CITTA' DI TEMPIO PAUSANIA

C.A.P. 07029 PIAZZA GALLURA N.3 - PROVINCIA DI OLBIA TEMPIO

Servizio ICT

CAPITOLATO TECNICO

per la procedura di appalto avente ad oggetto:

FORNITURA DI UNA PIATTAFORMA DI APPLICATIVI GESTIONALI IN MODALITA' SAAS (SOFTWARE AS A SERVICE) E DEI SERVIZI DI CONFIGURAZIONE, MIGRAZIONE DATI, SUPPORTO OPERATIVO E INTERVENTI POST AVVIO. PNRR M1C1 ASSE 1 INVESTIMENTO 1.2. CUP [C51C22000080006], CIG [9274318154]. ANNUALITA' 2022(quota)-2023-2024-2025-2026-2027-2028.

Indice dei contenuti

1. PREMESSA

Il presente documento ha lo scopo di descrivere i contenuti ed i requisiti minimi in termini di quantità, qualità

e livelli di servizio relativi alla fornitura dei servizi cui deve riferirsi il Fornitore per la formulazione dell'Offerta Economica.
Oggetto dell'appalto è la stipula di un Contratto per l'affidamento dei servizi elencati nel seguito del documento in favore del Comune di Tempio Pausania e che dovranno essere erogati nell'arco di sette anni:
Nel presente documento le caratteristiche minime e i requisiti minimi, ove il Fornitore non fornisca in sede di gara una offerta tecnica inequivocabilmente migliorativa per l'Ente sono da intendersi obbligatori e vincolanti.
La "giornata" o i "giorni" vanno intesi come solari, salvo ove diversamente specificato.
Le "ore" vanno intese come naturali e consecutive, salvo ove diversamente specificato come ore lavorative.

1.1. ACRONIMI

RUP: Responsabile Unico del Procedimento
AgID: Agenzia per Italia Digitale
CAD: Codice dell'Amministrazione Digitale
CONSIP: Consip S.p.A.
SaaS: Software as a Service
ICT: Information and Communication Technology
PA: Pubblica Amministrazione
HTTP: Hyper Text Transport Protocol
HTTPS: Secure HyperText Markup Language
SAL: Stato Avanzamento Lavori

RPO (Recovery Point Objective): rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso;
RTO (Recovery Time Objective): rappresenta la durata di tempo e di un livello di Servizio entro il quale un business process (ovvero il Sistema Informativo primario) deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili;

1.2. DEFINIZIONI

Aggiudicatario/Fornitore/Appaltatore: va intesa l'Impresa/RTI aggiudicataria dell'appalto;

"l'Amministrazione", o "l'Ente" si intende il Comune di Tempio Pausania, con sede in Tempio Pausania, 07029, P.zza Gallura 3.

Modalità "As a Service": Servizio erogato da remoto attraverso i Centri Servizi

Modalità "On premise": Servizio erogato presso le strutture dell'Amministrazione o altre strutture indicate dalla stessa.

2. CONTESTO E AMBITO DI APPLICAZIONE

Il sistema informativo del Comune di Tempio Pausania utilizza attualmente una piattaforma di applicativi gestionali ospitati presso il datacenter comunale in un sistema di cloud privato interno, che rientra nella categoria B secondo la classificazione prevista da AgID.
A seguito dell'introduzione dell'obiettivo di dismissione dei datacenter della categoria B, in favore della migrazione al cloud, l'Amministrazione intende effettuare tale passaggio contestualmente alla migrazione ad una nuova piattaforma di software ritenuti più adeguati alle attuali esigenze dell'Ente.
Le attività correlate a tale intervento sono di molteplice natura e di elevata complessità; per questo motivo l'Ente intende avviare le attività nel corso del 2022 e proseguire per step successivi fino a concludere tutte le attività nelle annualità 2023 e 2024, come dettagliato nel seguito del documento.

Il Fornitore si impegna ad erogare i servizi oggetto dell'appalto secondo le caratteristiche minime ed i livelli di servizio specificati nel seguito del documento e nell'allegato A.

Ai fini del corretto dimensionamento delle risorse dell'infrastruttura di cloud computing e del corretto calcolo

dei canoni annuali, si forniscono i seguenti dati relativi alla dimensione degli archivi attualmente gestiti dall'Ente:

- Dimensione del database relativo a tutte le procedure specificate in 3.1 (tipo SQL Server, file mdf e file ldf): circa 60GB complessivi;
- Dimensione totale allegati per tutte le procedure specificate in 3.1: 538GB;
- Dimensione cartella allegati protocollo anno 2021 : 56GB
- Dimensione cartella allegati protocollo primo semestre 2022 : 29GB
- numero unità in conservazione a norma: 117901;
- numero documenti in conservazione a norma: 231446;
- spazio attualmente occupato in conservazione a norma: 26738 Mb;

3. OGGETTO DELL'APPALTO

L'appalto è strutturato nei seguenti macro gruppi:

a) fornitura di una piattaforma di software applicativi per il supporto alla attività istituzionale dell'Ente in modalità c.d. Software As a Service (SaaS);

b) servizi accessori correlati all'ordinaria gestione di detta piattaforma;

c) servizi ed attività di migrazione delle banche dati attualmente utilizzate dagli attuali server locali ad apposita piattaforma cloud, per la relativa fruizione attraverso i nuovi software applicativi.

d) servizi a supporto degli utenti e dell'amministrazione nella fase di passaggio ai nuovi applicativi. Lo scopo di questi servizi è organizzare, condurre, supportare e coordinare tutte le attività propedeutiche, realizzative e di collaudo relative al passaggio dall'attuale modalità di lavoro che utilizza sistemi server ospitati dalle infrastrutture dell'Ente, alla nuova modalità dove i servizi sono erogati su infrastrutture di terzi in modalità SaaS.

e) servizi di assistenza tecnica, manutenzione ordinaria e straordinaria sugli applicativi.

Maggiori dettagli sull'oggetto dell'appalto sono indicati nei paragrafi che seguono.

3.1. FORNITURA DI UNA PIATTAFORMA DI SOFTWARE APPLICATIVI

Il fornitore si impegna a fornire in modalità SaaS (Software as a Service) l'utilizzo di una piattaforma di software gestionali in grado di gestire i seguenti ambiti di lavoro di interesse dell'Amministrazione, con le funzionalità tipiche richieste dalla normativa:

AREA SCRIVANIA DIGITALE, ARCHIVIO DOCUMENTALE, WORKFLOW, AREA AMMINISTRATIVA

- Scrivania digitale, Archivio documentale, Workflow
- Protocollo
- Modulo versamento verso Sistema di Conservazione
- Conservazione a norma
- Gestione atti Amministrativi: delibere, determine, decreti, ordinanze
- Contratti
- Albo pretorio digitale
- Notifiche di atti e provvedimenti
- Amministrazione trasparente D.Lgs 33/2013 con servizio web
- Sportello servizi al cittadino (istanze on line, ecc.)
- App IO interscambio tra gestionali e APP io
- Conservazione a norma delle attuali tipologie già conservate

AREA SERVIZI DEMOGRAFICI
- Anagrafe, AIRE, LEVE, C.I. SAIA, APR4
- Stato Civile
- Elettorale, Risultati elettorali
- Interscambio con Enti XML-SAIA2/AP5
- Stradari Comunali
- Gestione interfacciamento con Sistema ANPR
- sistema WS interscambio ANPR
- Censimento e toponomastica
- Gestione cimiteriale

AREA ECONOMICO FINANZIARIA
- Contabilità economica patrimoniale D.Lgs. 118/2011
- Contabilità finanziaria
- Contabilità IVA
- Tesoreria, ordinativo informatico
- Cassa Economale
- Contabilita Economato
- Inventario, Patrimonio
- Fattura PA
- Piattaforma PagopA
- Interfaccia con sistema front office Regione Sardegna
- Mutui, Economato, Siope+
- Intermediazione SIOPE +
- Controllo di gestione

TRIBUTI LOCALI
- TARSU
- ICI
- TOSAP
- Cassetto fiscale web del contribuente

RISORSE UMANE
- gestione economica (Paghe) e giuridica personale
- Modello 770
- Gestione rilievo presenze/assenze del personale
- Soprtello web dipendente

AREA TECNICA
- Gestione pratiche edilizie
- Appalti
- GIS/SIT

3.2. SERVIZI ACCESSORI

A corredo della fornitura di software applicativi, dovranno essere erogati i servizi accessori di Backup e di Disaster Recovery in grado di soddisfare le esigenze di continuità operativa contraddistinte da valori di RPO e RTO indicati nei seguenti paragrafi insieme alle caratteristiche minime del servizio.
Sarà inoltre erogato il servizio di conservazione a norma.

3.2.1. BACKUP

I backup dovranno essere eseguiti in modo tale da proteggere almeno le seguenti componenti:
- database server;

- application server;
- storage;
- servizi di infrastruttura;
- database

Le politiche di backup dovranno rispettare le modalità ed i valori descritti nell'allegato A.

In ogni caso dovrà sempre essere possibile per l'ente, a semplice richiesta, il download dei backup in un formato standard che consenta il ripristino su infrastruttura dell'ente, almeno dei database e degli allegati.

3.2.2. DISASTER RECOVERY

Il Disaster Recovery, definito come un insieme di strumenti, procedure e persone, ed in generale di risorse materiali ed immateriali atte a consentire il ripristino delle normali condizioni di operatività del servizio, nel caso in cui si presentasse un evento di qualsiasi natura e di qualsiasi origine tale da compromettere il corretto funzionamento dei sistemi o l'integrità e fruibilità delle banche dati dell'Ente attraverso i sistemi software oggetto del presente documento.
Il servizio di disaster recovery dovrà essere assicurato mediante una replica su altro datacenter e dovrà rispettare i valori di RTO ed RPO indicati nell'allegato A.

3.2.3. SERVIZIO DI CONSERVAZIONE A NORMA

Il servizio prevede la conservazione secondo la normativa vigente dei documenti gestiti dall'amministrazione secondo le seguenti modalità:

a) documenti prodotti automaticamente dai software applicativi e di cui è previsto il trasferimento al sistema di conservazione come il registro di protocollo giornaliero;
b) documenti gestiti tramite gli applicativi gestionali della piattaforma software; sarà previsto il trasferimento in conservazione delle classi documentali di seguito descritte:

DESCRIZIONE	**TEMPI DI CONSERVAZIONE**
DETERMINAZIONI	10 ANNI
ATTI DI LIQUIDAZIONE	10 ANNI
DELIBERE DI GIUNTA	10 ANNI
DELIBERE DI CONSIGLIO	10 ANNI
DELIBERE COMMISSARIALI	10 ANNI
ORDINANZE SINDACALI	10 ANNI
ORDINANZE DIRIGENZIALI	10 ANNI
DISPOSIZIONI SINDACALI	10 ANNI
ORDINI DI SERVIZIO	10 ANNI
PROVVEDIMENTI ORGANIZZATIVI (ALTRI ATTI)	10 ANNI
PROTOCOLLO GENERALE	10 ANNI
PEC – PROTOCOLLO	10 ANNI
PEC – FATTURE PA (estratte dal protocollo)	10 ANNI
PROTOCOLLO REGISTRO GIORNALIERO	10 ANNI
CONTRATTI	10 ANNI
FASCICOLI ELETTORALI	10 ANNI
FATTURE ELETTRONICHE (estratte dalla	10 ANNI

DESCRIZIONE	TEMPI DI CONSERVAZIONE
contabilità)	
FLUSSI SIOPE+	10 ANNI

Nella precedente tabella per “tempi di conservazione” si intende il tempo per il quale il Fornitore si obbliga a conservare, senza costi aggiuntivi rispetto a quelli indicati nell’offerta economica, i documenti attualmente in conservazione presso altro conservatore, **secondo il numero di documenti e la dimensione complessiva indicati al punto 2 e con una stima di 25.000 documenti/anno per i documenti prodotti sulla nuova suite di software**. Resta inteso che al termine di tale periodo temporale dovranno essere rinegoziate le condizioni per una eventuale prosecuzione del servizio.
Il Fornitore si impegna a non porre limiti alle dimensioni, sia del singolo documento che cumulative, dei documenti trasferibili, garantendo l’applicazione delle condizioni economiche stabilite in sede di offerta economica.

3.3. SERVIZI DI MIGRAZIONE AL CLOUD DELLE BANCHE DATI DELL’ENTE

Ai fini della corretta attivazione della piattaforma di software applicativi in modalità SaaS il Fornitore si impegna ad effettuare la corretta e completa migrazione delle banche dati relative ai software gestionali attualmente utilizzati dall’Amministrazione.
Alla corretta conclusione delle operazioni di migrazione, l’Amministrazione dovrà poter accedere ai dati storici contenuti nelle banche dati da migrare, con modalità e funzionalità equivalenti a quelle consentite per i dati inseriti direttamente sugli applicativi e non oggetto di migrazione, con l’eccezione di quei dati che sono stati inseriti in periodi nei quali la normativa prevedeva regole del tutto differenti; a titolo di esempio, i dati contabili antecedenti al passaggio alla contabilità armonizzata ex D.lgs. 118/2011 dovranno essere resi disponibili in modalità “ente storico”, ovvero in una modalità che consente l’accesso ai dati corretti anche se con visualizzazione orientata al D.Lgs.118/2011.
Maggiori dettagli sul processo di migrazione sono contenuti nel paragrafo 4 (Modalità e tempistiche per il completamento delle attività tecniche)

3.4. SUPPORTO POST AVVIO

Successivamente al corretto collaudo della piena funzionalità delle procedure software del Fornitore e alla prima verifica di correttezza ed accessibilità dei dati migrati, il Fornitore si impegna a fornire un supporto agli operatori dell’Ente con **livelli di servizio potenziati.**
Durante questo periodo, che avrà una durata pari a sessanta giorni dalla data di collaudo della singola procedura, il Fornitore si impegna a rendersi disponibile a fornire supporto almeno telefonico ed in teleassistenza per tutte le richieste fatte per il tramite degli operatori del Servizio ICT dell’Ente.
Resta inteso che il Servizio ICT offrirà comunque un primo livello di assistenza per le funzionalità non specialistiche (che richiedano cioè competenze specifiche della materia), ed i servizi di supporto post avvio saranno richiesti solamente se lo staff del Servizio ICT non sarà in grado di fornire risposta agli operatori per le seguenti motivazioni:

- argomento, funzionalità o casistica non trattata o non completamente sviluppata in sede di prima formazione agli operatori dell’Ente;
- eccessivo numero di chiamate agli operatori del Servizio ICT per problematiche legate alla non piena padronanza delle nuove procedure software, attribuendo in questo caso la motivazione dell’elevato numero di chiamate ad una prima formazione non completa.

In ogni caso si conviene che il supporto richiesto per più di due volte per il medesimo argomento e per il medesimo ufficio sarà considerato come non ricadente nella categoria del supporto post avvio e sarà pertanto regolarmente fatturata secondo i prezzi orari stabiliti, previa autorizzazione del RUP/DEC o altra persona da questo autorizzata.

4. MODALITÀ E TEMPISTICHE PER IL COMPLETAMENTO DELLE ATTIVITÀ TECNICHE

In considerazione della complessità delle attività tecniche, e del potenziale impatto che la sostituzione degli applicativi, potrebbero avere sull'attività degli uffici, dovrà essere posta particolare attenzione alla pianificazione delle attività ed al coordinamento con l'amministrazione. Per questo motivo dovrà essere garantito un costante interfacciamento del personale del Fornitore coinvolto nell'esecuzione del contratto, ed in particolare di quello coinvolto nelle attività di migrazione, con il RUP/DEC individuato dall'Amministrazione. Per le stesse motivazioni, è prevista una migrazione graduale dei vari moduli applicativi attualmente in uso; il cronoprogramma per l'esecuzione di dette attività è dettagliato nei paragrafi da 4.1 a 4.3.

Per ciascun blocco di attività, come descritti nei seguenti punti da 4.1 a 4.4, si procederà come segue:

1. Al termine delle attività il Fornitore invierà comunicazione formale al RUP/DEC indicando il "pronti al collaudo";
2. il RUP/DEC concorderà con il Fornitore una data per l'esecuzione delle attività di collaudo, che non dovrà comunque superare il termine di giorni 7 (sette) dalla comunicazione di cui al punto 1. Questo periodo di tempo sarà sempre conteggiato ai fini del calcolo di eventuali penali.
3. nel caso in cui l'Ente dovesse ritenere di dover superare il termine indicato al punto precedente, la differenza in giorni fra la data di effettivo collaudo e detto termine non sarà considerata ai fini del calcolo di eventuali penali.
4. Il RUP/DEC invierà formalmente al Fornitore l'esito del collaudo.
5. Nel caso in cui il collaudo dovesse evidenziare delle anomalie, dati incongruenti o altre riserve, il RUP/DEC segnalerà al Fornitore dette anomalie; il Fornitore procederà alla correzione di dette anomalie nel termine massimo di 45 giorni; l'ente potrà procedere a segnalare ulteriori problematiche dovessero rendersi evidenti durante questo periodo.
6. Al termine di questo periodo, si procederà con un secondo collaudo da parte del RUP/DEC;
7. Nel caso in cui anche il secondo collaudo dovesse evidenziare delle riserve, verranno applicate le penali previste al paragrafo 6 (SLA).
8. I tempi ai fini del calcolo di eventuali penali sarà interrotto esclusivamente da un collaudo positivo della singola area così come definita in 3.1.

4.1. ATTIVAZIONE/MIGRAZIONE DEL PRIMO BLOCCO DI APPLICATIVI

Il primo blocco di attività comprenderà l'attivazione dei moduli software (e della migrazione delle relative banche dati dell'ente se presenti) indicati di seguito:

AREA SCRIVANIA DIGITALE E AMMINISTRATIVA, ARCHIVIO DOCUMENTALE, WORKFLOW, AREA AMMINISTRATIVA

- Protocollo
- Modulo versamento verso Sistema Conservazione
- Conservazione a norma
- Gestione atti Amministrativi: delibere, determine, decreti, ordinanze
- Contratti
- Albo pretorio digitale
- Notifiche di atti e provvedimenti
- Amministrazione trasparente D.Lgs 33/2013 con servizio web
- Sportello servizi al cittadino (istanze on line, per un totale di ottanta moduli)

Al fine di non riversare sugli uffici un carico di lavoro eccessivo nei mesi più impegnativi, le attività dovranno rispettare le tempistiche di seguito riportate:

- entro 90 giorni dalla data di sottoscrizione del verbale di consegna del servizio dovrà essere predisposto, in accordo con il RUP, un piano di formazione a tutti i dipendenti dell'Ente sull'utilizzo dei nuovi moduli applicativi;
- entro 105 giorni dalla data di sottoscrizione del verbale di consegna del servizio saranno completate le attività di:

  - Conservazione a norma delle attuali tipologie già conservate
  - Riversamento dei dati dall'attuale sistema di Conservazione a quello nuovo di destinazione
- entro lo stesso termine di 105 giorni dovrà essere comunicato al RUP il "pronti al collaudo";
- entro 120 giorni dalla data di sottoscrizione del verbale di consegna del servizio tutti i moduli sopra indicati dovranno essere correttamente utilizzabili dalla nuova piattaforma, fermo restando che eventuali anomalie dovranno comunque essere risolte entro le tempistiche specificate al paragrafo 4.

Resta inteso che per il corretto collaudo dei servizi dovranno obbligatoriamente essere state completate tutte le configurazioni relative alla profilazione degli utenti rispetto all'organigramma dell'Ente, alla configurazione, all'interno delle procedure, delle caselle di posta elettronica ordinaria e certificata utilizzate dall'Ente, alle firme digitali utilizzate, ed al funzionamento degli automatismi correlati alla generazione del registro giornaliero di protocollo.

4.2. ATTIVAZIONE/MIGRAZIONE DEL SECONDO BLOCCO DI APPLICATIVI

Entro il primo giorno di novembre 2022 dovranno essere avviate le attività per la migrazione dei seguenti pacchetti applicativi:

AREA SERVIZI DEMOGRAFICI
- Anagrafe, AIRE, LEVE, C.I. SAIA, APR4
- Stato Civile
- Elettorale, Risultati elettorali
- Interscambio con Enti XML-SAIA2/AP5
- Stradari Comunali
- Gestione interfacciamento con Sistema ANPR
- sistema WS interscambio ANPR
- Censimento e toponomastica
- Gestione cimiteriale

AREA ECONOMICO FINANZIARIA
- Contabilità economica patrimoniale D.Lgs. 118/2011
- Contabilità finanziaria
- Contabilità IVA
- Tesoreria, ordinativo informatico
- Cassa Economale
- Contabilità Economato
- Inventario, Patrimonio
- Fattura PA
- Piattaforma PagopA
- Interfaccia con sistema front office Regione Sardegna
- Mutui, Economato, Siope+
- Intermediazione SIOPE +
- Controllo di gestione

RISORSE UMANE
- gestione economica (Paghe) e giuridica personale
- Modello 770
- Gestione rilievo presenze/assenze del personale
- Soprtello web dipendente

TRIBUTI LOCALI
- TARSU
- ICI
- TOSAP
- Cassetto fiscale web del contribuente

Le attività procederanno secondo il seguente cronoprogramma:

Per i moduli di Contabilità e Paghe la comunicazione di “pronti al collaudo” dovrà pervenire entro il giorno 15 Gennaio 2023.

Per gli applicativi relativi all’area dei Servizi Demografici la comunicazione di “pronti al collaudo” dovrà pervenire entro il 30 marzo 2023.

Per gli applicativi relativi all’area dei Tributi Locali la comunicazione di “pronti al collaudo” dovrà pervenire entro il 30 aprile 2023.

Per le modalità per il collaudo, l’eventuale segnalazione di anomalie, e le tempistiche per la relativa correzione ed il calcolo dei tempi per le penali, si procederà con le medesime modalità previste per il primo blocco.

4.3. ATTIVAZIONE/MIGRAZIONE DEL TERZO BLOCCO DI APPLICATIVI

Successivamente al positivo collaudo delle attività previste per il secondo blocco di applicativi, si procederà con le attività previste per il terzo blocco, che comprenderà:

SERVIZI WEB
- App IO interscambio tra gestionali e App IO

AREA TECNICA
- Gestione pratiche edilizie
- Appalti
- GIS/SIT

A decorrere dalla richiesta del RUP, le attività di avvio e migrazione (dove siano presenti dati pregressi) dovranno essere concluse entro il termine di 180 giorni.
Per le modalità per il collaudo, l’eventuale segnalazione di anomalie, e le tempistiche per la relativa correzione ed il calcolo dei tempi per le penali, si procederà con le medesime modalità previste per il primo blocco.

4.4. CONSERVAZIONE

Le attività alla base del procedimento di conservazione a norma rappresentano il cuore del servizio in quanto assicura che i documenti vengano conservati nel rispetto delle norme in vigore.

Acquisizione di documenti conservati pregressi
Il Fornitore si impegna ad acquisire ed inviare in conservazione presso le strutture del Conservatore scelto, tutti i dati già conservati dall’Ente in conformità alla norma vigente presso l’attuale Conservatore dall’Amministrazione. Resta inteso che non sarà richiesta la migrazione di dati che non dovranno essere gestiti con software del Fornitore, come ad esempio i dati SUAPE.

La verifica di tali conformità è preventiva rispetto all’accettazione dei dati conservati da migrare.

Il Responsabile del sistema di conservazione risponde della corretta conservazione dei documenti nei confronti dell’Ente, conformemente a quanto stabilito nelle regole tecniche, e quanto sancito dalla procedura riportata nel “modulo di affidamento del procedimento di conservazione digitale” che viene siglato con l’Amministrazione.
Il manuale della conservazione costituisce uno strumento indispensabile ai fini organizzativi e procedurali per la conservazione dei documenti informatici: il Fornitore del servizio, in qualità di conservatore accreditato delegato dal Cliente, ne garantisce la corretta tenuta e l’aggiornamento rendendolo disponibile all’interno del sito web dell’Agenzia per l’Italia Digitale.

4.5. SERVIZIO DI MANUTENZIONE ORDINARIA E STRAORDINARIA

Durante tutta la durata del contratto, sarà garantito un servizio di manutenzione ordinaria e straordinaria che coprirà le le seguenti casistiche:

- Adeguamenti per correggere anomalie ed errori dovuti a difetti di sviluppo del software;
- Adeguamenti necessari per il rispetto della normativa;

4.6. SUPPORTO ALL'AVVIO

Al corretto collaudo di ciascuna procedura software corrisponderà un adeguato programma di supporto degli utenti che dovranno utilizzare le procedure stesse.
Detto programma sarà concordato con l'Amministrazione secondo i massimali indicati nell'offerta economica, secondo lo schema di offerta proposto.
In ogni caso dovrà essere garantita e compresa nell'offerta economica l'erogazione del seguente numero minimo di giornate di supporto:

Area Gestione Documentale, modulo protocollo: n.2 giornate on site e n.2 giornate da remoto;
Area amministrativa: n.3 giornate on site e n.3 giornate da remoto;
Area demografici: n.4 giornate on site e n.2 giornate da remoto;
Area economico finanziaria: n.6 giornate on site e n.4 giornate da remoto;
Area Tributi Locali: n.2 giornate on site e n.1 giornata da remoto;
Area Risorse umane, moduli paghe e presenze: n.4 giornate on site e n.2 giornate da remoto;
Area servizi web, moduli servizi al cittadino e App IO: n.2 giornate da remoto;
Area Tecnica: n.2 giornate on site e n.6 giornate da remoto;

5. SERVIZIO DI HELP DESK E FORMAZIONE POST AVVIO

Durante tutta la durata del contratto, sarà garantito un servizio di help desk e supporto post-avvio per gestire le seguenti esigenze:

a) Supporto per la correzione di errori causati dagli operatori dell'Ente;
b) Supporto per l'inserimento di un nuovo operatore;
c) Supporto/Formazione generica sull'uso dei software;

Le attività di cui al precedente elenco saranno regolarmente fatturate secondo i prezzi stabiliti in sede di offerta economica, e a seguito di una separata procedura di impegno di spesa.

Si precisa che il costo orario degli interventi che non risultino fra quelli da erogarsi a titolo gratuito, secondo quanto stabilito nel presente Capitolato Tecnico, sarà quello di una giornata/uomo (da offerta economica) diviso per sei (durata in ore della giornata lavorativa).

Il fornitore si impegna a rendere a titolo gratuito gli interventi di supporto di durata inferiore a 30 minuti, con le seguenti limitazioni:

- la richiesta dovrà preliminarmente essere valutata dal Servizio ICT dell'Ente;
- il numero complessivo di richieste dovrà comunque rimanere contenuto all'interno di un perimetro di buona fede e leale collaborazione con il Fornitore;

Il servizio dovrà essere attivo con i seguenti canali:

1. Richiesta telefonica (per le urgenze);
2. Richiesta via servizio di gestione ticket messo a disposizione dal Fornitore;

Le tempistiche di intervento dovranno in ogni caso rispettare quanto stabilito nel paragrafo 6. (SLA).

6. SERVICE LEVEL AGREEMENT (SLA)

Nel presente paragrafo sono indicati i livelli di servizio che dovranno essere garantiti per tutta la durata del contratto, insieme alle penali relative al mancato rispetto degli stessi.

6.1 SLA PER EROGAZIONE SERVIZI CLOUD

DESCRIZIONE	INDICATORE	LIVELLO RICHIESTO	PENALI
Disponibilità servizi SaaS (escluse finestre di manutenzione)	Percentuale disponibilità mensile (uptime)	99,5%	1‰ dell'importo contrattuale ogni 0,1% di sforamento rispetto al livello richiesto.
RPO (backup)	Tempo in ore	8 ore	1‰ dell'importo contrattuale ogni ora di sforamento rispetto al livello richiesto.
RTO (backup)	Tempo in ore	24 ore	1‰ dell'importo contrattuale ogni ora di sforamento rispetto al livello richiesto.
RPO (Disaster Recovery)	Tempo in ore	24 ore	1‰ dell'importo contrattuale ogni ora di sforamento rispetto al livello richiesto.
RTO (Disaster Recovery)	Tempo in ore	24 ore	1‰ dell'importo contrattuale ogni ora di sforamento rispetto al livello richiesto.

Nella precedente tabella, per finestra di manutenzione si intende la fascia oraria dalle ore 18.00 alle ore 8.00 del giorno seguente.
L'accesso alle applicazioni sarà garantito tutti i giorni lavorativi dal lunedì al venerdì dalle ore 8:00 alle ore 18:00. Al di fuori dell'orario garantito, le applicazioni saranno accessibili, salvo interruzioni necessarie per attività di ordinaria manutenzione quali: l'aggiornamento del sistema, l'esecuzione di attività sistemistiche, backup, etc.. Eventuali interventi straordinari per la risoluzione di malfunzionamenti bloccanti potranno essere eseguiti in qualsiasi momento.

Eventuali attività di manutenzione ordinaria che possano determinare l'indisponibilità anche parziale del servizio saranno comunicate con 3 giorni di anticipo.

I servizi di ripristino da backup saranno disponibili in orario lavorativo da lunedì a venerdì dalle 8:00 alle 18:00.

6.2. SLA PER MANUTENZIONE ORDINARIA E STRAORDINARIA

DESCRIZIONE	INDICATORE	LIVELLO RICHIESTO	PENALI
Manutenzione correttiva per interventi classificati GRAVI	Tempo di risoluzione (anche con workaround).	entro 2 ore lavorative successive alla presa in carico nel 90% delle segnalazioni ed entro 8 ore lavorative successive alla presa in carico nel 10% delle	€ 20,00 ogni ora di sforamento rispetto al livello richiesto.

		segnalazioni	
Manutenzione correttiva per interventi classificati NON GRAVI	Tempo di risoluzione (anche con workaround).	entro 24 ore lavorative successive alla presa in carico nel 90% delle segnalazioni ed entro 48 ore lavorative successive alla presa in carico nel 10% delle segnalazioni	€ 5,00 ogni ora di sforamento rispetto al livello richiesto.

Le segnalazioni saranno considerate GRAVI in questi casi: uno o più servizi sono completamente bloccati oppure nessun servizio SaaS è bloccato, ma le funzionalità critiche di uno o più moduli dell'applicazione non sono disponibili o sono malfunzionanti.

I servizi professionali a supporto del servizio SaaS saranno garantiti tutti i giorni lavorativi dal lunedì al venerdì dalle ore 8:00 alle ore 18:00, tramite un portale di Trouble Ticketing utilizzabile per sottomettere le richieste di assistenza, reso disponibile 24 ore al giorno per 365 giorni all'anno.

Ogni richiesta sarà presa in carico dall'operatore di Help Desk in orario lavorativo da lunedì a venerdì dalle 8:00 alle 18:00 entro le 2 ore lavorative successive.

L'operatore analizza e classifica la richiesta per livello di gravità. Le tipologie previste sono riconducibili a:

(a) manutenzione correttiva: alle segnalazioni classificate come GRAVI sarà fornita la soluzione del problema secondo i livelli di servizio indicati nella tabella; alle altre segnalazioni (NON GRAVI), sarà fornita la soluzione tempestiva del problema, anche temporaneamente tramite l'adozione di workaround. Lo stato di avanzamento delle richieste sottomesse dovrà essere consultabile via web;

(b) manutenzione normativa ordinaria: prevede il rilascio degli aggiornamenti in tempo utile per garantire la regolare operatività in funzione della data imposta dalla nuova disposizione;

(c) assistenza utente: l'utente verrà ricontattato da un consulente via telefono o e-mail, con tempestività, sulla base della richiesta. Eventuali chiarimenti, suggerimenti o istruzioni saranno forniti purché di rapida e semplice comprensione. Qualora la richiesta comporti un'attività riconducibile a formazione o ad una specifica esigenza di configurazione funzionale, verrà proposta la pianificazione di un intervento dedicato che sarà fatturato secondo le modalità previste al punto 5.

(d) aggiornamento dei moduli applicativi attivati all'ultima versione rilasciata: le procedure per il passaggio in esercizio delle modifiche applicative e normative al software oppure gli interventi sull'ambiente di produzione, saranno effettuati, previa comunicazione, dopo le ore 18:00 dei giorni lavorativi, oppure nei giorni di sabato e domenica. Qualora si renda necessario procedere diversamente sarà onere del Fornitore concordare con l'Ente preventivamente il giorno e l'ora in cui sarà attivato l'aggiornamento.

6.3. SLA PER SUPPORTO/FORMAZIONE POST AVVIO E HELP DESK

Nel periodo e per servizi specificati al paragrafo 5 dovranno essere rispettati i seguenti livelli di servizio:

DESCRIZIONE	INDICATORE	LIVELLO RICHIESTO	PENALI
Supporto per risoluzione di problemi causati dall'utente	Tempo di intervento	entro 24 ore lavorative successive alla chiamata nel 90% dei casi ed entro 48 ore lavorative successive alla chiamata nel 10% dei casi	0,5‰ dell'importo contrattuale ogni punto percentuale di sforamento rispetto ai livelli richiesti.
Richiesta di formazione generica	Tempo di intervento	entro 48 ore lavorative successive alla chiamata nel 90% dei casi ed entro	0,5‰ dell'importo contrattuale ogni punto percentuale

		96 ore lavorative successive alla chiamata nel 10% dei casi	di sforamento rispetto ai livelli richiesti.

6.4. SLA PER AVVIO/MIGRAZIONE DATI

In caso di ritardo rispetto alle tempistiche previste nel paragrafo 4, e nei casi previsti nello stesso, si applicheranno i seguenti livelli di servizio e relative penali:

DESCRIZIONE	INDICATORE	LIVELLO RICHIESTO	PENALI
Ritardo rispetto ai tempi previsti per l'attivazione del servizio o della risoluzione delle anomalie	Giorni di ritardo rispetto ai tempi previsti per il collaudo positivo	0 giorni	1‰ dell'importo contrattuale ogni giorno di ritardo

6.5. ALTRE PENALITÁ

In caso di parziale o totale inadempimento degli obblighi contrattuali assunti, ferma restando la facoltà della Stazione Appaltante di risoluzione del contratto ove ne ricorrano i presupposti, l'Appaltatore ha l'obbligo di ovviare in un termine stabilito dal Responsabile del Procedimento all'infrazione contestatale ed al pagamento degli eventuali maggiori danni subiti dalla Stazione Appaltante a causa dell'inadempimento.

In ogni caso, il mancato rispetto dei requisiti minimi richiesti nell'allegato A, anche solo per un periodo di tempo limitato, costituisce valida motivazione per la risoluzione contrattuale.

In ogni caso saranno garantiti i seguenti ulteriori livelli di servizio:

DESCRIZIONE	INDICATORE	LIVELLO RICHIESTO	PENALI
Ritardo rispetto alla richiesta di download di una copia di backup dei dati dell'ente.	Giorni che intercorrono fra la il momento della richiesta ed il momento in cui si ha la disponibilità dei dati	7 giorni	1‰ dell'importo contrattuale ogni giorno di ritardo

7. MODALITÁ DI APPLICAZIONE DELLE PENALI

Gli eventuali scostamenti degli indicatori indicati in tabella che daranno luogo all'applicazione delle corrispondenti penali, verranno contestati all'aggiudicatario per iscritto dal RUP/DEC. L'aggiudicatario dovrà comunicare in ogni caso le proprie deduzioni al RUP/DEC nel termine massimo di 5 (cinque) giorni lavorativi dalla stessa contestazione. Qualora dette deduzioni non siano accoglibili a giudizio del RUP ovvero non vi sia stata risposta o la stessa non sia giunta nel termine indicato, potranno essere applicate le penali sopra indicate.
Nel caso di applicazione delle penali, l'Ente provvederà a recuperare l'importo sulle relative fatture, ovvero, in alternativa, all'escussione delle garanzie definitive per la quota parte relativa alla penale calcolata come sopra indicato.

8. GESTIONE DELLA SICUREZZA

I livelli minimi di sicurezza, insieme ad altre caratteristiche ritenute essenziali ai fini della corretta conduzione dell'appalto sono dettagliate nell'allegato A, da considerarsi parte integrante e sostanziale del presente documento.

9. INDICAZIONI GENERALI PER L'EROGAZIONE DEI SERVIZI

Le prestazioni contrattuali dovranno essere eseguite secondo le specifiche contenute nel presente documento. L'Appaltatore si impegna ad eseguire le predette prestazioni, senza alcun onere aggiuntivo, salvaguardando, per quanto possibile, le esigenze dell'Ente e di terzi autorizzati, senza recare intralci, disturbi o interruzioni all'attività lavorativa in atto salvo quelle necessarie per lo svolgimento delle attività.
Per l'erogazione dei servizi sopra indicati, l'aggiudicatario dovrà operare con strumenti software di sua proprietà. L'Ente garantirà comunque l'accesso alle risorse dell'infrastruttura informatica che si renderanno necessarie ai fini della corretta esecuzione dell'appalto; per tale motivo, l'aggiudicatario potrà avere accesso agli uffici comunali nell'orario di apertura degli uffici, subordinato alla presenza di un referente dell'Amministrazione, o accesso alle banche dati dell'Ente mediante il supporto di un referente del Servizio ICT.
L'aggiudicatario si impegna a:

- non installare prodotti software di cui non siano presenti le relative licenze;
- non connettere dispositivi hardware di alcun genere alla rete informatica dell'Ente se non autorizzata preventivamente dall'amministratore di sistema o dal Direttore dell'esecuzione del contratto.

10. COLLAUDO E DECORRENZA DEI TEMPI

Vista la complessità delle attività di migrazione, la relativa durata prevista, nonché le possibili problematiche che potrebbero presentarsi, portando ad un allungamento dei tempi di migrazione, la migrazione di ogni procedura sarà soggetta a collaudo da parte del RUP.
Il Fornitore si impegna a:

1. fatturare esclusivamente le attività eseguite ed approvate dal RUP;
2. fatturare i canoni di manutenzione ordinaria e straordinaria per le sole procedure software correttamente attivate, a seguito di collaudo ed approvazione da parte del RUP;

11. PROPRIETÀ DEI DATI

Tutti i dati migrati sulle procedure software oggetto dell'appalto e tutti quelli che verranno prodotti sono di proprietà dell'Ente.
Al termine del contratto, nel caso in cui questo non dovesse essere rinnovato, il Fornitore si impegna:

- ad agevolare le normali operazioni necessarie per la migrazione dei dati dell'Ente verso altra piattaforma software di terzi;
- a consegnare all'Ente una copia di tutti i dati di sua proprietà e gestiti mediante gli applicativi software del Fornitore, in formati standard e senza limitazione alcuna di accesso o utilizzo. A tale scopo saranno forniti, a titolo esemplificativo e non esaustivo: basi di dati, file, documenti informatici di qualsiasi natura allegati, caricati e prodotti nell'utilizzo delle procedure software, sia da parte degli operatori dell'Ente che da parte degli utilizzatori esterni (cittadini, imprese, altri enti).
- Fornire all'Ente tutte le credenziali e le informazioni di carattere tecnico eventualmente necessarie per il corretto utilizzo dei dati indicati al punto precedente.

12. PRIVACY

12.1 NOMINA DEL RESPONSABILE DEL TRATTAMENTO

L'Appaltatore verrà formalmente nominato Responsabile del trattamento ai sensi dell'art. 4, comma 1, lett. *h)* del decreto legislativo 30 giugno 2003, n. 196 e ss.mm.ii.

12.2. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

Il Fornitore si impegna a:

- effettuare le operazioni di trattamento dei Dati solo per le finalità connesse allo svolgimento delle attività oggetto del Contratto;
- implementare le misure tecniche ed organizzative ritenute adeguate dal Titolare;
- attenersi alle istruzioni comunicate dal Titolare;
- effettuare le operazioni di trattamento dei Dati per un periodo di tempo non superiore alla durata del Contratto. Al termine del Contratto, il Fornitore si impegna a cancellare o distruggere, su scelta ed indicazione scritta del Titolare, tali Dati, salva la possibilità di conservarli per periodi più lunghi a fini di archiviazione nel pubblico interesse o a fini statistici.
- assistere e collaborare con il Titolare nell'adempimento degli obblighi di cui agli artt. 32-36 del GDPR tenuto conto della natura del trattamento e nella misura ragionevolmente necessaria, quali a titolo esemplificativo: (i) la notifica all'Autorità Garante di una eventuale violazione dei Dati; (ii) l'effettuazione dell'analisi del rischio dei trattamenti posti in essere;
- informare il Titolare, in caso di violazione dei Dati, entro 48 (quarantotto) ore dopo essere venuto a conoscenza della violazione, (includendo, se possibile, la natura della violazione, le categorie di Dati violati e il numero approssimativo di interessati).
- informare il Titolare di qualsiasi richiesta legalmente vincolante, ricevuta da un'Autorità incaricata dell'applicazione della legge, di divulgazione dei dati personali oggetto del trattamento tenuto conto della natura dello stesso e nella misura ragionevolmente necessaria, fatto salvo che tale divulgazione non sia espressamente vietata delle norme di legge in vigore.

Così come specificato nelle linee guida n.8 di ANAC sull'acquisizione di software, per scongiurare la possibilità di lock-in il Fornitore si impegna altresì ad esportare gratuitamente, in ogni momento e a richiesta dell'Ente con preavviso di dieci giorni, l'intera base di dati (inclusi di ogni tipo di indice o metadato utilizzato per implementare le funzionalità del software stesso) in formato standard, aperto e documentato.

12.3. OBBLIGHI DEL TITOLARE

Il Titolare garantisce di adempiere ai propri obblighi previsti dalla Normativa Privacy e, pertanto, il Responsabile potrà lecitamente effettuare le operazioni di trattamento dei Dati necessarie ai fini dell'esecuzione delle attività oggetto del Contratto; il Titolare manleva pertanto il Responsabile da qualsiasi conseguenza in relazione alla garanzia che precede.
Il Titolare comunicherà al Responsabile del trattamento eventuali variazioni e rettifiche dei Dati, nonché qualsiasi richiesta da parte di un interessato relativa alla cancellazione o rettifica, opposizione o limitazione al trattamento.

13. FATTURAZIONE E PAGAMENTI

Per il pagamento dei corrispettivi l'aggiudicatario dovrà inviare conforme fattura elettronica all'indirizzo IPA di fatturazione elettronica **BUQWB1** che sarà onorata nei termini di legge, fermo restando i controlli fiscali e le liberatorie previdenziali ed assistenziali.
Ciascuna fattura dovrà contenere il riferimento al codice CIG associato alla presente procedura.

L'importo delle predette fatture verrà corrisposto con bonifico bancario, previo accertamento della/e prestazione/i effettuata/e, entro 30 (trenta) giorni dalla data di ricevimento della fattura, sul/i conto/i corrente/i indicati ai sensi della normativa sulla tracciabilità dei flussi finanziari per la Pubblica Amministrazione.
L'Appaltatore, sotto la propria esclusiva responsabilità, renderà tempestivamente note all'Ente le variazioni che si verificassero circa le modalità di accredito di cui sopra. In difetto di tale comunicazione, anche se le

variazioni venissero pubblicate nei modi di legge, l'Appaltatore non potrà sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti.

In ogni caso la fatturazione seguirà le indicazioni specificate nei paragrafi 13.1 e 13. 2.

13.1 ATTIVITÀ UNA TANTUM

Fermo restando quanto stabilito nei precedenti paragrafi circa le tempistiche, il collaudo e le eventuali penali, ai fini del pagamento del corrispettivo contrattuale, l'Appaltatore emetterà fatture posticipate in una o più rate relative agli stati di avanzamento;

13.2 CANONI

I canoni relativi al servizio SaaS di utilizzo delle procedure software e dei servizi connessi (manutenzione ordinaria e straordinaria) seguiranno una fatturazione posticipata a cadenza semestrale.

In ogni caso resta inteso che il canone di una singola area, così come intese nei paragrafi da 4.1 a 4.3, comprende l'utilizzo di tutti i moduli della stessa anche di quelli non ancora richiesti o attivati.

13.3 ATTIVITÁ DI SUPPORTO POST AVVIO

Le attività di supporto post-avvio che non rientrino fra quelle da erogarsi a titolo gratuito secondo quanto indicato nel presente Capitolato Tecnico, seguiranno una fatturazione con frequenza massima bimestrale se non programmate. Le attività programmate potranno essere fatturate subito dopo il positivo collaudo del RUP/DEC.

Allegati:
Allegato A – MISURE MINIME DI SICUREZZA;

Allegato A

MISURE MINIME DI SICUREZZA

Sommario

SUITE DI APPLICATIVI GESTIONALI

Il presente documento descrive le caratteristiche tecniche minime che devono essere possedute dai sistemi software oggetto della procedura di gara in ambito di sicurezza informatica e rispetto dei principi e delle prescrizioni del GDPR e del D.lgs. 196/2003 e ss.mm.ii.

GDPR E CLOUD

La suite di prodotti software oggetto di appalto deve basarsi su una piattaforma di cloud computing conforme alle leggi sulla privacy tra Unione Europea e Stati Uniti e alle clausole del modello UE con criteri di privacy e misure di sicurezza per proteggere i dati nel cloud, incluse le categorie di dati personali specificate dal GDPR.

- Gestione delle identità e controllo dell'accesso: autorizzazione mediante integrazione con i controller di Active Directory (Microsoft AD) dell'Ente. Solo gli utenti autorizzati possono accedere ad ambienti, ai dati e alle applicazioni; le operazioni effettuate dal singolo utente applicativo sono tracciate in tempo reale;
- Sono utilizzate le seguenti tecnologie (o equivalenti) per rispettare gli obblighi del GDPR:
    - crittografia automatica dei dati by design secondo standard quali AES 256 o di equivalente sicurezza.
    - anonimizzazione dei dati sensibili
    - controllo e registrazione degli eventi, con identificazione e correzione dei problemi di sicurezza (Log Analytics)
- I DBMS Server ed i database dovranno essere di livello adeguato a fornire servizi di tipo enterprise e standard di sicurezza avanzati, con criteri che rispettano le politiche di *privacy by design e by default* tipiche del GDPR.

Le funzionalità di sicurezza predefinite devono consentire la riduzione dei rischi e l'adeguamento ai principi del Regolamento europeo in materia di protezione dei dati personali. Fra queste sono richieste:

- firewall per limitare l'accesso ai singoli database all'interno del server; l'accesso è quindi consentito esclusivamente alle connessioni autorizzate.
- L'autenticazione garantisce l'accesso al server di database ai soli utenti autorizzati con credenziali valide. Le autorizzazione del DBMS permettono di gestire gli accessi ai dati in base al principio dei privilegi minimi.
- La mascheratura dei dati dinamica per limitare l'esposizione dei dati sensibili.

La protezione dei dati personali dalle minacce alla sicurezza, per soddisfare il requisito relativo alla notifica delle violazioni dei dati imposto dal GDPR, dovrà essere garantita inoltre da:

- Transport Layer Security (TLS) per la protezione dei dati in transito nelle connessioni al database.
- Audit Log con cui è possibile produrre un log di controllo in grado di identificare le possibili minacce o i casi sospetti di abuso o violazione della sicurezza.
- Sistema di rilevamento delle minacce integrato, per rilevare attività insolite e sospette.

POLITICHE DI BACKUP

Deve essere garantita l'esecuzione periodica e programmata di procedure di backup per consentire di far fronte alle situazioni in cui sussiste una esigenza di immediato recupero dei dati a prescindere dalla causa.

BACKUP DI TIPO POINT-IN-TIME

Restore automatico (point-in-time) che garantisca il ripristino su un periodo fino a 20 gg precedenti dalla data attuale.
La periodicità con cui i backup vengono effettuati automaticamente è di 20 minuti o inferiore.

BACKUP DI TIPO LONG-TERM

Deve essere conservato un backup settimanale del database per 8 anni dalla data di esecuzione.

BUSINESS CONTINUITY E DISASTER RECOVERY

I dati e l'intera infrastruttura è replicata su in una diversa regione rispetto a quello del sito primario.

ACCESSO AI DATI E ALL'APPLICATIVO

L'accesso agli applicativi e quindi ai dati avviene esclusivamente tramite browser su protocollo https, i dati scambiati vengono protetti dal protocollo TLS (Transport Layer Security).

POLICY PASSWORD DI ACCESSO

Il sistema di autenticazione, integrabile con l'identity manager interno dell'Ente (Active Directory) impone un cambio password periodico e una complessità minima.
È gestita la politica "Strong password".

AUTENTICAZIONE MEDIANTE ACTIVE DIRECTORY

La suite consente l'accesso per mezzo delle credenziali di dominio Active Directory, in modo da non richiedere credenziali aggiuntive agli utenti rispetto a quelle necessarie per l'accesso alle proprie postazioni di lavoro.

UTILIZZO SPAZI DI ARCHIVIAZIONE

Lo storage di archiviazione per i file prodotti nell'uso degli applicativi utilizza un sistema di crittografia/decrittografia trasparente con algoritmi conformi a FIPS 140-2.

GESTIONE IDENTITA' - PRESENZA DI UN IDENTITY MANAGER ALL'INTERNO DELL'ENTE

Il sistema deve essere predisposto per attivare IM centralizzati (es. LDAP, Active directory) integrandosi nativamente con l'IM già in dotazione dell'Ente.

ACCESSO ALL'APPLICATIVO

Agli applicativi si deve accedere tramite portale o webservice solo previa autenticazione.
Il protocollo utilizzato per i portali che espongono il servizio in internet è *https.*

CONDIVISIONE DI RISORSE

Il sistema non condivide risorse se non tramite webservices opportunamente configurati ed abilitati, sottoposti a rigorose regole di visibilità.

ACCESSO AL DATABASE

Il sistema non dispone di un accesso diretto sui DBMS e non mette a disposizione alcun metodo o tool per interrogare lo schema. Nel DBMS ogni schema ha una profilatura minima che consente di operare solo sui dati relativi all'applicazione.

POLITICHE DI BACKUP

Sono applicati i seguenti livelli minimi:

- RTO (recovery time objective): 8 h
- RPO (recovery point objective): 24 h
- Retention: 15 gg per i componenti; database 15 gg + 1 backup per ciascuna settimana dell'ultimo mese, 1 copia mensile per 6 mesi.

DISASTER RECOVERY

In caso di Disastro vengono ripristinati i backup ed attivato il sito di DR (disaster recovery) con i seguenti livelli di servizio minimi:

- RTO (recovery time objective): 24 h
- RPO (recovery point objective): 24 h
- Retention: 48 h

SERVIZI DI INFRASTRUTTURA

Per consentire personalizzazioni o customizzazioni in sicurezza deve essere consentito l'accesso ad un ambiente protetto e differente da quello in produzione:

- su macchine dedicate e con servizi preservati
- creando un ecosistema virtuale per ciascun accesso in modo da impedire il libero accesso alla macchina
- creando un accesso alla singola parte necessaria dell'installazione dell'ente.

SITO WEB: FRONT END SERVIZI ON LINE

L'accesso per le seguenti tipologie:

- operatori dell'ente
- cooperazione applicativa
- cittadini ed imprese

è previsto esclusivamente tramite protocollo HTTPS.

ACCESSO DEDICATO AGLI OPERATORI DELL'ENTE

Tutti gli accessi vengono rilevati e dettagliati in file log, dove viene tracciato oltre al giorno e l'ora dell'accesso anche l'IP dal quale viene eseguito l'accesso stesso.

Sono utilizzati diversi profili di accesso amministrativo al sistema:

- utente amministratore: è l'unico accesso che può visualizzare in chiaro le informazioni relative ai cittadini, inclusi i dati personali forniti dall'utente stesso in fase di primo accesso al sistema (registrazione e/o accesso mediante SPID o sistema terzo).

- amministratori di servizio / operatori: hanno accesso solo ed esclusivamente alle proprie funzioni senza poter accedere alla consultazione dei dati personali dei cittadini censiti nel sistema

ACCESSO IN COOPERAZIONE APPLICATIVA

I servizi erogati nel portale devono interagire con i sistemi dell'ente in modalità di cooperazione applicativa. Tutti i webservice esposti dal sistema gestiscono il livello di autenticazione.

ACCESSO DEDICATO AI CITTADINI ED ALLE IMPRESE

L'accesso all'area riservata avviene mediante protocollo HTTPS.

Il sistema ha un suo repository utenti, ma interagisce con sistemi terzi certificati come SPID (Sistema Pubblico Identità Digitale).

GESTIONE INFORMATIVE E CONSENSI

Tutti i servizi esposti al cittadino consentono all'Ente di erogare in modalità web – online i propri servizi istituzionali.
Vengono richieste al cittadino anche ulteriori informazioni quali email e/o SMS che vengono poi utilizzati per facilitare l'erogazione dei servizi mediante invio di apposite comunicazioni o notifiche automatiche.

INFORMATIVA

Sono previste apposite informative personalizzabili.

CONSENSO

Per tutti gli utenti di portale (cittadini, imprese, etc.), all'atto del primo accesso, qualunque sia il sistema di autenticazione adottato, viene richiesto di autorizzare il trattamento dei dati descrivendone gli aspetti tecnici ed operativi legati alla soluzione.

RICHIESTA CANCELLAZIONE DATI

È prevista apposita funzione attraverso la quale il cittadino potrà richiedere la cancellazione dei propri dati. La richiesta viene tracciata nel sistema ed inviata al Responsabile del Trattamento dei dati dell'Ente. Sempre attraverso apposita funzione è possibile procedere con la cancellazione come richiesto. Le informazioni che verranno cancellate sono il profilo dell'utente con tutte le informazioni di contatto.

RETTIFICA DATI

Per quanto concerne la rettifica dei propri dati personali, il cittadino può procedere in autonomia modificando quanto precedentemente dichiarato.

PSEUDONIMIZZAZIONE DEI DATI

Il sistema, nativamente, prevede la separazione fra le informazioni necessarie all'accesso, i dati anagrafici e personali degli individui e le informazioni poi generate nei singoli ambiti applicativi.

L'accesso alla sezione dove sono visibili le informazioni degli individui è consentito solo all'amministratore.

Nelle altre sezioni sono presenti solo le informazioni specifiche ed un riferimento al solo nome e cognome senza ulteriori informazioni e quindi di fatto senza poter risalire con certezza alla persona.

Allegato A

MISURE MINIME DI SICUREZZA

Sommario

SUITE DI APPLICATIVI GESTIONALI

Il presente documento descrive le caratteristiche tecniche minime che devono essere possedute dai sistemi software oggetto della procedura di gara in ambito di sicurezza informatica e rispetto dei principi e delle prescrizioni del GDPR e del D.lgs. 196/2003 e ss.mm.ii.

GDPR E CLOUD

La suite di prodotti software oggetto di appalto deve basarsi su una piattaforma di cloud computing conforme alle leggi sulla privacy tra Unione Europea e Stati Uniti e alle clausole del modello UE con criteri di privacy e misure di sicurezza per proteggere i dati nel cloud, incluse le categorie di dati personali specificate dal GDPR.

- Gestione delle identità e controllo dell'accesso: autorizzazione mediante integrazione con i controller di Active Directory (Microsoft AD) dell'Ente. Solo gli utenti autorizzati possono accedere ad ambienti, ai dati e alle applicazioni; le operazioni effettuate dal singolo utente applicativo sono tracciate in tempo reale;
- Sono utilizzate le seguenti tecnologie (o equivalenti) per rispettare gli obblighi del GDPR:
    - crittografia automatica dei dati by design secondo standard quali AES 256 o di equivalente sicurezza.
    - anonimizzazione dei dati sensibili
    - controllo e registrazione degli eventi, con identificazione e correzione dei problemi di sicurezza (Log Analytics)
- I DBMS Server ed i database dovranno essere di livello adeguato a fornire servizi di tipo enterprise e standard di sicurezza avanzati, con criteri che rispettano le politiche di *privacy by design e by default* tipiche del GDPR.

Le funzionalità di sicurezza predefinite devono consentire la riduzione dei rischi e l'adeguamento ai principi del Regolamento europeo in materia di protezione dei dati personali. Fra queste sono richieste:

- firewall per limitare l'accesso ai singoli database all'interno del server; l'accesso è quindi consentito esclusivamente alle connessioni autorizzate.
- L'autenticazione garantisce l'accesso al server di database ai soli utenti autorizzati con credenziali valide. Le autorizzazione del DBMS permettono di gestire gli accessi ai dati in base al principio dei privilegi minimi.
- La mascheratura dei dati dinamica per limitare l'esposizione dei dati sensibili.

La protezione dei dati personali dalle minacce alla sicurezza, per soddisfare il requisito relativo alla notifica delle violazioni dei dati imposto dal GDPR, dovrà essere garantita inoltre da:

- Transport Layer Security (TLS) per la protezione dei dati in transito nelle connessioni al database.
- Audit Log con cui è possibile produrre un log di controllo in grado di identificare le possibili minacce o i casi sospetti di abuso o violazione della sicurezza.
- Sistema di rilevamento delle minacce integrato, per rilevare attività insolite e sospette.

POLITICHE DI BACKUP

Deve essere garantita l'esecuzione periodica e programmata di procedure di backup per consentire di far fronte alle situazioni in cui sussiste una esigenza di immediato recupero dei dati a prescindere dalla causa.

BACKUP DI TIPO POINT-IN-TIME

Restore automatico (point-in-time) che garantisca il ripristino su un periodo fino a 20 gg precedenti dalla data attuale.
La periodicità con cui i backup vengono effettuati automaticamente è di 20 minuti o inferiore.

BACKUP DI TIPO LONG-TERM

Deve essere conservato un backup settimanale del database per 8 anni dalla data di esecuzione.

BUSINESS CONTINUITY E DISASTER RECOVERY

I dati e l'intera infrastruttura è replicata su in una diversa regione rispetto a quello del sito primario.

ACCESSO AI DATI E ALL'APPLICATIVO

L'accesso agli applicativi e quindi ai dati avviene esclusivamente tramite browser su protocollo https, i dati scambiati vengono protetti dal protocollo TLS (Transport Layer Security).

POLICY PASSWORD DI ACCESSO

Il sistema di autenticazione, integrabile con l'identity manager interno dell'Ente (Active Directory) impone un cambio password periodico e una complessità minima.
È gestita la politica "Strong password".

AUTENTICAZIONE MEDIANTE ACTIVE DIRECTORY

La suite consente l'accesso per mezzo delle credenziali di dominio Active Directory, in modo da non richiedere credenziali aggiuntive agli utenti rispetto a quelle necessarie per l'accesso alle proprie postazioni di lavoro.

UTILIZZO SPAZI DI ARCHIVIAZIONE

Lo storage di archiviazione per i file prodotti nell'uso degli applicativi utilizza un sistema di crittografia/decrittografia trasparente con algoritmi conformi a FIPS 140-2.

GESTIONE IDENTITA' - PRESENZA DI UN IDENTITY MANAGER ALL'INTERNO DELL'ENTE

Il sistema deve essere predisposto per attivare IM centralizzati (es. LDAP, Active directory) integrandosi nativamente con l'IM già in dotazione dell'Ente.

ACCESSO ALL'APPLICATIVO

Agli applicativi si deve accedere tramite portale o webservice solo previa autenticazione.
Il protocollo utilizzato per i portali che espongono il servizio in internet è *https.*

CONDIVISIONE DI RISORSE

Il sistema non condivide risorse se non tramite webservices opportunamente configurati ed abilitati, sottoposti a rigorose regole di visibilità.

ACCESSO AL DATABASE

Il sistema non dispone di un accesso diretto sui DBMS e non mette a disposizione alcun metodo o tool per interrogare lo schema. Nel DBMS ogni schema ha una profilatura minima che consente di operare solo sui dati relativi all'applicazione.

POLITICHE DI BACKUP

Sono applicati i seguenti livelli minimi:

- RTO (recovery time objective): 8 h
- RPO (recovery point objective): 24 h
- Retention: 15 gg per i componenti; database 15 gg + 1 backup per ciascuna setti-

mana dell'ultimo mese, 1 copia mensile per 6 mesi.

DISASTER RECOVERY

In caso di Disastro vengono ripristinati i backup ed attivato il sito di DR (disaster recovery) con i seguenti livelli di servizio minimi:

- RTO (recovery time objective): 24 h
- RPO (recovery point objective): 24 h
- Retention: 48 h

SERVIZI DI INFRASTRUTTURA

Per consentire personalizzazioni o customizzazioni in sicurezza deve essere consentito l'accesso ad un ambiente protetto e differente da quello in produzione:

- su macchine dedicate e con servizi preservati
- creando un ecosistema virtuale per ciascun accesso in modo da impedire il libero accesso alla macchina
- creando un accesso alla singola parte necessaria dell'installazione dell'ente.

SITO WEB: FRONT END SERVIZI ON LINE

L'accesso per le seguenti tipologie:

- operatori dell'ente
- cooperazione applicativa
- cittadini ed imprese

è previsto esclusivamente tramite protocollo HTTPS.

ACCESSO DEDICATO AGLI OPERATORI DELL'ENTE

Tutti gli accessi vengono rilevati e dettagliati in file log, dove viene tracciato oltre al giorno e l'ora dell'accesso anche l'IP dal quale viene eseguito l'accesso stesso.

Sono utilizzati diversi profili di accesso amministrativo al sistema:

- utente amministratore: è l'unico accesso che può visualizzare in chiaro le informazioni relative ai cittadini, inclusi i dati personali forniti dall'utente stesso in fase di primo accesso al sistema (registrazione e/o accesso mediante SPID o sistema terzo).
- amministratori di servizio / operatori: hanno accesso solo ed esclusivamente alle proprie funzioni senza poter accedere alla consultazione dei dati personali dei cittadini censiti nel sistema

ACCESSO IN COOPERAZIONE APPLICATIVA

I servizi erogati nel portale devono interagire con i sistemi dell'ente in modalità di cooperazione applicativa. Tutti i webservice esposti dal sistema gestiscono il livello di autenticazione.

ACCESSO DEDICATO AI CITTADINI ED ALLE IMPRESE

L'accesso all'area riservata avviene mediante protocollo HTTPS.

Il sistema ha un suo repository utenti, ma interagisce con sistemi terzi certificati come SPID (Sistema Pubblico Identità Digitale).

GESTIONE INFORMATIVE E CONSENSI

Tutti i servizi esposti al cittadino consentono all'Ente di erogare in modalità web – online i propri servizi istituzionali.
Vengono richieste al cittadino anche ulteriori informazioni quali email e/o SMS che vengono poi utilizzati per facilitare l'erogazione dei servizi mediante invio di apposite comunicazioni o notifiche automatiche.

INFORMATIVA

Sono previste apposite informative personalizzabili.

CONSENSO

Per tutti gli utenti di portale (cittadini, imprese, etc.), all'atto del primo accesso, qualunque sia il sistema di autenticazione adottato, viene richiesto di autorizzare il trattamento dei dati descrivendone gli aspetti tecnici ed operativi legati alla soluzione.

RICHIESTA CANCELLAZIONE DATI

È prevista apposita funzione attraverso la quale il cittadino potrà richiedere la cancellazione dei propri dati. La richiesta viene tracciata nel sistema ed inviata al Responsabile del Trattamento dei dati dell'Ente. Sempre attraverso apposita funzione è possibile procedere con la cancellazione come richiesto. Le informazioni che verranno cancellate sono il profilo dell'utente con tutte le informazioni di contatto.

RETTIFICA DATI

Per quanto concerne la rettifica dei propri dati personali, il cittadino può procedere in autonomia modificando quanto precedentemente dichiarato.

PSEUDONIMIZZAZIONE DEI DATI

Il sistema, nativamente, prevede la separazione fra le informazioni necessarie all'accesso, i dati anagrafici e personali degli individui e le informazioni poi generate nei singoli ambiti applicativi. L'accesso alla sezione dove sono visibili le informazioni degli individui è consentito solo all'amministratore.

Nelle altre sezioni sono presenti solo le informazioni specifiche ed un riferimento al solo nome e cognome senza ulteriori informazioni e quindi di fatto senza poter risalire con certezza alla persona.