Finanziato dall'Unione europea
NextGenerationEU

COMUNE DI MELITO DI NAPOLI

Città Metropolitana di Napoli

Primo settore

Allegato tecnico n. 1 al

Capitolato speciale d'appalto e di disciplinare di gara

1.2 "Abilitazione e facilitazione migrazione al Cloud";

Procedura negoziata senza bando per l'affidamento di contratti pubblici di servizi e forniture sottosoglia comunitaria con il criterio dell'offerta economicamente più vantaggiosa sulla base del miglior rapporto qualità/prezzo, per l'acquisizione di beni e servizi informatici, finanziati dalle misure del PNRR erogate dalla Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale.

Sommario

ALLEGATO TECNICO N.1

1.2 ABILITAZIONE E FACILITAZIONE MIGRAZIONE AL CLOUD
PROCEDURA NEGOZIATA SENZA BANDO, PER L'ATTIVAZIONE DEI SERVIZI RELATIVI ALLA MISURA 1.2 ABILITAZIONE AL CLOUD PER LE PA LOCALI

ACRONIMI E TERMINI CHIAVE

Acronimo	Descrizione
DTD	Dipartimento per la Trasformazione Digitale
DNSH	Do No Significant Harm, principio che impone che gli interventi previsti dai PNRR nazionali non arrechino nessun danno significativo all'ambiente
PNRR	Piano Nazionale di Ripresa e Resilienza
App IO	App Input/Output per i Servizi Pubblici
pagoPA	Piattaforma Digitale Pagamenti Pubblica Amministrazione
SPID	Sistema Pubblico di Identità Digitale
CIE	Carta d'identità Elettronica Italiana
eIDAS	Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (electronic IDentification, Authentication and trust Services
RTI	Raggruppamento Temporaneo di Imprese
SA	Stazione Appaltante
AGID, AGENZIA	Agenzia per l'Italia Digitale
Codice /Codice dell'Amministrazione Digitale/CAD	Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.
Cloud della PA	Insieme di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio

CSP	Cloud Service Provider, fornitore di servizi Cloud
CSC	Cloud Service Consumer acquirente e fruitore di servizi erogati in modalità Cloud
CSN	Cloud Service Partner, è un soggetto terzo che può svolgere attività di supporto o di consulenza per conto del CSP, del CSC o di entrambi
Marketplace Cloud AGID	Piattaforma digitale che permette la selezione e l'acquisto di servizi IaaS e PaaS offerti dai CSP qualificati da AgID, nonché i servizi SaaS qualificati ai sensi della Circolare AgID "Criteri per la qualificazione di servizi SaaS per il Cloud della PA"
SaaS	Software as a Service Tra i modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) è il servizio fully-managed in cui il gestore del servizio si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso, lasciando al fruitore del servizio il solo ruolo di utilizzatore delle funzionalità offerte e che, quindi, non senza oneri di gestione, gestisce o controlla l'infrastruttura cloud necessaria all'erogazione del servizio sottostante
PaaS	Platform as a Service Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo programmatico ovvero il CSC può amministrare, dispiegare ed eseguire applicazioni Cloud utilizzando uno o più linguaggi di programmazione, uno o più ambienti di sviluppo/esecuzione supportati dal CSP
IaaS	Infrastructure as a Service Una categoria di servizi cloud in cui le funzionalità cloud offerte sono di tipo infrastrutturale, tali funzionalità consentono al CSC di disporre autonomamente in modo programmatico di risorse di computing, di storage e networking
RUP	Responsabile Unico del Procedimento
DEC	Direttore Esecuzione Contratto
ACN	Agenzia per la Cybersicurezza Nazionale

1. MIGRAZIONE AL CLOUD

L'appalto riguarda la fornitura di servizi SaaS (Software as a Service) per la gestione applicativa e sistemistica al fine della migrazione al cloud delle basi dati e delle applicazioni e servizi dell'Amministrazione, a valere sui finanziamenti erogati dal PNRR.

L'esecuzione della fornitura si conforma necessariamente alle prescrizioni contenute:

1) Nelle "*Raccomandazioni tecniche per la corretta attuazione delle strategie di cui all'Avviso Pubblico Missione 1 Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa NextGenerationEU, Investimento 1.2 ABILITAZIONE AL CLOUD PER LE PA LOCALI*", emanate dalla Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale, che sono parte integrante e sostanziale del presente documento.
2) "Linee guida per i Soggetti attuatori individuati tramite Avvisi Pubblici a lump sum - (ZIP)" reperibili al seguente indirizzo "https://assets.innovazione.gov.it/1666021877-221017_lg-avvisi-lump-sum.zip, che sono parte integrante e sostanziale del presente documento.

Nell'ambito dell'Avviso, i Soggetti Attuatori ammissibili si candidano per l'implementazione di un piano di migrazione al cloud (comprensivo delle attività di assessment, pianificazione della migrazione, esecuzione e completamento della migrazione, formazione) delle basi dati e delle applicazioni e servizi dell'amministrazione secondo le indicazioni dell'Allegato 2 all'Avviso.

I Soggetti Attuatori dovranno effettuare la migrazione avvalendosi del modello di migrazione come delineato nella Strategia Nazionale per il Cloud:

- Aggiornamento in sicurezza di applicazioni in Cloud (repurchase/replatform).

L' Aggiornamento in sicurezza di applicazioni in Cloud, offre la possibilità di migrare le applicazioni utilizzando una tra le strategie repurchase/replace e replatform. Per repurchase/replace si intende l'acquisto di una soluzione nativa in Cloud, in genere erogata in modalità Software as a Service, mentre per replatforming si intende la riorganizzazione dell'architettura applicativa sostituendo intere componenti del servizio in favore di soluzioni Cloud native in modo da usufruire dei benefici dell'infrastruttura Cloud.

L'ambiente cloud di destinazione dovrà essere di tipo: Public Cloud Qualificato o Infrastruttura della PA idonea e si dovrà rispettare il principio DNSH.

2. SERVIZI OGGETTO DI MIGRAZIONE

I servizi oggetto di migrazione sono tutti quelli riportati nel Piano di migrazione presentato in fase di adesione all'AVVISO PUBBLICO - PIANO NAZIONALE DI RIPRESA E RESILIENZA - MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.2 "ABILITAZIONE AL CLOUD PER LE PA LOCALI" COMUNI ed allegato al presente documento che ne costituisce parte integrante e sostanziale.

Si riporta di seguito la tabella contenente l'elenco dei servizi oggetto della migrazione, con il nome del servizio da migrare e la relativa tipologia di migrazione selezionata.

Servizio Applicativo	Modalità di migrazione	Servizio richiesto con la domanda per l'avviso della Misura 1.2
DEMOGRAFICI -ANAGRAFE	Aggiornamento in sicurezza di applicazioni in cloud	SI
DEMOGRAFICI – STATO CIVILE	Aggiornamento in sicurezza di applicazioni in cloud	SI
DEMOGRAFICI – LEVA MILITARE	Aggiornamento in sicurezza di applicazioni in cloud	SI
DEMOGRAFICI - GIUDICI POPOLARI	Aggiornamento in sicurezza di applicazioni in cloud	SI
DEMOGRAFICI -ELETTORALE	Aggiornamento in sicurezza di applicazioni in cloud	SI
STATISTICA	Aggiornamento in sicurezza di applicazioni in cloud	SI
PROTOCOLLO	Aggiornamento in sicurezza di applicazioni in cloud	SI
ALBO PRETORIO	Aggiornamento in sicurezza di applicazioni in cloud	SI
CONTABILITA' E RAGIONERIA	Aggiornamento in sicurezza di applicazioni in cloud	SI
ECONOMATO	Aggiornamento in sicurezza di applicazioni in cloud	SI
GESTIONE ECONOMICA	Aggiornamento in sicurezza di applicazioni in cloud	SI
GESTIONE PERSONALE	Aggiornamento in sicurezza di applicazioni in cloud	SI
CONTRATTI	Aggiornamento in sicurezza di applicazioni in cloud	SI
ORDINANZE	Aggiornamento in sicurezza di applicazioni in cloud	SI

Tabella 1 - Servizi oggetto di migrazione

Nell'offerta tecnica è opportuno che l'operatore economico descriva per ogni servizio oggetto della migrazione elencato nella Tabella 1, in maniera esaustiva i requisiti minimi e funzionali del servizio.

La soluzione proposta deve essere già qualificata da AgID e pubblicata nel cloud Marketplace della PA; quindi, dovrà essere conforme a una serie di requisiti organizzativi, di sicurezza, di performance e scalabilità, interoperabilità e portabilità fissati dalle circolari Agid n. 2 e n. 3 del 9 aprile 2018.

Inoltre, poiché

- con la Determina 307 del 18 gennaio 2022 dell'ACN, il processo di qualificazione dei servizi Cloud è diventato di competenza della stessa ACN (Agenzia per la Cybersecurity Nazionale), che ha definito nell'Allegato alla stessa determina anche i requisiti di qualificazione,
- con il decreto direttoriale dell'ACN del 2 gennaio 2023, la stessa Autorità ha stabilito che entro i1 Agosto 2023 verranno determinate le nuove modalità di qualificazione che diventeranno obbligatorie a partire dal 19 Gennaio 2024, il fornitore dovrà qualificare i propri servizi secondo le modalità stabilità dall'ACN, non più tardi del 31 marzo 2024.

In particolare, la soluzione proposta dovrà essere predisposta, almeno per i dati ordinari, alla gestione crittografica indicata dall' Allegato B2 alla Determina 307 del 18 gennaio 2022 dell'ACN, requisito prs.ds-1 capoverso 4 (pag. 8/26) ovvero, cit. "Il soggetto (il fornitore della soluzione S.a.a.s) garantisce autonomia all'Amministrazione nella gestione delle proprie chiavi crittografiche ",

La Stazione Appaltante si riserva, nel caso quanto previsto nel punto precedente diventi obbligatorio durante l'espletamento della gara, di richiedere ai concorrenti la dichiarazione che la propria soluzione rispetti quanto previsto nell'Allegato B2 alla Determina 307 del 18 gennaio 2022 dell'ACN, requisito prs.ds-1 capoverso 4 (pag. 8/26) ovvero, cit. "Il soggetto (il fornitore della soluzione S.a.a.s) garantisce autonomia all'Amministrazione nella gestione delle proprie chiavi crittografiche ".

Nel caso quanto indicato al capoverso precedente durante la realizzazione del Progetto diventi obbligatorio, il fornitore dovrà consegnare la chiave di crittografia all'Ente per rendere collaudabile il Progetto.

3. INFRASTRUTTURA TECNOLOGICA E CSP (DNSH)

È richiesto che il CSP (Cloud Solution Provider) qualificato offerto fornisca sufficienti garanzie relativamente al regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) e l'eventuale aderenza a standard internazionali come la ISO 27701 di supporto alla conformità.

È fondamentale che il CSP sia compliant con la checklist DNSH (Do No Significant Harm) consultabile tramite l'allegato 4 dell'Avviso 1.2, a **pena dell'irricevibilità dell'offerta tecnica proposta**.

Il CSP dovrà rispettare i principi di liceità, correttezza e trasparenza, oltre che di data protection-by-design, necessità e minimizzazione. Il trattamento di dati personali da parte del CSP dovrà avvenire sulla base di un'adeguata base giuridica e dovrà prevedere un periodo di data retention coerente con la finalità del trattamento.

È opportuno che l'offerta tecnica evidenzi gli aspetti relativi:

- all'ubicazione dei dati nel data center del CSP evidenziando eventuali trasferimenti elaborativi extra-UE che non prevedono lo storage del dato in territori extra-UE (ad esempio, per la presenza di subappaltatori del CSP per servizi ancillari es. trouble-shooting, assistenza);
- all'esistenza di eventuali impegni del CSP alla conservazione dei dati in determinate "regional zones", onde evitare di incorrere in trasferimenti transfrontalieri di dati personali;
- alla possibilità e alle modalità, da parte del CSP, di monitorare l'utilizzo dei servizi cloud richiesti, nei casi in cui tale controllo comporti l'accesso a dati personali, il trasferimento di dati diagnostici, dati su incidenti di sicurezza e telemetria;
- alla possibilità di effettuare audit precontrattuali, penetration test, così come audit e/o log test in corso di contratto, anche nei confronti dei sub-fornitori;
- alla verifica di un processo strutturato di gestione della continuità operativa (Business Continuity) in linea con standard internazionali come la ISO 22301;
- alla verifica delle policy di sicurezza implementate dal CSP ed in linea con standard di sicurezza (ad esempio, ISO 27001, 27017, 27018) o sulla base di certificazioni rilasciate da organismi indipendenti;
- alla verifica di meccanismi e soluzioni di crittografia che garantiscano la cifratura del dato a riposo (Data Encryption at rest) ed in transito (End-to-End Encryption);
- alla rilevazione e alla segnalazione di data breach;
- alla data retention da parte del CSP (in caso di cessazione del contratto, ovvero per esigenze regolatorie o di enforcement);
- alla data portability in caso di migrazione dei dati ad altro CSP. Si richiede infatti che i dati vengano resi disponibili in formati aperti alla luce della portabilità dei dati personali garantita all'interessato dal GDPR.

Con riferimento ai requisiti sopra elencati, si richiedere un rapporto dettagliato, in relazione alle garanzie e certificazioni offerte dal CSP selezionato.

Ulteriori elementi di valutazione dell'offerta sono quelli che riguardano il rispetto delle specifiche nell'ambito della gestione documentale digitale, della conservazione dei documenti nel tempo, della sicurezza dei sistemi e della riservatezza dei dati personali durante il loro trattamento.

Si richiede di seguire in fase di offerta tecnica le raccomandazioni e le linee guida in continuo aggiornamento di seguito elencate:

- Raccomandazioni sul cloud computing descritte su Docs Italia: https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/cloud-della-pa.html#il-cloud-della-pa

- Nuove linee guida del Garante per la Privacy sui servizi Cloud: Docs Italia: https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/perche-usare-il-cloud.html#sicurezza-e-privacy
  Parere del garante privacy: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9740711

Nell'ambito delle attività di manutenzione, bisognerà garantire la costante aderenza alle norme in materia di privacy e sicurezza. È necessario che la documentazione e le procedure tecniche ed organizzative siano costantemente allineate al quadro normativo e allo stato di fatto dei sistemi.

4. SERVIZI DI AVVIAMENTO E IMPLEMENTAZIONE DEL SISTEMA

Al fine di effettuare l'avvio dei servizi oggetto di migrazione, l'attivazione in esercizio e la successiva manutenzione, **il Fornitore dovrà prevedere al minimo la predisposizione delle seguenti attività di avviamento ed implementazione del sistema**:

- Avvio del progetto - Analisi delle attività di start-up
- Piano di gestione del progetto contenente Piano di output e deliverable di fornitura
- Definizioni delle Interfacce API ed integrazioni (lì dove applicabile)
- Creazione Interfacce API ed integrazioni (lì dove applicabile)
- Parametrizzazione dei moduli applicativi
- Definizione delle modalità di caricamento dei dati di avvio, anche attraverso migrazione dei dati dai sistemi preesistenti
- Installazione e configurazione degli ambienti compresa migrazione dati
- Testing
- Collaudo
- Formazione utenti
- Completamento migrazione dati
- Go live di fase e rilascio in esercizio
- Supporto correttivo e fine tuning
- Consegna deliverable
- Training on the job

Le attività elencate si raggruppano in fasi di progetto, potranno essere concatenate rispettando le propedeuticità ed i vincoli che si generano tra i moduli e le relative fasi di realizzazione. La proposta di pianificazione, ovvero GANTT, e la concatenazione delle stesse in fasi di progetto sono a carico del Fornitore che nell'offerta tecnica fornirà il dettaglio della proposta. Preliminarmente al passaggio alla fase successiva, dovrà avvenire la formale accettazione del deliverable prodotto mediante comunicazione del RUP o del DEC.

Il Fornitore si farà carico della fornitura di un sistema che rispetti i principi guida del Piano Triennale per l'informatica della Pubblica Amministrazione e che sia:

- digital & mobile first (digitale e mobile come prima opzione), le pubbliche amministrazioni devono realizzare servizi primariamente digitali;
- digital identity only (accesso esclusivo mediante identità digitale), le PA devono adottare in via esclusiva

sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;

- servizi inclusivi e accessibili, le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- dati pubblici un bene comune, il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- interoperabile by design, i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API. Deve permettere l'utilizzo di interfacce di servizi per lo scambio dati e l'accesso alle funzionalità;
- sicurezza e privacy by design, i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- user-centric, data driven e agile, le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.
- once only, le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni giàfornite;transfrontaliero by design (concepito come transfrontaliero), le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- integrato, deve garantire la perfetta integrazione fra le componenti del servizio;
- open source, le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice sorgente aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente;
- standard, deve permettere l'utilizzo di best practices per la gestione dei processi. Prediligere l'uso di standard e formati di dati aperti per permettere il riuso;
- modulare, deve consentire l'incremento delle funzionalità operative attraverso l'implementazione di moduli aggiuntivi.

Le componenti applicative dovranno essere percepite dagli utilizzatori come parti di un sistema unico. L'interfaccia utente e la logica di funzionamento del sistema dovranno essere quindi omogenei all'intera soluzione applicativa, che pertanto dovrà presentare maschere, modalità operative, parametri, tasti funzione ecc. tra loro congruenti e consistenti, indipendentemente dalle funzionalità associate. Il termine "integrato" indica che le informazioni sono gestite una sola volta ed in un solo modo, cioè a livello sufficientemente dettagliato da poter essere utilizzate per le diverse finalità necessarie alle aree coinvolte. Si richiede di eliminare ridondanze e duplicazioni nei dati al fine di garantire unicità dei dati e delle funzioni gestite in ogni singolo insieme rispetto al sistema integrato.

5. SERVIZI PROFESSIONALI DI ASSISTENZA E SUPPORTO ORGANIZZATIVO

Al fine di supportare l'Ente nelle attività di Abilitazione al Cloud sono previsti un insieme di servizi professionali di assistenza e supporto organizzativo.

Il Fornitore sarà tenuto all'erogazione dei servizi in conformità ai processi, alle procedure ed alle responsabilità attribuite secondo le direttive dell'Amministrazione, che verranno definite e condivise nella fase di avvio della fornitura, nonché aggiornate durante il corso del contratto esecutivo in funzione delle eventuali evoluzioni.

Il fornitore deve operare in conformità alle linee guida del Cloud Enablement Program e di AgID, in particolare per l'Acquisizione e riuso di software per le Pubbliche Amministrazioni e il Modello di interoperabilità.

Il fornitore deve garantire la non regressione funzionale e il miglioramento -o almeno mantenimento- dei livelli di qualità del sw al termine delle attività di migrazione.

Per consentire le attività di verifica e validazione da parte dell'Amministrazione il fornitore deve disporre e rendere accessibili strumenti, preferibilmente automatici, per la misurazione degli indicatori e del raggiungimento degli obiettivi di migrazione.

5.1 REQUISITI ORGANIZZATIVI

Il Fornitore è tenuto ad impiegare i referenti di seguito indicati, quali ruoli minimi di coordinamento delle attività contrattuali previste. In caso di inadeguatezza, impreparazione e/o incompetenza, il referente dovrà immediatamente essere sostituito con una figura rispondente ai requisiti minimi richiesti e con l'eventuale applicazione dei rilievi e/o delle penali contrattualmente previsti.

Per tutti i referenti richiesti e/o offerti, il Fornitore dovrà indicare un numero di telefono cellulare e un indirizzo di posta elettronica attivo durante l'orario di lavoro richiesto per la fornitura e garantire la risposta ai quesiti posti dall'Amministrazione entro 8 ore lavorative dall'inoltro o dal contatto telefonico.

Si fa presente, inoltre, che tutti i referenti devono essere disponibili in modalità operativa presso l'Amministrazione ove necessario e/o richiesto per l'espletamento di tutte le attività contrattuali.

5.1.1 RUOLI DI COORDINAMENTO RICHIESTI

5.1.1.1 RESPONSABILE UNICO DELLE ATTIVITA' CONTRATTUALI

Per ogni singolo Contratto esecutivo, il Fornitore dovrà indicare un **Responsabile unico delle attività contrattuali** (di seguito per brevità anche "***RUAC***"). Il RUAC dovrà riferire alle Amministrazioni su tutte le tematiche contrattuali, quali ad esempio:

- correttezza nell'esecuzione dei servizi (ad esempio, la stima, la pianificazione e la consuntivazione degli Obiettivi, gli adempimenti legati alla qualità, il controllo dell'avanzamento lavori, la verbalizzazione degli incontri con l'utenza, il controllo del Piano dei Fabbisogni e del Piano Operativo, le attività di valutazione e contenimento dei rischi, l'efficacia e l'efficienza dell'attività di test, ecc.);
- pieno adempimento degli impegni assunti nella documentazione di comprova – scheda tecnica: disponibilità delle banche dati, knowledge management, soluzioni, ecc. secondo quanto indicato nella documentazione tecnica;
- correttezza e tempestività dell'utilizzo del Portale della fornitura e degli strumenti in uso presso l'Amministrazione e/o proposti nella documentazione di comprova – scheda tecnica;
- verifica dei livelli di servizio sulle attività oggetto della fornitura ed individuazione delle eventuali azioni correttive a fronte del mancato rispetto delle soglie previste e/o a fronte di rilievi;
- eventuali azioni da intraprendere per migliorare l'erogazione dei servizi e valutarne i risultati ottenuti;
- garanzia di unitarietà, integrazione, omogeneità e sinergia nelle singole erogazioni dei servizi;
- adozione di idonei strumenti per facilitare la comunicazione e lo scambio di informazioni tra i vari attori coinvolti nella Fornitura;
- eventuali azioni correttive proposte a fronte di situazioni critiche e/o di risultati di iniziative di Customer Satisfaction;
- rendicontazione settimanale, durante il periodo di subentro, dello stato di avanzamento e partecipazione a tutti i momenti di "check" con l'Amministrazione.

Trattandosi della fornitura di prodotti informatici, il RUAC potrà anche essere un responsabile commerciale del

Fornitore.

5.1.1.2 RESPONSABILE TECNICO PER L'EROGAZIONE DEI SERVIZI

Il **Responsabile Tecnico** per l'erogazione dei servizi è il referente operativo del Fornitore per le attività di erogazione dei servizi. Il Fornitore dovrà rendere disponibile per ciascun Contratto esecutivo, in funzione dei servizi erogati, almeno un responsabile tecnico.

Il responsabile dovrà garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori previsti dal Capitolato Tecnico e relative Appendici.

A titolo esemplificativo si riportano le attività principali in carico al responsabile tecnico:

- verifica sull'erogazione dei servizi, conformemente ai requisiti minimi di qualità della fornitura;
- partecipazione alle riunioni di avanzamento e/o a riunioni indette dalle Amministrazioni.

Il profilo professionale minimo per tali figure deve essere **almeno equivalente al RUAC (la figura può coincidere).**

In considerazione della natura delle attività da svolgere e a garanzia dell'operatività dei servizi, i Responsabili tecnici e il RUAC devono essere reperibili telefonicamente dal lunedì al venerdì, dalle ore 8:00 alle ore 20:00 e sempre tramite posta elettronica e garantire la presenza presso l'Ente di un certo numero di giorni (da indicare nel progetto da parte del fornitore) nell'arco dell'anno solare, a tale disponibilità verrà assegnato un punteggio nell'ambito della valutazione del progetto tecnico.

5.1.2 CODICE DI CONDOTTA

Costituisce requisito minimo di esecuzione l'adozione da parte dei Fornitori dei principi di cui alla "*Carta dei principi tecnologici del procurement"* che definisce i principi per lo sviluppo di servizi digitali della Pubblica Amministrazione che:

- soddisfino le esigenze degli utenti/cittadini;
- siano facilmente manutenibili;
- siano capaci di evolvere in base alle esigenze dei cittadini e al progresso tecnologico;
- siano indipendenti da singole componenti architetturali di terze parti;
- diminuiscano le situazioni di dipendenza da un ristretto numero di fornitori (lock-in).

La carta dei principi tecnologici del procurement raccoglie ed estende le linee guida definite dal Codice dell'Amministrazione Digitale e dal Piano Triennale per fornire una visione organica dei principi che la Pubblica Amministrazione e i suoi fornitori dovrebbero rispettare per lo sviluppo di nuovi servizi digitali e per la gestione del ciclo di vita di tali servizi.

Si veda quanto in dettaglio espresso dalla carta al link:

https://carta-dei-principi-tecnologici-del-procurement.readthedocs.io/it/latest/

5.1.3 TEAM DI LAVORO

Il servizio di Assistenza e Manutenzione per i servizi oggetto del Piano di Migrazione al Cloud, erogato dal Fornitore per l'intera durata del progetto, dovrà fornire tutte le informazioni necessarie a supportare l'Amministrazione nell'utilizzo delle infrastrutture tecnologiche e delle applicazioni, nonché a garantire gli interventi necessari a fronte di segnalazioni di malfunzionamento.

Il servizio di assistenza dovrà essere erogato in accordo a quanto indicato nel Regolamento AgID sui servizi cloud del 15 dicembre 2021, visibile al seguente link:

https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/#:~:text=Regolamento%20AgID%20sui,15%20dicembre%202021

I Servizi cloud, i servizi informatici e risorse computazionali erogati su richiesta tramite internet da un fornitore, sono differenziati, sulla base del modello computazionale offerto, in tre categorie di servizi:

- sistemistici infrastrutturali, c.d. Infrastrutture-as-a-Service (IaaS), per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati;
- piattaforme computazionali, c.d. Platform-as-a-Service (PaaS), per l'erogazione di ambienti, pre[1]configurati e amministrati per lo sviluppo di specifiche applicazioni, ad esempio per lo sviluppo software, la gestione di dati o di applicazioni;
- applicativi, c.d. Software-as-a-Service (SaaS), per l'erogazione di un'applicazione agli utenti finali, ad esempio la posta elettronica o altri sistemi di collaborazione remota.

Per erogare i servizi il fornitore dovrà disporre delle competenze, esperienze e capacità richieste ai profili professionali indicati nel seguito, che devono [tutte obbligatoriamente] far parte del Team di Lavoro (o Team Ottimale) del servizio.

Il Team di Lavoro è sotto la responsabilità e l'organizzazione del fornitore.

Profili Professionali previsti nel Team di Migrazione Applicativa al Cloud:

- Project Manager
- DevOps Expert
- Business Analyst
- System Analyst
- Enterprise Architect
- Cloud Application Architect
- Developer/Cloud/Front-End Developer
- Test Specialist
- Database Specialist and Administrator
- System and network administrator
- Cloud Application Specialist
- Cloud Security Specialist
- UX Designer

Il Fornitore sarà libero di organizzare le suddette figure nell'ambito del proprio Team Ottimale, rendendosi disponibile a eventuali verifiche dell'Amministrazione in fase di esecuzione.

Per ogni figura professionale elencata la Stazione Appaltante valuterà assegnando un ponteggio per le certificazioni (dove presenti) e le competenze richieste che dovranno risultare aggiornate alle ultime versioni/tecnologie per tutta la durata del Contratto.

Il fornitore dovrà rendere disponibili all'Amministrazione degli estratti di curriculum vitae delle figure professionali da impiegare nei vari servizi evidenziando le capacità tecniche e le certificazioni dove presenti, il

fornitore per ogni CV deve esplicitamente indicare a quale figura professionale corrisponde. Ogni figura professionale potrà assumere più ruoli tra quelli elencati.

6. SERVIZIO DI FORMAZIONE E AFFIANCAMENTO

È necessario che le attività di migrazione al cloud dei singoli servizi siano accompagnate da una fase di formazione sui sistemi cloud (SaaS) e sul loro utilizzo.

Il fornitore dovrà prevedere un programma di formazione dettagliato che tenga conto dell'addestramento sia del personale tecnico dell'Amministrazione (CED) sia di quello operativo dei vari Settori/Servizi dell'Ente.

Dovrà essere prodotto, durante la fase iniziale di avvio della fornitura, un documento di "Specifiche e pianificazione del servizio di supporto all'avviamento", in cui saranno indicate le tempistiche e le modalità delle attività di formazione da erogare.

In fase di avvio dei servizi migrati in ambiente cloud saranno altresì utili delle sessioni di affiancamento o di supporto da remoto, indipendentemente dalla strategia di migrazione adottata.

Per l'addestramento si potranno prevedere delle sessioni plenarie per l'illustrazione dei servizi e delle loro funzionalità.

Le sessioni dovranno essere erogate contemporaneamente a tutto il personale coinvolto nell'uso dello specifico modulo/servizio, oppure, tramite training on the job per l'addestramento all'uso delle specifiche funzionalità di ogni modulo/servizio utilizzato nei settori/servizi dell'Ente coinvolti.

Nell'ambito del piano di formazione e affiancamento, il fornitore dovrà indicare chiaramente il numero di giornate di formazione da erogare presso la sede dell'Ente, il numero di giornate di formazione da erogare da remoto e il numero di giornate di affiancamento all'avviamento che prevede presso la sede Comunale.

Il piano dei servizi di formazione e affiancamento sarà oggetto di valutazione attraverso l'assegnazione di punteggio tecnico.

7. PHASE IN

A partire dalla data di stipula del contratto, il Fornitore potrà richiedere il supporto dell'Amministrazione contraente o di terzi da essa designati al fine di permettere al proprio personale la presa in carico delle attività di fornitura e di acquisire le conoscenze necessarie al corretto svolgimento dei servizi richiesti per il periodo definito congiuntamente all'Amministrazione contraente nel piano di migrazione; le attività di phase in non comporteranno ulteriori oneri per l'Amministrazione contraente. Resta inteso che l'attività di phase in non potrà avere una durata tale da impattare le milestone progettuali dell'attività di migrazione dell'Amministrazione contraente.

L'attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. elenco degli asset informatici, catalogo dei sistemi e delle applicazioni, documentazione relativa agli sviluppi in corso, base dati dei contratti con terzi, etc.) con assistenza di personale esperto, affiancamento nell'operatività quotidiana condotta dall'eventuale fornitore uscente. Qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del passaggio di consegne. Tale verbale dovrà essere sottoscritto dai due Fornitori, l'uscente e il subentrante (ovvero tra l'Amministrazione contraente e l'Aggiudicatario) e consegnato all'Amministrazione. In tal caso sarà cura del Fornitore Aggiudicatario aggiornare la documentazione incompleta oppure produrre la documentazione non presente che dovrà essere consegnata a chiusura del phase in.

Durante le attività di training on the job la responsabilità delle operazioni continuerà ad essere in capo al Fornitore uscente, se presente. Le modalità di fruizione e la relativa pianificazione di tale addestramento dovranno essere

concordate con l'Amministrazione contraente, anche sulla base di eventuali proposte che il Fornitore effettuerà.

8. PHASE OUT

All'approssimarsi della scadenza del contratto ed in mancanza di rinnovo, o in caso di esplicita comunicazione, da parte dell'Ente, di passaggio ad altro fornitore, o in caso di revoca della qualificazione da parte dell'AgID, il Fornitore dovrà garantire (a titolo gratuito) il corretto svolgimento di tutte le seguenti azioni, volte ad assicurare una corretta e trasparente transizione verso il nuovo scenario:

- rilasciare, in formato aperto e tecnologicamente adeguato alle successive operazioni di import nei database del nuovo sistema, tutti i dati a qualunque titolo trattati;
- rilasciare, ove applicabile, tutto il codice sorgente, inteso come l'intera codebase (production, preproduction, test, staging, development; configurazioni, file di risorse, dipendenze, ecc.), in formato tecnologicamente adeguato alle successive operazioni di trasferimento nel repository del nuovo Revision Control System nonché nel workspace del nuovo Integrated Development Environment;
- consegnare, ove applicabile, snapshots e/o exports dell'intero ambiente virtuale in cloud (virtual machines, containers; infrastructure as code, orchestrator configuration files, ecc.);
- consegnare l'intera documentazione di progetto (disegni, diagrammi, schemi, manuali, processi, servizi, procedure amministrative ed operative, ecc.);
- rilasciare tutti i log necessari ai fini della tracciabilità delle operazioni effettuate dagli utenti del sistema;
- rilasciare tutte le statistiche ed i report relativi al monitoraggio delle performance e dello status del sistema;
- fornire, per una durata di tempo congrua (da concordare con il Soggetto Attuatore e che potrà estendersi anche oltre la data di switch effettivo), adeguato supporto e formazione al personale del Soggetto Attuatore e/o del nuovo fornitore in merito a tutto quanto sia necessario conoscere ed attuare per assicurare il corretto funzionamento dell'intero sistema nel nuovo scenario.

In aggiunta, qualora il fornitore dovesse risultare inadempiente all'esecuzione corretta e tempestiva delle attività indicate, ovvero non garantisca la prosecuzione efficace ed in continuità dei servizi, l'Amministrazione si riserva di non riconoscere i corrispettivi dei servizi erogati nel periodo di transizione in uscita.

Inoltre, al fine di prevenire e contrastare il fenomeno del *vendor lock-in*, il Fornitore deve garantire il rispetto dei requisiti di interoperabilità e portabilità (RIP) contenuti nella Circolare n. 3 dell'AgID del 9 Aprile 2018, di seguito riportati.

Requisiti SaaS (Circolare n. 3):

- RIP1 - Il Fornitore SaaS dichiara che il servizio SaaS espone opportune Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità applicative, di gestione e configurazione del servizio;
- RIP2 - Il Fornitore SaaS dichiara se il servizio SaaS è interoperabile con i servizi pubblici SPID e PagoPA;
- RIP3 - Il Fornitore SaaS garantisce all'Acquirente la possibilità di estrarre in qualsiasi momento una copia completa di dati, metadati e documenti memorizzati dal servizio SaaS in formati pubblici e aperti;
- RIP4 - Allo scopo di consentire la migrazione da un altro Fornitore SaaS o servizio SaaS, il Fornitore SaaS garantisce all'Acquirente la possibilità di importare i dati all'interno del servizio SaaS tramite formati pubblici e aperti;
- RIP5 - Il Fornitore SaaS dettaglia le procedure per garantire la reversibilità del servizio SaaS.

Infine, per una maggiore garanzia di portabilità dei dati (articolo 6 del REGOLAMENTO (UE) 2018/1807 - libera circolazione dei dati non personali), è opportuno che il Fornitore risulti aver aderito ai Codici di Condotta elaborati

dallo SWIPO (associazione senza scopo di lucro facilitata dalla Commissione Europea) ed aver pubblicato il relativo Transparency Statement contenente tutte le informazioni necessarie a valutare ed effettuare eventuali operazioni di data porting per effettuare il provider switching.

9. INSTALLAZIONE SERVIZI CLOUD IN MODALITÀ SaaS

L'ammissibilità degli interventi di migrazione è disciplinata dall'art. 6 ("Interventi finanziabili") dell'avviso di Investimento 1.2 "Abilitazione al cloud per le PA Locali" e dai suoi allegati.

La Stazione Appaltante dichiara che il modello di migrazione dei 14 servizi elencati nella tabella 1 è di tipo Repurchase/Rehost.

Le attività di installazione dovranno essere precedute dalla redazione, da parte del Fornitore, di un piano di installazione/manutenzione dei servizi, nel quale sono da tenere in considerazione: gli interventi effettuati in intervalli orari definiti con l'Amministrazione e coerentemente con le proprie esigenze di operatività.

Una volta eseguita l'installazione sul nuovo ambiente in cloud è necessario effettuare i test di accettazione prima della messa in produzione così così da garantire che tutti i dati siano stati effettivamente migrati correttamente.

Al fine di verificare la corretta erogazione dei servizi e la costante adeguatezza delle soluzioni scelte si richiede l'impegno del fornitore ad eseguire dei test periodici (i test vanno pianificati e dettagliati nel documento piano dei test) al fine di garantire il tempestivo ripristino ove necessario.

10. MIGRAZIONE DEI SERVIZI IN AMBIENTE CLOUD

Nell'ambito dell'Avviso di Investimento 1.2 "Abilitazione al cloud per le PA Locali - Allegato 2 – Definizione dei Servizi e modalità di migrazione" è necessario che il Questionario di Assessment deve essere compilato dall'Ente a processo di migrazione iniziato per ogni servizio migrato e con il supporto del fornitore contrattualizzato.

A tal fine il fornitore dovrà farsi carico di tutte le attività necessarie alla migrazione e alla progettazione del processo di migrazione per ogni servizio candidato alla migrazione in cloud. Questa è una fase ricorsiva per ogni applicazione/servizio e incrementale, di modo che si possa verificare che le applicazioni/servizio funzionino correttamente, una volta migrate.

Nel rispetto della continuità del servizio, è necessario garantire il massimo parallelismo delle attività al fine di minimizzare i tempi di migrazione/attivazione che dovranno essere completate in massimo **cinquecentoquaranta (540)** giorni naturali e consecutivi decorrenti dalla data successiva alla stipula del contratto. In mancanza del rispetto del già menzionato termine verrà applicata una penale per come disciplinato nel paragrafo 25.

Per ogni applicazione/servizio si dovrà effettuare la revisione della sicurezza applicativa e dell'infrastruttura attraverso l'applicazione delle misure di sicurezza ICT per le Pubbliche Amministrazioni, così come emanate dall'AgID e per quanto riguarda le web application security, è necessario applicare i controlli legati alle vulnerabilità più comuni.

11. INTEROPERABILITÀ CON ALTRI SISTEMI INFORMATIVI

Il nuovo Modello di Interoperabilità dell'AgID, consultabile a questo link:

- https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita

rappresenta un asse portante del Piano Triennale per l'informatica nella Pubblica Amministrazione, necessario per il funzionamento dell'intero Sistema informativo della PA. Il modello rende possibile la collaborazione tra pubbliche amministrazioni e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l'interazione e lo scambio di informazioni senza vincoli sulle implementazioni.

Il nuovo Modello di Interoperabilità rende possibile la collaborazione tra Pubbliche amministrazioni e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l'interazione e lo scambio di informazioni senza vincoli sulle implementazioni, evitando integrazioni ad hoc, in particolare:

- abilita lo sviluppo di nuove applicazioni per gli utenti della PA;
- assicura, nel rispetto del diritto alla privacy, l'accesso ai dati della Pubblica amministrazione anche a soggetti terzi;
- è progettato in coerenza con i principi declinati nel nuovo European Interoperability Framework (EIF) oggetto della Comunicazione COM(2017) 134 della Commissione Europea adottata il 23 marzo 2017.

AgID, con Determinazione n. 547 del 1° ottobre 2021, ha adottato le Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni e le Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici che tutte le pubbliche amministrazioni devono adottare al fine di garantire l'interoperabilità dei propri sistemi con quelli di altri soggetti e favorire l'implementazione complessiva del Sistema informativo della PA.

Tutte le amministrazioni devono aderire agli standard tecnologici ed utilizzare pattern e profili del nuovo Modello di interoperabilità, che consentirà di definire ed esporre Application Programming Interface (API) conformi agli standard consolidati anche in ambito EU. Le API realizzate in conformità con il nuovo Modello di Interoperabilità garantiscono in particolare:

- tracciabilità delle diverse versioni delle API, allo scopo di consentire evoluzioni non distruttive (versioning);
- documentazione coordinata con la versione delle API (documentation);
- limitazioni di utilizzo collegate alle caratteristiche delle API stesse e della classe di utilizzatori (throttling);
- tracciabilità delle richieste ricevute e del loro esito (logging e accounting);
- un adeguato livello di servizio in base alla tipologia del servizio fornito (SLA);
- configurazione scalabile delle risorse.

Nello specifico:

- le "Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni" individuano (1) l'insieme delle tecnologie che abilitano l'interoperabilità tra PA, cittadini e imprese, (2) i pattern di interoperabilità (interazione e sicurezza) e (3) i profili di interoperabilità e il modello di governance applicato dall'Agenzia per l'Italia Digitale per il loro aggiornamento;
- le "Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici" individuano le soluzioni tecniche idonee a garantire l'autenticazione dei soggetti coinvolti e la

protezione, l'integrità e la riservatezza dei dati scambiati nelle interazioni tra sistemi informatici della pubblica amministrazione e di questi con i sistemi informatici di soggetti privati per il tramite di API.

Il nuovo Modello di interoperabilità rappresenta un asse portante del Piano triennale per l'informatica nella PA 2021-2023.

Nell'ambito del nuovo Modello di Interoperabilità:

- in attuazione del comma 2 dell'articolo 50-ter del Decreto Legislativo 7 marzo 2005, n. 82, AgID ha adottato, con Determinazione n. 627 del 15 dicembre 2021 le "Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati" relative all'infrastruttura tecnologica che rende possibile l'interoperabilità tramite API dei sistemi informatici e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici mediante l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti aderenti;

- in attuazione dell'articolo 64-bis del Decreto Legislativo 7 marzo 2005, n. 82, AgID ha adottato, con Determinazione n. 598 dell'8 novembre 2021 le "Linee guida sul punto di accesso telematico ai servizi della Pubblica Amministrazione" e con Determinazione n. 172 del 17 giugno 2022 ha adottato le "Regole tecniche per la gestione delle sessioni di autenticazione e del single sign-on" relative al punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri attraverso cui i soggetti di cui all'articolo 2, comma 2 del Decreto Legislativo 7 marzo 2005, n. 82 rendono fruibili i propri servizi in rete.

E' pertanto necessario che la soluzione offerta supporti nativamente, senza costi aggiuntivi per l'Ente e con il pieno e costante supporto dell'Affidatario, il predetto Modello d'Interoperabilità AgID.

In particolare, è anche espressamente richiesto il supporto alle previsioni d'interoperabilità dei seguenti interventi finanziati dalla Presidenza del Consiglio dei Ministri – Dipartimento per la Trasformazione Digitale:

- 1.4.1 Esperienza del Cittadino nei servizi pubblici;
- 1.4.3 Adozione pagoPA e app IO;
- 1.4.4 Adozione identità digitale;
- 1.4.5 Digitalizzazione degli avvisi pubblici – Integrazione con la Piattaforma delle Notifiche Digitali;

come visibili nel sito apposito del Dipartimento a questo link:

https://padigitale2026.gov.it/

Quindi, i servizi oggetto della migrazione dovranno essere predisposti per l'integrazione con altri sistemi e sottosistemi, già presenti nel sistema informativo dell'ente e con sistemi terzi.

Tutte le componenti dovranno quindi essere in grado di interfacciarsi dal punto di vista tecnologico utilizzando standard riconosciuti e aperti al fine di interagire con le informazioni provenienti dagli altri moduli e dagli altri sottosistemi o sistemi informativi terzi.

Dovrà essere facilmente attuabile la gestione di eventuali caricamenti massivi di dati mediante procedure automatiche.

L'interoperabilità dovrà essere garantita nel rispetto delle linee guida di interoperabilità tecnica della pubblica amministrazione e dei documenti operativi allegati. Le strategie e le modalità di interoperabilità dovranno tenere conto anche del dispiegamento di servizi eterogenei su cloud distinti, con policy di rete opportunamente disegnate nel rispetto delle best practice di sicurezza.

In particolare, il Fornitore deve garantire il rispetto dei requisiti di interoperabilità e portabilità (RIP) contenuti nella Circolare n. 2 e nella Circolare n.3 dell'AGID del 9 Aprile 2018, già riportati nel Paragrafo 8 - PHASE OUT

del presente documento

Il modello di Interoperabilità e in particolare l'interoperabilità con i sistemi oggetto di intervento di finanziamento PNRR da parte Dipartimento per la Trasformazione Digitale saranno oggetto di assegnazione di un punteggio tecnico.

12. SERVIZIO DI MANUTENZIONE CORRETTIVA E ADEGUATIVA

Nell'ambito dell'appalto e per tutta la sua durata, senza alcuna interruzione, il Fornitore provvederà a offrire il Servizio di manutenzione correttiva e adeguativa (MAC).

Per servizio di manutenzione correttiva si intende la diagnosi e la rimozione delle cause e degli effetti, sia sulle interfacce utente che sulle basi dati, dei malfunzionamenti delle procedure e dei programmi in esercizio ed in genere di tutti i componenti del sistema non in garanzia.

La manutenzione adeguativa sarà volta ad assicurare la costante aderenza delle procedure e dei programmi all'evoluzione dell'ambiente tecnologico del sistema informativo o relativa ad altri interventi minimali di adeguamento che non modificano le funzionalità del software.

12.1 ARTICOLAZIONE DEL SERVIZIO DI MANUTENZIONE CORRETTIVA E ADEGUATIVA

La manutenzione correttiva viene innescato da una segnalazione di impedimento all'uso dell'applicazione di una o più delle sue funzioni. Per impedimento si intende una malfunzione vera e propria dell'applicazione o gli effetti che tale malfunzione ha causato alla base dati (es. anomalie in un programma batch che corrompono la base dati).

I malfunzionamenti, le cui cause non sono imputabili a difetti presenti nel software applicativo, ma ad errori tecnici, operativi o d'integrazione con altri sistemi (ad esempio interruzione del collegamento TP, uso improprio delle funzioni, ecc.), oppure relativi a software in garanzia (del fornitore uscente), comportano, da parte del servizio di manutenzione correttiva, il solo supporto all'attività diagnostica sulla causa del malfunzionamento, a fronte della segnalazione pervenuta, ma sono poi risolti da altre strutture di competenza. Analogamente per il software realizzato/modificato nel corso del medesimo appalto, i malfunzionamenti dovranno essere risolti nell'ambito dei servizi realizzativi in quanto coperto dalla garanzia.

La manutenzione adeguativa riguarda tutte le tipologie di intervento non correttivo ad impatto da limitato a medio. In generale può includere interventi di di customizing e adeguamenti di portata da lieve a media entità.

Sono parte integrante del servizio di Manutenzione Correttiva ed Adeguativa le seguenti attività:

- contributi di competenza sistemistica e specialistica di prodotto necessari alla corretta soluzione del malfunzionamento;
- attivazione del gruppo di sviluppo per adeguare l'eventuale software in corso di sviluppo/modifica/collaudo;
- test in ambiente assimilabile all'ambiente di esercizio della soluzione realizzata;
- gestione della configurazione;
- in caso di malfunzioni su programmi di interfaccia verso l'esterno, validazione tecnica e controllo dei risultati del contenuto dei flussi informativi destinati a strutture esterne o dei dati esposti negli elaborati del sistema;
- allineamento della documentazione.

Tutti i moduli oggetto della fornitura si intendono coperti da manutenzione per il periodo di durata del presente appalto.

I livelli di servizio riguardati la Manutenzione Correttiva ed Adeguativa saranno oggetto di valutazione attraverso assegnazione di punteggio tecnico

13. ACCESSIBILITA' E USABILITA'

Nel caso di migrazione di tipo Repurchase, il Fornitore dovrà garantire che i servizi rispettino le Linee Guida sull'accessibilità degli strumenti informatici, in linea con le disposizioni dell' art. 11 della L. 4/2004.

I siti e le applicazioni WEB dovranno garantire la conformità con il livello "AA" delle Web Content Accessibility Guidelines (WCAG 2.1). I documenti non web dovranno invece essere realizzati nel rispetto dei punti 10 e 11 della norma UNI EN 301549:2018. Particolare attenzione dovrà dunque essere prestata a tutta la documentazione, report, stampe, ecc. che i servizi permetteranno di produrre e per i quali non sarà prevista una fruizione in veste "web" e accessibile.

14. PROTEZIONE DATI PERSONALI

Il servizio/servizi dovrà prevedere, in ottemperanza di disposizioni e/o provvedimenti normativi sulla protezione dei dati personali, sistemi di gestione, configurazione, monitoraggio, meccanismi di autenticazione, autorizzazione e profilatura per l'accesso alle funzionalità previste, ai dati e ai file trattati.

Per il trattamento dei dati personali e sensibili dovrà essere garantita la tutela e la riservatezza dei dati stessi in conformità con quanto disposto dalla normativa vigente (decreto legislativo 30 giugno 2003, n.196 " codice in materia di protezione dei dati personali" e successive modificazioni ed integrazioni), ivi comprese le relative misure di sicurezza previste dal codice.

Particolare attenzione dovrà essere assicurata per la gestione di informazioni di carattere sensibile, per le quali sarà garantita una soluzione che comporti il pieno rispetto della normativa sopra citata e della ulteriore normativa di settore applicabile.

All'affidatario compete la responsabilità di assicurare la sicurezza sia fisica che logica lungo tutto il ciclo di vita delle informazioni e per tutta la durata del contratto, vigilandone l'effettiva attuazione ed efficacia nel rispetto dei requisiti di sicurezza ai sensi dell'art. 28 del regolamento ue 2016/679 (gdpr), costituenti parte integrante del contratto di appalto.

15. REQUISITI MINIMI DI SICUREZZA

I servizi oggetto di migrazione dovranno rispettare i requisiti di riservatezza, autenticità, integrità, e disponibilità.

Nell'ambito dell'erogazione del servizio di sicurezza ICT, il Fornitore è deputato all'analisi e verifica dei livelli di sicurezza complessiva dell'architettura e della valutazione di eventuali azioni di perfezionamento della security stessa.

Può essere effettuata all'interno di questo servizio anche la progettazione di contromisure ad attacchi e tentativi di intrusione, inserimento di nuove e più efficaci regole di protezione nonché l'esecuzione di test e simulazioni di attacco ed intrusione (penetration test).

Il fornitore dovrà introdurre tutte le contromisure di tipo tecnologico volte alla difesa perimetrale e di contenuto del servizio migrato. Tuttavia, considerando la responsabilità generale del Fornitore di mantenere i sistemi in perfetta efficienza, risulta evidente che le attività di rilevazione e di bonifica delle vulnerabilità potranno essere svolte anche in modo autonomo, indipendentemente dall'attività di verifica da parte dell'Ente.

Sarà ritenuto elemento di valutazione migliorativa la possibilità per gli utenti di utilizzare lo SPID come strumento di autenticazione.

16. BACK-UP E RESTORE

Il fornitore dovrà prevedere, per ciascuno dei servizi offerti, l'attivazione delle rispettive funzionalità di backup e restore. L'offerta tecnica dovrà prevedere al minimo: le procedure automatiche di copia e salvataggio delle configurazioni operative in un ambiente protetto mediante l'utilizzo di supporti esterni; la conseguente possibilità di ripristinarne i contenuti in caso di indisponibilità/danneggiamento dei contenuti negli ambienti operativi. Il fornitore ha facoltà di proporre gli strumenti che ritiene più idonei per il raggiungimento degli obiettivi dichiarati.

L'Affidatario, nelle fasi iniziali (periodo di transizione iniziale), verificherà l'infrastruttura e le policy di backup e restore esistenti, concorderà con l'Ente eventuali variazioni delle policy dove queste non siano più ritenute adeguate. Si occuperà di implementare le nuove policy di backup concordate, compatibilmente con l'infrastruttura di backup messa a disposizione sul Cloud, provvedendo alla documentazione ed all'aggiornamento delle procedure di dettaglio utilizzate per il backup ed il restore dei dati.

L'Affidatario nel corso delle attività operative è tenuto a verificare l'adeguatezza delle policy di backup, mediante opportuni test e simulazioni al fine di garantire gli aspetti di continuità operativa. Nello specifico l'art. 51, comma 1 del CAD, le Linee Guida adottate ai sensi dell'art. 71 CAD; l'art. 51 CAD, il comma 2-quater, il quale obbliga le pubbliche amministrazioni tenute all'attuazione del CAD, alla predisposizione di piani di emergenza, conformi alle Linee guida di AgID, in grado di assicurare sia la continuità operativa delle operazioni indispensabili a garantire la fruibilità dei servizi, sia il ritorno alla normale operatività. Dovrà quindi proporre all'Ente tutti gli adeguamenti, anche di infrastruttura, necessari alla corretta esecuzione dei backup e restore e la predisposizione di piani di emergenza per assicurare la continuità operativa.

17. DISASTER RECOVERY E-BUSINESS CONTINUITY

Il Fornitore dovrà redigere un Piano di disaster recovery nel quale descriverà le strategie attuate, tra quelle previste dal paragrafo 5.3.10 "Disaster recovery" del Manuale di Abilitazione al Cloud. Le procedure di backup e restore dovranno essere accuratamente progettate e documentate e dovranno tenere conto della mole di dati da trattare e del tempo necessario per le operazioni. Il Fornitore dovrà, periodicamente, verificare e attuare le procedure, in modo tale da garantire il loro corretto funzionamento in ogni dato momento.

18. QUESTIONARIO DI ASSESSMENT

Il Questionario di Assessment, previsto dall'Avviso 1.2 di Migrazione al cloud, ha lo scopo di raccogliere le informazioni circa lo stato di avanzamento della migrazione e creare una modalità di rappresentazione sintetica dell'avanzamento delle attività. La sua corretta compilazione ed il puntuale aggiornamento fino alla conclusione delle attività rappresentano un onere che il Fornitore assume per supportare il Soggetto Attuatore per la compilazione degli aspetti tecnici del questionario al fine di permettere di tenere traccia dello stato di esecuzione dei lavori. I Servizi identificati nel Questionario di Assessment devono corrispondere con i servizi affidati al Fornitore. Per ogni servizio devono essere elencati tutti gli applicativi ad esso associati e oggetto di migrazione.

Deve essere compilato a processo di migrazione iniziato per ogni servizio oggetto di affidamento alla migrazione, deve essere periodicamente aggiornato ogni volta intercorre un evento significativo rispetto al contenuto tracciante del questionario. Alla conclusione del processo di migrazione il questionario conterrà lo stato "Completato" rispetto ai singoli servizi.

Sono previste due differenti tipologie di Questionario di Assessment a seconda della strategia adottata per la migrazione in cloud del singolo servizio:

- Questionario di Assessment per Trasferimento in sicurezza dell'Infrastruttura IT, include al suo interno le informazioni necessarie per identificare l'origine della migrazione;
- Questionario di Assessment per Aggiornamento in Sicurezza di applicazioni in Cloud, in caso di Aggiornamento in Sicurezza del servizio in Cloud.

Per lo schema di riferimento del Questionario di Assessment è necessario far riferimento all'Allegato 2.x dell'avviso 1.2 di Migrazione al Cloud dei Comuni, compilando l'ultima versione resa disponibile rispetto al momento in cui si: avvia il processo di migrazione, verifica un evento di cui tenere traccia, conclude l'attività di migrazione.

19. FORM DI CONFORMITA' ALLA MIGRAZIONE

Il Form di Conformità della migrazione, definito nell' "Allegato 1 - Completamento delle attività e verifiche tecniche Avvisi 1.2" alle "Linee Guida per i Soggetti attuatori individuati tramite AVVISI PUBBLICI A LUMP SUM " , rappresenta il modello di form che deve essere utilizzato dal Soggetto Attuatore, ovvero la Stazione Appaltante, per fornire le informazioni richieste dall'asseveratore alla conclusione del processo di Migrazione al Cloud.

Esso si differenzia in tre modelli diversi:

- un Form per l'indicazione di dati e documenti necessari all'Asseveramento della "Migrazione per "Trasferimento in sicurezza dell'Infrastruttura IT", ovvero migrazione di un servizio applicativo ad un IaaS qualificato;
- un Form per l'indicazione di dati e documenti necessari all'Asseveramento della "Migrazione per "Aggiornamento in Sicurezza di applicazioni in Cloud" di tipo replatform, ovvero migrazione di un servizio applicativo ad un PaaS qualificato;
- un Form per l'indicazione di dati e documenti necessari all'Asseveramento della "Migrazione per "Aggiornamento in Sicurezza di applicazioni in Cloud" di tipo repurchase, ovvero migrazione di un servizio applicativo ad un SaaS qualificato.

Si chiede al fornitore di assistere la stazione appaltante nella compilazione di tale form al fine del raggiungimento di un giudizio positivo all'Asseveramento.

20. SERVIZI DI MANUTENZIONE SISTEMISTICA SULLA PIATTAFORME DI SERVIZI

Al Fornitore è richiesto che, terminata l'implementazione del Piano di migrazione al cloud delle basi dati, delle applicazioni e dei servizi dell'amministrazione, sia effettuata l'ottimizzazione ed il fine tuning dei parametri di configurazione dell'ambiente cloud in funzione dei dati di carico a disposizione, dei test effettuati e delle prime attività d'esercizio. Lo svolgimento dell'attività di fine-tuning si rende necessaria a garantire, nell'esercizio quotidiano, le prestazioni ottimali per i servizi applicativi, le riconfigurazioni ambientali (processi, priorità ecc.) e le attività di riorganizzazione delle basi di dati, dei file system e, se necessario, di un giusto dimensionamento delle risorse computazionali anche in un'ottica di risparmio economico.

Nell'ambito dei Servizi di manutenzione sistemistica e per tutti i servizi IaaS e SaaS previsti in fornitura, il Fornitore dovrà erogare i servizi di gestione sistemistica. Si elencano i seguenti sistemi che, ove presenti, rientrano nell'ambito tecnologico server in esame:

- sistema operativo: Windows, Unix e Linux;
- middleware: intesi come pila/stack che va dal Sistema Operativo al DB/applicativo (con questi esclusi).

I servizi relativi alla gestione dei server virtuali riguardano i servizi di elaborazione e i servizi di archiviazione. Il servizio di gestione in ambito sistemistico riguarda la gestione di tutti gli elementi/apparati/sistemi sopra descritti, mediante la disponibilità continuativa di risorse del Fornitore, durante l'orario corrispondente contrattualizzato. Il servizio include tutte le attività necessarie per prendere in carico, condurre e mantenere sempre efficiente l'infrastruttura dei sistemi server. A titolo indicativo e non esaustivo, nel seguito vengono descritte alcune delle attività minime che il Fornitore dovrà svolgere, distinte fra interventi svolti autonomamente (in maniera continuativa e proattiva) e interventi di gestione a richiesta dell'Amministrazione:

1. Attività svolte autonomamente dal Fornitore:
   - installazione di patch, hot fix e service pack relativi a tutte le componenti software in gestione, inclusiva di: costante monitoraggio dei rilasci; verifica preventiva dell'applicabilità di tali patch nell'ambiente dell'Amministrazione e valutazione del loro impatto; richiesta delle patch/hot fix qualora non disponibili; definizione di un piano di installazione concordato con l'Amministrazione (date ed ambiti di intervento); predisposizione di apposite procedure di salvataggio;
   - cambiamenti di configurazione, con particolare riferimento alle regole di sicurezza informatica, da concordare con l'Amministrazione a seguito di cambi di policy, nuove regole di sicurezza, modificazione nell'allocazione delle risorse per l'ottimizzazione delle prestazioni o altre motivazioni che dovessero emergere dall'attività di conduzione e monitoraggio, secondo le modalità previste dal processo di change management;
   - amministrazione dei sistemi e settaggio di configurazioni del sistema operativo e dei servizi infrastrutturali attivi, amministrazione delle macchine virtuali;
   - elaborazioni batch e schedulazione;
   - amministrazione utenti a livello sistema operativo;
   - supporto alla manutenzione dei middleware;
   - monitoraggio, raccolta e storicizzazione dei valori del carico dei server della disponibilità, della capacità, dell'utilizzo e delle performance dei sistemi su base oraria, giornaliera e mensile, allo scopo di garantire l'efficienza di tutte le componenti (CPU, memorie, BUS di sistema e dispositivi di I/O), al fine di determinare possibili aree di inefficienza o colli di bottiglia dell'intera infrastruttura, definendo soglie di utilizzo delle risorse ed intervenendo prontamente a fronte di eventuali malfunzionamenti;
   - monitoraggio dello scanner per la sicurezza dei sistemi e la protezione da virus;
   - monitoraggio delle security policy;
   - capacity planning volto alla determinazione e alla messa in esercizio di configurazioni adeguate a ogni componente dei server virtualizzati;
   - in particolare, per i server infrastrutturali più diffusi, si citano le attività tipiche:
     - per i Directory Server (es.: Active Directory/LDAP): amministrazione domini, amministrazione policy e profili di sicurezza; backup/ripristino dei dati di configurazione; allineamento e sincronizzazione di directory server multipli; verifica periodica dell'integrità dei dati;
     - per i Network Server (es.: DHCP/WINS/DNS): amministrazione delle configurazioni di network, delle policy di sicurezza; backup/ripristino dei dati di configurazione; verifica periodica dell'integrità dei dati;
     - per i File Server: gestione quote di spazio disco ed amministrazione dei permessi di accesso; monitoraggio occupazione spazio disco e segnalazione di criticità; rilascio ed amministrazione di network drives; gestione servizi FTP;

2. Interventi di gestione a richiesta dell'Amministrazione
   - richieste di riconfigurazione apparati;
   - attività inerenti all'aggiornamento e/o installazione di componenti middleware forniti dall'Amministrazione al Fornitore;
   - monitoraggio, raccolta e storicizzazione, a richiesta, dei valori del carico dei server virtuali della disponibilità, della capacità, dell'utilizzo e delle performance dei sistemi su base oraria, giornaliera e

mensile.

21. AZIONI CONTRATTUALI

Ogni inadempimento contrattuale darà origine ad un'azione commisurata alla criticità della violazione.

I principali aspetti delle prestazioni contrattuali vengono presidiati da appositi indicatori di qualità, specialmente laddove vengono definite specifiche misure. Altri aspetti non sono oggetto di misurazioni strutturate di cui agli "Indicatori di qualità", ma per disservizi ritenuti gravi vengono direttamente presidiate nel contratto.

Pertanto, il mancato rispetto dei requisiti minimi richiesti e/o come migliorati dal fornitore in Offerta tecnica determina azioni contrattuali conseguenti che possono consistere in una o più delle seguenti azioni:

- coinvolgimento di un livello più elevato di interlocutori, sia del fornitore, che della stazione appaltante, allo scopo di prendere le decisioni necessarie al ripristino delle situazioni fuori soglia o fuori controllo (attivazione di una procedura di escalation);
- ripetizione da parte del fornitore dell'erogazione di una prestazione, rifacimento di una attività, riconsegna di un prodotto (chiusura di una non conformità);
- azione di intervento sui processi produttivi del fornitore per evitare il ripetersi di sistematiche non conformità (esecuzione di una azione correttiva);
- applicazione di rilievi, se previsti dall'Amministrazione;
- perdita della quota variabile del corrispettivo legato al raggiungimento di un livello di qualità minimo, se previsti dall'Amministrazione;
- applicazione di penali;
- azioni aggiuntive (richiesta danni, risoluzione anticipata del contratto, ecc.) laddove previsto contrattualmente.

22. FATTURAZIONE E PAGAMENTI

Il pagamento per l'importo dovuto per la fase di deployment avverrà secondo le seguenti modalità:

• Al termine della fase di deployment.

• Il pagamento della fase a regime avverrà, a partire dall'esito positivo dalla verifica di conformità della soluzione, con canone trimestrale anticipato su base annuale.

Il pagamento dell'importo di ciascuna fattura, al netto di eventuali penali che dovessero essere comminate, avverrà entro 30 giorni dal ricevimento della fattura elettronica, la cui data sarà comprovata dalla registrazione al Protocollo Generale del Comune di Melito di Napoli, previa verifica della regolarità di esecuzione della fornitura.

Qualsiasi irregolarità riscontrata nella qualità del servizio, nonché nell'emissione della fattura interromperà il termine indicato. Il pagamento dei corrispettivi è subordinato all'acquisizione della documentazione di regolarità contributiva e retributiva, rilasciata dagli enti competenti.

Il pagamento è comunque subordinato all'ottenimento dell'esito positivo dell'asseverazione progetto "'Investimento 1.2 ABILITAZIONE AL CLOUD PER LE PA LOCALI COMUNI (LUGLIO 2022)' - M1C1 PNRR FINANZIATO DALL'UNIONE EUROPEA – NextGenerationEU", oggetto del presente bando.

I pagamenti, relativi al presente contratto, dovranno essere effettuati nel rispetto delle disposizioni di cui alla L.

136/2010 art. 3 (tracciabilità dei flussi finanziari). Il mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti idonei a garantire la piena tracciabilità delle operazioni determinerà la risoluzione di diritto del contratto.

23. RILIEVI

I rilievi sono le azioni di avvertimento da parte dell'Amministrazione conseguenti il non rispetto degli adempimenti contenuti nella documentazione contrattuale. Pertanto oltre a quanto esplicitamente previsto potrà essere emesso un rilievo su qualunque inadempimento se non diversamente sanzionato. Sono notificati al Fornitore tramite comunicazione anche via pec, ognuna delle quali potrà contenere uno o più rilievi.

I rilievi non prevedono di per sé l'applicazione di penali e, se reiterati e accumulati, danno luogo a penali e/o altre azioni contrattuali. Pertanto, l'utilizzo di questa sanzione comporta la presenza in "Indicatori di qualità" di un livello di servizio che determina il numero massimo di rilievi tollerati al cui superamento si un'azione di livello superiore, perdita quota sospesa o penale.

Qualora il Fornitore ritenga di procedere alla richiesta di annullamento del rilievo dovrà sottoporre all'Amministrazione un documento con elementi oggettivi ed opportune argomentazioni entro il termine definito dall'Amministrazione (in genere 3 giorni lavorativi dall'emissione della nota di rilievo).

24. OFFERTA MIGLIORATIVA PER LA REALIZZAZIONE DEI SERVIZI

L'Ente valuterà attentamente le offerte migliorative che potranno arrivare dai singoli operatori economici, in termini di prodotti e di servizi

25. PENALI

Lo scopo delle penali è quello di riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dall'Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate a regola d'arte.

Le penali da adottare sono individuate contrattualmente e normalmente sono organizzate in modo progressivo in relazione alla gravità o al ripetersi della mancata soddisfazione degli adempimenti richiesti.

Qualora successivamente alla sottoscrizione del contratto venga accertato che la qualificazione del Cloud della PA scelto per il presente appalto non sia conforme alle già menzionate previsioni di AgID, l'Ente si riserva il diritto di applicare una penale minima pari 10% del valore dell'intero affido, salvo il maggior danno, e provvederà alla risoluzione del contratto in danno dell'appaltatore.

Resta fermo che in tale evenienza l'Ente provvederà anche ed in ogni caso alla segnalazione all'Autorità Giudiziaria delle dichiarazioni mendaci, affinché vengano perseguite secondo norme vigenti.

26. VERIFICHE DI CONFORMITÀ

Il soggetto deputato all'esecuzione delle attività di verifica di conformità, dopo aver acquisito la documentazione tecnico-funzionale dei servizi (sia a carattere continuativo che progettuale), procederà a certificare la corretta esecuzione degli stessi.

Della verifica di conformità si darà apposita comunicazione al fornitore che potrà parteciparvi. Al termine della suddetta verifica verrà data comunicazione formale al fornitore

27. TEMPI DI RISPOSTA PER ASSISTENZA

Il Fornitore è tenuto a garantire ed assicurare:

1. **interventi a chiamata** con le seguenti due modalità:
    - gli interventi per la risoluzione di guasto bloccante che impedisca qualsiasi prosecuzione dell'attività, il fornitore deve indicare il numero di ore necessarie alla risoluzione della problematica dal momento della ricezione della richiesta di intervento;
    - gli interventi su altre problematiche, il fornitore deve indicare il numero di ore necessarie alla risoluzione della problematica dal momento della ricezione della richiesta di intervento;
2. **interventi su attività programmata**, ovvero concordati sulla base di un calendario nell'ambito della manutenzione periodica;
3. **presidio on site** che richiede la presenza del fornitore presso le sedi del Committente, l'operatore economico dovrà indicare il numero di giorni di presenza presso il cliente nell'arco dell'anno solare nel rispetto delle fasce orarie lavorative, secondo una programmazione che sarà comunicata e concordata con congruo anticipo.

Il Committente si riserva la possibilità di attivare, ognuna delle già menzionate modalità (interventi a chiamata, interventi su attività programmata e presidio on site) sulla base delle esigenze rilevate.

Gli interventi di assistenza potranno essere prestati dal Fornitore da remoto e/o telefonicamente; se non risolvibili in tali modalità, saranno effettuati mediante interventi del personale tecnico del Fornitore presso la sede nella quale si rende necessario adoperarsi;

Gli interventi dovranno essere effettuati normalmente durante l'orario di servizio dell'Ente, salvo i casi in cui si renda necessaria una diversa articolazione oraria al fine di non impattare le attività lavorative dell'Amministrazione.

L'attività di installazione/configurazione, verifica del corretto funzionamento e del ripristino delle funzionalità è a carico del personale tecnico individuato dal Fornitore.

28. REQUISITI DI QUALITÀ DELLA FORNITURA

Nell'esecuzione delle attività contrattualmente previste il Fornitore dovrà:

- rispettare i principi di assicurazione e di gestione della qualità della norma EN ISO 9001, rispetto alla quale gli è richiesta la certificazione;
- implementare e perseguire le soluzioni migliorative proposte dal Fornitore in sede di offerta;
- avanzamento e di controllo e di rendicontazione interna ed esterna, le modalità e gli strumenti per il test funzionale e no, ecc.;
- garantire il corretto e razionale evolversi delle attività contrattualmente previste, nonché la trasparenza e la tracciabilità di tutte le azioni messe in atto dalle parti in causa, il Fornitore e l'Amministrazione contraente;
- rispettare quanto previsto dalla normativa di riferimento.

Il piano di qualità dovrà essere approvato prima dell'avvio delle attività contrattuali e potrà essere aggiornato su richiesta dell'Amministrazione.

29. CRITERI DI AGGIUDICAZIONE

L'aggiudicazione avverrà secondo il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'art. 50, comma 1, lett. e) del D.Lgs n. 36/2023 e ss.mm.ii., con l'acquisizione delle analisi dei prezzi mediante procedure telematiche. Le offerte presentate dalle imprese offerenti saranno analizzate con un sistema di elementi di valutazione esclusivamente matematici.

L'importo a base d'asta è di **€ 135.000,00 (euro centotrentacinque/00)**, oltre IVA comprensivo sia del costo di attivazione dei servizi che del costo della manutenzione e del canone cloud per un periodo di almeno un anno.

Ai fini dell'individuazione dell'offerta più vantaggiosa la stazione appaltante assume gli elementi ed i relativi fattori ponderati di seguito indicati:

QUALITÁ (offerta tecnica): punti massimi 80

PREZZO (offerta economica): punti massimi 20

Totale punti massimi 100

30. ATTRIBUZIONE DEL PUNTEGGIO ALL'OFFERTA TECNICA

All'offerta tecnica verrà attribuito un massimo di 80 punti.

L'Amministrazione, giovandosi dell'ausilio di una Commissione Tecnica, esprime una scelta insindacabile del soggetto la cui offerta tecnica è considerata preferibile, sulla base degli elementi di valutazione (attribuzione dei voti e dei giudizi in relazione a ciascun elemento di valutazione) riportati nelle tabelle da pag. 31 in poi.

31. ATTRIBUZIONE DEL PUNTEGGIO ALL'OFFERTA ECONOMICA

All'offerta economica verrà attribuito un massimo di 20 punti. Al fine dell'applicazione della formula matematica sotto riportata e dell'attribuzione dei conseguenti punteggi, la commissione di gara provvederà a trasformare il prezzo totale offerto indicato dal concorrente, in percentuale di ribasso, rispetto all'importo complessivo a base di gara. Nel caso in cui il totale dell'offerta indicato dal concorrente non corrisponda alla sommatoria dei prezzi offerti per ciascuna Sezione descritta nel capitolato di gara redatto dall'Amministrazione, verrà mantenuto immutato il costo unitario di quest'ultime e si provvederà d'ufficio alla correzione del totale dell'offerta complessiva. Il ribasso percentuale corrispondente a tale prezzo sarà l'unico elemento considerato ai fini dell'attribuzione del punteggio relativo all'offerta economica. Ai fini della determinazione dei coefficienti (punteggi) relativi all'elemento "offerta economica" si applicheranno le seguenti formule:

Ci (per Ai<= A soglia) = 0,85 * Ai / Asoglia

Ci (per Ai> A soglia) = 0,85 + (0,15) * [(Ai-Asoglia) / (Amax – A soglia)]

Dove:

Ci = coefficiente attribuito al concorrente iesimo;

Ai = valore dell'offerta del concorrente iesimo;

Asoglia = media aritmetica dei valori delle offerte dei concorrenti;

32. TEMPI PER L'INVIO DELL'OFFERTA TECNICO / ECONOMICO

Agli operatori invitati sarà assegnato un termine per la presentazione delle offerte tecnico economiche di giorni **10 (dieci)** decorrenti dalla data di invio della lettera di invito che avverrà attraverso RdO sulla piattaforma MEPA.

33. TEMPI DI REALIZZAZIONE DEL PROGETTO

Le attività di progettazione e sviluppo previste dai richiamati Avvisi PNRR **dovranno essere completate entro 540 giorni dalla contrattualizzazione.**

La manutenzione e il canone Cloud dei servizi attivati dovranno essere assicurati per un periodo almeno di un anno.

34. SCHEDA PER LA VALUTAZIONE DEL PROGETTO TECNICO

	Punti di verifica di conformità tecnica del progetto: Aggiornamento in Sicurezza di applicazioni in Cloud

Verifica di conformità tecnica del progetto realizzato e di raggiungimento degli obiettivi prefissati		**PUNTEGGIO MASSIMO ASSEGNABILE**	**Elenco dei documenti verificati/utilizzati per la verifica**	**Note**
P.1.1	Valutazione del cronoprogramma e tempistiche di rilascio.	5		
P.1.2	Valutazione dei requisiti minimi e funzionali dei 14 servizi oggetto della migrazione	3		
P.1.3	Valutazione della disponibilità delle due figure professionali, Responsabile Tecnico e RUAC, rispetto alla reperibilità telefonica dal lunedì al venerdì, dalle ore 8:00 alle ore 20:00 e sempre tramite posta elettronica e al numero di giorni di presenza presso l'Ente nell'anno solare.	15		
P.1.4	Valutazione delle certificazioni (dove presenti) e delle competenze richieste per ogni figura professionale elencata nel paragrafo 5.1.3 (Team di Lavoro).	3		

P.1.5	Valutazione del Piano dei servizi di formazione e affiancamento	15		
P.1.6	Valutazione dell'interoperabilità con altri dei sistemi e in particolare con i seguenti interventi finanziati dalla Presidenza del Consiglio dei ministri – Dipartimento per la Trasformazione Digitale: 1.4.1 Esperienza del Cittadino nei servizi pubblici; 1.4.4 Adozione identità digitale; 1.4.5 Digitalizzazione degli avvisi pubblici – Integrazione con la Piattaforma delle Notifiche Digitali;	5		
P.1.7	Valutazione dei livelli di servizio riguardati la Manutenzione Correttiva ed Adeguativa	2		
P.1.8	Tempi di Risposta del Servizio di assistenza - Interventi a chiamata per la risoluzione di guasto bloccante che impedisca qualsiasi prosecuzione delle attività	3		
P.1.9	Tempi di Risposta del Servizio di assistenza - Interventi a chiamata per la risoluzione di altre problematiche non bloccanti per la prosecuzione delle attività	3		

P.1.10	Tempi di Risposta del Servizio di assistenza - Interventi su attività programmata, ovvero concordati sulla base di un calendario nell'ambito della manutenzione periodica	1		
P.1.11	Tempi di Risposta del Servizio di assistenza - Presidio on site che richiede la presenza del fornitore presso le sedi del Committente	5		
P.1.12	Valutazione dei piani di Backup / Restore e Disaster / Recovery e business continuity	2		
P.1.13	Valutazione della possibilità per gli utenti di utilizzare lo SPID come strumento di autenticazione	3		
P.1.14	Adozione da parte del Fornitore dei principi di cui alla "Carta dei principi tecnologici del procurement"	2		

P.1.15	Valutazione dell'offerta migliorativa	10		
P.1.16	Valutazione dei principi di protezione dei dati	1		
P.1.17	Valutazione dei principi di accessibilità e usabilità	1		
P.1.17	Valutazione dei requisiti minimi di sicurezza	1		

Firmato digitalmente da:

LUIGI PANZERA