IAM, al fine di consentire la definizione e la gestione, in un unico punto, dei profili (e dei relativi attributi) delle utenze presenti in ID repository; tale modulo deve garantire al personale abilitato la gestione anagrafica degli utenti, oltre che dei profili, ed integrarsi con le <i>Authority Registry di altri enti federati</i>, consentendo la creazione del portafoglio delle asserzioni per l'inoltro di una richiesta di servizio ad un service provider.</p>
---	--

<p>Modulo per il monitoraggio</p>	<p>Il data hub dovrà rendere disponibili al personale abilitato degli specifici servizi:</p> <ul style="list-style-type: none"> ○ per verificare lo stato di alimentazione della base dati (ID repository) e la presenza di discordanze (su uno o più campi) su dati provenienti da fonti di popolamento diverse, ○ per estrarre informazioni di natura statistica sulle informazioni presenti in ID repository.
<p>Modulo per l'interrogazione dell'ID repository</p>	<p>Il data hub dovrà rendere disponibili degli specifici servizi:</p> <ul style="list-style-type: none"> ○ che permettano ad ogni ente federato (in SPICCA) di ottenere le informazioni contenute in ID Repository (per dare modo, ad es., ad un ente federato di effettuare una verifica, non bloccante, sulla correttezza dei dati immessi quando un cittadino si accredita al suo sistema informativo); ○ che permettano al cittadino di accedere, anche via CNS, all'ID Repository per visualizzare i propri dati ed integrare, ove previsto, i dati aggiuntivi della propria identità digitale (ad es. email, telefono ecc..).
<p>Modulo per l'autenticazione web multimodale</p>	<p>Il data hub dovrà rendere disponibile un sistema di autenticazione web multimodale, composto di due componenti principali:</p> <ol style="list-style-type: none"> a. un componente server per le funzioni amministrative e la gestione delle diverse modalità di autenticazione, b. un componente client per l'utilizzo dei servizi di autenticazione web, da mettere a disposizione ai gestori di siti istituzionali per l'accesso dei propri utenti. <p>Tale sistema dovrà essere in grado di:</p> <ul style="list-style-type: none"> ○ effettuare la mutua autenticazione delle parti connesse (server e utente) attraverso certificati digitali in formato X.509, ○ garantire, in alternativa, anche modalità di autenticazione debole (con username e password) basati su ID Repository. <p>Il <u>componente client</u> (di cui al punto b) dovrà essere compatibile:</p> <ul style="list-style-type: none"> ○ con tutti i principali Web Server (Apache, Microsoft Internet Information Server,...), ○ con tutti i principali browser attualmente disponibili (Internet Explorer, Firefox, Safari, Chrome, ...). <p>Per il <u>componente client</u> (di cui al punto b) dovrà essere predisposta una configurazione completa e universale e quindi dovranno essere:</p> <ul style="list-style-type: none"> ○ fornite le librerie di funzioni crittografiche di alto livello conformi agli standard CSP per Microsoft e PKCS#11 per i sistemi Mac OS X e Linux, ○ forniti i driver per lettori di smart-card conformi agli standard PC/SC (Token per i sistemi Apple), ○ indicati i lettori di Smart Card supportati, ○ specificate le tipologie di Smart Card supportate, ○ fornite le utility per la gestione, la configurazione e l'utilizzo delle Smart Card degli utenti finali, compatibili almeno con i 3 sistemi operativi Microsoft (XP e successivi), Apple Mac OS X (10.5 e successivi) e Linux, ○ implementare un'area del un sito web istituzionale dell'amministrazione regionale per garantire il supporto agli utenti nelle operazioni di primo accesso, configurazione, cambio/recupero password, ecc.

Vanno poi messe in atto tutte le operazioni propedeutiche al popolamento e alla gestione del ID Repository

- a. procedure (es. script,...) per l'importazione delle basi dati dalle diverse fonti di popolamento,
- b. reportistica per evidenziare le difformità/anomalie presenti,

- c. strumenti e politiche di gestione e correzione delle inconsistenze,
- d. strumenti e politiche di gestione dell'aggiornamento delle informazioni,
- e. politiche di generazione di open-data.

Si rappresenta che la soluzione offerta per il Data hub della circolarità anagrafica dovrà avere un'architettura modulare e altamente scalabile e flessibile in termini di performance e affidabilità.

4.2.2 SPERIMENTAZIONE N. 2 - CIRCOLARITÀ ANAGRAFICA

Facendo seguito a quanto già riportato al par. 2.2 – **Collegamento all'Indice Nazionale delle Anagrafi**, ad oggi, si è conclusa positivamente la verifica della corretta comunicazione tra il CNSD INA-SAIA e la Regione Campania: i dati richiesti transitano attraverso il modulo SS_BKPDD CNSD della Porta di Dominio del CNSD e trasmesse tramite SPC al modulo SS_BKPDD integrato con la Porta di Dominio della Regione. Inoltre, il Ministero degli Interni ha implementato i web services esposti da XML-SAIA Server. Tale CNSD INA-SAIA espone (attraverso XML-SAIA Server) diversi web services, tra i quali:

1. **Servizio di registrazione dei soggetti di competenza** ⁶ (**Invio Competenza Persone**): questo servizio consente di inviare al SAIA una comunicazione di sottoscrizione o cancellazione della sottoscrizione alle comunicazioni riguardanti uno o più cittadini appartenenti alla propria anagrafe sanitaria.
2. **Servizi di Notifica variazione anagrafica (Scarica variazione anagrafica)**: questo servizio consente di ricevere tutte le comunicazioni di interesse relative alle variazioni anagrafiche.
3. **Servizi di Allineamento Anagrafi**: questo servizio consente di inviare al SAIA le richieste **asincrone** di Allineamento Anagrafi inviate dalle ASL verso l'Indice Nazionale delle Anagrafi. Si può verificare lo stato dell'operazione utilizzando il servizio di **verifica dello stato della richiesta**. Si potrà recuperare le informazioni di interesse utilizzando il servizio di **presa in carico delle risposte**.

In tale contesto il ruolo del data hub regionale sarà quello di gestire le variazioni anagrafiche (di provenienza INA-SAIA) per garantire l'aggiornamento delle anagrafi sanitarie regionali; ciò avverrà attraverso l'attuazione delle seguenti azioni:

- A. invocazione del servizio del CNSD di notifica delle variazioni anagrafiche e presa in carico degli esiti,
- B. inoltro delle variazioni ai database delle anagrafi sanitarie ⁷.

Ai fini dell'effettuazione della **sperimentazione** va implementato un ambiente di test attraverso il quale possa simularsi l'accesso, l'importazione e l'aggiornamento di un'anagrafe sanitaria (su tracciati standard quali XML-SAIA AP5) secondo la modalità indicata ai precedenti punti A e B del presente paragrafo.

4.3 START-UP DEL SISTEMA

A seguito della verifica di conformità intermedia (cfr. par 6.7) con esito positivo si effettuerà lo **start-up** di quanto realizzato.

Il Fornitore dovrà presentare il piano di start-up nei modi e nei tempi specificati ai successivi capitoli **5 e 6.3**.

Nel corso di tale fase è previsto il raggiungimento dei seguenti obiettivi:

- o messa in esercizio della piattaforma infrastrutturale di circolarità anagrafica attraverso:
 1. supporto sistemistico, applicativo, tecnico ed operativo per le seguenti attività:
 - o installazioni,
 - o integrazione, tuning e, ove necessario, migrazione nel Data Center regionale,

⁶ Per allineare i dati regionali a quelli dell'INA, preliminarmente all'avvio dei **servizi di notifica variazione anagrafica** tra l'Ente regionale ed CNSD dell'INA, l'Ente deve inviare al CNSD tutti i Codici Fiscali dei soggetti di competenza dell'anagrafe sanitaria (elenco assistiti) secondo le modalità operative e di sicurezza indicate dal Ministero degli Interni; tale invio rappresenta una richiesta di registrazione per ogni singolo soggetto di propria competenza (anche ai fini dell'abilitazione per le successive operazioni di modifica/cancellazione dei dati).

⁷ In base al comune cui fa riferimento il dato anagrafico da allineare, la variazione andrà ad aggiornare il database dell'anagrafe assistibili dell'ASL di diretta competenza.

- configurazione ottimale dell'ambiente di esercizio, al fine di soddisfare i requisiti prestazionali, di scalabilità, di bilanciamento e di affidabilità; tali attività di supporto dovranno riguardare sia la piattaforma di Circolarità anagrafica oggetto della fornitura che la preesistente piattaforma di Cooperazione Applicativa SPICCA,
- 2. importazione dalle diverse fonti di popolamento e successiva bonifica dei dati che andranno a popolare l'ID Repository;
- attività di manutenzione correttiva e adeguativa su quanto realizzato,
- attuazione dello scenario di sperimentazione del sistema IAM (cfr. par. 4.1.4.2),
- attuazione dello scenario di sperimentazione del data hub della circolarità anagrafica (cfr. par. 4.2.2),
- addestramento del personale sull'utilizzo di quanto realizzato,
- predisposizione ed esecuzione del piano di affiancamento e presa in carico di quanto oggetto della presente fornitura al fine di assicurare il subentro, al termine dell'appalto, del personale regionale o di altri soggetti diversamente indicati dall'Amministrazione regionale. Tale attività di affiancamento e presa in carico per il subentro (passaggio di consegne) dovrà avere una durata non inferiore a 2 mesi e sarà attivata dall'Amministrazione in prossimità della data di scadenza del contratto.

Per l'intera durata della fase di start-up, il Fornitore dovrà, inoltre, obbligatoriamente:

- A) provvedere all'adeguamento alle specifiche DigitPA delle componenti della piattaforma di Cooperazione Applicativa SPICCA;
- B) mettere a disposizione dell'Amministrazione regionale una **Piattaforma di gestione delle anomalie (Bug tracking system)** che consenta di:
 - gestire l'intero processo di richiesta di interventi (così come riportato nell'allegato "Service Level Agreement E Penali" ai paragrafi 3.6 e 3.7); a titolo esemplificativo si riportano alcune delle funzionalità richieste:
 - comunicazione delle anomalie con specifica della classe di gravità (da parte dell'Amministrazione),
 - notifica di avvenuta presa in carico (da parte del Fornitore),
 - notifica di avvenuta risoluzione del problema (da parte del Fornitore),
 - riscontro positivo della risoluzione del problema evidenziato (da parte dell'Amministrazione);
 - storicizzare tutte le fasi ed i tempi di presa in carico e risoluzione delle anomalie evidenziate, con possibilità di predisporre apposita reportistica riepilogativa (ai fini delle misure degli SLA contrattuali).

Per le attività di addestramento si evidenzia, inoltre, quanto segue.

Gli interventi di addestramento interesseranno un **gruppo di lavoro** (composto da personale tecnico individuato dall'amministrazione regionale in numero massimo di 14 componenti) che sarà chiamato a garantire la conduzione e il regolare esercizio della piattaforma in fornitura. Pertanto, finalità dell'addestramento sarà garantire che tale personale tecnico possa assicurare, in autonomia:

- l'esercizio di tutti i componenti della piattaforma in fornitura,
- la manutenzione adattativa, correttiva ed evolutiva del sistema installato.

Si fa, inoltre, presente che:

- le sessioni di addestramento dovranno essere erogate, previo accordo con l'Amministrazione regionale, nel periodo contrattuale in maniera anche non continuativa e con pianificazione coerente con i piani di rilascio delle funzionalità della piattaforma;
- le sessioni di addestramento si svolgeranno presso sedi regionali o presso sedi indicate dall'amministrazione ubicate sul territorio regionale;
- dovranno essere forniti tutti i manuali operativi in italiano di quanto oggetto della fornitura.

In aggiunta si dovrà prevedere anche la predisposizione di appositi moduli attraverso i quali, utilizzando strumenti di Web Based Training (WBT) già nelle disponibilità dell'amministrazione regionale, possa garantirsi l'addestramento del personale in modalità e-learning. Tali moduli:

- dovranno essere di tipo 'interattivo' e dovranno essere implementati secondo standard internazionali quali AICC e SCORM, affinché ne sia garantita l'interoperabilità e la portabilità nel tempo.
- andranno strutturati in unità didattiche autoesautive (learning object), finalizzate alla acquisizione di competenze per realizzare uno o più compiti di un ruolo professionale;
- saranno di proprietà di Regione Campania che potrà quindi disporre autonomamente nelle forme e modalità di erogazione e concessione in uso;

- dovranno essere consegnati contestualmente alla comunicazione di “pronti al verifica di conformità intermedia” affinché sia possibile verificarne la completezza e la rispondenza ai contenuti dell’attività di addestramento che verrà successivamente erogata.

La Regione Campania si riserva, comunque, di richiedere eventuali correzioni e/o integrazioni ai contenuti dei moduli laddove si individuino difformità e/o mancanze.

4.3.1 PROFILI PROFESSIONALI RICHIESTI

Si riporta di seguito un **elenco minimale** delle figure professionali e dei relativi profili, richiesti per l’erogazione dei servizi di **start-up** oggetto della fornitura.

Information Systems Project Manager (Capo Progetto)	
Titolo di studio	Laurea in discipline tecnico/informatiche
Esperienze	Anzianità lavorativa di almeno 12 anni, con almeno 4 di provata esperienza lavorativa nella specifica funzione su progetti complessi. E’ particolarmente apprezzata la conoscenza del settore pubblico, preferibilmente nella Pubblica Amministrazione italiana. Almeno 2 anni di provata esperienza di consulenze su temi organizzativi, di controllo di gestione, analisi e progettazione di sistemi informativi, package e procedure complesse nel settore pubblico, con periodi di permanenza continuativa presso lo stesso cliente non inferiori a 6 mesi.
Conoscenze	Possiede approfondite conoscenze ed esperienze di: <ul style="list-style-type: none"> • Metodologie di misura progetti • Metodologie di sviluppo • Tematiche applicative gestionali nell’ambito della Pubblica Amministrazione • Redazione di specifiche di progetto • Controllo realizzazione procedure • Stima di risorse per realizzazione di progetto • Stima di tempi • Analisi di processi • Analisi e progettazione di sistemi informativi e procedure complesse • Conoscenze ed uso di tecniche e prodotti software per project management e risk management • Responsabilità su gruppi di progetto

Business Analyst (Analista Funzionale)	
Titolo di studio	Laurea in discipline tecnico/informatiche
Esperienze	Anzianità lavorativa di almeno 6 anni, di cui 3 come analista. Ha partecipato a progetti di sviluppo presso realtà della Pubblica Amministrazione facendo esperienza nei seguenti ambiti: <ul style="list-style-type: none"> • Redazione di specifiche di progetto • Redazione di modelli dei processi • Controllo realizzazione procedure • Stima di risorse per realizzazione di progetto • Stima di tempi • Coordinamento di gruppi di lavoro • Disegno e progettazione di test
Conoscenze	Nelle esperienze lavorative ha approfondito la conoscenze relativa a: <ul style="list-style-type: none"> • Metodologie di analisi dei processi • Metodologie di analisi e disegno di prodotti SW • Metodologie di analisi e disegno dati • Tecniche di controllo di progetto e di programmazione strutturata • Tecniche di programmazione • Tematiche applicative/ gestionali, preferibilmente in ambito di controllo di gestione di processi relativi alla Pubblica Amministrazione • Caratteristiche e possibilità di riuso dei pacchetti software

Database Manager	
Titolo di studio	Laurea in informatica o in discipline scientifiche oppure Diploma di scuola media superiore più corsi di formazione su tematiche IT
Esperienze	Almeno 6 anni, di cui almeno 3 nella funzione
Conoscenze	<ul style="list-style-type: none"> • Data modeling • Tecniche di disegno di DB applicativi e DB conoscitivi • Tecniche di gestione di dizionari dati aziendali e, più in generale, delle informazioni aziendali • Tecniche di Integrazione di dati provenienti da sistemi diversi • Data quality measurement and assessment • Tecniche di data clearing • Sistemi operativi

IT System Architect	
Titolo di studio	Laurea in Informatica o Ingegneria Informatica
Esperienze	<p>Anzianità lavorativa significativa da 5 a 10 anni come capo progetto. Ha partecipato a progetti di sviluppo presso realtà della Pubblica Amministrazione facendo esperienza nei seguenti ambiti:</p> <ul style="list-style-type: none"> • Redazione di specifiche di progetti distribuiti • Redazione di modelli dei processi e loro orchestrazione • Progettazione e realizzazione di sistemi interoperabili • Stima di risorse e dei tempi per realizzazione di progetto • Coordinamento di gruppi di lavoro
Conoscenze	<p>Nelle esperienze lavorative ha approfondito la conoscenze relativa a:</p> <ul style="list-style-type: none"> • Paradigmi di progettazione architetture orientati alla SOA e relative tecnologie • Metodologie e standard di sicurezza • Soluzioni infrastrutturali per la conduzione dei sistemi in esercizio e delle metodologie di ottimizzazione delle prestazioni • Metodologie per la realizzazione di assessments degli apparati e dei servizi di rete • Capacità di progettare adeguatamente la topologia logica e fisica di rete • Metodologie di analisi dei sistemi SW interoperabili e processi • Tecniche di controllo di progetto • Tematiche infrastrutturali riguardanti la cooperazione applicativa tra Pubbliche Amministrazioni utilizzando le specifiche del modello SPC

Information System Analyst	
Titolo di studio	Laurea in informatica o in discipline scientifiche oppure Diploma di scuola media superiore più corsi di formazione su tematiche IT
Esperienze	<p>Anzianità lavorativa di almeno 4 anni nel settore "Sistemi". Possiede conoscenze ed esperienze di:</p> <ul style="list-style-type: none"> • modelli di erogazione di servizi in ambito pubblico • architetture dei sistemi software, dei sistemi operativi, di DBMS, di linguaggi ed applicativi INTERNET e INTRANET , di prodotti e tecnologie HW/SW presenti sul mercato • problem solving operativo, di orientamento al risultato, di coordinamento di gruppi di lavoro e di integrazione in gruppi compositi; flessibilità nell'utilizzo di tecnologie innovative • assistenza di tipo specialistico sull'utilizzo dei sistemi e sui prodotti/programmi di ausilio al sistema operativo
Conoscenze	<ul style="list-style-type: none"> • Progettazione di dettaglio e conduzione di sistemi operativi complessi o di rete, assicurando il loro aggiornamento periodico • Realizzazione di programmi che interfacciano il sistema operativo di base e/o la sua estensione partecipando all'installazione, configurazione, personalizzazione delle componenti software e hardware di base, di ambiente e di rete • Gestione della configurazione hardware e software di base, tecniche di controllo

	<p>dello stato delle basi dati, utilizzo di strumenti e modalità per assicurare la loro efficienza e protezione</p> <ul style="list-style-type: none"> • Metodologie di verifica funzionale e di benchmarking prestazionali, da applicare a nuovi prodotti e tecnologie, delle problematiche di sicurezza dati e protezione archivi • Metodologie e tecniche relative alla sicurezza informatica
--	--

Le competenze ed esperienze professionali del personale coinvolto nella fase di start-up nonché la tipologia stessa dei profili professionali richiesti, sono da considerarsi **requisiti minimi**; in sede di proposta tecnica, il Fornitore potrà proporre figure professionali con competenze ed esperienze migliorative rispetto a quelle precedentemente indicate nonché ulteriori profili professionali specifici, quali fattori premianti in sede di valutazione dell'offerta (cfr. Disciplinare di gara, art.8 Procedura di gara e criteri di aggiudicazione).

Il Fornitore garantisce che tutte le risorse umane che impiegherà per l'erogazione dei servizi di start-up oggetto della fornitura, anche in caso di integrazioni e/o sostituzioni, saranno in possesso delle competenze minime elencate nella descrizione dei profili professionali precedentemente riportati oppure, laddove migliorative, delle competenze indicate, per ognuno dei profili professionali, dal Fornitore stesso in sede di proposta tecnica.

Si specifica inoltre che:

- i curriculum vitae del personale da impiegare in tali fasi dovranno essere:
 - presentati a Regione Campania ed inclusi nella documentazione di gara (Busta B – Proposta tecnica) a corredo del documento PROPOSTA TECNICA,
 - compilati secondo il template dell'Allegato "Curriculum vitae" al Disciplinare di Gara;
- i profili delle figure descritte, non sono da considerarsi esaustivi delle esigenze della fornitura in quanto Regione Campania potrà richiedere in corso di esecuzione del Contratto competenze specifiche in relazione ad ulteriori tematiche, prodotti, sistemi e metodologie;
- per il personale ritenuto inadeguato, qualunque sia il ruolo ed il servizio impiegato, Regione Campania potrà richiederne formalmente la sostituzione.

5 ELENCO DELLE ATTIVITÀ E TEMPI

La realizzazione dell'intervento avverrà attraverso la definizione di specifiche fasi ed attività riportate nel seguito.

A. Pianificazione generale della fornitura: fase successiva alla stipula del contratto finalizzata alla definizione del cronoprogramma dell'intervento e alla predisposizione della documentazione di qualità e sicurezza. Nel corso di tale fase il Fornitore sarà chiamato a predisporre la seguente documentazione

- **Piano di lavoro generale**
- **Piano della qualità**
- **Piano di sicurezza informatica**

redatti sulla base delle specifiche del par. 6.3, nei quali si definiscono le attività da svolgere, le relative tempificazioni e modalità esecutive, il processo di verifica dei risultati e la governance dell'intervento; tali documenti verranno anche utilizzati durante l'evoluzione dell'intervento per monitorarne lo svolgimento e al fine di verificare il raggiungimento degli obiettivi prefissati (sia intermedi che finali). Il Fornitore dovrà consegnare all'Amministrazione regionale la citata documentazione di fase entro 15 giorni lavorativi dalla data di stipula del contratto. L'approvazione di tutta la documentazione da parte dell'Amministrazione regionale concluderà tale fase e darà avvio a quella successiva.

B. Realizzazione ed installazione della piattaforma infrastrutturale di circolarità anagrafica: comprende le attività di progettazione, sviluppo e integrazione ai fini della realizzazione di quanto definito nella fase Pianificazione della Fornitura per il rilascio della piattaforma infrastrutturale di Circolarità Anagrafica sia nelle singole componenti che nella sua totalità. Nel corso di tale fase verranno effettuate le seguenti attività:

- B.1 Analisi e progettazione e sviluppo della piattaforma infrastrutturale di circolarità anagrafica.
- B.2 Integrazione di quanto realizzato per il rilascio della piattaforma infrastrutturale di cooperazione applicativa.
- B.3 Predisposizione degli scenari di sperimentazione.
- B.4 Predisposizione del piano di start-up.

Al termine delle attività di cui alle fasi A e B, si avvierà la **verifica di conformità intermedia** (cfr. paragrafo 6.7.1) volta ad attestare, ai sensi dell'art. 312 del DPR 207/2010, la conformità dell'infrastruttura di Circolarità Anagrafica, nel suo complesso e nelle sue componenti, ai requisiti funzionali, tecnici, architetture e di qualità. Si rappresenta inoltre che, stante la necessità e l'urgenza di garantire la messa a disposizione del Sistema informativo della Regione Campania di alcune componenti strategiche oggetto della presente fornitura, **il rilascio della piattaforma SOA e dello IAM (Obiettivo n. 1 di cui al par. 6.4.1) dovrà avvenire entro e non oltre 8 mesi dall'avvio della Fase B.**

- C. Start-up del sistema: messa in esercizio della piattaforma infrastrutturale di circolarità anagrafica, addestramento, attuazione degli scenari di sperimentazione e passaggio di consegne.** Tale fase prende avvio a seguito della verifica di conformità intermedia con esito positivo; nel corso di tale fase verranno effettuate le attività specificate al par. 4.3.

Al termine delle attività di cui alla fase C, si avvierà la **verifica di conformità finale** (cfr. paragrafo 6.7.2) volta ad attestare, ai sensi dell'art. 312 del DPR 207/2010, la conformità della fornitura nel suo complesso e nelle sue componenti, ai requisiti funzionali, tecnici, architetture e di qualità.

La **durata complessiva del progetto** dovrà essere pari, al massimo, a **24 (ventiquattro) mesi**, dei quali:

- **16 (sedici) mesi**, al massimo, dovranno essere impiegati per completare le **fasi A - B**
- **8 (otto) mesi** saranno impiegati per completare la **fase C**.

Il diagramma di Gantt dell'intervento è allegato al presente Capitolato (**Allegato DIAGRAMMA DI GANTT**).

6 MODALITÀ DI SVOLGIMENTO DEL CONTRATTO

6.1 DIREZIONE DELL'ESECUZIONE DEL CONTRATTO

La Direzione dell'esecuzione del Contratto verrà effettuata da apposita Commissione, nominata dall'Amministrazione Regionale, che sarà chiamata a gestire il processo di sviluppo dell'intero intervento e tutte le attività di seguito indicate.

Ai fini del monitoraggio e della verifica dei risultati raggiunti, in termini di efficacia, efficienza e qualità delle prestazioni dei servizi erogati, compreso l'attività di vigilanza sull'esecuzione del contratto, l'Amministrazione regionale nominerà all'uopo un'apposita Commissione, composta da dipendenti regionali, a cui sarà demandata la Direzione dell'esecuzione del Contratto a norma dell'art. 300 del regolamento n. 207/2010. Sarà compito della Direzione dell'esecuzione del Contratto:

- definire in modo dettagliato le modalità e i criteri per la direzione ed esecuzione del contratto,
- approvare i piani di lavoro generale e di ciascun obiettivo (validando, ove necessario, le scelte tecniche ed architetture per l'implementazione della infrastruttura),
- approvare i piani di qualità e di sicurezza informatica,
- verificare in itinere lo stato di avanzamento delle attività affinché sia coerente con la documentazione di progetto approvata,
- gestire le attività afferenti il ciclo di vita degli obiettivi della fornitura,
- certificare la conformità, sia intermedia che finale, di tutto quanto è oggetto della fornitura,
- coordinare e gestire la fase di start-up..

6.2 COMUNICAZIONI

Ogni comunicazione relativa allo svolgimento del Contratto dovrà essere formalmente indirizzata ai referenti dell'ente regionale (RUP e Direzione dell'esecuzione del Contratto). Ogni consegna dei supporti ottici/elettronici (cd, dvd, ecc.) di fornitura va effettuata accompagnandola da una comunicazione scritta alla succitata Direzione dell'esecuzione del Contratto (lettera di consegna, di cui il supporto ottico contenente il materiale di consegna è l'allegato).

6.3 PIANIFICAZIONE DELLE ATTIVITA'

Il Fornitore dovrà produrre e mantenere costantemente aggiornata la pianificazione di tutte le attività, consegnando la seguente documentazione, secondo le modalità e nei tempi indicati nel seguito del presente Capitolato:

- I. **n. 1 Piano di Lavoro generale**, comprensivo della pianificazione dell'intera fornitura;
- II. **n. 1 Piano della Qualità**;
- III. **n. 1 Piano di sicurezza informatica**;
- IV. **n. 4 Piani di Lavoro di obiettivo**, uno per ciascuno degli obiettivi indicati al paragrafo 6.4.1.

Ognuno dei suddetti documenti di pianificazione della fornitura dovrà essere approvato formalmente dalla Direzione dell'esecuzione del Contratto e non è prevista approvazione per tacito assenso.

Dopo la prima approvazione, sarà cura del Fornitore comunicare proattivamente e con la massima tempestività qualsiasi criticità, ritardo o impedimento che modifichino i piani concordati e ad inviare una proposta di ripianificazione delle attività, aggiornando e riconsegnando a Regione Campania la relativa documentazione nelle modalità specificate nel presente Capitolato. La documentazione così aggiornata dovrà essere formalmente approvata dalla Direzione dell'esecuzione del Contratto.

In nessun caso la pianificazione delle attività potrà essere rimodulata dal Fornitore in seguito ad uno o più rilievi da parte della Direzione dell'esecuzione del Contratto.

Una volta approvata dall'Amministrazione, la documentazione di pianificazione (comprensiva delle eventuali modifiche) certifica ai fini contrattuali gli obblighi formalmente assunti dal Fornitore, e accettati da Regione Campania, su stime e tempi di esecuzione delle attività e sulle relative date di consegna dei prodotti (scadenze).

Con riferimento ai **documenti di cui ai precedenti punti I – III** (di cui alla fase A, Pianificazione generale della fornitura, al par. 5), il Fornitore dovrà consegnare all'Amministrazione regionale detta documentazione entro 15 giorni lavorativi dalla data di stipula del contratto. Tale documentazione dovrà essere approvata da parte della Direzione dell'esecuzione del Contratto per dare avvio alla fase B (Realizzazione ed installazione della piattaforma infrastrutturale di circolarità anagrafica) dell'intervento.

Relativamente ai **documenti di cui al precedente punto IV**, si faccia riferimento al par. 6.4.1.

Il Fornitore dovrà, inoltre, predisporre e consegnare alla Direzione dell'esecuzione del Contratto (con periodicità, al massimo, quadrimestrale) apposite relazioni sullo stato delle attività, contenenti almeno:

- la descrizione e lo stato di avanzamento delle attività svolte/in corso di svolgimento,
- task effettuati, deliverable rilasciati e percentuale di raggiungimento degli obiettivi attesi.

Tutta la documentazione dovrà essere consegnata dal Fornitore sia in formato cartaceo che su supporti magnetici e/o ottici.

6.3.1 PIANO DI LAVORO GENERALE

Il Piano di Lavoro Generale è volto a descrivere la pianificazione delle attività di carattere generale, in particolare dovrà includere, almeno:

- le modalità organizzative dell'intervento,
- il cronoprogramma delle attività con il dettaglio delle date di avvio di ogni singolo obiettivo,
- il peso percentuale di ogni singolo obiettivo rispetto all'intero progetto, sulla base delle gg/uu impiegate per la realizzazione dello stesso,
- il numero di giornate uomo, totali e suddivise per singolo obiettivo, necessarie alla realizzazione del progetto.

Il Fornitore dovrà, inoltre, predisporre un format di Relazione sullo stato delle attività (di cui al paragrafo precedente).

6.3.2 PIANO DELLA QUALITÀ

La qualità della fornitura dovrà essere assicurata dal Fornitore rispettando:

1. i requisiti minimi delle metriche di qualità previsti per la fornitura elencati all'Allegato "Service Level Agreement E Penali" del presente documento,
2. i requisiti delle metriche di qualità espressamente previsti dal Fornitore nella propria proposta tecnica, laddove migliorativi rispetto a quelli indicati nell'Allegato "Service Level Agreement E Penali" del presente documento
3. i criteri di qualità del proprio processo specificati nel Piano della Qualità.

Il Fornitore deve assicurare la qualità di tutti i servizi erogati nell'ambito del presente Capitolato, attraverso la predisposizione di specifiche funzioni di verifica, validazione, riesame, assicurazione qualità sui prodotti e sui processi, che si devono basare su standard riconosciuti.

Il Piano della Qualità proposto dovrà indicare:

- metodologie a garanzia della qualità del progetto;
- metodologie e procedure per la realizzazione e gestione del progetto;
- procedure di gestione e misurazione delle metriche di qualità previste per la fornitura nell'allegato "Service Level Agreement E Penali" o di quelle migliorative previste in sede di proposta tecnica;
- specifica degli indicatori temporali per la misurazione delle metriche sulle transazioni della piattaforma SOA nell'allegato "Service Level Agreement E Penali";
- gestione della configurazione (configuration management);
- identificazione dei controlli (test, review, verifiche, validazioni) che il Fornitore intende svolgere internamente per assicurare la qualità della fornitura e relativi piani;
- specifiche responsabilità riguardo ai controlli da svolgere e riguardo alla gestione della configurazione e delle non conformità.

6.3.3 PIANO DI SICUREZZA INFORMATICA

Per gli aspetti di sicurezza il Fornitore dovrà riferirsi alla disciplina vigente all'atto della messa in esercizio della piattaforma di Circolarità anagrafica; in tale documento, partendo da un'analisi dettagliata dei rischi sulla sicurezza, saranno definite tutte le misure necessarie per realizzare un sistema adeguatamente protetto.

Il piano di sicurezza informatica:

- sarà realizzato a partire da un assessment preliminare della sicurezza delle reti e dei sistemi correnti,
- sarà un input per la progettazione architeturale al fine di realizzare un sistema che sia garantito dal punto di vista della sicurezza.

Il documento dovrà contenere almeno:

- la valutazione dei rischi,
- la gestione dei rischi,
- le politiche di gestione e monitoraggio della sicurezza applicata alla realizzazione del sistema,
- il piano degli interventi strutturali da compiere sulla sicurezza in termini fisici, tecnologici, architetture ed organizzativi.

6.3.4 PIANI DI LAVORO DI OBIETTIVO

La fornitura è stata suddivisa in n. 4 obiettivi, come indicato al par. 6.4.1.

Per ogni obiettivo specificato al par. 6.4.1, il Fornitore dovrà predisporre un Piano di Lavoro di Obiettivo, volto a descrivere la pianificazione specifica delle attività di ognuno di esso.

Ciascun obiettivo sarà suddiviso in una o più fasi, in funzione della complessità dell'obiettivo e dello specifico ciclo di vita assegnato. In particolare il Piano di Lavoro di Obiettivo dovrà indicare e descrivere almeno le fasi riportate rispettivamente nelle tabelle dei successivi paragrafi, 6.4.1.1 (per gli obiettivi progettuali a corpo), oppure 6.4.1.2 (per gli obiettivi di sviluppo software).

Infine, fermo restando le specifiche di cui al par. 4.3, nel **Piano di Obiettivo di start-up**, dovranno essere anche definiti:

- gli interventi e le attività che caratterizzano lo start-up,
- i ruoli e le procedure necessari per la completa ed autonoma gestione dell'intero sistema fornito,
- le modalità organizzative delle sessioni di addestramento finalizzato al trasferimento del know-how al gruppo di lavoro,
- le modalità organizzative ed operative del passaggio di consegne,
- quantità e tipologia di figure professionali coinvolte nello start-up del sistema, nell'affiancamento per il subentro e nell'addestramento del gruppo di lavoro.

6.4 ESECUZIONE DELLA FORNITURA

6.4.1 OBIETTIVI E CLASSI DI FORNITURA

Tutto quanto oggetto della fornitura, descritto in dettaglio al cap. 4, viene scomposto in Obiettivi, distinti e specifici, al fine di garantire il governo ottimale della fornitura.

Per ciascuno degli obiettivi il Fornitore dovrà predisporre il Piano di Lavoro di Obiettivo, che andrà approvato dalla Direzione dell'esecuzione del Contratto. Ciascun obiettivo è suddiviso in più fasi, in funzione della complessità dell'obiettivo e del ciclo di vita associato.

Nella tabella successiva si specificano n. **4 Obiettivi** del progetto che sono associati ad una specifica classe di fornitura, in base alle caratteristiche degli stessi. Con la dizione "Classe di fornitura" si definisce l'insieme di attività omologhe che possono essere gestite con la stessa modalità.

Nel caso specifico si individuano n. 2 distinte classi di fornitura:

1. Progettuale a corpo,
2. Sviluppo di componenti software.

La modalità di gestione di tali classi definisce il ciclo di vita dell'obiettivo, come dettagliato nei successivi paragrafi 6.4.1.1 e 6.4.1.2.

La colonna *Riferimenti* della tabella indica il paragrafo del seguente Capitolato speciale che contiene i requisiti minimi degli specifici obiettivi. La colonna *Termine di consegna*, inoltre, riporta il termine di consegna di ognuno dei Piani di Lavoro di Obiettivo.

	Obiettivi	Classe di fornitura	Riferimenti	Termine di consegna del Piano
1	<ul style="list-style-type: none"> • Implementazione della piattaforma SOA • Realizzazione di un sistema IAM 	Progettuale a corpo	Par. 4.1	Entro <u>10 gg. lavorativi</u> dall'approvazione del Piano di Lavoro generale
2	<ul style="list-style-type: none"> • Integrazione IAM e Identità Federata SPICCA • Realizzazione dello scenario di sperimentazione n. 1: integrazione dello IAM con applicativo regionale 	Sviluppo componenti software	Par. 4.1.4.1 Par. 4.1.4.2	
3	<ul style="list-style-type: none"> • Realizzazione del data hub per la Circolarità Anagrafica e per l'Identità Digitale • Realizzazione dello scenario di sperimentazione n. 2: Circolarità Anagrafica 	Sviluppo componenti software	Par. 4.2 Par. 4.2.2	Almeno <u>15 gg. lavorativi</u> prima della data fissata per l'avvio del corrispondente obiettivo nel Piano di Lavoro generale
4	Start-Up	Progettuale a corpo	Par. 4.3	

6.4.1.1 CICLO DI VITA DEGLI OBIETTIVI PROGETTUALI A CORPO

Nella tabella che segue si descrive il **ciclo di vita** da prendersi a riferimento per le **attività progettuali a corpo** che saranno a carico del Fornitore.

Il Piano di Lavoro di Obiettivo dovrà indicare almeno le fasi riportate nella tabella seguente alle quali corrispondono altrettanti atti che formalizzano lo stato di avanzamento dell'obiettivo. L'approvazione formale del Piano di Lavoro di Obiettivo da parte della Direzione dell'esecuzione del Contratto costituisce atto di avvio delle attività previste nel ciclo (che viene gestito come descritto nel paragrafo successivo 6.5.1).

	Fasi	Prodotti di fase	Chiusura Attività (a carico della Direzione dell'esecuzione del Contratto)
Gestione obiettivo: stima, pianificazione, qualità, review, risk management, consuntivazione	Definizione	Specifica dei requisiti utente	Attivazione ⁸
		Piano della qualità dell'obiettivo ⁹	
	Realizzazione	Prodotti e servizi oggetto della fornitura: <ul style="list-style-type: none"> intermedi (di fase), finali. 	Accettazione
	Verifica e validazione	Lista componenti software rilasciati	Approvazione per l'avvio in esercizio
		Documentazione tecnica	
		Piano di integrazione sistemistica	
		Piano di verifica di: <ul style="list-style-type: none"> componenti software rilasciati integrazione sistemistica documentazione 	
	Manuali d'uso e gestione dei prodotti forniti		
	Rapporto conclusivo sugli indicatori di qualità di obiettivo		
Consegna e messa in esercizio		Verifica di conformità dell'obiettivo	

6.4.1.2 CICLO DI VITA DEGLI OBIETTIVI SVILUPPO DI COMPONENTI SOFTWARE

Nella tabella che segue si descrive il **ciclo di vita** da prendersi a riferimento per le **obiettivi di sviluppo di componenti software** che saranno a carico del Fornitore.

Il Piano di Lavoro di Obiettivo dovrà indicare almeno le fasi riportate nella tabella seguente alle quali corrispondono altrettanti atti che formalizzano lo stato di avanzamento dell'obiettivo. L'approvazione formale del Piano di Lavoro di Obiettivo da parte della Direzione dell'esecuzione del Contratto costituisce atto di avvio delle attività previste nel ciclo (che viene gestito come descritto nei paragrafi 6.5.2 e 6.5.3).

	Fasi	Prodotti di fase	Chiusura attività (a carico della Direzione dell'esecuzione del Contratto)
	Definizione	Specifica dei requisiti utente	Attivazione ¹⁰
		Piano della qualità dell'obiettivo ¹¹	
		Stima di conteggio dei FP ¹²	

⁸ L'Attivazione include l'approvazione dei prodotti dell'attività

⁹ Il Piano della Qualità dell'obiettivo viene richiesto solo nei casi in cui l'obiettivo ha caratteristiche specifiche e va in deroga al Piano della Qualità già approvato .

¹⁰ L'Attivazione include l'approvazione dei prodotti dell'attività

Gestione obiettivo: stima, pianificazione, qualità, review, risk management, consuntivazione	Analisi e Disegno	Specifiche dell'intervento: ○ Requisiti funzionali ○ Architettura software ○ Progetto di dettaglio	Approvazione
		Piano di test: ○ del sistema, ○ di integrazione, ○ dei moduli software	
		Documentazione dati	
		Prototipo ¹³	
		Conteggio FP – Modulo per conteggio	
		Altri documenti (eventuali)	
	Realizzazione	Prodotto software in formato sorgente e librerie (Codice sorgente)	Accettazione
		Piano di test	
		Documentazione utente	
		Documentazione delle procedure batch/DTS	
		Manuale di gestione applicativo	
		Conteggio FP – Modulo per conteggio	
		Lista Oggetti Software	
		Report sulla qualità del software	
		Altri documenti	
Piano di adeguamento degli ambienti			
Test: ○ del sistema, ○ di integrazione, ○ dei moduli software			
Verifica e validazione	Rapporto conclusivo sugli indicatori di qualità di obiettivo	Approvazione	
Consegna e messa in esercizio		Verifica di conformità dell'obiettivo	

6.4.2 LUOGO DI LAVORO ED AMBIENTI PER LE VERIFICHE DI CONFORMITA' E MESSA IN ESERCIZIO

L'Amministrazione rende disponibili al Fornitore gli ambienti per le verifiche di conformità e l'esercizio (produzione) dei servizi oggetto della Fornitura garantendone disponibilità ed adeguato dimensionamento rispetto ai requisiti richiesti.

Il luogo di esecuzione principale della fornitura è presso il CED Regionale sito in via Don Bosco 9/E – Napoli. Presso la sede suddetta dovranno essere svolte obbligatoriamente le seguenti attività/servizi, seppur in una lista non esaustiva:

- incontri con tecnici di Regione Campania;
- incontri con la Direzione dell'esecuzione del Contratto e con il Responsabile Unico del Procedimento;
- consegna prodotti;
- verifiche di conformità e test di certificazione (lì dove richiesto);
- start-up;
- addestramento del Gruppo di Lavoro preposto alla conduzione del sistema,
- affiancamento al soggetto indicato dall'Amministrazione per il passaggio di consegne.

¹¹ Il Piano della Qualità dell'obiettivo viene richiesto solo nei casi in cui l'obiettivo ha caratteristiche specifiche e va in deroga al Piano della Qualità.

¹² Il calcolo della stima in FP va effettuato secondo le metodologie e le tecniche riportate nel manuale IFPUG versione 4.2 o successiva.

¹³ Laddove tecnicamente opportuno ed in ogni caso su richiesta di Regione Campania.

Regione Campania metterà a disposizione, in modalità gratuita e non esclusiva, locali idonei ad accogliere gruppi di lavoro, dotati della normale attrezzatura d'ufficio e cablati per il collegamento alle rete LAN dell'Amministrazione.

Il Fornitore è tenuto ad attrezzare a proprie spese tali posti di lavoro del necessario corredo di strumenti Hardware e Software (anche software di base, dei programmi antivirus e tutti gli strumenti software necessari all'esecuzione dei servizi contrattuali).

6.5 GESTIONE DELLA FORNITURA

Nella fase di verifica e validazione che precede l'avvio in esercizio del prodotto di fase, Regione Campania procederà all'approvazione dei prodotti e ne darà comunicazione al Fornitore, con gli effetti previsti dal contratto.

Nel caso di mancata chiusura di una qualsiasi delle fasi previste nel ciclo di vita a causa di non accettazione/attivazione/approvazione da parte della Direzione dell'esecuzione del Contratto, il Fornitore sarà tenuto, senza alcun onere aggiuntivo, a riconsegnare i prodotti della fase in oggetto, modificati sulla base dei rilievi sollevati, fermo restando l'applicazione di eventuali penali come previsto nell'allegato "Service Level Agreement E Penali".

6.5.1 GESTIONE DEGLI OBIETTIVI A CORPO

Gli obiettivi ricadenti nella classe di fornitura Progettuale a corpo verranno gestiti nel rispetto delle fasi scandite, nel piano di progetto, dai rispettivi Piani di lavoro di obiettivo redatti dal Fornitore secondo le indicazioni del **par. 6.4.1.1.**

6.5.2 GESTIONE DEGLI OBIETTIVI DI SVILUPPO SOFTWARE

Gli obiettivi ricadenti nella classe di fornitura *Sviluppo di componenti software* dovranno essere:

- redatti dal Fornitore,
- riportati nel Piano di lavoro di Obiettivo nella schematizzazione indicata al precedente par. 6.4.1.2.
- gestiti nel rispetto delle fasi indicate nel Piano di lavoro di Obiettivo.

Le attività su ogni specifico obiettivo di sviluppo software a carico del Fornitore dovranno svolgersi in aderenza a quanto previsto dal Ciclo di Sviluppo adottato per la presente fornitura (cfr. par. 6.4.1.2).

Nel caso l'iniziativa abbia poi seguito, l'impegno relativo alla fase di Definizione sarà riassorbito nei costi dell'Obiettivo.

Al termine della fase di Definizione, Regione Campania, in considerazione della stima dell'obiettivo in FP proposta dal Fornitore, potrà procedere all'attivazione delle fasi successive finalizzate al raggiungimento dell'obiettivo e ne darà comunicazione al Fornitore, con gli effetti operativi e contrattuali che ne conseguiranno.

Il **dimensionamento di ciascuno degli Obiettivi di Sviluppo Software**, effettuato in fase di Definizione, costituirà un riferimento fisso ai fini della fatturazione, indipendentemente dall'effettivo consumo di risorse a cui il Fornitore potrà andare incontro in corso d'opera. Solo in casi eccezionali, a fronte di eventi impreveduti di forza maggiore, tale valore potrà essere riconsiderato, previa approvazione da parte di Regione Campania.

6.5.3 RIDEFINIZIONE DEGLI OBIETTIVI DI SVILUPPO SOFTWARE

La Regione Campania si riserva la possibilità di **variare, sia in termini di potenziamento che di riduzione, nonché di cancellare specifici Obiettivi di Sviluppo software** in ragione di mutate esigenze (previa comunicazione formale al Fornitore).

Nel caso di **cancellazione** per cause non direttamente imputabili al Fornitore:

1. prima dell'avvio delle attività, nulla verrà riconosciuto al Fornitore in merito alla realizzazione dell'obiettivo cancellato;

2. nel corso delle attività previste dal relativo ciclo di vita, al Fornitore verrà riconosciuto un corrispettivo pari all'impegno massimo impiegato per effettuare le fasi già completate al momento della cancellazione, così come riportato nella tabella di seguito nella colonna "avanzamento cumulativo".

Fase	Impegno	Avanzamento cumulativo
Definizione	10%	10%
Analisi	25%	35%
Disegno	15%	50%
Realizzazione	40%	90%
Consegna e messa in esercizio	10%	100%

Nel caso in cui tale cancellazione sia motivata, invece, da eccezioni da parte di Regione Campania di mancato adempimento contrattuale da parte del Fornitore, nulla verrà riconosciuto allo stesso in merito alla realizzazione dell'obiettivo cancellato.

Le economie derivanti da **cancellazione** di obiettivo, saranno convertite dal Fornitore in Function Point in base al valore indicato dallo stesso in sede di presentazione della proposta tecnica; tali Function Point potranno essere destinati, a discrezione dell'Amministrazione, per il **potenziamento** di specifici obiettivi già previsti o per la **creazione** di nuovi obiettivi, con il conseguente avvio di un nuovo ciclo di sviluppo software secondo lo schema e le modalità di gestione già descritte.

La ridefinizione degli obiettivi, in ogni caso, **non potrà ripercuotersi sulle dimensioni del progetto, sia in termini economici che di Function Point spendibili.**

Il Fornitore non potrà esigere il pagamento del corrispettivo:

1. della quota parte di obiettivi di sviluppo software non realizzati (a seguito, ad es. di cancellazione senza ridefinizione),
2. dei Function Point non utilizzati.

6.6 CONSUNTIVAZIONE DELLE ATTIVITA'

La consuntivazione delle attività svolte dovrà essere predisposta dal Fornitore, con cadenza al più quadrimestrale, aggiornando la **sezione Stato Avanzamento Lavori di ciascun Piano di Lavoro (Generale e di Obiettivi)** relativamente a ciascuna area applicativa e ciascun servizio: in tale ambito il Fornitore deve evidenziare le fasi chiuse, riportando gli eventuali scostamenti rispetto alla pianificazione concordata.

Il Fornitore dovrà mantenere aggiornato lo stato di avanzamento dei lavori relativamente ai Piani di Lavoro approvati, fornendo tempestivamente indicazioni sulle attività concluse ed in corso, esplicitandone la percentuale di avanzamento, su eventuali rischi/criticità/ritardi, su eventuali impatti dei rischi/criticità, su azioni di recupero e razionali dello scostamento, sulle attività in servizio esteso ed in reperibilità.

6.7 VERIFICHE DI CONFORMITA'

Le operazioni di verifica di conformità verranno effettuate secondo quanto previsto da:

- Decreto legislativo. n. 163/2006 – Codice dei contratti pubblici relativi a lavori, servizi e forniture;
- D.P.R 5 ottobre 2010 n. 207 - Regolamento di esecuzione ed attuazione del decreto legislativo 12 aprile 2006 n. 163.

Le Verifiche di conformità sono volte all'accertamento dell'effettiva rispondenza a quanto richiesto dal disciplinare di gara e dal presente capitolato speciale, nonché a quanto previsto dalla proposta tecnica e dalle specifiche tecniche e funzionali che verranno preparate dal Fornitore nel corso dell'esecuzione dell'appalto e approvate dalla Direzione dell'esecuzione del Contratto.

L'Amministrazione regionale monitorerà, per tutta la durata del contratto, il regolare funzionamento di quanto realizzato, nel rispetto dei livelli di servizio (SLA) contrattualmente previsti.

Attiene al Fornitore la responsabilità su quanto da esso sviluppato, sui prodotti di terze parti (anche se previsto un servizio di intervento da parte del produttore del software), nonché sulle estensioni, e parametrizzazioni.

Tutte le componenti della soluzione realizzata verranno verificate dalla Direzione dell'esecuzione del Contratto.

6.7.1 VERIFICA DI CONFORMITÀ DELL'OBIETTIVO

Ciascuno dei cicli di vita contemplati per gli obiettivi della fornitura (cfr. paragrafi 6.4.1.1 e 6.4.1.2) prevede come ultima fase la verifica di conformità dell'obiettivo. Tale verifica sarà effettuata nel rispetto delle norme richiamate al precedente paragrafo e avrà lo scopo di accertare la rispondenza di quanto specificato nel Piano di Lavoro di Obiettivo consegnato dal Fornitore¹⁴.

La verifica riguarderà, a seconda della classe di fornitura, componenti software rilasciati, integrazione sistemistica, documentazione e livelli di servizio previsti all'Allegato "Service Level Agreement E Penali" del presente documento.

Si precisa che tale verifica è subordinata all'esito positivo di ciascuna delle fasi precedenti dello specifico ciclo di vita dell'obiettivo.

6.7.2 VERIFICA DI CONFORMITÀ INTERMEDIA

La verifica intermedia comporta la verifica di conformità del sistema realizzato nella sua globalità. Tale verifica va fatta obbligatoriamente prima dello start-up ed è propedeutica al suo avvio.

Al termine delle attività di cui alle fasi A e B (di cui al cap. 5), il Fornitore farà formale comunicazione all'Amministrazione regionale di "Pronti alla Verifica intermedia".

Prima dell'avvio delle operazioni di verifica intermedia, è fatto obbligo al Fornitore di predisporre il Piano di Test del Sistema di circolarità anagrafica (es. test di integrazione dei componenti, test di stress dell'intero sistema, ecc.) e proporlo per l'approvazione alla Direzione dell'esecuzione del Contratto che ha facoltà di modificarlo ovvero integrarlo con ulteriori prove anche in corso di verifica.

Si precisa che l'avvio della fase di verifica intermedia è subordinata:

- alla conclusione positiva delle verifiche di conformità degli obiettivi 1, 2 e 3 (cfr. par. 6.4.1),
- alla consegna all'Amministrazione, in formato cartaceo ed elettronico, di tutti i manuali e la relativa documentazione, sia tecnica che operativa, che servirà al corretto uso del sistema in tutti i suoi aspetti, articolazioni e componenti,
- all'accettazione del citato Piano di Test del Sistema di Circolarità anagrafica.

Il Fornitore dovrà provvedere all'esecuzione di ogni eventuale intervento correttivo prescritto e necessario al superamento della verifica intermedia, secondo la tempistica indicata dall'Amministrazione e senza oneri aggiuntivi.

Il Fornitore deve fornire e predisporre tutti gli strumenti di automazione necessari per l'esecuzione dei test e per la valutazione dei risultati da parte della Direzione dell'esecuzione del Contratto.

Il Fornitore deve altresì garantire il presidio e l'assistenza sistemistica e applicativa necessaria all'effettuazione della verifica e all'analisi e risoluzione di eventuali anomalie riscontrate. Il Fornitore è tenuto a risolvere nel più breve tempo possibile ogni anomalia riscontrata.

La verifica intermedia prevede altresì:

- la verifica sistemistica di tutte le componenti tecnologiche annoverate nel progetto;
- la verifica applicativa del sistema e verifica della corretta predisposizione degli scenari di sperimentazione;
- l'accertamento della corrispondenza tra i dati risultanti dalla contabilità, i documenti giustificativi e le risultanze di fatto.

La verifica si considererà conclusa positivamente quando tutte le attività previste nel Piano di Test del Sistema di Circolarità anagrafica si saranno concluse con esito positivo.

Al termine della verifica, verrà redatto dalla Direzione dell'esecuzione del Contratto e controfirmato dalle parti ai sensi dell'art. 319 del D.P.R. 5 ottobre 2010 n. 207:

1. il **Certificato di conformità intermedia**,

¹⁴ Si dovrà accertare la corrispondenza anche del Piano della Qualità di Obiettivo nel caso in cui esso sia stato richiesto, in deroga al Piano della Qualità già approvato, date le caratteristiche specifiche dell'obiettivo stesso.

2. il **Rapporto di verifica intermedia** (quale allegato al Certificato) in cui sono tracciate le attività svolte durante la verifica stessa; nel caso di esito positivo, verrà anche fissata la data di “pronto per l'uso” del sistema e dell'avvio della fase di start-up.

La presenza di anomalie che, a giudizio della Direzione dell'esecuzione del Contratto, per gravità o numerosità, non consentano lo svolgimento o la prosecuzione delle attività di verifica provocherà la sospensione della verifica stessa. I nuovi termini di inizio e fine verifica decorreranno dalla consegna della versione corretta dei prodotti.

La rimozione delle eventuali anomalie riscontrate durante la fase di verifica è assoggettata ai livelli di servizio previsti all'Allegato “Service Level Agreement E Penali” del presente documento.

6.7.3 VERIFICA DI CONFORMITÀ FINALE

A seguito della verifica di conformità con esito positivo dell'Obiettivo 4 (Start-Up), la Direzione dell'esecuzione del Contratto redigerà, ai sensi dell'art. 319 del D.P.R 5 ottobre 2010 n. 207:

1. il **Certificato di conformità finale** (controfirmato dalle parti),
2. il **Rapporto di verifica finale** (allegato al certificato) in cui sono tracciate tutte le attività svolte nel corso dell'intera fornitura.

La presenza di anomalie che, a giudizio della Direzione dell'esecuzione del Contratto, per gravità o numerosità, non consentano lo svolgimento o la prosecuzione delle attività di verifica provocherà la sospensione della verifica stessa. I nuovi termini di inizio e fine verifica decorreranno dalla consegna della versione corretta dei prodotti.

La rimozione delle eventuali anomalie riscontrate durante la fase di verifica è assoggettata ai livelli di servizio previsti all'Allegato “Service Level Agreement E Penali” del presente documento.

In aggiunta, si precisa che, prima della verifica finale, il Fornitore dovrà consegnare all'Amministrazione la baseline di calcolo dei FP del software sviluppato (in base alle regole dell'IFPUG v.4.2), necessaria per il successivo passaggio di consegne al soggetto incaricato della gestione del sistema informatico regionale.

6.7.4 STANDARD DELLA DOCUMENTAZIONE FORNITA

Tutta la documentazione fornita all'Amministrazione regionale dovrà essere realizzata in forma documentale in formato OASIS “Open Document Format For Office Applications” (.odt) e/o PDF/A-1a (.pdf).

I modelli ed i diagrammi dovranno essere conformi allo Unified Modeling Language (UML) nella sua ultima versione, utilizzando il set di diagrammi adeguato per rappresentare sia gli aspetti strutturali (sia a livello logico che di deployment) che comportamentali (behavior) del sistema complessivo e dei componenti. I modelli dovranno essere rilasciati anche in formato XMI (OMG Xml Metadata Interchange 2.1 o superiore) e tramite l'eventuale formato proprietario dello strumento di modellazione concordato all'inizio del progetto. Per la rappresentazione dei processi sarà utilizzato lo standard BPMN nella sua ultima versione.

Il sorgente del codice sviluppato *ad hoc* dovrà essere scritto a regola d'arte ed adeguatamente formattato e commentato.

La qualità della documentazione fornita è valutata mediante apposito indicatore di qualità (cfr. Allegato “Service Level Agreement E Penali”).

6.8 RILIEVI E PENALI

I rilievi sono le azioni di avvertimento da parte di Regione Campania conseguenti il non rispetto delle indicazioni contenute nella documentazione contrattuale (Contratto, Disciplinare, Capitolato e suoi allegati, Offerta, Piano di Lavoro Generale, Piano di Lavoro di Obiettivo e Piano della Qualità).

Quindi possono essere emessi rilievi oltre che per i casi contemplati in Allegato “Service Level Agreement E Penali” anche per qualunque altra non conformità ai dettami contenuti nella documentazione contrattuale e tutti i suoi allegati.

Essi consistono di comunicazioni formali al Fornitore che non prevedono di per sé l'applicazione di penali, ma costituiscono un avvertimento sugli aspetti critici della fornitura e, se reiterate e accumulate, possono dar adito a penali, secondo quanto previsto in Allegato “Service Level Agreement E Penali” nonché ad altri meccanismi sanzionatori così come determinato nel Contratto.

I rilievi possono venire emessi dalla Direzione dell'esecuzione del Contratto di Regione Campania, dai responsabili di progetto e/o di servizio di Regione Campania e/o da strutture di Regione Campania preposte o di supporto al controllo e/o monitoraggio della fornitura e sono formalizzati attraverso una nota di rilievo. Si sottolinea che ai fini della rilevazione degli indicatori di qualità i rilievi verranno riferiti e conteggiati a livello di obiettivo, area applicativa e di fornitura.

Qualora il Fornitore ritenga di procedere alla richiesta di annullamento del rilievo dovrà sottoporre a Regione Campania un documento con elementi oggettivi ed opportune argomentazioni entro 3 giorni lavorativi dall'emissione della nota di rilievo. Trascorso tale termine il rilievo non è più annullabile.

6.9 GARANZIA

Il Fornitore dovrà garantire un **periodo di garanzia** su quanto implementato di almeno **24 mesi**, a decorrere dalla **data di verifica di conformità finale** con esito positivo da parte dell'amministrazione. Durante tale periodo, lo stesso è tenuto tempestivamente, senza alcun onere aggiuntivo, a garantire la correzione dei difetti su tutto il software sviluppato e/o modificato. Si precisa che saranno a carico del Fornitore, nel citato periodo di garanzia, tutti gli oneri derivanti dal ripristino della funzionalità dell'intero sistema dovuto a cause imputabili a difetti di quanto oggetto di fornitura.

7 INDICATORI DI QUALITÀ E LIVELLI DI SERVIZIO

Il profilo di qualità richiesto dalla fornitura e gli indicatori di qualità, nonché le relative modalità di calcolo, sono descritti in Allegato "Service Level Agreement E Penali".

Nel caso in cui il Fornitore produca, in sede di offerta, degli indicatori di qualità aggiuntivi rispetto a quelli previsti e/o modalità di calcolo e/o valori di soglia migliorativi di quelli richiesti da Regione Campania, tale nuovo profilo di qualità sarà assunto come base di riferimento per il Piano della Qualità.

Le modalità di calcolo e gli algoritmi applicati per i singoli indicatori di qualità dovranno essere indicati nel Piano di Qualità proposto dal Fornitore ed approvato da Regione Campania.

Il Fornitore può proporre un'eventuale soluzione informatica per il monitoraggio degli indicatori di qualità del servizio e strumenti di inquiry ad uso della committenza per la consultazione di tali dati.

Il Fornitore è tenuto a rendicontare i risultati della misurazione di tutti gli indicatori di qualità per tutta la durata contrattuale attraverso report consegnati contestualmente alla consuntivazione delle attività come da par. 6.6, nonché nella fase precedente la chiusura di ogni obiettivo come indicato in ciascun ciclo di vita (cfr. 6.4.1.1 e 6.4.1.2).

Si precisa che il mancato rispetto dei livelli di servizio previsti nel Piano della Qualità genererà le azioni contrattuali descritte nell'Allegato "Service Level Agreement E Penali".

7.1 REVISIONE DEGLI INDICATORI DI QUALITÀ

Durante l'intero periodo contrattuale ciascun indicatore di qualità potrà essere riesaminato su richiesta di Regione Campania; il riesame potrà derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del Contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli indicatori di qualità che sono risultate non sufficientemente efficaci.

8 INADEMPIMENTI

Fermo restante quando già riportato al capitolo 6, l'Amministrazione regionale si riserva il diritto di verificare in ogni momento l'esatto adempimento da parte del Fornitore di tutte le attività specificate nel Capitolato Speciale d'Appalto, quali obbligazioni essenziali.

In caso di mancato rispetto dei termini contrattuali e/o delle modalità di espletamento dell'appalto, fatti salvi i casi di forza maggiore o i fatti imputabili direttamente a Regione Campania, la stessa provvederà ad applicare specifiche penali commisurate all'entità dell'inadempimento e/o del ritardo, come determinate nell'allegato "Service Level Agreement E Penali" con la modalità specificata al paragrafo 6.8. L'applicazione delle penali non pregiudicherà, in ogni caso, il diritto da parte dell'Amministrazione regionale ad ottenere la prestazione dei servizi secondo quanto previsto dal Contratto d'appalto stipulato tra le parti, fatto salvo il

risarcimento del danno, compreso il danno all'immagine. La Regione Campania si riserva di applicare le predette penali attraverso corrispondente decurtazione degli importi dovuti a titolo di corrispettivo dell'appalto, oppure mediante escussione parziale della cauzione definitiva. Resta inteso che il pagamento delle penali non pregiudicherà il diritto per la Regione Campania di richiedere il risarcimento di eventuali danni subiti. L'applicazione di tutte le penali di cui al presente articolo, avverrà secondo la disciplina civilistica. A seguito dell'applicazione di penali per un importo superiore a 20.000,00 (ventimila/00) euro semestrali, la Regione Campania, ritenendo ciò lesivo e pregiudizievole per il buon andamento del rapporto negoziale, oltre che della propria immagine, si riserva la facoltà di risolvere il contratto ai sensi dell'art. 1456 del Codice Civile, dandone comunicazione al Fornitore mediante lettera raccomandata con avviso di ricevimento e/o a mezzo P.E.C. ed incamerando l'intero importo della cauzione, salvo il diritto al risarcimento del maggior danno.

9 RESPONSABILE OPERATIVO DELL'APPALTO PER IL FORNITORE

Al fine di seguire, controllare e coordinare le attività di realizzazione della fornitura, prima dell'inizio delle attività il legale rappresentante del Fornitore nominerà mediante comunicazione scritta all'Amministrazione, il Responsabile operativo dell'appalto, il quale avrà specifico mandato di rappresentare ed impegnare il Fornitore per tutte le attività inerenti la fornitura.

Il Responsabile operativo sarà l'unico interlocutore e referente della Direzione dell'esecuzione del Contratto per tutti gli aspetti relativi alla presente fornitura.

Il Fornitore potrà sostituire il proprio responsabile, dandone comunicazione scritta alla Direzione dell'esecuzione del Contratto prima della sostituzione, senza potere, per questo, invocare una sospensione dei termini per la fornitura.

10 VARIANTI

Durante la fase di definizione contrattuale e/o in fase di esecuzione dell'appalto, l'Amministrazione si riserva la possibilità di richiedere varianti finalizzate al miglioramento funzionale e prestazionale delle implementazioni previste, ovvero ad adeguare l'erogazione dei servizi in funzione del migliore raggiungimento degli obiettivi indicati nel presente Capitolato.

Le varianti potranno essere, altresì, volte ad accogliere soluzioni tecniche suggerite dall'avvento di nuove tecnologie e dovranno essere equivalenti o migliorative sotto il profilo tecnico e/o economico per l'Amministrazione e consentire il soddisfacimento degli obiettivi dell'appalto.

Le soluzioni proposte dal Fornitore per varianti richieste dovranno comunque essere approvate dalla Direzione dell'esecuzione del Contratto. Nel caso in cui le varianti si dovessero rendere necessarie per la correzione di errori, trascuratezza o mancata attenzione da parte del Fornitore circa la definizione della propria offerta, tali varianti, se necessarie a garantire il rispetto delle condizioni contrattuali, dovranno essere obbligatoriamente eseguite senza ulteriori oneri per l'Amministrazione ed a totale carico del Fornitore.

Resta salva la disciplina di cui al combinato disposto degli artt. 114 e 132 del D. Lgs. 163/06.

11 CORRISPETTIVI

Il corrispettivo della fornitura è pari al prezzo offerto in gara dal Fornitore. Durante il periodo di vigenza contrattuale sono esclusi ulteriori oneri per l'Amministrazione oltre quelli indicati nell'offerta. Nel corrispettivo così calcolato si intendono pertanto compresi tutti gli oneri relativi all'esecuzione del Contratto, tutto incluso e nulla escluso.

Tutti gli obblighi ed oneri derivanti al Fornitore dall'esecuzione del Contratto e dall'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti autorità, sono compresi nel corrispettivo contrattuale.

I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore di ogni relativo rischio e/o alea.

Il Fornitore non potrà vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.

I corrispettivi sono da intendersi al netto di IVA.

12 ESECUZIONE IN DANNO

Nel caso in cui il Fornitore non provveda agli interventi richiesti nei termini e con le modalità di cui ai precedenti articoli, l'Amministrazione potrà procedere ad affidare gli interventi ad altra Ditta con spesa a carico del Fornitore. La spesa relativa sarà liquidata dall'Amministrazione e successivamente detratta dall'importo dovuto al Fornitore all'atto del primo pagamento utile o anche dalla garanzia definitiva.

In caso di fallimento del Fornitore o di grave inadempienza del medesimo l'Amministrazione si riserva di ricorrere alla procedura di cui all'art. 140 del D. Lgs. n. 163/06.

13 OBBLIGHI A CARICO DEL FORNITORE

Il Fornitore, ai fini dell'affidamento del servizio, si obbliga a:

1. garantire l'esecuzione delle attività previste dall'incarico in stretto contatto con le competenti Strutture della Regione Campania, secondo il Piano di Lavoro Generale e i Piani di Lavoro degli Obiettivi;
2. segnalare immediatamente tutte quelle circostanze e fatti che, rilevati nell'espletamento del proprio compito, possano pregiudicare il regolare svolgimento dei servizi;
3. sollevare l'Amministrazione da qualunque azione intentata da terzi, per mancato adempimento degli obblighi contrattuali, per trascuratezza o per colpa nell'adempimento dei medesimi;
4. effettuare il servizio impiegando, a propria cura e spese, tutte le strutture ed il personale necessario per la realizzazione degli stessi secondo quanto precisato nel presente capitolato;
5. nell'adempimento delle proprie prestazioni ed obbligazioni, osservare tutte le indicazioni operative, di indirizzo e di controllo che a tale scopo saranno predisposte e comunicate dall'Amministrazione;
6. comunicare tempestivamente all'Amministrazione le eventuali variazioni della propria struttura organizzativa coinvolta nell'esecuzione dell'appalto, indicando analiticamente le variazioni intervenute ed i nominativi dei nuovi responsabili;
7. non creare conflitti d'interesse nello svolgimento delle attività da realizzare.

14 OBBLIGAZIONI DERIVANTI DAL RAPPORTO DI LAVORO

Il Fornitore si obbliga ad ottemperare a tutti gli impegni verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, previdenza e disciplina infortunistica, assumendo a proprio carico tutti gli oneri relativi.

Il Fornitore si obbliga altresì ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, le condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro applicabili, alla data della stipulazione del contratto, alla categoria e nelle località di svolgimento delle attività, nonché le condizioni risultanti da successive modifiche ed integrazioni.

Il Fornitore si obbliga altresì, fatto in ogni caso salvo il trattamento di miglior favore per il dipendente, a continuare ad applicare i suindicati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione.

Gli obblighi relativi ai contratti collettivi nazionali di lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui questo non aderisca alle associazioni stipulanti o receda da esse per tutto il periodo di validità del contratto.

15 RESPONSABILITÀ CIVILE

Il Fornitore assume in proprio ogni responsabilità per infortuni o danni eventualmente subiti da parte di persone o di beni, tanto dello stesso Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

Nessun ulteriore onere potrà dunque derivare a carico dell'Amministrazione oltre al pagamento del corrispettivo contrattuale.

16 SICUREZZA

L'impresa è obbligata ad osservare scrupolosamente tutte le norme antinfortunistiche vigenti ed a farle osservare al proprio personale che, in conformità alle vigenti disposizioni di legge in materia (ex D.Lgs. 81/2008), doterà, inoltre, di tutto quanto necessario per la prevenzione degli infortuni.

17 OBBLIGHI DI RISERVATEZZA

Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del Contratto.

L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del presente Contratto.

L'obbligo di cui al comma 1 non concerne i dati che siano o divengano di pubblico dominio.

Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di riservatezza anzidetti.

In caso di inosservanza degli obblighi di riservatezza, l'Amministrazione ha la facoltà di dichiarare risolto di diritto il presente Contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare alla stessa.

Il Fornitore potrà citare i termini essenziali del presente Contratto, nei casi in cui fosse condizione necessaria per la partecipazione del Fornitore stesso a gare e appalti.

Il Fornitore si impegna, altresì, a rispettare quanto previsto dal D.Lgs 196/2003 in materia di trattamento dei dati personali.

18 TRATTAMENTO DEI DATI

Per la esecuzione del servizio descritto dal presente capitolato, con riferimento ai dati ed alle informazioni fornite dal Fornitore alla Stazione appaltante, anche sotto forma documentale, e che rientrano nell'ambito di applicazione del d.lgs.n.196/2003 (Codice in materia di protezione dei dati personali), si precisa quanto segue:

Finalità del trattamento: In relazione alle finalità del trattamento dei dati forniti si precisa che i dati comunicati vengono acquisiti ai fini della esecuzione delle prestazioni disciplinate nel presente capitolato e, in particolare, ai fini della esecuzione delle prestazioni contrattuali nonché in adempimento di precisi obblighi di legge, compresi gli adempimenti contabili ed il pagamento del corrispettivo contrattuale;

Dati sensibili: I dati forniti dal Fornitore non rientrano tra i dati classificabili come "sensibili";

Modalità del trattamento dei dati: Il trattamento dei dati verrà effettuato in modo da garantire la sicurezza e la riservatezza e potrà essere attuato mediante strumenti manuali, informatici e telematici idonei a memorizzarli, gestirli e trasmetterli. Tali dati potranno essere anche abbinati a quelli di altri soggetti in base a criteri qualitativi, quantitativi e temporali di volta in volta individuati.

Categorie di soggetti ai quali i dati possono essere comunicati: I dati potranno essere comunicati a: soggetti esterni, nell'ambito dello svolgimento delle funzioni e dei compiti svolti dall'Ufficio, Dipartimento della Funzione Pubblica, Ministero dell'Economia e delle Finanze, altri concorrenti che facciano richiesta di accesso ai documenti di gara nei limiti consentiti ai sensi della Legge n. 241/1990, consiglieri regionali;

Diritti del Fornitore: Relativamente ai suddetti dati, al Fornitore, in qualità di interessato, vengono riconosciuti i diritti di cui al citato decreto legislativo. Acquisite le suddette informazioni con la sottoscrizione del contratto ed eventualmente nella fase di esecuzione dello stesso, egli acconsente espressamente al trattamento dei dati personali secondo le modalità indicate precedentemente.

Si precisa, altresì, che la Stazione appaltante dovrà utilizzare tutti i dati di cui verrà a conoscenza per soli fini istituzionali, assicurando la protezione e la riservatezza delle informazioni secondo la vigente normativa.

19 MANLEVA, BREVETTI E DIRITTI D'AUTORE

L'Amministrazione non assume alcuna responsabilità nel caso in cui il Fornitore abbia usato, nell'esecuzione del servizio, dispositivi o soluzioni tecniche di cui altri abbiano ottenuto la privativa.

Il Fornitore, pertanto, si assume ogni responsabilità nei confronti dei terzi per l'uso di programmi informatici, dispositivi, brevetti, attrezzature o per l'adozione di soluzioni tecniche o di altra natura che violino brevetti o diritti d'autore, sollevandone espressamente l'Amministrazione. Il Fornitore assume l'obbligo di tenere indenne l'Amministrazione appaltante da ogni pretesa da chiunque azionata, nonché da tutti i costi, le spese o responsabilità relativi, ivi comprese le spese legali eventualmente conseguenti, per la violazione di diritti d'autore, di marchio o brevetto, comunque connessi alle prestazioni contrattuali.

Ciascuna parte si obbliga a dare immediato avviso all'altra di qualsiasi azione di rivendicazione o questione di terzi, di cui al precedente comma, qualora ne sia venuto a conoscenza.

Il Fornitore, nel caso in cui riceva comunicazione scritta di qualsiasi azione o rivendicazione per la quale essa stessa sia tenuta a lasciare indenne l'Amministrazione, deve garantire, senza limitazione alcuna e a proprie spese, l'Amministrazione contro tali azioni o rivendicazioni e pagherà i costi, i danni e gli onorari degli avvocati posti a carico dell'Amministrazione in qualsiasi di tali azioni o rivendicazioni, fermo restando che il Fornitore avrà il diritto di essere sentito circa l'eventualità di tali azioni o rivendicazioni.

L'Amministrazione può svolgere, a spese del Fornitore, tutti i passi che potranno essere ragionevolmente richiesti dalla stessa in relazione a tali transazioni o difese.

20 PROPRIETA'

Tutte le eventuali licenze software richieste o comunque previste nella fornitura dovranno:

- o essere sempre di tipologia perpetua,
- o garantire l'assistenza e l'upgrade del software all'ultima versione per una durata di 24 mesi a partire dalla certificazione di Conformità Finale della Direzione dell'esecuzione del Contratto.

Le componenti del sistema non soggette a licenza (componenti software sviluppate ad hoc, configurazioni, basi dati, loro contenuto informativo, basi di conoscenza, manualistica, ecc.), al termine del contratto, resteranno di proprietà, anche intellettuale, dell'Amministrazione Regionale.

Si richiede al Fornitore di specificare nell'Offerta Economica (Sezione Licenze) l'eventuale costo annuale di assistenza e upgrade all'ultima versione delle licenze previste nella fornitura. Tale costo:

- o va indicato solo ai fini della definizione, da parte di questa Amministrazione, dei costi di esercizio della piattaforma,
- o non sarà oggetto di valutazione in fase di aggiudicazione della gara.

Tutta la documentazione prodotta, in formato cartaceo e elettronico, dovrà essere consegnata all'Amministrazione e rimarrà di proprietà della stessa.

Qualunque opera od elaborato prodotto dal Fornitore nell'espletamento del presente incarico rimane di proprietà piena ed esclusiva della Regione Campania, la quale si riserva ogni diritto e facoltà in ordine alla loro utilizzazione, incluso la cessione in riuso, nonché ad ogni eventuale modifica ritenuta opportuna a suo insindacabile giudizio.

È fatto divieto al Fornitore di utilizzare i risultati dell'attività oggetto del presente appalto per proprie pubblicazioni, ovvero fornirli a terzi senza la preventiva autorizzazione scritta della Regione Campania.

Al termine del servizio e, per richiesta, anche in corso d'opera, i materiali multimediali (fotografici, editoriali e audiovisivi), e quant'altro realizzato nell'ambito della produzione del servizio dovranno essere consegnati alla Regione Campania.

21 DIVIETO DI CESSIONE DEL CONTRATTO E CESSIONE DEL CREDITO

E' fatto assoluto divieto al Fornitore di cedere, a qualsiasi titolo, il contratto a pena di nullità della cessione medesima.

L'impresa può cedere a terzi i crediti derivanti alla stessa dal presente contratto, ma tale cessione è subordinata all'accettazione espressa da parte dell'Ente.

La cessione di azienda e gli atti di trasformazione, fusione e scissione relativi al Fornitore non hanno singolarmente effetto nei confronti delle Amministrazioni contraenti fino a che il cessionario, ovvero il

soggetto risultante dall'avvenuta trasformazione, fusione o scissione, non abbia comunicato all'Amministrazione l'avvenuta cessione, e ferma restando la responsabilità solidale della società cedente o scissa. Nei novanta giorni successivi a tale comunicazione l'Amministrazione può opporsi al subentro del nuovo soggetto nella titolarità del contratto, con effetti risolutivi sulla situazione in essere, laddove ritenga che siano venuti meno i requisiti di carattere tecnico e professionale e i requisiti di carattere economico e finanziario presenti in capo all'originaria concessionaria.

In caso di inadempimento da parte del Fornitore degli obblighi di cui al presente articolo, l'Amministrazione, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolto il contratto.

22 DIVIETO DI SOSPENSIONE DEL SERVIZIO

Il Fornitore non può sospendere forniture o servizi con sua decisione unilaterale, in nessun caso, nemmeno quando siano in atto controversie con la Regione Campania. La sospensione unilaterale da parte del Fornitore costituisce inadempienza contrattuale tale da motivare la risoluzione del contratto ex art. 1456 del c.c.. Restano a carico dello stesso Fornitore tutti gli oneri e le conseguenze derivanti da tale risoluzione.

23 CAUSE DI RISOLUZIONE DEL CONTRATTO

In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con il presente Contratto che si protragga oltre il termine, non inferiore a 15 (quindici) giorni, che verrà assegnato dall'Amministrazione per porre fine all'inadempimento, la stessa Amministrazione ha la facoltà di considerare risolto il Contratto e di ritenere definitivamente la garanzia, ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.

Si conviene invece che l'Amministrazione potrà risolvere il contratto di diritto ai sensi dell'art. 1456 cod. civ., previa contestazione degli addebiti al Fornitore e assegnazione di un termine non inferiore a quindici giorni per la presentazione delle controdeduzioni nei seguenti casi:

1. fatto salvo quanto previsto dall'art. 71 comma 3 del D.P.R. 445/00, qualora fosse accertata la non veridicità del contenuto delle dichiarazioni sostitutive di certificazioni ed atti di notorietà rilasciate dal Fornitore ai sensi e per gli effetti degli artt. 38, 46 e 47 del D.P.R. 445/00, il contratto si intenderà risolto di diritto anche relativamente alle prestazioni già eseguite o in corso di esecuzione;
2. in caso di ottenimento del documento unico di regolarità contributiva dell'affidatario del contratto negativo per due volte consecutive;
3. qualora gli accertamenti antimafia presso la Prefettura competente risultassero positivi;
4. mancato adempimento delle prestazioni contrattuali a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel presente Capitolato;
5. mancata reintegrazione della garanzia eventualmente escussa entro il termine di 10 (dieci) giorni dal ricevimento della relativa richiesta da parte dell'Amministrazione;
6. azioni giudiziarie intentate da terzi contro l'Amministrazione per fatti o atti compiuti dal Fornitore nell'esecuzione del servizio;
7. in caso di mancato rispetto del Protocollo di Legalità sottoscritto il 01.08.07 tra la Regione Campania e il Prefetto di Napoli;
8. In caso di mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti idonei a garantire la piena tracciabilità delle operazioni;
9. negli altri casi previsti dal presente capitolato.

Si rinvia in ogni caso alla disciplina codicistica per quanto concerne tutte le ipotesi di risoluzione del contratto.

La risoluzione fa sorgere in capo alla stazione appaltante il diritto di incamerare la cauzione definitiva, di sospendere i pagamenti, nonché il diritto al risarcimento di tutti i danni diretti ed indiretti, oltre che alla corresponsione delle maggiori spese che la Regione Campania dovrà sostenere per il restante periodo contrattuale, affidando a terzi il servizio o la sua parte rimanente in danno dell'affidatario inadempiente.

24 RECESSO

La Regione Campania, ai sensi dell'art. 1373 del codice civile, potrà recedere in ogni momento dal contratto, previa comunicazione scritta, senza che il Fornitore possa vantare diritti a compensi ulteriori, risarcimenti o indennizzi a qualsiasi titolo. In caso di recesso, al Fornitore saranno corrisposti esclusivamente i compensi per le prestazioni che risulteranno effettivamente eseguite alla data del recesso stesso.

25 TRACCIABILITA' DEI PAGAMENTI

In ottemperanza all'obbligo di tracciabilità dei flussi finanziari, di cui all'art. 3 della Legge n. 136/2010 e alle Deliberazioni dell'Autorità di vigilanza per i contratti pubblici, il pagamento da parte della Stazione appaltante all'Impresa aggiudicataria sarà eseguito mediante bonifico bancario o postale nelle modalità indicate all'art. 20 del Disciplinare di Gara.

26 NORME - RINVIO

Per tutto quanto non previsto specificatamente nel Bando di gara, nel presente Disciplinare di gara e nel Capitolato Speciale d'Appalto si fa espresso rinvio alla vigente normativa in materia, comunitaria, nazionale e regionale, nonché al Manuale di Attuazione del POR-FESR 2007-2013 approvato con D.G.R. n. 1715 del 20/11/2009.

27 STAZIONE APPALTANTE E RIFERIMENTI

La Stazione Appaltante è la Giunta Regionale Campania, con sede in Napoli alla Via S. Lucia n. 81.

La procedura di gara è affidata al Settore 03 "Centro Regionale Elaborazione Dati" dell'A.G.C. 06 "Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica" (Settore espletante), tel.: 081.7968382; fax: 081.7968380.

Il Responsabile unico del procedimento è l'ing. Vito Merola, i cui contatti sono:

tel. 081 7968385 - email: cred-bando-ca@regione.campania.it.

28 ALLEGATI

Allegato "PREESISTENZE"

Allegato "DIAGRAMMA DI GANTT"

Allegato "SERVICE LEVEL AGREEMENT E PENALI"